Share

Work

Online

Secret

Share

Masterarbeit 2019 Ein hochsicheres Betriebssystem

Master of Advance Studies in Human Computer Interaction Design (HCID)

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

Universität
Basel

Master of Advance Studies in Human Computer Interaction Design (HCID)

Masterarbeit 2019 Ein hochsicheres Betriebssystem

Autoren : Aaron Wyder, Adrian Schmid
Betreuer : Christian Heusser
Co-Betreuer : Dr. Marcel Uhr

Share
Work
Secret
Online
Share

Es ist wie im Tennis. In diesem Projekt wussten wir nie, in welchem Feld (Zone) der Ball (Daten) aufschlägt.

Die Autoren

Der vollständige Bericht der Masterarbeit darf erst zwei Jahre nach der Diplomierung der Studierenden auf dem ePrints der HSR publiziert werden.

Erklärung der Selbstständigkeit

Hiermit bestätigen wir,

dass wir die hier vorliegende Arbeit selbst und ohne fremde Hilfe durchgeführt haben, ausser derjenigen, welche explizit beschrieben sind,

dass wir sämtliche verwendeten Quellen erwähnt und gemäss gängigen wissenschaftlichen Regeln korrekt zitiert haben und

dass wir keine durch Copyright geschützten Materialen (z.B. Bilder) in dieser Arbeit in unerlaubter Weise genutzt haben.

dass wir in dieser Arbeit keine Adressen, Telefonnummern und andere persönlichen Daten von Personen die nicht zum Kernteam gehören publizieren.

Aaron Wyder Adrian Schmid

Danksagung

Unser Dank geht an alle, die uns während unserer Masterarbeit unterstützt haben:

- Sid Hussmann von gapfruit AG für die Zusammenarbeit und die regelmässigen Inputs
- Christian Heusser für das Coaching, die Flexibilität und die wertvolle Unterstützung während der schwierigen Phasen im Projekt
- Dr. Marcel Uhr für das mitlesen und mitbewerten dieser Arbeit
- Chri Hübscher für das ausserordentliche Coaching zum Thema Lean UX bei der Neuausrichtung und dem Wechsel des Vorgehensmodells im Projekt
- Prof. Dr. Markus Stolze für die unkomplizierte Möglichkeit zur überraschend späten Restrukturierung des Teams
- Dr. Raphael Reischuk, Jonas Wettstein und Peter Merker für die Inputs im Rahmen der geführten Experten-Interviews
- Sahra Ali für die Inputs und das Gegenlesen der Masterarbeit
- Markus Flückiger für die praxisnahen Tipps und Ideen während der Durchführung der Masterarbeit
- Den verschiedenen Testpersonen, die uns für Benutzertests und Interviews im Rahmen der durchgeführten Experimente zur Verfügung standen

Inhaltsverzeichnis

Even better than good error messages is a careful design which prevents a problem from occurring in the first place. Either eliminate error-prone conditions or check for them and present users with a confirmation option before they commit to the action.

Norman Nielsen – 10 Usability Heuristic for User Interface Design

Abstract

Das Startup Unternehmen gapfruit AG entwickelt ein hochsicheres Betriebssystem auf Basis der Sicherheitsanforderungen von Behörden, Regierungen und Verteidigungsorganisationen, mit der Vision, dieses in den Corporate- und Consumer-Bereich zu bringen. Die aktuelle Bedrohungslage sowie die rasant wachsende Schadensumme in Unternehmen verursacht durch Cyberkriminalität legitimieren dabei ihr Vorhaben. Traditionelle Sicherheitsmechanismen wie Antivirenprogramme, Spam-Filter und Firewalls sind zwar bereits in fast allen Unternehmen implementiert, reichen jedoch für einen umfassenden Schutz vor Cyberattacken bei weitem nicht mehr aus. Gemäss Schätzungen werden die jährlich verursachten Schäden durch Cyberkriminalität bis zum Jahr 2021 auf 6 Billionen US Dollar anwachsen.

Durch die Einführung eines Zonenkonzepts zur Isolation unterschiedlicher Sicherheitskontexte (bspw. im Internet surfen vs. Arbeit an vertraulichen internen Dokumenten) verhindert das Betriebssystem eine Kompromittierung interner Ressourcen und verhindert damit Einbrüche und Datendiebstähle. Dieses Zonenkonzept wirkt sich jedoch direkt auf die Interaktion des Benutzers mit dem System aus. Es führt ungewohnte Abläufe und zusätzliche Hürden bei der Erledigung der täglichen Arbeitsaufgaben ein. An diesem Punkt setzt die Aufgabenstellung der Masterarbeit ein. Durch ein benutzerzentriertes Vorgehen sollen Ansätze für ein minimal-invasives Interaktionskonzept zum Umgang mit dem eingeführten Zonenkonzept erarbeitet werden.

Mit Lean UX konnte ein Vorgehensmodell gefunden werden, das dem Umstand der Abwesenheit von Testkunden zwecks Benutzerforschung Rechnung getragen hat. Da sich die Auftraggeber zu Beginn des Projektes auf keine konkrete Zielgruppe fokussieren wollte, bestand die Hauptaufgabe des Projektes in der Untersuchung und Erhebung potentieller Benutzer und deren Anwendungskontext. Die Resultate dieser aufwendigen Untersuchungen liegen als Liste potentieller Berufsgruppen mit Einsatzzweck für ein hochsicheres Betriebssystem sowie der darauf basierenden Proto-Personas vor. Als Nebenprodukt entstand im Rahmen der durchgeführten Experimente gemäss Lean UX ein Lo-Fi MVP Prototyp mit einem ersten Ansatz für ein einfach bedienbares Interaktionskonzept. Der Fokus des Prototyps lieg auf einer verständlichen Visualisierung der unterschiedlichen Zonen sowie dem Transfer von Dateien zwischen diesen Zonen.

Vorwort

Im Verlauf des Projektes haben sich der Fokus und die Lieferobjekte der Arbeit stark verändert. Die grösste Herausforderung hierbei war der fehlende Zugang zu künftigen Benutzern des zu entwickelnden Systems. Auf Seiten der Auftraggeber war explizit keine konkrete Zielgruppe definiert bzw. erhoben worden. Die Auftraggeber stammen ursprünglich aus dem Hochsicherheitsbereich für Behörden und Regierungen und waren zu der Überzeugung gelangt, dass ihr System für alle Benutzer relevant und sinnvoll ist.

Im neu gegründeten Startup Unternehmen gapfruit AG arbeiten die Auftraggeber in der selben Konstellation, wie bereits bei ihrem vorherigen Arbeitgeber vor der eigenen Firmengründung. Das Startup ist im vor allem im Bereich IT Security tätig und entwickelt ein neues, hochsicheres Betriebssystem. Das Betriebssystem basiert auf einer Microkernel-Architektur mit beliebig vielen virtualisierten Gastsystemen [vgl. 1.3 Ausgangslage]. Der Unterschied des neu entwickelten Produkts im Vergleich zu ähnlichen, bereits existierenden Produkten von spezialisierten Herstellern für Behörden, Regierungen und Landesverteidigung [vgl. 4.1 Geschlossene Systeme für Behörden und Regierungen] definiert sich wie folgt:

1. **Das zukünftige Betriebssystem wird nicht an eine spezifische Hardware gekoppelt, wie bei anderen Herstellern von hochsicheren Betriebssystemen und**
2. **Es soll für alle Benutzer, nicht nur für spezialisierte Benutzer- oder Berufsgruppen wie bspw. Regierungsbehörden, einfach zugänglich und sinnvoll einsetzbar sein.**

Bereits beim Kick-off Meeting [vgl. Anhang 9.1 Protokolle] wurde von den Autoren die Annahme einer sehr spezifischen, expliziten Benutzergruppe formuliert. Dieser Annahme widersprachen die Auftraggeber zu jenem Zeitpunkt. Dies führte über folgenden Projektverlauf wiederholt zu Diskussionen und Meinungsverschiedenheiten zwischen Auftraggeber und Autoren. Die Auftraggeber stellten insbesondere die aus Sicht der Autoren notwendige, ausgedehnte User Research Phase in Frage und erachteten diese als unnötig. Das Produkt des Auftraggebers befand sich zum Zeitpunkt des Projektstarts inmitten der Implementation des Unterbaus für ihr Konzept zur Lösung sicherheitskritischer Aspekte. Für die Autoren standen deshalb als Startpunkt nur die Annahmen der Auftraggeber, das vordefinierte Zonenkonzept [vgl. 1.3.2 Lösungsansatz mit gapfruitOS] sowie die Funktionsweise konzeptionell ähnlicher Produkte [vgl. 4.1 Geschlossene Systeme für Behörden und Regierungen] zur Verfügung.

Über die ersten drei Monate versuchten die Autoren die Auftraggeber mittels aufwendiger Präsentationen und Diskussionen für den User Centered Design Ansatz des ausgewählten Vorgehensmodells zu gewinnen und von dessen Sinnhaftigkeit zu überzeugen. Dabei stand insbesondere die Wichtigkeit einer sorgfältig durchgeführten User Research Phase für ein derartiges Produkt im Vordergrund. Da keine Einigung erzielt werden konnte und unter dem Druck der schwindenden Projektzeit sahen sich die Autoren zu einer Neuausrichtung, entgegen dem klassischen «Vorgehen nach Schulbuch» [vgl. 3 Methodik und Vorgehen], gezwungen.

Um ein besseres und unabhängiges Bild der Domäne IT Sicherheit zu erhalten, führten die Autoren im Alleingang Interviews mit ausgewiesenen Domänenexperten [vgl. 2.3 Interviews mit Subject Matter Experts]. Die gewonnenen Erkenntnisse erwiesen sich im weiteren Projektverlauf als sehr wertvoll und stützten die initialen Hypothesen der Autoren zu einem grossen Teil.

Basierend auf dieser Ausgangslage wurden schliesslich erste, Annahmen-basierte Vorgehensmodelle besprochen, welche Benutzerforschung parallel zur Ausarbeitung von Ideen für ein Interaktionskonzept ermöglichen. Wie in Kapitel 3 Methodik und Vorgehen beschrieben, erforderte dieser Ansatz jedoch eine Änderung des Vorgehensmodelles, sowie eine komplette Neuausrichtung und Planung. In Absprache mit den Coaches entschieden sich die Autoren diesen Wechsel zu vollziehen.

Der neue, Annahmen-basierte Ansatz führte auch dazu, dass gegen Ende der Projektzeit die Erwartungen zwischen Auftraggeber und Autoren näher zusammenrückten. Aus Sicht der Autoren veränderte sich die Denkweise der Auftraggeber über den Projektverlauf, unter anderem durch die Auswertungen der geführten Interviews vor und innerhalb der Experimente. Am Ende des Projektes sind auch die Auftraggeber der Auffassung, dass für ihr Betriebssystem eine eher spezifische Anwendergruppe existiert und sie sich, für die zukünftige Weiterentwicklung des Systems, auf diese Zielgruppe fokussieren werden.

Es danken die Autoren
Aaron und Adrian

Glossar

Angriffsvektor = Möglicher Angriffsweg und Angriffstechnik, welche ein unbefugter Eindringling nutzen kann, um ein fremdes Computersystem zu kompromittieren. [1]

Compartmentalisation = Die Unterteilung der verschiedenen Sicherheitskontexte auf dem Computer des Anwenders in separate, abgeschottete Systeme. Damit wird verhindert, dass bei Übernahme eines einzelnen Compartments ebenfalls auf die Anwendungen und Daten der anderen Compartments zugegriffen werden kann. Der Angreifer kann so nicht das gesamte System auf einmal übernehmen und den Benutzer aussperren. [2]

Cyberattacke = Gezielter Angriff auf eine spezifische IT Infrastruktur bzw. Netzwerk

Cybercrime-as-a-Service = Cyberattacken und andere Dienstleistungen im Bereich der Cyberkriminalität auf Bestellung gegen Bezahlung durch einen Auftraggeber.

DDoS = Eine Distributed Denial of Service Attacke ist ein bösartiger Versuch, die normale Funktion eines Zielservers, Dienstes oder Netzwerks durch Überflutung mit Netzwerkanfragen zu stören bzw. lahmzulegen. Dabei werden kompromittierte Computersysteme als Quellen für die Anfragen genutzt. [3]

Endpoint/Endpunkt = Ein internetfähiges Endgerät wie bspw. ein Desktop Computer, Laptop, Smartphone, Tablet, etc., welches an einem Netzwerk hängt.

Gastsystem = Das Betriebssystem innerhalb des isolierten Software-Containers bzw. die virtuelle Maschine.

General-Purpose Betriebssystem = Es existieren verschiedene Arten von Betriebssystemen. Ein General-Purpose OS wird für Systeme und Applikationen verwendet, welche nicht zeitkritisch sind. Alle bekannten Endbenutzer Betriebssysteme, wie Windows, Linux, Unix, Mac OS fallen in diese Kategorie. Ein Real-Time OS wird im Gegensatz dazu für zeitkritische Systeme eingesetzt. [4]

Härten = Der Prozess der Absicherung eines Systems durch die Reduktion von möglichen Angriffsvektoren bspw. durch das Abschalten unsicherer Funktionen oder Verändern von Standardeinstellungen [5]

Hostsystem = Das Betriebssystem auf dem physischen Computer oder Server, welches den isolierten Software-Container (= virtuelle Maschine) ausführt.

[1] «Angriffsvektor», Wikipedia. 17-Feb-2014.

[2] «Security through compartmentalisation», 2004.

[3] «What is a Distributed Denial-of-Service (DDoS) attack?», Cloudflare. [Online]. Verfügbar unter: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/. [Zugegriffen: 26-Dez-2018].

[4] Differences between a GPOS (Normal OS) and an RTOS (Real Time OS)», Electronic Circuits and Diagrams-Electronic Projects and Design, 12-Juni-2012. [Online]. Verfügbar unter: http://www.circuitstoday.com/gpos-versus-rtos-for-an-embedded-system. [Zugegriffen: 20-Juli-2018].

[5] «Hardening (computing)», Wikipedia. 31-Dez-2018.

Kaspersky Labs = Russischer Anbieter von Cybersecurity und Anti-Virus Produkten

Malware = Überbegriff für alle Arten von Schadsoftware wie bspw. Viren, Trojaner, Ransomware, Spyware, etc.

Microkernel = Minimales Stück Software, welches nur die notwendigsten Mechanismen zur Implementierung eines Betriebssystems zur Verfügung stellt. Im Gegensatz zu den monolithischen Kernen der gewöhnlichen Betriebssysteme besteht ein Mikrokern nur aus wenigen Tausend Zeilen Code. Komplizierte und dadurch eher anfällige Komponenten, wie Treiber, File Systeme, Kommunikations-Stacks etc. befinden sich ausserhalb im User-Mode.

Ransomware = eine Form von Malware welche die Festplatte eines Computers verschlüsselt. Der Anwender wird aufgefordert zur Entschlüsselung und damit erneuten Freigabe seiner Daten ein Lösegeld an den/die Angreifer zu überweisen.

Trojaner = Schadsoftware getarnt als nützliche Anwendung welche im Hintergrund ohne Wissen des Anwenders eine andere Funktion erfüllt [6]

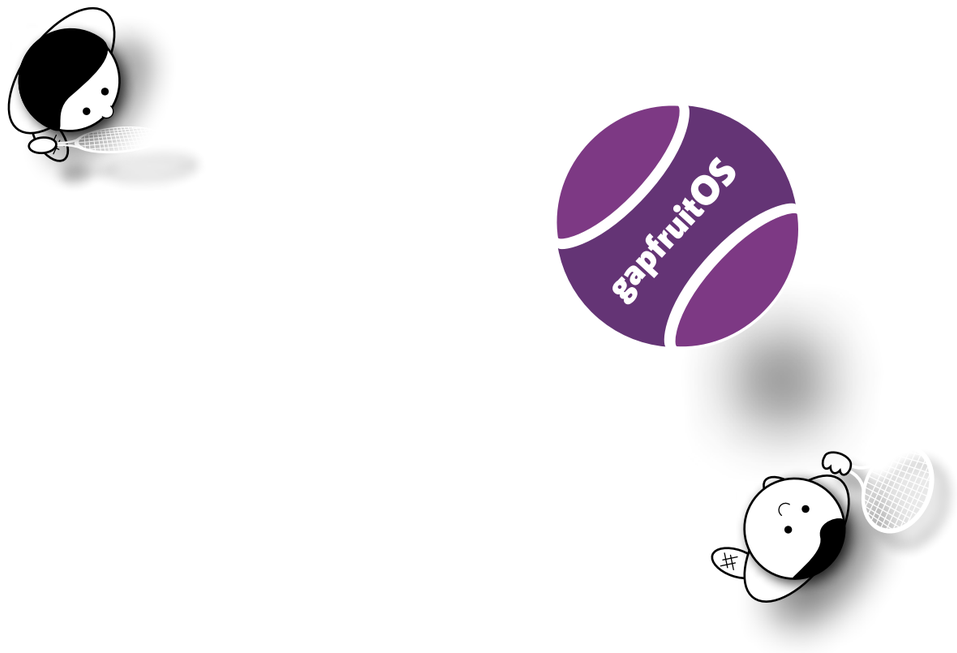
Remote Desktop = Software zum Zugriff via Internet auf eine virtualisierte Windows Instanz auf einem entfernten Server in der Cloud, ermöglicht Arbeiten wie mit einer lokalen Windows Installation

Virtualisierung = Ein virtuelles Computersystem – die so genannte virtuelle Maschine (VM) – ist ein vollständig isolierter Software-Container mit einem Betriebssystem und Anwendungen. Jede eigenständige VM ist völlig unabhängig. Die Nutzung mehrerer VMs auf einem einzigen Computer ermöglicht die Ausführung mehrerer Betriebssysteme und Anwendungen auf nur einem physischen Host. [7]

Sandbox = Ist ein abgeschlossener, nach aussen hin abgeriegelter Sicherheitskontext oder Container. Für ein laufendes Programm bedeutet das bspw., dass kein Zugriff auf Ressourcen ausserhalb der Sandbox möglich ist. Durch diese Isolation wird sichergestellt, dass unsicherer oder bösartiger Code nicht auf das System ausserhalb der Sandbox übergreifen kann.

[6] «Trojanisches Pferd (Computerprogramm)», Wikipedia. 30-Sep-2018.

[7] «Virtualisierung und Software für virtuelle Maschinen»..



1 Einleitung und Projektrahmen

1.1 Einleitung

Die vorliegende Masterarbeit wurde im Rahmen des berufsbegleitenden Master of Advanced Studies in Human Computer Interaction Design an der Hochschule Rapperswil und der Universität Basel erstellt. Die Autoren widmeten sich einer Praxisarbeit zum Thema Benutzerforschung und Interaktionsdesign für ein alltagstaugliches, hochsicheres Betriebssystem. Dabei wurden auch gewisse Forschungsaspekte in den Bereichen Desktop Metapher, Window Management, File Management und Usable Security tangiert.

Auftrag- und Ideengeber ist ein junges Startup Unternehmen bestehend aus ehemaligen Mitarbeitenden eines Konzerns für Sicherheitslösungen für Behörden, Verteidigungsorganisationen sowie diplomatische Organisationen. Die Vision des Startups ist es, ähnliche hochsichere IT Lösungen in den Corporate- und Consumer-Bereich zu bringen.

1.2 Kontext der Arbeit

Verfeinerte Angriffsmethoden, neue Technologien und Infrastrukturen in Unternehmen sowie die immer engere Verknüpfung interner und externer betrieblicher Abläufe mit Informationstechnologie stellen die IT Sicherheit in Unternehmen stets vor neue Herausforderungen. Traditionelle Sicherheitsmechanismen wie Antivirenprogramme, Spam-Filter und Firewalls sind zwar flächendeckend in fast allen Unternehmen implementiert, reichen jedoch für einen umfassenden Schutz bei weitem nicht mehr aus [8]. Daher kommt der Absicherung der Endpoints in Unternehmensnetzwerken eine besonders wichtige Rolle zu. Endpoints sind die zentrale Schnittstelle zwischen den Anwendern und der Informationstechnologie innerhalb der Organisation [9].

[8] «IDC Studie zu Next Gen Endpoint Security in deutschen Unternehmen: Gefahr erkannt, aber nicht gebannt». [Online]. Verfügbar unter: https://idc.de/de/ueber-idc/press-center/64840-idc-studie-zu-next-gen-endpoint-security-in-deutschen-unternehmen-gefahr-erkannt-aber-nicht-gebannt. [Zugegriffen: 25-Juli-2018].

[9] M. Zacher, «Next Gen Endpoint Security in Deutschland 2017»

Neben den technischen Massnahmen hängt Sicherheit immer auch vom Verhalten des Anwenders im Umgang mit seinem Zugriffspunkt auf Unternehmensinformationen ab [10]. In über 95% der Fälle sind gemäss IBM menschliche Faktoren Ursache bzw. Treiber für Einbrüche und Datendiebstähle [11]. Durch Unwissen oder nachlässiges Verhalten von Anwendern erhalten Angreifer die Möglichkeit, technische Schwachstellen auszunutzen und Systeme zu kompromittieren.

1.2.1 Gründe für die steigende Cyberkriminalität

Auf Desktops, Laptops und auch auf Mobilgeräten werden ständig sensible und vertrauliche Unternehmensdaten erstellt oder manipuliert. Die Endpoints stellen ausserdem ein Einfallstor zum Unternehmensnetzwerk dar. Ein Angreifer kann bspw. durch die Platzierung eines Trojaners Zugriff auf Anmeldedaten für zentrale Unternehmenssysteme erhalten. Gemäss Kaspersky Labs sind Endpoints aus diesen Gründen von besonderem Interesse als Angriffsziel von Cyberattacken [12].

Die Attraktivität von Cyberkriminalität steigt für Angreifer unter anderem durch die zunehmend einfachere Monetarisierung über den Schwarzmarkt via Kryptowährungen. Für Cyberkriminelle entwickeln sich lukrative Geschäftsfelder, mit denen sie hunderttausende Dollar verdienen können – die Chance erwischt zu werden tendiert gegen Null. Durch neue technologische Errungenschaften, bekanntwerdende Sicherheitslücken und die stetig wachsende Anzahl von Internetbenutzern steigt auch die Zahl der Angriffsvektoren. Automatisierte Möglichkeiten verwundbare Ziele ausfindig zu machen und ***Cybercrime-as-a-Service*** [13] machen es für Cyberkriminelle immer einfacher Attacken auszuführen.

1.2.2 Verursachte Schäden durch Cyberkriminalität

Gemäss aktuellen Untersuchungen des Sicherheitsherstellers McAfee [14] liegen die Kosten für den durch Cyberkriminalität entstandenen Schaden weltweit auf dem dritten Platz, hinter Regierungskorruption und Drogenhandel. Im Jahr 2017 entstanden durch Cyberattacken global Schäden in Höhe von etwa 600 Milliarden USD. Dies ist eine Steigerung um rund 100 Milliarden USD seit der letzten Untersuchung 2014. Cybersecurity Ventures schätzt in ihrem Cybercrime Report von 2017 [15] den jährlichen Schaden durch Cyberkriminalität bis zum Jahr 2021 sogar auf 6 Billionen (=6000 Milliarden) USD.

Ein Bericht des Ponemon Institute [15] geht vor allem auf den Schaden für Unternehmen ein. Die Kosten von Cyberkriminalität stiegen 2017 für Unternehmen um rund 23 Prozent im Vergleich zum Vorjahr und beliefen sich durchschnittlich auf 11.7 Millionen USD. Diese Kosten beinhalten sowohl die Ausgaben für die Behandlung von Cyberangriffen als auch diejenigen zur Wiederherstellung des Tagesgeschäfts nach einem Vorfall. Gemäss den Untersuchungen nahm die durchschnittliche jährliche Anzahl von erfolgreichen Datendiebstählen um mehr als 27 Prozent zu. Allein Ransomware Attacken stiegen um mehr als das Doppelte von 13 auf 27 Prozent. Malware wie WannaCry oder Petya trafen tausende von Zielen und unterbrachen öffentliche Versorgungsbetriebe sowie grosse Unternehmen weltweit. Am häufigsten von Attacken betroffen sind Finanzdienstleister, insbesondere Banken.

Primärangriffe bei Cyberkriminalität

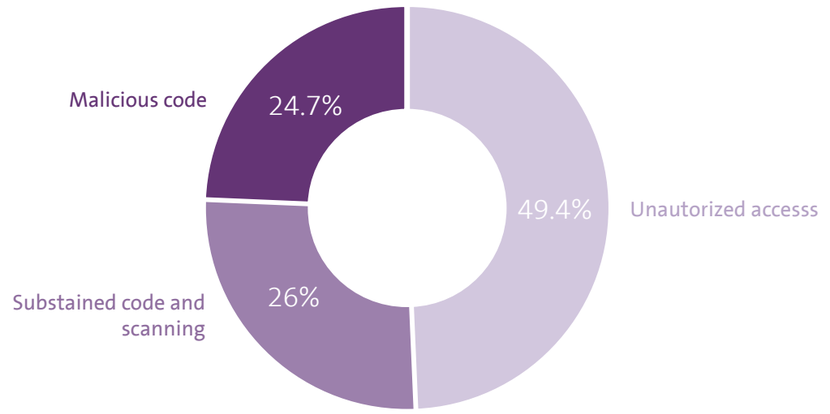


Abbildung 1: Primäre Angriffsmodi in der Cyberkriminalität [11]

[10] «iX extra: Endpunkt-Sicherheit», März 2014.

[11] «Human Error Accounts for Over 95% of Security Incidents, Reports IBM», The Duo Security Bulletin. [Online]. Verfügbar unter: https://duo.com/blog/human-error-accounts-for-over-95-percent-of-security-incidents-reports-ibm. [Zugegriffen: 20-Juli-2018].

[12] «Whitepaper Angriffsziel Endpoint», 2010

[13] C. Cooper, «The rise and rise of Cybercrime as a Service», CSO Online, 27-Juli-2017. [Online]. Verfügbar unter: https://www.csoonline.com/article/3205253/data-breach/the-rise-and-rise-of-cybercrime-as-a-service.html. [Zugegriffen: 20-Juli-2018].

[14] McAfee, «Economic Impact of Cybercrime 2017», Februar 2018, S. 28.

[15] Cybersecurity Ventures und S. Morgan, «2017 Cybercrime Report».

[16] Ponemon Institute und Accenture, «Cost of Cybercrime Study 2017»

1.3 Ausgangslage

Sowohl aus Unternehmenssicht wie auch im privaten Umfeld existieren unterschiedliche Sicherheitskontexte. Diese sind meist durch unabhängige Netzwerke getrennt. Im einfachsten Fall, bspw. in einem Heimnetzwerk, existieren nur zwei unterschiedliche Sicherheitskontexte, so genannte Zonen. Dabei besteht einerseits der Anschluss ans öffentliche Internet und andererseits der interne Bereich, welcher zum Datenaustausch zwischen Endgeräten innerhalb des internen Netzwerkes verwendet wird.

In einem grösseren Unternehmen mit eigener Produktentwicklung könnte es aber bspw. auch drei verschiedene, voneinander getrennte Netzwerke geben. Dabei existiert ein Netzwerk für hochsensible und geheime Forschungsdaten, auf welches nur wenige Personen Zugriff haben. Dieses Netzwerk ist zusätzlich über den so genannten ***Air Gap*** physisch vom Internet und anderen internen Netzwerken getrennt. Neben dieser sensiblen Zone existiert ein weiteres internes Netzwerk mit Intranet und anderen firmenspezifischen Diensten. Durch ein drittes Netzwerk wird schliesslich der Zugang zum Internet für Recherchen und die Kommunikation nach aussen realisiert.

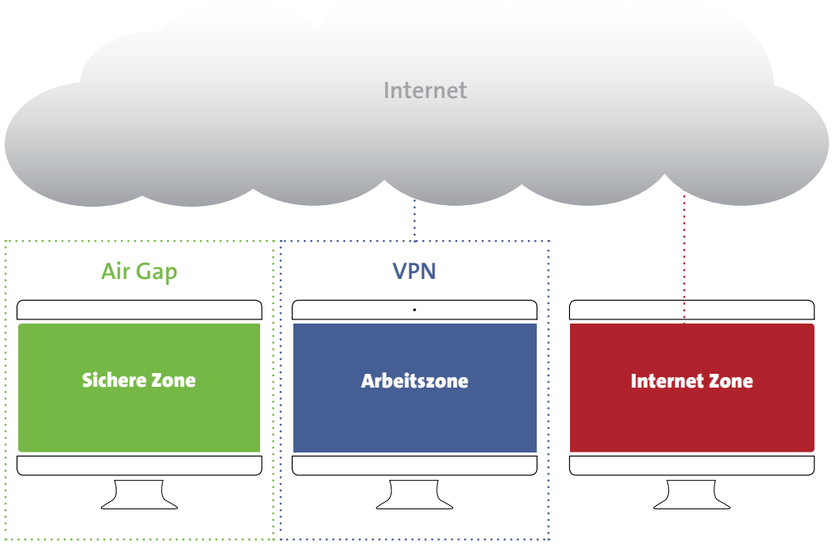


Abbildung 2: Netzwerksegmentierung zur Trennung der unterschiedlichen Sicherheitskontexte

1.3.1 Problemstellung

Die heutzutage auf den Endpunkten eingesetzten General-Purpose Betriebssysteme wie bspw. Windows, Linux oder Mac OS sind über viele Jahre hinweg gewachsen und bestehen mittlerweile aus mehreren Millionen Zeilen Code. Ihr Fokus liegt vor allem auf Usability, Performance und Portabilität. Aus der Security-Perspektive betrachtet haben sie alle ein gemeinsames Problem: Sie besitzen einen monolithischen Kern und es existiert keine effektive Isolation zwischen den verschiedenen, laufenden Programmen auf einem Computer. Wird über eine Sicherheitslücke eine Kernkomponente durch eine Schadsoftware kompromittiert, kann keines dieser Betriebssysteme eine komplette Übernahme des Systems inklusive aller Anwendungen und Daten verhindern.

Hat ein Angreifer ein System erfolgreich unter seine Kontrolle gebracht, sind auch die anderen Endpunkte und damit ihre Daten in allen Netzwerken, auf welche der kompromittierte Rechner Zugriff hat, in Gefahr. Um ein sicheres Arbeiten in den unterschiedlichen Sicherheitskontexten zu ermöglichen, wäre mit einem gewöhnlichen Betriebssystem aufgrund der beschriebenen Schwachstellen für jeden Sicherheitskontext ein eigener Computer notwendig [vgl. Abb. 3].

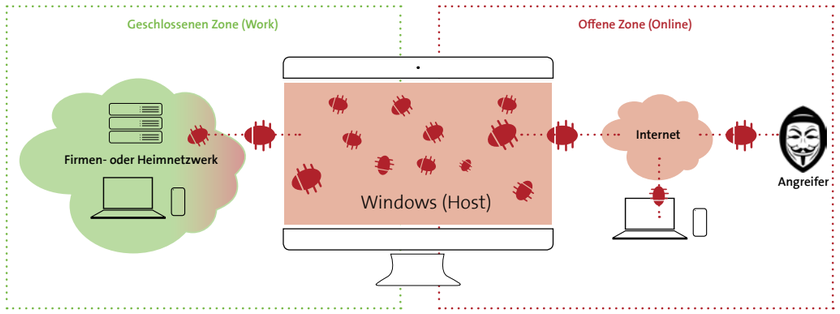


Abbildung 3: Arbeiten in unterschiedlichen Sicherheitskontexten mit einem gewöhnlichen Betriebssystem

1.3.2 Lösungsansatz mit gapfruitOS

Zur Lösung dieser Problematik entwickelt die Auftraggeberin, die Firma gapfruit AG, ein Betriebssystem für die gleichzeitige Arbeit in den unterschiedlichen Sicherheitskontexten auf einem einzigen Computer. Die strikte Separierung der unterschiedlichen Zonen auf dem Endpunkt wird durch ein neues Betriebssystem auf Microkernel-Basis sichergestellt. Die softwareseitige Isolation der einzelnen Zonen wird durch ein minimales Hostsystem (gapfruitOS) mit virtualisierten Gastsystemen (Windows oder Unix/Linux) umgesetzt. Jedes Gastsystem implementiert jeweils

einen Sicherheitskontext. Wird ein Gastsystem durch Malware kompromittiert, verhindert die Systemarchitektur einen Befall der anderen Zonen [vgl. Abb. 4]. Das Betriebssystem soll ausserdem für Unternehmen, die bereits auf eine Microsoft-Windows-Infrastruktur setzen, einen möglichst einfachen Migrationspfad bieten.

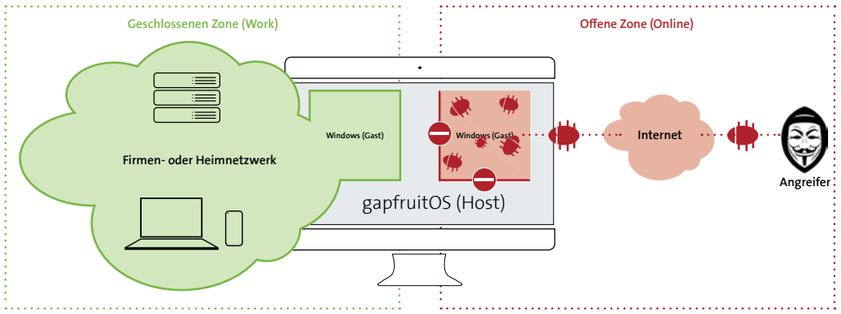


Abbildung 4: Sicheres Arbeiten in unterschiedlichen Sicherheitskontexten mit gapfruitOS

1.3.3 Zonenkonzept in gapfruitOS

Eine Zone (auch Compartment genannt) in gapfruitOS definiert einen isolierten Sicherheitskontext. Sie wird durch eine virtuelle Maschine mit einem bestimmten Gastsystem realisiert. Für jede dieser virtuellen Maschinen kann der Hardware- und Netzwerkzugriff, entsprechend des Sicherheitskontextes, rigoros reguliert werden. Weiter kann festgelegt werden, ob ein Datentransfer in die Zone bzw. aus der Zone heraus erlaubt ist. Falls ein Datentransfer erlaubt ist, können zusätzliche Sicherheitsmechanismen wie bspw. eine Überprüfung auf Viren und Malware oder ein manueller Check bei der Ausführung erzwungen werden. Auf diese Weise erfolgt ein Datentransfer zwischen zwei Zonen immer kontrolliert.

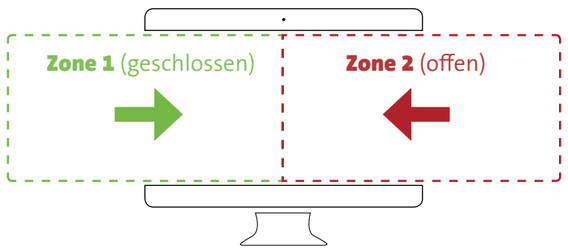


Abbildung 5: Zwei-Zonen-Konzept offene Zone, geschlossenen Zone

Im Verlauf der durchgeführten Experimente [vgl. 5 Experimente] hat sich gezeigt, dass die meisten Benutzer im Firmenkontext wohl nur Verwendung für zwei Zonen haben, eine offene Zone und eine Corporate Zone.

1.4 Aufgabenstellung

Die Architektur und die Funktionsweise von gapfruitOS haben einen direkten Einfluss auf die Art, wie der Benutzer mit dem System interagieren muss. Sie setzen ungewohnte Arbeitsabläufe voraus. Für diese durch das Sicherheitskonzept vorgegebenen Abläufe soll ein Interaktionskonzept entwickelt werden, welches möglichst minimal-invasiv auf die gewohnten Arbeitsabläufe des Anwenders einwirkt. Im Zentrum der Betrachtungen soll das Verständnis des Zonenkonzepts sowie der Wechsel zwischen den einzelnen Zonen stehen. Weiterhin ist ein Datentransfer zwischen den Zonen unerlässlich, damit der Anwender bspw. Dokumente aus einer Internetrecherche in seine Arbeitszone bringen kann. Umgekehrt besteht in gewissen Situationen auch die Notwendigkeit, in der Arbeitszone erstellte Artefakte via E-Mail über das Internet zu versenden oder auf einen Cloud-Dienst hochzuladen.

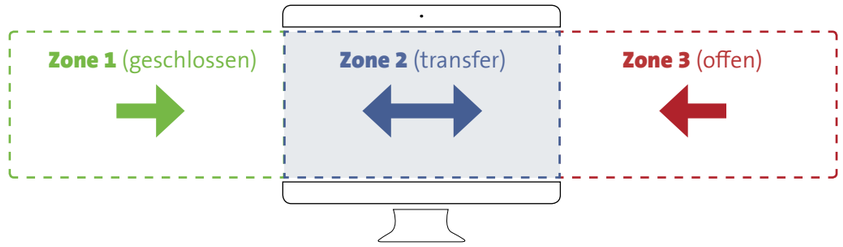


Abbildung 6: Umschalten und Datentransfer zwischen verschiedenen Sicherheitskontexten (=Gastsystemen) in gapfruitOS

1.4.1 Lieferobjekte

1. Untersuchungen zur Benutzergruppe eines hochsicheren Betriebssystems im Firmenkontext
2. Proto-Personas und potentielle Anwendungsszenarien von gapfruitOS
3. Ansätze für ein Interaktionskonzept mit Fokus auf Verständlichkeit des Zonenkonzepts sowie dem Wechsel und Datentransfer zwischen den einzelnen Zonen
4. Empfehlungen für das weitere Vorgehen an den Auftraggeber

2 Einführung in die Domäne

Nach einem initialen Kick-Off Meeting mit den Auftraggebern [vgl. Anhang 9.1 Protokolle] ging es für die Autoren darum, sich einen breiteren Überblick innerhalb der Problemdomäne zu verschaffen. Um ein Verständnis der vorliegenden Problematik sowie der von den Auftraggebern angedachten Lösungsansätze erreichen zu können, waren die Autoren darauf angewiesen, sich ein breiteres Wissen bestimmter Aspekte der komplexen und oft sehr techniklastigen IT Security Domäne anzueignen. Da keiner der drei Autoren mit genügend Vorwissen aufwarten konnte, war die Einführung sowie das Coaching durch die Auftraggeber bei spezifischen Fragestellungen und später auch gewissen Designentscheidungen von entscheidender Wichtigkeit.

2.1 Problemverständnis und Knowhow-Transfer

In einem ersten gemeinsamen Workshop stellten die Auftraggeber den Autoren die Problematik der unterschiedlichen Sicherheitskontexten vor, in welchen sich ein Anwender bei der täglichen Nutzung seines Computers bewegt [vgl. 1.3.1 Problemstellung] und die daraus resultierenden Angriffsvektoren für Unternehmen und Private. Ziel dabei war ein schneller und kompakter Knowhow-Transfer zu Problemstellung und Lösungsansatz. Im weiteren Verlauf wurden auch bestehende Lösungen anderer Anbieter ähnlicher Lösungen im Bereich Behörden, Regierungen und Landesverteidigung diskutiert [vgl. 4.1 Geschlossene Systeme für Behörden und Regierungen].

2.1.1 Vorgehen und Durchführung

Nach der Einführung und dem Knowhow-Transfer durch die Auftraggeber wurde gemeinsam eine ***Problem Statement Map*** gemäss ***Collaborative UX Design*** [17] erarbeitet. Die Problem Statement Map hilft den Autoren herauszufinden, was innerhalb des Projektes wirklich erreicht werden soll und welche Randbedingungen dabei bestehen. Ausserdem fördert sie ein präzises Verständnis des Projektauftrages und hilft den Autoren die getroffenen Annahmen bezüglich festgelegten Projektzielen zu identifizieren [18].

[17] T. Steimle und D. Wallach, Collaborative UX Design, 1. Aufl. dpunkt, 2018.

[18] Problem Statement. [Online]. Verfügbar unter: http://collaborative-uxdesign.com/scoping/problem-statement. [Zugegriffen: 10-Jan-2019]

Zu Beginn des Workshops wurden von den Autoren die unten abgebildeten Überschriften (blau) mittels Post-it Zetteln an eine freie Wand gehängt. Zu diesen Überschriften wurden nun die so genannten ***Problem Statements*** formuliert. Dazu konnte jeder Teilnehmer eigene Post-it zu den jeweiligen Überschriften formulieren. In der folgenden Gruppendiskussion wurden die gefundenen Punkte ausführlich besprochen, konsolidiert und zu den entsprechenden Überschriften gehängt

Problem Statement Map

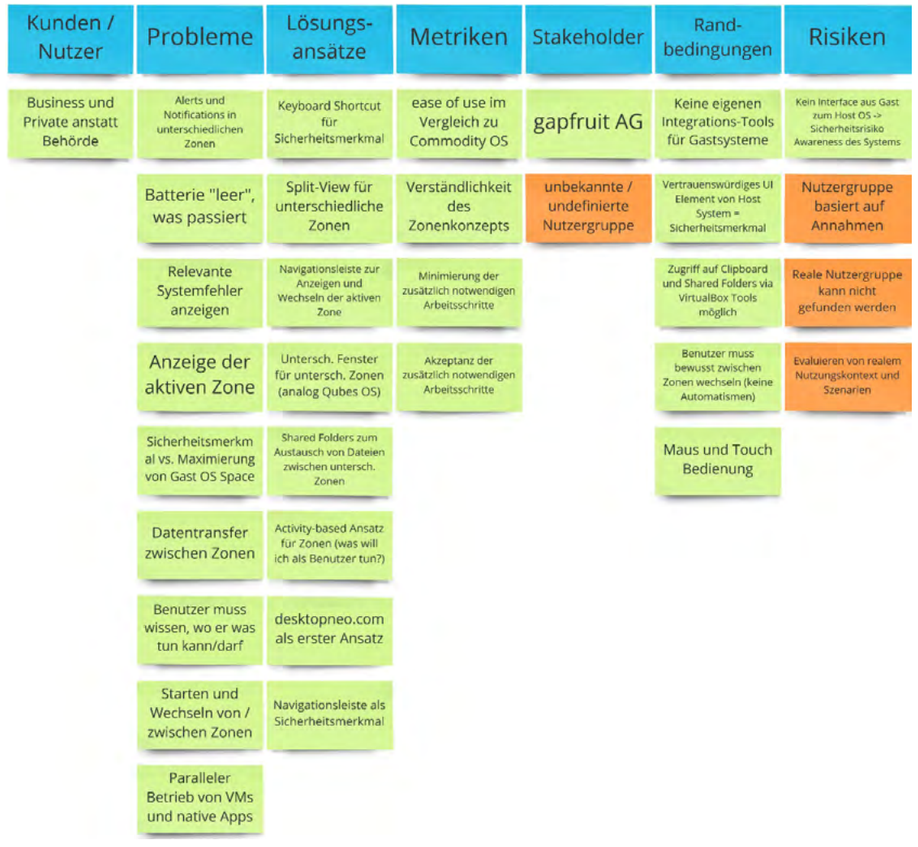


Abbildung 7: Vollständige Problem Statement Map
(orange = nachträgliche Ergänzungen durch die Autoren)

2.1.2 Auswertung und Zusammenfassung der Resultate

Aus den gesammelten ***Problem Statements*** liessen sich bestimmte Aspekte herausfiltern, die sich hinsichtlich ihrer Kernaussage bündeln liessen und eine erste übergeordnete Gliederung ermöglichten. Wie aus der nachfolgenden Übersicht zu entnehmen ist, gingen dabei eine Vielzahl an Themen hervor, bei der die Problematik rund um die Bedien- und Nutzungsweise eines solchen Zonenkonzepts evident wurde.

- Transparenz des Zonenkonzepts: Der Endbenutzer soll durch das eingeführte Zonenkonzept [vgl. 1.3.3. Zonenkonzept in gapfruitOS] möglichst nicht tangiert werden und nur so wenig Einschränkung wie nötig im Vergleich zu einem gewöhnlichen Betriebssystem wie Windows oder Mac OS erfahren. Da dieses Zonenkonzept aber essentiell zur Einhaltung des Sicherheitsaspektes ist, muss der Benutzer andererseits bewusst die Entscheidung treffen, in welcher Zone er eine bestimmte Aufgabe ausführt, um Zugriff auf die gewünschten Ressourcen wie beispielsweise Netzwerk, Datenablage oder auch Programme zu erhalten.

- Orientierung & Navigation: Da die Einführung verschiedener Sicherheitszonen eine Verteilung der Arbeitstätigkeiten über die unterschiedlichen Zonen hinweg mit sich zieht, muss der Benutzer sich jederzeit bewusst sein, in welcher Zone er sich aktuell befindet sowie ob und in welche Zone er wechseln muss, um die nächste Tätigkeit auszuführen.

- Datentransfer: Um bestimmte aufeinanderfolgende Tätigkeiten im Rahmen eines übergreifenden Workflows ausführen zu können, muss der Benutzer in der Lage sein, Daten zwischen diesen Zonen auszutauschen. Existieren benötigte Dokumente bspw. nicht in der aktuellen Zone, müssen diese unter Umständen erst aus einer anderen Zone in die aktuelle transferiert werden.

- Sicherheitsmerkmal: Weitere wichtige Punkte sind die Information des Benutzers und das so genannte Sicherheitsmerkmal. Das Sicherheitsmerkmal ist ein Bereich des Bildschirms, der für die Gastsysteme weder sicht- noch zugreifbar ist. Dieser Bereich ist exklusiv dem Hostsystem, bspw. zur Anzeige eines Navigationsbars mit den verschiedenen Zonen, analog Tabs in einem Browser, vorbehalten. Das Sicherheitsmerkmal dient in erster Linie dazu, bei einem kompromittiertem Gastsystem die Übernahme des gesamten Bildschirms zu verhindern. Somit kann der Anwender auch in diesem Fall auf den anderen Zonen weiterarbeiten, bis der Systemadministrator die kompromittierte Zone neu aufgesetzt hat.

- Benachrichtigungskonzept: Daneben muss der Benutzer auch zonenübergreifend über Benachrichtigungen wie zum Beispiel den Eingang einer E-Mail innerhalb eines Gastsystems informiert werden. Zur Information des Benutzers zählen aber auch neuartige Benachrichtigungen über sicherheitsrelevante Aktivitäten, welche durch das Hostsystem erzwungen werden. Wird beispielsweise bei oben erwähntem Datentransfer zwischen zwei Zonen eine Sicherheitsprüfung verletzt, wird die Datei nicht transferiert und der Benutzer muss mit entsprechenden Handlungsoptionen darüber informiert werden.

- Interaktionsform: Zu guter Letzt hinterfragen die Auftraggeber für ihr neues System auch bestimmte Aspekte der seit bald 40 Jahren im Einsatz stehenden Desktop Metapher. Insbesondere das Konzept der überlappenden Fenster soll zu Gunsten einer Idee analog der Konzeptstudie ***Desktop Neo*** von Lennart Ziburski [19] überdacht werden. Dieser stellt sich auf den Standpunkt, dass anstelle von überlappenden Fenstern auf einem Bildschirm nur nebeneinanderstehende Paneele in voller Bildschirmhöhe existieren sollten. In aktuellen Versionen der meisten bekannten Betriebssysteme existiert dieser Modus ebenfalls als so genannte «Split Screen» Ansicht neben den gewöhnlichen, überlappenden Fenstern.

  Neben der fraglichen Konkurrenzfähigkeit des zu entwickelnden Produktes mit der guten Usability und Performance von gewöhnlichen Betriebssystemen wie Windows oder Mac OS besteht das grösste Risiko in der fehlenden Fokussierung auf eine bestimmte Benutzergruppe und ihre spezifischen Anwendungsfälle. Die Auftraggeber haben keine spezifischen Anwendungsfälle erhoben und möchten dieses hochsichere Betriebssystem möglichst generisch für Firmen und Private entwickeln.

2.1.3 Nächste Schritte

In den geführten Diskussionen tat sich wie erwartet ein breites Problemfeld auf, welches weit über den Rahmen der vorliegenden Masterarbeit hinausgeht. In der Folge wird die Problemstellung gemeinsam mit den Auftraggebern eingegrenzt. Es werden konkrete Anwendungsszenarien von realen Benutzern erhoben, um sinnvolle Ideen und Entscheidungen für ein künftiges Interaktionsdesign zu treffen. Die in der Problem Statement Map festgehaltenen Annahmen werden von den Autoren identifiziert und verifiziert oder widerlegt.

[19] «Desktop Neo – rethinking the desktop interface for productivity.».

2.1.4 Reflexion zur Methode Problem Statement Map

Die Problem Statement Map eignet sich sehr gut, um die unterschiedlichen Facetten einer Problemstellung zu identifizieren und zu visualisieren. Die geführten Diskussionen bei der Konsolidierung fördern ein gemeinsames Verständnis des Problemraumes sowie möglicher Lösungsansätze. Der Einbezug der Auftraggeber und nach Möglichkeit auch der beteiligten Stakeholder bringt einen immensen Wert, da Ihre Perspektive von Beginn an berücksichtigt und infolgedessen die Entwicklung einer gemeinsamen Vision beschleunigt wird. Der visuelle Aspekt der ganzen Problemstellung auf einer einzigen Wand ermöglicht es jedem Teammitglied auf «einen Blick» die relevanten Aspekte zu memorieren.

Aus Sicht der Autoren hat die Problem Statement Map jedoch nur einen dauerhaften Wert, wenn sie jederzeit sichtbar in den Arbeitsräumen des Projektteams hängt. Insbesondere bei Projekten, die kein Standardproblem lösen oder ein gänzlich neues Produkt entwickeln sind zum Zeitpunkt der Erstellung der Map nicht alle Aspekte der Problemstellung bekannt. Oftmals verändert sich mit der Dauer des Projektes und den gewonnenen Erfahrungen der Fokus der Arbeiten. Somit ist die Problem Statement Map über den Projektverlauf hinweg ein sich stetig veränderndes und weiterentwickelndes Artefakt.

2.2 Use Cases und User Story Mapping

Bei der Einführung hatten die Auftraggeber bereits eine Fülle von Use Cases für das neue Produkt ausgearbeitet [vgl. Tabelle Use Cases seitens Auftraggeber]. Da im Rahmen der vorliegenden Arbeit nur ein kleiner Teil der bestehenden Use Cases bearbeitet werden konnte, wurde der Fokus ausschliesslich auf die Endbenutzer-Seite gelegt. Innerhalb dieses Fokus wurde eine weitere Eingrenzung auf die zwei wichtigsten Use Cases «Wechseln zwischen laufenden VMs» und «Daten von einer VM in eine andere kopieren» vorgenommen.

Use Cases seitens Auftraggeber

Administrator-Seite	Endbenutzer-Seite
Erstellen und Löschen von VMs/Zonen	Starten und stoppen von VMs (Zonen)
Klonen von VMs/Zonen	Wechseln zwischen laufenden VMs (Zonen)
Konfigurieren von VMs/Zonen (RAM, CPU, Speicherplatz, Hardware Zugriff)	Umorganisieren von laufenden VMs (Zonen)
Backup und Wiederherstellung von VMs (Zonen)	USB Gerät mit VM verbinden
Konfigurieren von Regeln bezüglich Datenaustausch zwischen VMs (Zonen)	Daten von einer VM (Zone) in eine andere kopieren
Konfigurieren von Firewall Regeln	Mit WLAN Netzwerk verbinden
Konfigurieren der Netzwerkkarte	Keyboard Layout konfigurieren
Konfigurieren von VPN Verbindungen	Monitor konfigurieren
Update/Upgrade von gapfruitOS	

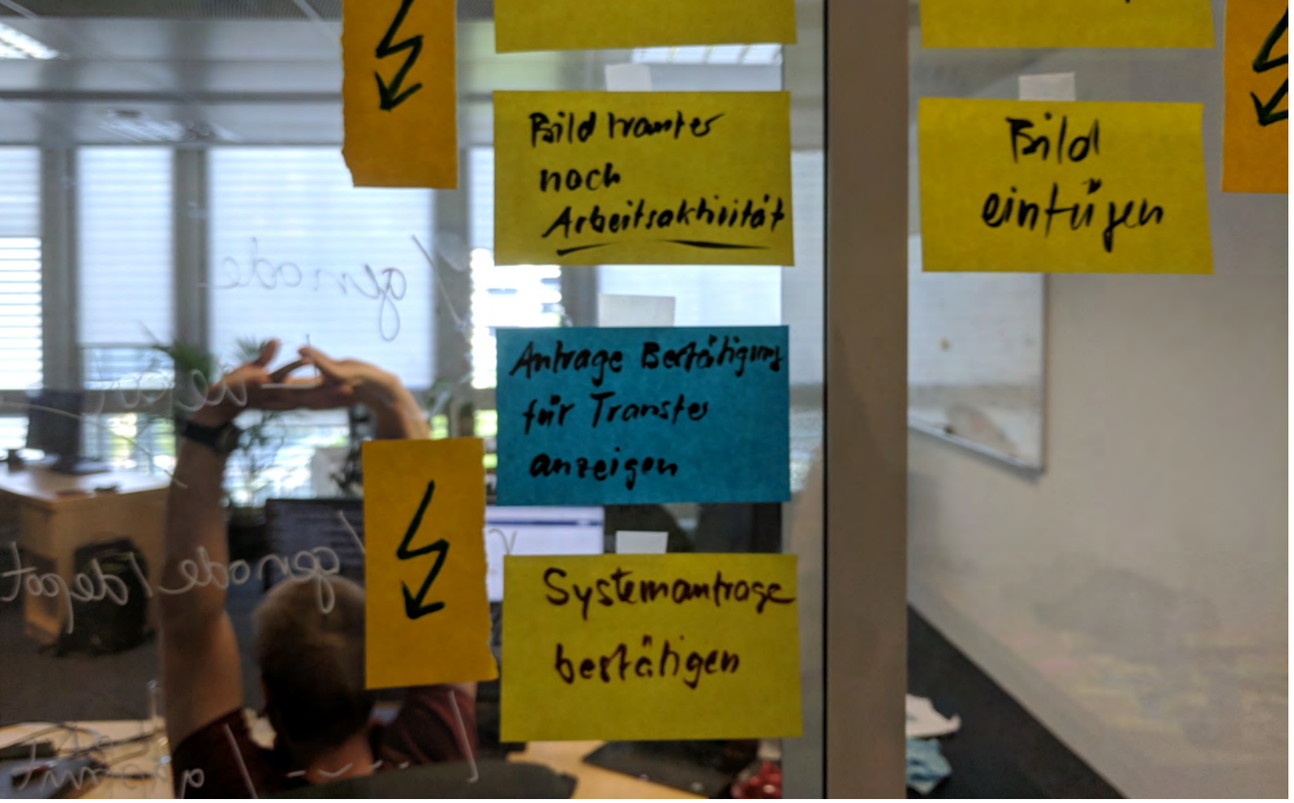
Neben den erwähnten Use Cases wurden auch vier User Szenarien [vgl. Anhang 9.2 User Szenarien gapfruit AG] an die Autoren herangetragen. Die Szenarien illustrieren hauptsächlich die Gefahren von Cyberkriminalität in unterschiedlichen Situationen und warum ein hochsicheres Betriebssystem auch im Firmenumfeld eingesetzt werden sollte. Sie rechtfertigen damit den Einsatz des Produktes, zeigen jedoch keine konkreten oder erhobenen Arbeitsabläufe bei potentiellen Benutzergruppen auf.

2.2.1 Vorgehen und Durchführung

Da die Autoren keinen Zugang zu Testkunden hatten, wurde mit den Auftraggebern ein ***User Story Map*** durchgeführt. Das Ziel dabei war es, konkrete Anwendungsszenarien eines hochsicheren Betriebssystems im realen Nutzungskontext aus der Erfahrung der Auftraggeber im Zusammenhang mit den fokussierten Use Cases aufzubauen. Nach einer kurzen Einführung in das Prinzip des ***User Story Map***, konnten die Diskussionen gestartet und eine ***User Story Map*** nach den Ausführungen der Auftraggeber aufgebaut werden.

2.2.2 Auswertung und Zusammenfassung der Resultate

Am Ende des Workshops konnte ein relevantes, potentielles Anwendungsszenario eruiert werden. Dieses beschreibt jedoch nur den generischen Ablauf einer Recherche, wobei ein Dokument in der unsicheren Zone aus dem Internet her-



untergeladen und in die sichere Arbeitsumgebung transferiert wird. Das Szenario enthält jedoch keine näheren Kontextinformationen wie Benutzer- oder Berufsgruppe, konkreter Arbeitsablauf in welchem das Szenario durchgeführt wird, Häufigkeit der Tätigkeit oder ähnliches. Das Szenario beschreibt nur den aus technischer Sicht notwendigen Ablauf, um Dokumente aus dem unsicheren Internet in die sichere Arbeitsumgebung zu bringen.

Nächste Schritte

Da nach wie vor weder konkrete Anhaltspunkte für Benutzergruppen oder Kontextszenarien bestehen, ist ein vertiefter User Research unerlässlich. Die Autoren möchten sich ausserdem einen vollständigeren Überblick und einen neutralen Kontext mittels einer ***Ask the Experts*** [20] Runde schaffen, in der Hoffnung erste potentielle Anwender und Nutzungsszenarien identifizieren zu können. Dazu wurden Interviews mit Fachleuten aus der IT Security Branche sowie mit Vertretern aus IT Infrastruktur und Betrieb von Unternehmen geplant.

[20] «The Design Sprint — GV». [Online]. Verfügbar unter: http://www.gv.com/sprint/. [Zugegriffen: 01-Jan-2019]..

User Story Map

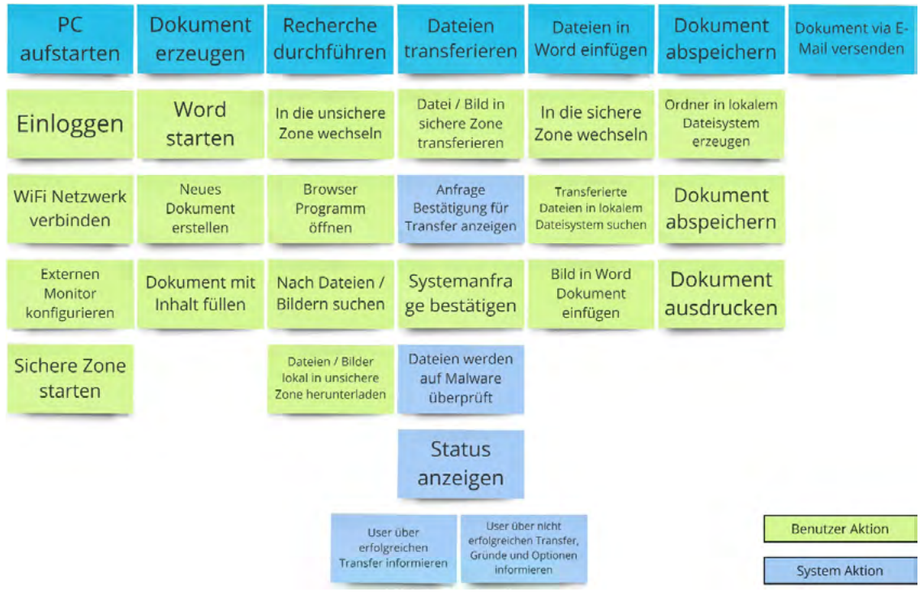


Abbildung 8: User Story Map Szenario «Internet Recherche»

2.2.3 Reflexion zur Methode User Story Mapping

User Story Mapping ist ein effektives und effizientes Tool um Abläufe zu visualisieren. Die Methode eignet sich auch gut zur Strukturierung von Prozessen. Im angewandten Fall führte die Methode jedoch nicht zu den gewünschten Ergebnissen, da keine effektiven User Szenarien abgebildet werden konnten. Lediglich ein technisch durch das System vorgegebener Prozess konnte aufgezeigt werden. Welche Anwendungsfälle potentielle Benutzer mit dem Betriebssystem durchführen würden blieb nach wie vor unklar.

2.3 Interviews mit Subject Matter Experts

Um die Herausforderungen und den Kontext des Projektes besser verstehen zu können, wurden Interviews im Sinne einer ***Ask the Experts*** Runde aus dem Google Design Sprint [21] mit Experten im Bereich IT Security und IT Infrastruktur durchgeführt. Einerseits sollten die Experten-Interviews den Autoren einen tieferen Einblick in die Problematik von unsicheren IT Systemen, den Ursachen für Einbrüche und Datendiebstähle sowie möglichen bzw. sinnvollen Gegenmassnahmen liefern. Auch die Rolle der Anwender in Bezug auf Verständnis und Akzeptanz von Sicherheitsmassnahmen sollte beleuchtet werden. Andererseits erhofften sich die Autoren eine neutrale Einschätzung zu Notwendigkeit und Sinnhaftigkeit des zu entwickelnden Produktes im Firmenumfeld sowie erste Hinweise auf potentielle Einsatzgebiete und Anwendergruppen.

2.3.1 Vorgehen und Durchführung

Die Befragungen wurden in Form von halbstandardisierten Interviews [22] durchgeführt. Ein vorgängig erstellter und an die Teilnehmer versandter Fragebogen half die groben Leitplanken für die Befragten zu setzen. Zur Durchführung der Interviews wurde der Fragebogen in einen Leitfaden [vgl. Anhang 9.6 Leitfaden Interviews Subject Matter Experts] verpackt und vom Interviewleiter zur Orientierung verwendet. Der Leitfaden stellte sicher, dass beim Interview keine wesentlichen Punkte vergessen gehen konnten. Zur Veranschaulichung der Produktidee wurde von den Autoren zusätzlich ein rudimentärer Prototyp erstellt, welcher bei den Interviews als Diskussionsgrundlage kurz vorgestellt wurde.

Als Teilnehmer rekrutierten die Autoren zwei Experten aus dem Bereich IT Security und einen aus dem Bereich IT Infrastruktur und Betrieb. Die Interviews waren auf 60 Minuten angesetzt und wurden zur späteren Auswertung mittels Audiorecorder (Mobile Phone) aufgezeichnet.

[21] J. Knapp, J. Zeratsky, und B. Kowitz, Sprint: How to solve big problems and test new ideas in just five days.

[22] C. Hauri und U. Suter, «Interviewtechnik». CAS Requirements Engineering 2016. Rapperswil: HSR Hochschule für Technik Rapperswil.

Interview Settings

Settings	Interview
3 Interviewpartner	Interview 1: Dr. Raphael Reischuk IT Security Researcher und Consultant, Zühlke Engineering AG
1 Audioaufzeichnung	Interview 2: Jonas Wettstein Services Expert IT Center, Zühlke Engineering AG
1 Interviewer	Interview 3: Peter Merker Chief Information Security Officer, Skyguide
2 Beobachter und Notizen	

2.3.2 Auswertung der Resultate mittels Affinity Diagram

Zur Auswertung der Interviews wurden die Aussagen der befragten Personen unter Zuhilfenahme der Audioaufnahmen transkribiert und mit den handschriftlichen Notizen der einzelnen Teammitglieder konsolidiert. Dabei wurden die für den weiteren Projektverlauf relevanten Aussagen gesammelt, auf digitale Post-it Zettel geschrieben und mittels Affinity Diagram geclustert [vgl. Anhang 9.7 Auswertung Interviews Subject Matter Experts]. Auf diese Weise konnte rasch ein Überblick gewonnen und ein Fazit für das weitere Vorgehen gezogen werden.

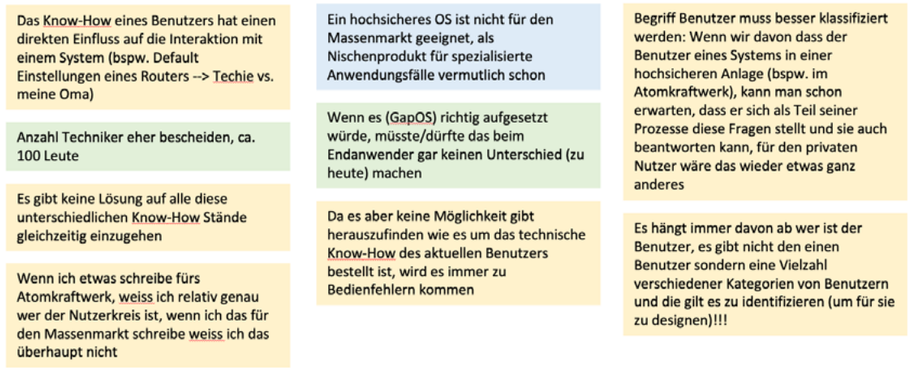


Abbildung 9: Ausschnitt Affinity Diagramm zur Auswertung der Experten-Interviews

2.3.3 Zusammenfassung der Resultate

Die Rückmeldungen der interviewten Experten zur vorgestellten Produktidee waren überwiegend zurückhaltend und zuweilen kritisch. Die Kosten zur Einführung eines neuen Systems in einer mittelgrossen Firma sind exorbitant. Die Einführung ist nur dann interessant, wenn der ***Return on Invest*** stimmt. Für eine Firma bedeutet dies, dass die Kosten für Einführung, Betrieb und Schulung der Mitarbeiter

markant kleiner sein müssen, als die potentiellen Kosten bei einem Datendiebstahl bzw. als die Kosten zur Wiederherstellung des Normalbetriebs.

Security Bedenken trotz gapfruitOS

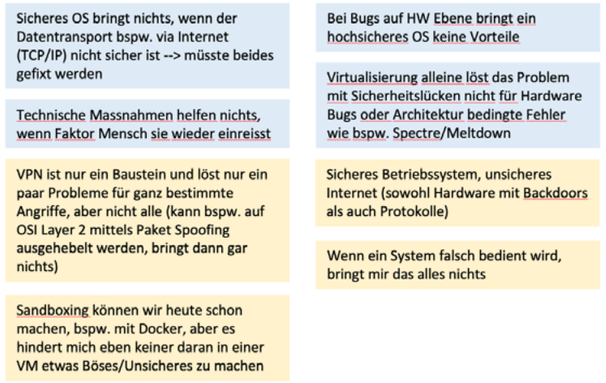


Abbildung 10: Ausschnitt Affinity Diagram zur Auswertung der Experten-Interviews

bei einer Kompromittierung des Systems. Interessanterweise gilt exakt dasselbe Prinzip auch auf der Seite der Angreifer. Ein bestimmtes Unternehmen lohnt sich als Ziel für eine Cyberattacke nur dann, wenn der Aufwand zum Einbrechen in das Firmennetzwerk kleiner ist, als die potentielle Monetarisierung der gestohlenen Daten. Es wird also von den Unternehmen selbst eine Einschätzung vorgenommen, welche Priorität das eigene Unternehmen bei Hackern hat. Die hängt massgeblich vom Wert der innerhalb des Unternehmens produzierten und verarbeiteten Daten ab.

Gemäss Aussagen des Security Consultants vermag das Zonenkonzept des Produktes die Probleme der IT Sicherheit nicht zu lösen, sofern nicht das gesamte Ökosystem (Netzwerk, Benutzer, etc.) abgesichert ist. Trotzdem existiert die Notwendigkeit für ein hochsicheres Betriebssystem definitiv. Der Bedarf ist jedoch aus verschiedenen Gründen nicht an die Notwendigkeit gekoppelt. Neben den beschriebenen Abwägungen zwischen Priorität bei Angreifern und Schadenspotential, existiert die Benutzerperspektive. Versteht der Benutzer das eingeführte System nicht oder erfährt durch die Bedienung zu viele Hürden bei seinen täglichen Arbeitsabläufen, wird er das Produkt nicht akzeptieren und sich Workarounds suchen. Hierbei muss zusätzlich zwischen zwei unterschiedlichen Anspruchsgruppen unterschieden werden, dem Endverbraucher, der das Produkt verstehen und effizient bedienen können muss und dem technischen Administrator, welcher

Dieser Wert einer hohen Usability ist heute so gigantisch, dass der Leidensdruck extrem sein muss, um die Extrameile für starke Security zu gehen.

Dr. Raphael Reischuk

das Produkt einführen, warten und betreiben muss. Das hochsichere Betriebssystem darf für den Endverbraucher kaum einen Unterschied in der Benutzung mit sich bringen. Die jetzige Usability darf (mit kleinen Kompromissen) nicht eingeschränkt werden, da sie viel höher priorisiert wird als die Security.

Ein hochsicheres Betriebssystem im diskutierten Sinn ist gemäss Meinung der Experten eher ein Nischenprodukt für eine relativ kleine, sehr spezifische Zielgruppe. Es ist nicht für den Massenmarkt geeignet, sondern für spezialisierte Anwendungsfälle, da es nicht möglich ist, ein solches System auf all die unterschiedlichen Knowhow-Stände der Mitarbeiter in einem Unternehmen gleichzeitig zu optimieren. Die Gestaltung des Systems ist abhängig vom Benutzer. In einem Unternehmen gibt es nicht den einen Benutzer, sondern eine Vielzahl verschiedener Kategorien von Benutzern und diese gilt es zu identifizieren, um für sie zu designen.

Ein weiterer wichtiger Punkt ist die Notwendigkeit um das Bewusstsein für sensitive Daten. Menschen, die in einem Umfeld mit besonders schützenswerten Daten wie bspw. Personen- und Gesundheitsdaten oder besonders sensitiven Daten wie bspw. Finanzdaten arbeiten, haben eine andere Einstellung im Umgang mit diesen Daten. Werden die bearbeiteten Daten als sehr sensitiv wahrgenommen, ist eher eine Bereitschaft vorhanden, zusätzliche Arbeitsschritte zu unternehmen, um die Daten nicht zu gefährden. Der Benutzer eines hochsicheren Betriebssystems muss also ganz genau wissen, wo ihm das System einen Mehrwert bringt, damit er es anwenden will. Dies trifft aber nur auf eine spezifische Benutzergruppe oder Art von Unternehmen zu, nämlich solche, die mit hochsensitiven Daten zu tun haben. Als Beispiel wurde ein Atomkraftwerk genannt.

Nächste Schritte

Die ausgewerteten Ergebnisse wurden dem Auftraggeber präsentiert. Ziel der Autoren war es, das Bewusstsein für die Existenz einer spezifischen Benutzergruppe und damit verbunden die zentrale Rolle, welche der Identifikation dieser Benutzergruppe zukommt, beim Auftraggeber zu wecken. Da die Auftraggeber bisher keine Notwendigkeit für einen User Research sahen, wurde im Rahmen der Präsentation zusätzlich das Prinzip des ***User Centered Designs*** [23], [24] vorgestellt und dessen Wert hervorgehoben.

[23] C. Hübscher, «Skript Vorgehensmodelle: User Centered Design 1». CAS Requirements Engineering 2016. Rapperswil: HSR Hochschule für Technik Rapperswil.

[24] C. Hübscher, «Skript Vorgehensmodelle: User Centered Design 2». CAS Interaction Design 2017. Rapperswil: HSR Hochschule für Technik Rapperswil.

2.3.4 Reflexion zur Methode

Die ***Ask the Experts*** Runde half dem Team bei der Einschätzung und Bewertung der Ausgangssituation. Es konnte viel zusätzliches Wissen aufgebaut und der Blickwinkel erweitert werden. Die Aussagen der Experten bestätigten Annahmen der Teammitglieder, insbesondere in Bezug auf die Benutzergruppe eines hochsicheren Betriebssystems. Auch die Methode der halbstrukturierten Interviews hat für diesen Zweck sehr gut funktioniert. Mit den vorgefertigten Kontext- und Fokusfragen [vgl. Anhang 9.6 Leitfaden Interviews Subject Matter Experts] konnte der Rahmen für die wichtigsten Themen gut abgesteckt und der Gesprächsfluss am Laufen gehalten werden. Neben den Antworten auf die vorgegebenen Fragen kamen auch viele neue und unerwartete Aspekte ans Licht. Die Gespräche waren so interessant, dass meist der zeitliche Aspekt zum Thema wurde. Hierbei halfen der Interview-Leitfaden und ein aufmerksamer Interviewleiter konnte die Gespräche bei Ausflügen wieder zurück in die Spur bringen.

3 Methodik und Vorgehen

3.1 Wahl des Vorgehensmodells

Zu Beginn des Projektes wurde aufgrund der strukturierten Arbeitsweise und des klar vorgegebenen Ablaufs ***Goal-Directed Design*** von Alan Cooper et al. [25] als Vorgehensmodell gewählt. Da bei den Autoren bereits von Anfang an die Vermutung nach einer sehr spezifischen Benutzergruppe bestand, erschien die ausgedehnte Research und Modeling Phase dieses Vorgehensmodells ideal. Die Auftraggeber waren zu diesem Zeitpunkt jedoch der strikten Überzeugung, dass ihr Produkt für alle Unternehmen und Privatpersonen interessant sein müsse, da es zu mehr Datensicherheit und weniger Schäden durch Cyberkriminalität führen kann. Aus diesem Grund sahen die Auftraggeber auch keinen Wert in einer ausgedehnten User Research Phase und erwarteten von den Autoren rasch erste konkrete Ideen für ein Interaktionskonzept.

Goal-Directed Design Prozess nach Alan Cooper

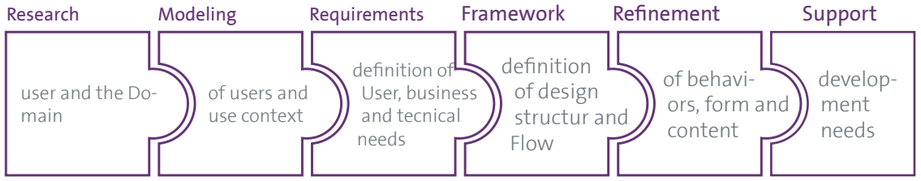
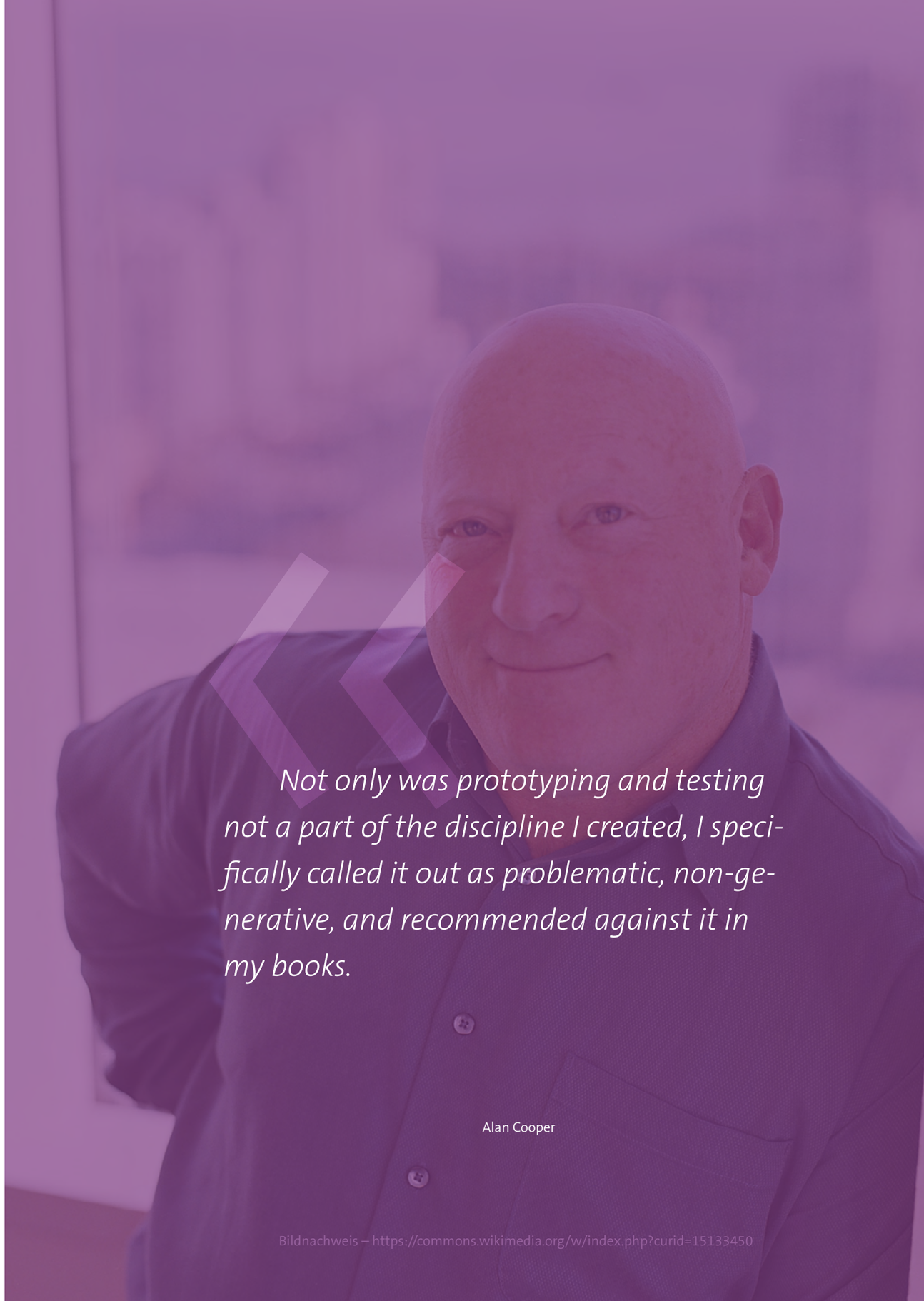


Abbildung 11: Goal-Directed Design Prozess aus About Face nach Alan Cooper

3.2 Neuausrichtung und Änderung des Vorgehensmodells

Unterschiedliche Ansichten über ein sinnvolles Vorgehen zwischen Auftraggebern und Autoren führten zu einer Eskalation im Projekt. Auf der einen Seite stand die Erwartungshaltung nach einem klugen, minimal-invasiven Interaktionskonzept für das zu entwickelnde Produkt, welches möglichst rasch ausgearbeitet und mittels interaktiver Prototypen getestet werden sollte. Auf der anderen Seite konnte den Autoren kein Zugang zu bestehenden Testkunden gewährt werden und es fehlte die Fokussierung auf eine konkrete Zielgruppe zur Erhebung der notwendigen Grundlagen innerhalb der Phasen ***Research*** und ***Modeling*** gemäss ***Goal-Direc-***

[25] A. Cooper, R. Reimann, D. Cronin, und C. Noessel, About Face, Fourth Edition



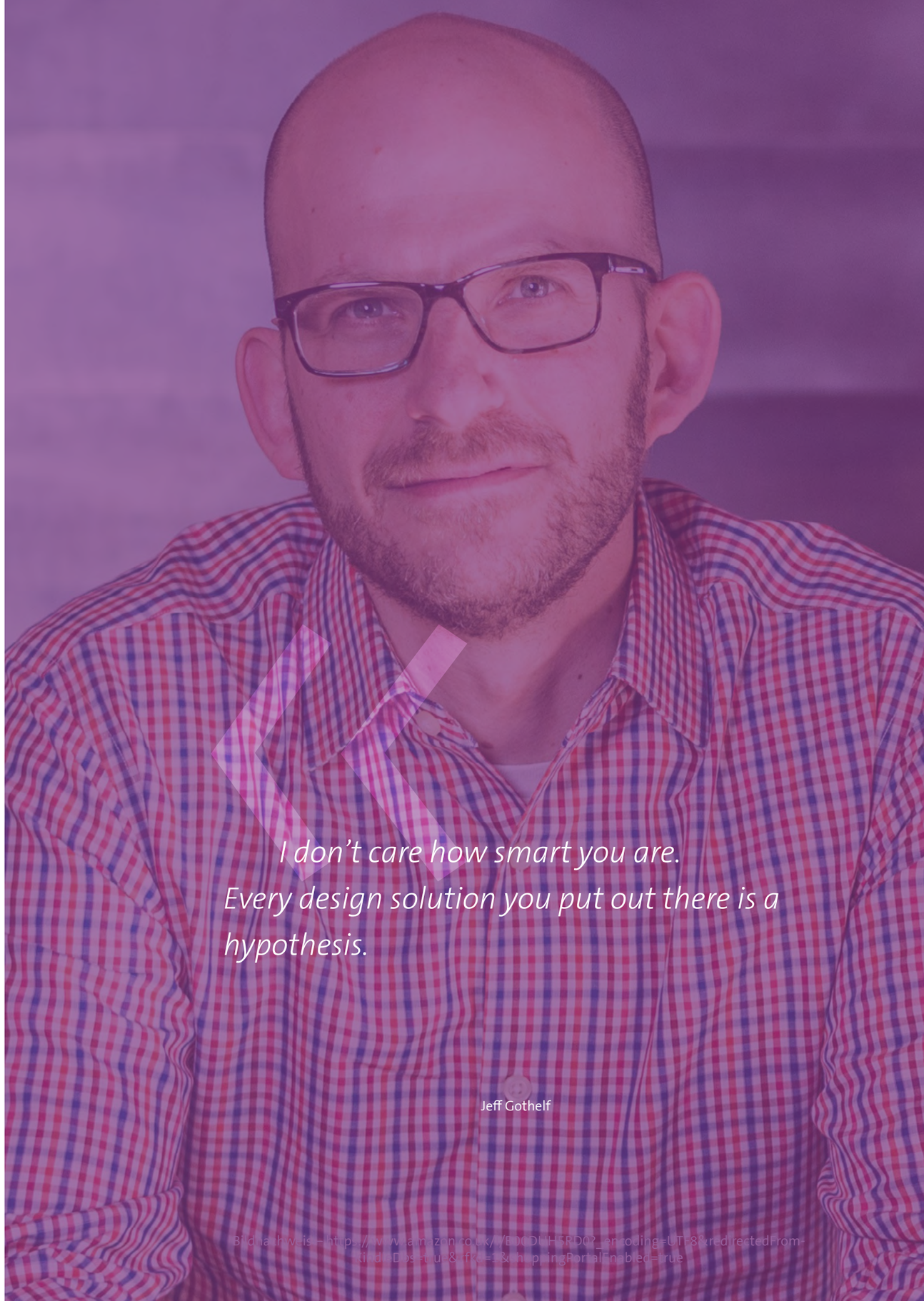
ted Design. Diese Situation gipfelte beinahe im Abbruch des Projekts. Durch einen Wechsel des Vorgehensmodells konnte mit ***Lean UX*** schliesslich ein für beide Seiten annehmbarer Ansatz gefunden werden.

Der definitive Wechsel erfolgte erst nach einer ausserordentlichen Coaching Sitzung mit ***Chri Hübscher***, dem ausgewiesenen Experten für Vorgehensmodelle im HCID Studiengang, da ***Lean UX*** im Rahmen der Ausbildung nicht gelehrt bzw. nur am Rande gestreift wurde. ***Lean UX*** verfolgt einen radikal anderen Ansatz als ***Goal-Directed Design***. Während ***Goal-Directed Design*** einen strikten, wasserfallartigen Ablauf vorgibt – erst die Anwender und den Kontext erheben/modellieren und erst dann mit dem Design des Systems beginnen – basiert ***Lean UX*** auf vielen kurzen, aufeinanderfolgenden ***Think – Make – Check*** Zyklen. Innerhalb dieser Zyklen werden unter anderem Prototypen erarbeitet und getestet, wovon Alan Cooper in seinem Vorgehensmodell vehement Abstand nimmt [26].

Durch seinen Annahmen-basierten ***Think – Make – Check*** Zyklus bietet sich der Lean-Ansatz, bzw. ***Lean UX*** insbesondere dann, wenn weder die Problem- noch die Lösungsdomäne vollständig und klar definiert sind.

3.3 Lean UX Prinzipien

Im Gegensatz zu ***Goal-Directed Design*** proklamiert ***Lean UX*** die kontinuierliche Forschung parallel zum Design des Systems. Dies unterstützt das kurzfristige Ziel des Auftraggebers, möglichst schnell mit einem MVP auf den Markt zu gehen sowie die längerfristige Vision, schrittweise den Weg von der klassischen Desktop-Metapher hin zu einem neuen, revolutionären Interaktionskonzept zu gehen. Traditionell wird bei UX Projekten von Anforderungen ausgegangen. ***Lean UX*** bricht mit diesem Konzept und geht von Annahmen anstelle von Anforderungen aus. Aus diesen Annahmen werden konkrete, überprüfbare Hypothesen gebildet und mittels eines MVP Prototyps regelmässig mit Benutzern getestet. Dieser ***Think – Make – Check*** Zyklus wird iterativ durchgeführt [27].



[26] A. Cooper, «The Endless Battle», Alan Cooper, 22-Okt-2017

[27] J. Gothelf und J. Seiden, Lean UX - Applying Lean Principles to Improve User Experience, 16. Aufl. O’Reilly Media

Lean UX Zyklus

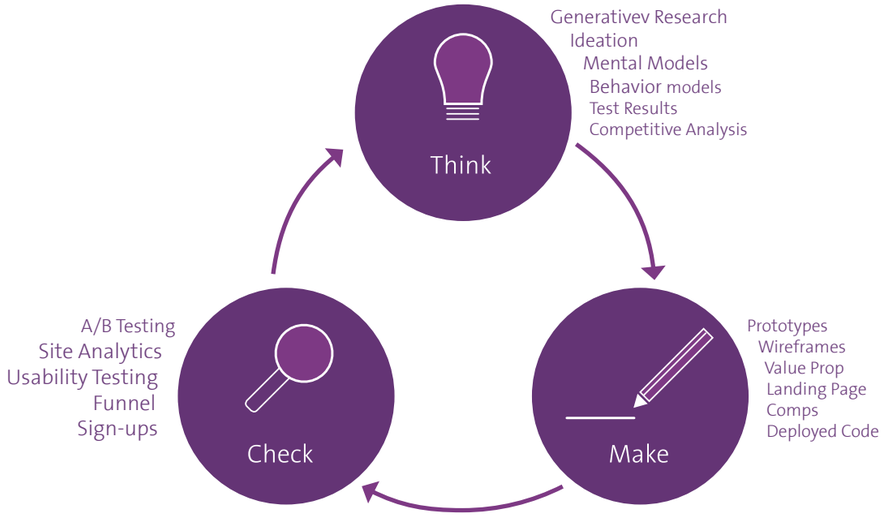


Abbildung 12: Think - Make - Check Zyklus

Folgendes sind die wichtigsten Prinzipien von Lean UX in Zusammenhang mit der vorliegenden Arbeit kurz zusammengefasst:

- ***Progress = Outcomes, Not Output*** – Features sind Outputs, Ziele der Kunden/Anwender, die damit erreicht werden sollen sind Outcomes. Bei der Voraussage welche Features spezifische Benutzer- oder Geschäftsziele erfüllen sollen handelt es sich meist um pure Spekulation. Erst wenn das erwünschte Resultat klar ist, kann entschieden werden ob ein Feature sinnvoll ist oder nicht.
- ***Small Batch Size*** – Es soll nur so viel Design umgesetzt werden, wie notwendig ist um mit dem Team vorwärts zu kommen. Dabei sollen keine ungenutzten oder ungetesteten Ideen im Backlog liegen bleiben.
- ***Continuous Discovery*** – Der Anwender soll fortlaufend in den Design- und Entwicklungsprozess mit einbezogen werden. Das Ziel hierbei ist es herauszufinden, was die Anwender mit dem Produkt tun und warum. Untersuchungen werden häufig und in regelmässigen Abständen durchgeführt.
- ***GOOB*** (Getting out of the Building) – Beschreibt die Erkenntnis, dass Debatten über Benutzeranforderungen hinter verschlossenen Türen diese nicht abschliessen klären können und somit nicht zum Ziel führen. Neue Ideen müssen in der Praxis auf Tauglichkeit getestet werden, solange noch nicht zu viel Zeit und Mühe hineingeflossen ist.
- ***Externalizing Your Work*** – Die Arbeit muss aus dem Kopf bzw. dem Computer der UX Designer in die Öffentlichkeit gebracht werden. Mittels Zeichnungen, Diagrammen, Wireframes oder Post-Its können die Ideen und Konzepte den Teamkollegen und Anwendern verständlich gemacht werden.
- ***Making over Analysis*** – Eine erste Version einer Idee umzusetzen bringt mehr Wert als lange über Vor- und Nachteile zu diskutieren. Ideen diskutieren ist Zeitverschwendung. Anstatt potentielle Szenarien zu analysieren soll etwas Konkretes erstellt und mit Anwendern getestet werden.

Iterations Prozess nach Lean UX

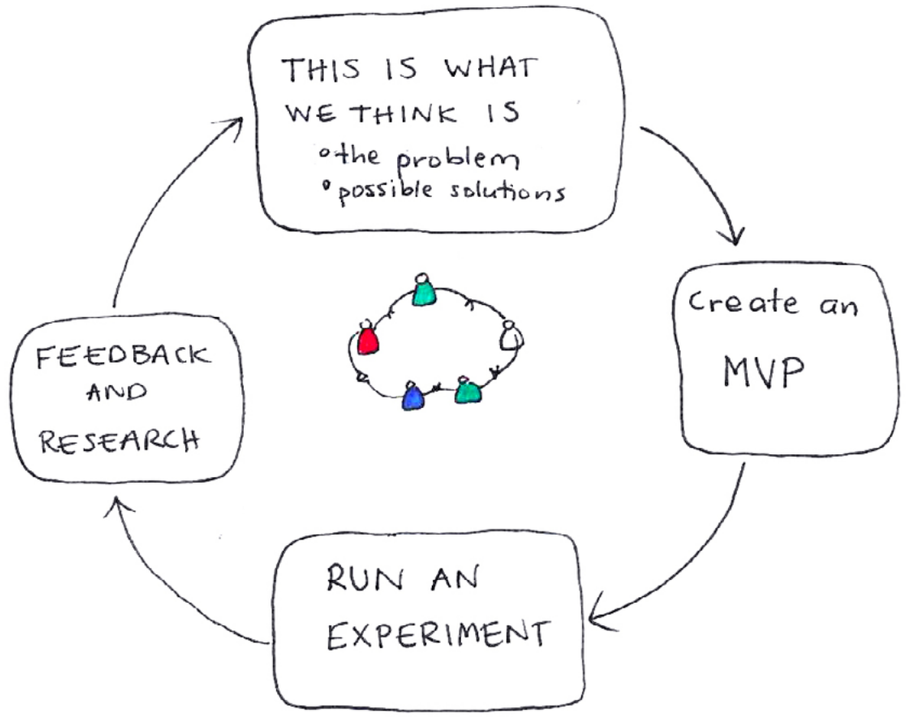


Abbildung 13: Lean UX Prozess nach Jeff Gothelf [27]

[27] J. Gothelf und J. Seiden, Lean UX - Applying Lean Principles to Improve User Experience, 16. Aufl. O'Reilly Media

Annahmen deklarieren

Annahmen sind High-Level-Deklarationen von Vorstellungen die als zutreffend erachtet werden. Aus diesen ***Annahmen*** werden verifizierbare ***Hypothesen*** gebildet. Eine ***Hypothese*** ist eine feinkörnigere Beschreibung einer ***Annahme***, welche spezifische Bereiche des zu erstellenden Produktes zwecks Erprobung der einzelnen Aspekte der Annahme betreffen. ***Ergebnisse*** sind Bewertungskriterien bzw. Marktsignale, die dabei helfen, die aufgestellten ***Hypothesen*** zu validieren oder zu widerlegen. Am Ende des Prozesses stehen die Features, Produktänderungen oder Verbesserungen, welche die gewünschten Ergebnisse herbeiführen sollen.

Im ***Lean UX*** Prozess werden ***Personas*** ebenfalls aus ***Annahmen*** in Form von ***Proto-Personas*** gebildet. ***Proto-Personas*** sind die bestmöglichen Vermutungen über die zukünftigen Benutzergruppen des Systems basierend auf dem aktuellen Wissensstand des Projektteams. Im Projektverlauf werden die ***Proto-Personas*** durch die kontinuierlichen Untersuchungen validiert und fortlaufend auf die real, existierenden Benutzergruppen angepasst.

MVPs erzeugen und Experimente durchführen

Zum Testen der ***Hypothesen*** wird ein so genanntes ***Minimum Viable Product*** (MVP) erstellt. ***MVPs*** helfen dabei, so rasch wie möglich herauszufinden, ob die eingeschlagene Richtung korrekt ist und welche Produkt-Features eine Investition wert sind. Die priorisierte Liste von ***Hypothesen*** gibt die verschiedenen Pfade zur Erforschung vor. Um diese Erforschung effizient zu gestalten wird nun das kleinstmögliche «Ding» erzeugt, mit welchem die Gültigkeit der einzelnen ***Hypothesen*** überprüft werden kann. Das ist das ***MVP***. Damit können die zur Verfügung stehenden Ressourcen schnell auf die erfolgversprechendsten Lösungen konzentriert werden.

Prototyping ist eine effektive Praktik zur Erstellung eines ***MVPs***. Da ***Lean UX*** ein kollaborativer Prozess ist, entstehen Design-Ideen für ***MVP Prototypen*** ebenfalls im Team. Dabei werden die zugrunde liegenden Konzepte vom gesamten Projektteam in gemeinsamen Sitzungen, bspw. in einem ***Design Studio***, erarbeitet. Diese enge Zusammenarbeit steigert die Akzeptanz für die erarbeiteten Lösungen. Das Design wird zum Kollektivbesitz, da es Ideen aller Teammitglieder beinhaltet. Ausserdem entwickelt das Team ein gemeinsames Verständnis für die Problemstellung und den gewählten Lösungsansatz.

Die ***MVP Prototypen*** werden in der Folge mit Teamkollegen, Stakeholdern und potentiellen Anwendern getestet. Dabei ist es wichtig herauszufinden, wie gut der Prototyp funktioniert, wie die Testpersonen damit umgehen und ob sich ein weiteres Investment lohnt. Je breiter getestet wird, desto mehr Erkenntnisse über die Gültigkeit der ***Annahmen*** ergeben sich.

3.3.1 Feedback und Recherche

Benutzerforschung ist der Kern der meisten UX Vorgehensmodelle. Zu oft findet der ***Research*** aber nur bei wenigen, bestimmten Gelegenheiten statt, zu Beginn oder am Ende des Projekts. ***Lean UX*** proklamiert eine ***kontinuierliche*** und ***kollaborative*** Vorgehensweise bei der ***Benutzerforschung***. Kontinuierlich heisst, dass informale, qualitative Studien während jeder Iteration durchgeführt werden. Kollaborativ bedeutet, ***Forschungsfragen***, ***Annahmen***, ***Hypothesen*** und ***MVPs*** werden gemeinsam im Team reviewt. Auch die Benutzertests werden jeweils zu zweit durchgeführt. Daneben sollte regelmässig der Auftraggeber miteinbezogen werden, um die Zeit zwischen Hypothesenbildung, Experiment Design und User Feedback zu minimieren.

Aktivitätskalender nach Lean UX

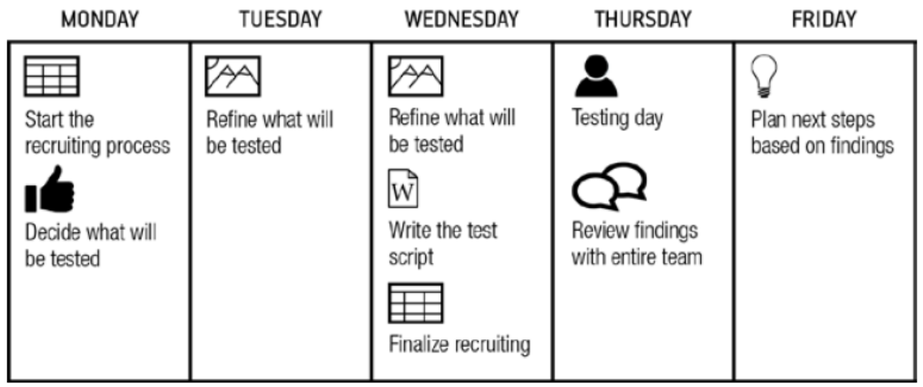


Abbildung 14: Lean UX Aktivitätskalender nach Jeff Gothelf [27]

Iterationen sind im ***Lean UX*** Prozess sehr kurz. Jeff Gothelf und Josh Seiden schlagen einen wöchentlichen ***3-12-1*** Rhythmus gemäss oben abgebildeter Tabelle vor. Dabei wird mit ***3*** Benutzern bis ***12*** Uhr mittags ***1*** Mal pro Woche getestet. Innerhalb dieser Woche durchläuft das Team den ganzen Prozess von der Ausarbeitung

[27] J. Gothelf und J. Seiden, Lean UX - Applying Lean Principles to Improve User Experience, 16. Aufl. O'Reilly Media

des Designs über die Erstellung eines Prototyps bis hin zum Testen und Sammeln der gewonnen Erkenntnisse.

Weiterhin soll eine ***Test-Everything*** Strategie verfolgt werden, was immer am Testtag bereit liegt, wird den Benutzern vorgelegt. Dabei kann es sich beispielsweise auch nur um Sketches handeln, die das aktuelle Konzept verdeutlichen. Damit können jedoch die wöchentlichen Test Sessions aufrechterhalten werden und das Team generiert Erkenntnisse zu jedem Zustand des Designs. Je nach Typ des testbaren Artefakts müssen jedoch die Erwartungen der Benutzer entsprechend gemanagt werden.

3.4 Projektplanung

Der Kick-Off Workshop mit den Auftraggebern erfolgte Anfang Mai 2019. Die Planung veränderte sich danach sehr stark im Verlauf des Projekts. Insbesondere der Wechsel des Vorgehensmodells erforderte eine komplette Neuausrichtung im August 2018, nach etwa einem Drittel der zur Verfügung stehenden Zeit. Gemäss der ursprünglichen Planung nach ***Goal-Directed Design*** in unten stehender Abbildung, sollten im August die ***Research*** und ***Modeling*** Phase bereits abgeschlossen und damit sowohl Benutzergruppen als auch Kontextszenarien für das Produkt erhoben worden sein.

Erste Projektplanung nach Goal-Directed Design

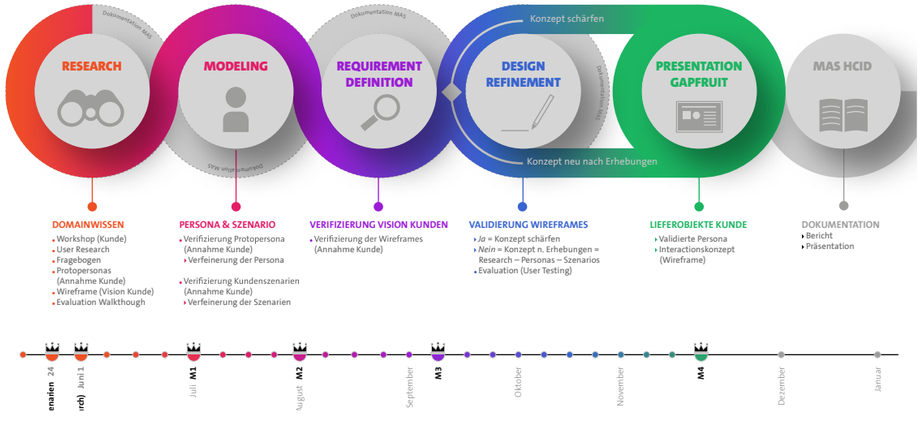


Abbildung 15: Erste Projektplanung nach Goal-Directed Design

Aufgrund der eingangs beschriebener Schwierigkeiten und dem notwendig gewordenen Wechsel des Vorgehensmodells, waren die Interviews mit Domänenexperten zu diesem Zeitpunkt die einzige, verlässliche Grundlage für die weiterhin notwendige Benutzerforschung. Daher wurden anhand des ***Lean UX Aktivitätskalenders*** gemäss Jeff Gothelf [27] vier weitere Iterationen mit Experimenten zwecks Ausarbeitung von Designhypothesen und für die Benutzerforschung eingeplant. Den Autoren stand grundsätzlich ein Tag pro Woche für das Projekt zur Verfügung. Deshalb wurde der wöchentliche Iterationsrhythmus gemäss Aktivitätskalender von ***Lean UX*** [vgl. Abb. 14] auf fünf Wochen ausgedehnt und über die restliche zur Verfügung stehende Zeit eingeplant. Das vollständige Dokument befindet sich im [vgl. Anhang 9.3 Projektplanung].

Mit der gewonnenen Erfahrung aus den ersten ***Experimenten*** konnte die ursprünglich geplante Dauer von fünf Wochen für eine einzelne Iteration verkürzt und die Anzahl durchgeführter ***Experimente*** von vier auf sieben erhöht werden.

3.5 Risikomanagement

Zu Beginn des Projektes wurden von den Autoren insbesondere zwei grosse Risiken für den weiteren Projektverlauf identifiziert, zum einen die fehlende Möglichkeit bestehende Testkunden zwecks Untersuchungen im Rahmen der Benutzerforschung anzugehen und zum anderen die fehlende Fokussierung des Produktes auf eine spezifische Zielgruppe. Wie in Kapitel 3.2 Neuausrichtung und Änderung des Vorgehensmodells beschrieben, trafen beide Risiken ein und konnten nur durch diese Neuausrichtung teilweise adressiert werden. Eine vollständige Liste mit der Risikoanalyse befindet sich im Anhang [vgl. Anhang 9.4 Risikoliste].

[27] J. Gothelf und J. Seiden, Lean UX - Applying Lean Principles to Improve User Experience, 16. Aufl. O'Reilly Media

4 Recherche und Marktanalyse

Betriebssysteme mit einer ähnlich sicheren Architektur wie das vom Auftraggeber entwickelte System existieren zurzeit beinahe ausschliesslich für Behörden und Regierungen. Diese Systeme basieren ebenfalls auf dem Prinzip der ***Compartmentalisation***. Die Produkte sind jedoch nicht öffentlich zugänglich und werden nur bei Demonstrationen durch die Hersteller, bspw. auf einschlägigen Messen, vorgeführt. Somit waren diese Systeme für das Projektteam nicht direkt test- und analysierbar. Alle Informationen zu diesen geschlossenen Systemen stammen ausschliesslich vom Auftraggeber und wurden wie erläutert in diese Arbeit übernommen [vgl. 4.1 Geschlossene Systeme für Behörden und Regierungen].

Neben den für das Projektteam nicht zugänglichen Systemen werden im Anhang [vgl. Anhang Recherchen und Marktanalyse] noch weitere interessante Produkte analysiert und für die vorliegende Arbeit eingeordnet.

4.1 Geschlossene Systeme für Behörden und Regierungen

Eine Reihe von Herstellern ist bereits mit ähnlichen Systemen wie das von den Auftraggebern entwickelte auf dem Markt. Obwohl aufgrund der Bedrohungslage und der durch Cyberkriminalität verursachten Schäden [vgl. 1.2 Kontext der Arbeit] der Einsatz derartiger Produkte für viele marktorientierte Unternehmen sinnvoll wäre, werden diese Systeme in der Privatwirtschaft praktisch gar nicht eingesetzt. Dies mag hauptsächlich daran liegen, dass die Produkte nur bedingt für den täglichen Gebrauch in den meisten Unternehmen geeignet sind. Im Anhang finden sich detailliertere Informationen zum Funktionsprinzip der analysierten Systeme [vgl. Anhang 9.5 Recherchen und Marktanalyse].

5 Experimente

Lean UX ist ein annahmen-basierter Ansatz. Um diese Annahmen zu überprüfen, bedient sich Lean UX hauptsächlich dem Konzept der Minimum Viable Products (MVP). Die getroffenen Annahmen werden als Designhypothesen mit minimalem Aufwand entweder direkt im realen Produkt oder als MVP Prototyp umgesetzt. Dabei wird nur genau diejenige Funktionalität gebaut, welche zum Prüfen einer Annahme notwendig ist. Es geht darum unnötige Arbeit zu vermeiden und möglichst schnell herauszufinden, welche Funktionen in einem Produkt dem Benutzer den meisten Wert bei der Lösung einer bestimmten Problemstellung liefern [27].

Im Rahmen von so genannten «Experimenten» werden die Annahmen schliesslich mit potentiellen Benutzern getestet. Dazu werden regelmässig Teilnehmer rekrutiert und Testtage organisiert. Wenn ein MVP oder ein MVP Prototyp zur Verfügung steht, kann mit den Teilnehmern ein klassischer Benutzertest durchgeführt werden. Wie in Kapitel 3 Methodik und Vorgehen dargelegt, verfolgt Lean UX eine ***Test-Everything*** Strategie. Wenn also an einem Testtag keine funktionstüchtige Software oder kein Prototyp zur Verfügung steht, kann den Testteilnehmern jedes andere bereitstehende Artefakt vorgelegt und über Walkthroughs, Interviews oder Diskussionen mit ihnen «getestet» werden.

5.1 Ziel der durchgeführten Experimente

Die grösste Schwierigkeit bei der Arbeit in unterschiedlichen Sicherheitskontexten, welche bei gapfruitOS durch unterschiedliche virtuelle Maschinen umgesetzt werden, sind die verschiedenen Dateisysteme und installierten Programme in den einzelnen VMs. Befindet sich ein Benutzer bspw. in der sicheren «Work Zone» und möchte für eine Internet-Recherche den Browser öffnen, muss er erst in die unsichere «Internet Zone» wechseln, den App Launcher öffnen und kann erst dann den Browser starten. In der jeweiligen Zone stehen nur die auf der zugehörigen VM installierten Programme zur Verfügung. Dieselbe Problematik ergibt sich auch mit den unterschiedlichen Dateisystemen. Jede VM und damit jeder Sicherheitskontext hat ein eigenes, isoliertes Dateisystem. Befindet sich der Benutzer in der sicheren «Work Zone» kann er bspw. nicht auf ein aus dem Internet heruntergeladenes Dokument in der unsicheren «Internet Zone» zugreifen.

[27] J. Gothelf und J. Seiden, Lean UX - Applying Lean Principles to Improve User Experience, 16. Aufl. O'Reilly Media

Beispiel mit zwei Zonen auf dem gapfruitOS Host

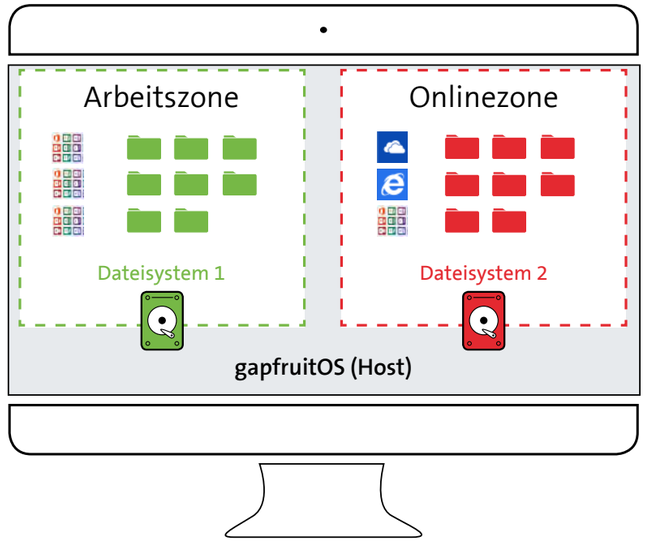


Abbildung 16: Vom Benutzer verwendete Dateien und Programme sind über verschiedene Zonen (virtuelle Maschinen) verteilt

Um das gewünschte Programm zu starten oder eine Datei zu öffnen, steht der Benutzer deshalb jeweils folgender Fragestellungen gegenüber:

A) **Wo befinde ich mich in diesem Moment?**

B) **Welche Programme und Dateien habe ich hier zur Verfügung?**

C) **Muss ich erst die Zone wechseln um die gewünschte Tätigkeit auszuführen?**

Die Handhabung dieser getrennten Kontexte erfordert konstant eine höhere kognitive Leistung [28] . Zur Generierung von Ansätzen für ein mögliches Interaktionsdesign gilt es also folgende Problematik zu klären:

Wie wird einem Benutzer eines derart komplexen Betriebssystems über das UI kommuniziert...

[28] C. Hübscher, «Slides Vorgehensmodelle: User Centered Design Grundlagen». CAS Requirements Engineering 2016. Rapperswil: HSR Hochschule für Technik Rapperswil.

A) **...in welchem Sicherheitskontext er sich gerade befindet?**

B) **...wie und was er im aktuellen Sicherheitskontext überhaupt machen kann/darf?**

C) **...wo er seine Dokumente speichern kann?**

D) **...wie er seine Dokumente von einer Sicherheitszone in eine andere verschieben kann?**

Wichtiger noch als die Ideengenerierung für erste Interaktionskonzepte war es für die Autoren Benutzerforschung zu betreiben und konkrete Benutzergruppen sowie Kontextszenarien für das geplante Produkt zu erheben.

5.2 Iterationen und Setting der Experimente

Der Durchführung von Experimenten kommt im Lean UX Prozess eine zentrale Rolle zu. Ein Experiment entspricht dabei einer Iteration und führt von der Deklaration der Annahmen über die Rekrutierung von Teilnehmern und Erstellung eines testbaren Artefakts bis hin zur Auswertung der Resultate. Die ausgeführten Tätigkeiten wiederholen sich dabei. Im Rahmen der vorliegenden Arbeit haben die Autoren innerhalb von 12 Wochen 7 Iterationen durchgeführt, 6 davon beinhalteten Usability Tests mit klickbaren Prototypen. Die übrige Iteration bestand aus der Vorstellung und Diskussion des Konzepts von gapfruitOS mit potentiellen Benutzern und anschliessendem Interview über die Arbeitsprozesse der einzelnen Teilnehmer.

Um die Übersichtlichkeit des Berichtes zu wahren und die Dokumentation der Experimente auf das Wesentliche zu beschränken werden die repetitiven Tätigkeiten im Folgenden zusammengefasst und in den Unterkapiteln 5.2.1 Rekrutierung von Teilnehmern und 5.2.2 Durchführung der Experimente einmalig beschrieben.

5.2.1 Rekrutierung von Teilnehmern

Bei der Rekrutierung starteten die Autoren mit gewöhnlichen Benutzern, die im Rahmen ihrer Arbeitstätigkeit meist nicht mit speziell sensitiven Daten zu tun hatten. Nach den ersten Iterationen folgte jedoch die Bestätigung der ursprünglichen Annahme, dass diese Berufsgruppen keinen Nutzen und keine Anwendungsfälle für ein hochsicheres Betriebssystem sehen. Danach wurden im Rahmen der zur Verfügung stehenden Möglichkeiten systematisch Benutzer aus Tätigkeitsfeldern im Umgang mit sensitiven Daten rekrutiert.

User Test Settings und Iterationen

Iteration 1 – Swisscom AG, Zürich, 07. September 2018

[vgl. 5.3 Experiment gapfruitOS Simulation]

Setup	Testpersonen (TP)
5 Testpersonen	TP1: Behindertenbetreuerin (PC Kenntnisse: Laie)
1 Testleiter	TP2: User Experience Consultant (Mac Kenntnisse: Anwender)
2 Beobachter	TP3: User Experience Designer (Mac Kenntnisse: Anwender)
1 Screen recording	TP4: Software Entwickler (Mac Kenntnisse: Fortgeschritten)
1 Porträtaufnahme (TP)	TP5: Software Entwickler (PC Kenntnisse: Fortgeschritten)

Iteration 2 – Diverse Standorte, Zürich, diverse Daten

[vgl. 5.4 Experiment Interviews potentielle Anwender]

Setup	Teilnehmer (T)
2 Teilnehmer	T1: Software Entwickler im Bankenumfeld (PC Kenntnisse: Fortgeschritten)
1 Interviewer	T2: Geschäftsführer und Revisionsspezialist Treuhandbüro (PC Kenntnisse: Anwender)
1 Audio recording	

Iteration 3 – Swisscom (Schweiz) AG, Zürich, 19. Oktober 2018

[vgl. 5.5 Experimente Shared Filesystem & Programs]

Setup	Testpersonen (TP)
4 Testpersonen	TP1: User Experience Designer (Mac Kenntnisse: Fortgeschritten) TP2: Software Entwickler (PC Kenntnisse: Fortgeschritten)
1 Testleiter	TP3: Visual Designer (Mac Kenntnisse: Anwender)
2 Beobachter	TP4: Software Entwickler (PC Kenntnisse: Fortgeschritten)
1 Screen recording	
1 Porträtaufnahme (TP)	

Iteration 4 – Zühlke Engineering AG, Schlieren, 30. Oktober 2018

[vgl. 5.5 Experimente Shared Filesystem & Programs]

Setup	Testpersonen (TP)
4 Testpersonen	TP1: Usability Engineering (PC Kenntnisse: Anwender)
1 Testleiter	TP2: Legal Counsel (PC Kenntnisse: Anwender)
2 Beobachter	TP3: Business Solution Manager (PC Kenntnisse: Anwender)
1 Screen recording	TP4: Usability Engineering (PC Kenntnisse: Fortgeschritten)

Iteration 5 – Diverse Standorte, Luzern, 23. November 2018

[vgl. 5.6 Experimente Labeling & Notifications]

Setup	Testpersonen (TP)
5 Testpersonen	TP1: Chief Operating Officer, Personalbüro (PC Kenntnisse: Anwender)
1 Testleiter	TP2: Leiterin Wissensmanagement (PC Kenntnisse: Laie)
2 Beobachter	TP3: IT Teamleader SAP (PC Kenntnisse: Anwender)
1 Screen recording	TP4: Event Management Premiumkunden Kreditkarten (PC Kenntnisse: Laie)
	TP5: Rechtsanwalt, Kanzlei (PC Kenntnisse: Anwender)

Iteration 6 – Zühlke Engineering AG, Schlieren, 26. November 2018

[vgl. 5.6 Experimente Labeling & Notifications]

Setup	Testpersonen (TP)
5 Testpersonen	TP1: Head HR Operations (PC Kenntnisse: Laie)
1 Testleiter	TP2: General Counsel (PC Kenntnisse: Laie)
2 Beobachter	
1 Screen recording	
1 Audio recording	

Iteration 7 – Diverse Standorte, Zürich, 30. November 2018

[vgl. 5.6 Experimente Labeling & Notifications]

Setup	Testpersonen (TP)
3 Testpersonen	TP1: CEO & IT Security Consultant (PC Kenntnisse: Fortgeschritten)
1 Testleiter	TP2: IT Security Consultant (PC Kenntnisse: Fortgeschritten)
1 Beobachter	TP3: Assistant Vice President Bank (PC Kenntnisse: Anwender)
1 Screen recording	
1 Audio recording	

5.2.2 Durchführung der Experimente

Die Experimente, welche Usability Tests beinhalteten, wurden immer nach demselben Schema durchgeführt. Gemäss Iterationsplan des Lean UX Prozesses [vgl. 3 Methodik und Vorgehen] wurden Annahmen definiert, die im Rahmen des Experiments überprüft werden sollten. Danach wurden Testszenarien und die zugehörigen Prototypen für die Usability Tests erstellt. Zur Durchführung des Experiments wurde von den Autoren ein Testleitfaden erstellt. Dieser enthielt neben der Aufgabenstellung auch einen Standard-Fragebogen zur Beurteilung der Usability des getesteten Prototyps sowie weitere kontextspezifische Interviewfragen. Während der abschliessenden Interviews wurden schwer testbare Annahmen auch direkt abgefragt und reale Anwendungsszenarien der einzelnen Teilnehmer erhoben.

Die Usability Tests inklusive Interviews dauerten 45-60 Minuten und wurden von einem Testleiter geführt. Nach Abschluss eines Experiments wurden die einzelnen Fragebogen der Teilnehmer sowie die Audio- und Videoaufnahmen der Usability Tests/Interviews von den Autoren ausgewertet. Aus den gewonnenen Erkenntnissen konnten schliesslich die getroffenen Annahmen validiert oder verworfen und das weitere Vorgehen beschlossen werden.

5.3 Experiment gapfruitOS Simulation

Die Grundidee des Interaktionskonzeptes von gapfruitOS wird mittels verfügbarer Betriebssysteme und Tools simuliert. Dazu wird ein Hostsystem mit der frei verfügbaren Virtualisierungssoftware Virtualbox [29] aufgesetzt. Zwei unterschiedliche Sicherheitskontexte «Internet» und «Work» werden als virtuelle Maschinen mit unterschiedlichen Betriebssystemen konfiguriert. Genau wie beim echten gapfruitOS besitzt jedes Gastsystem in der Simulation ein eigenes, abgetrenntes Dateisystem und eigene Programme. Ein direkter Zugriff auf Dateien oder Programme im jeweils anderen System ist somit nicht möglich. Durch einen geteilten Ordner (Shared Folder) können Daten zwischen der «Internet» und «Work» Zone ausgetauscht werden. Der Benutzer kann nur aus der «Internet» Zone via Browser auf das freie Internet zugreifen. In der «Work» Zone können zwar E-Mails versendet, jedoch keine Webseiten gebrowst oder Dateien heruntergeladen werden.

Erster Prototyp Simulation gapfruitOS

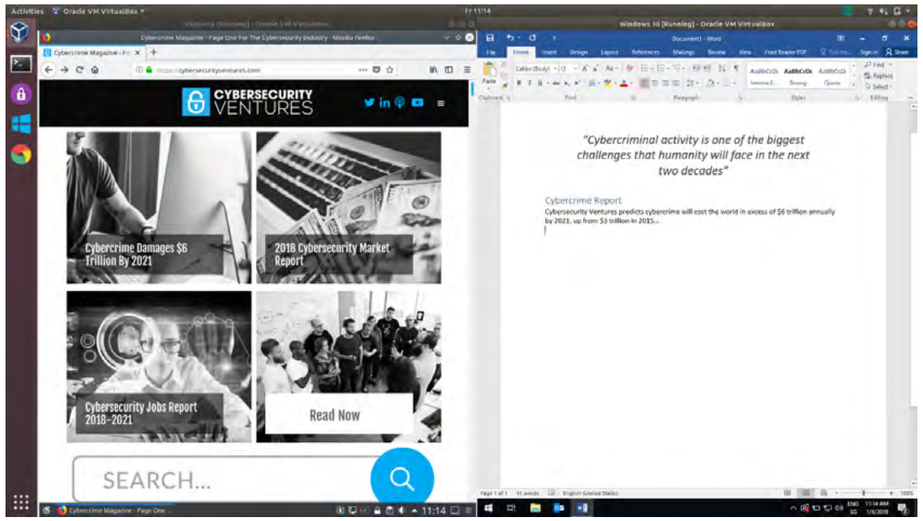


Abbildung 17: Simulation gapfruitOS mit existierenden Tools, «Internet» Zone links, «Work» Zone rechts

[29] «Oracle VM VirtualBox». [Online]. Verfügbar unter: https://www.virtualbox.org/. [Zugegriffen: 15-Jan-2019].

Vor Beginn jedes Usability Tests wurden die beiden virtuellen Maschinen «Internet» und «Work» gestartet und im Split-Screen Modus so auf dem Monitor platziert, dass jede der beiden VMs jeweils die halbe Breite und volle Höhe des Monitors ausnutzt. Der verwendete Testleitfaden mit Testszenario und Fragebogen befindet sich im Anhang [vgl. Anhang 9.8 Leitfaden Experiment gapfruitOS Simulation].

5.3.1 Annahmen

A1 Nicht jede Firma bzw. Berufsgruppe gehört zur potentiellen Benutzergruppe eines hochsicheren Betriebssystems. Menschen die im Rahmen ihrer Arbeitstätigkeit nicht mit sensitiven bzw. als sensitiv wahrgenommenen Daten in Berührung kommen, haben kein Verständnis und keine Toleranz für zusätzliche, sicherheitsrelevante Hürden im Arbeitsablauf.

A2 Mit einer Split-Screen Konfiguration auf einem gewöhnlichen 15‘ Monitor kann der Benutzer nicht vernünftig parallel in zwei unterschiedlichen Sicherheitskontexten (Internet: Web browsen, Work: Dokument erstellen) arbeiten.

A3 Durch die zusätzliche Verschachtelung (Fenster-Management im Hostsystem, Fenster-Management im Gastsystem, VMs erscheinen als Fenster im Host System und besitzen wiederum ein Fenster-Management für die installierten Applikationen) verliert der Benutzer schnell die Übersicht.

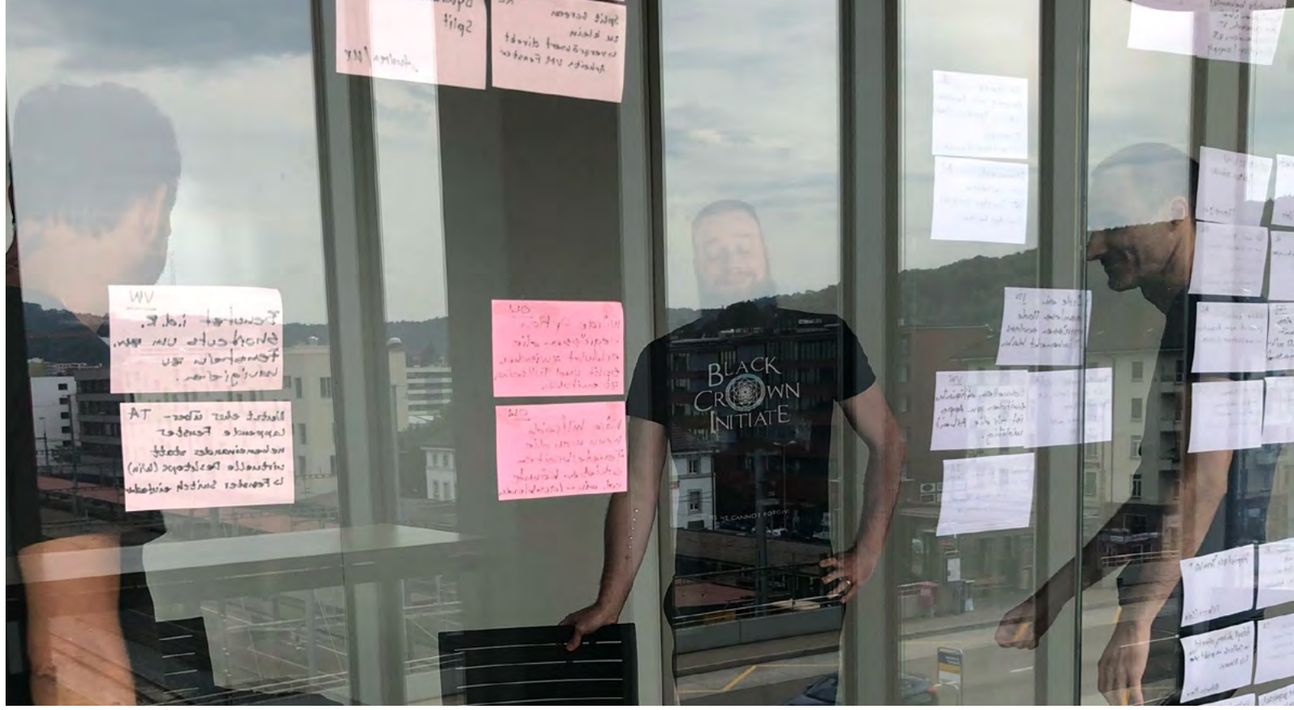
A4 Der Anwender verliert die Übersicht in welchem System bzw. Sicherheitskontext er sich befindet und weiss nicht mehr welche Dateien und Programme ihm jeweils zur Verfügung stehen.

5.3.2 Auswertung und Zusammenfassung der Resultate

Zur Auswertung der Resultate aus dem ersten Experiment wurden mit Hilfe der Videoaufnahmen relevante Aussagen der Probanden analysiert. In einem gemeinsamen Workshop wurden die Aussagen zusammengetragen mittels Affinity Diagramm ausgewertet. Eine vollständige Aufstellung der Resultate inkl. Affinity Diagramm findet sich im Anhang [vgl. Anhang 9.9 Auswertung Experiment gapfruitOS Simulation]. Die wichtigsten Erkenntnisse werden im Folgenden zusammengefasst.

Prototyp und Zonenkonzept von gapfruitOS

- Der permanente Wechsel und Datentransfer zwischen den unterschiedlichen Sicherheitskontexten über einen «Shared Folder» ist zu umständlich und inakzeptabel im Rahmen der Arbeitstätigkeit der befragten Testpersonen.



- Wären die Testteilnehmer gezwungen so zu arbeiten wie im Test simuliert, würden sie sich Umgehungslösungen und Workarounds suchen, um nur in einer einzigen Zone arbeiten zu müssen. Das Primärziel der befragten Personen ist die effektive und effiziente Erledigung ihrer Arbeitsaufgaben.
- Von einem Betriebssystem wird grundsätzlich erwartet, dass Sicherheit transparent gelöst ist. Der gewöhnliche Benutzer will sich nicht mit Sicherheitsfunktionen auseinandersetzten und delegiert die Verantwortung implizit ans System.
- Tendenziell gilt: Je grösser das technische Know-how, desto höher die Bereitschaft zur Risikoverminderung und zur Ergreifung von Gegenmassnahmen.
- Der permanente Split-Screen Modus macht für die Probanden keinen Sinn, da sie keine Anwendungsfälle zur parallelen Arbeit in zwei Sicherheitskontexten sehen. Der 15-Zoll Monitor ist ausserdem zu klein, um sinnvoll im Split-Screen Modus arbeiten zu können.

Umgang mit sensitiven Daten

- Obwohl in der Firma der befragten Personen klassifizierte, nicht für die Öffentlichkeit bestimmte Daten existieren versteht sich keine dieser Personen als Bearbeiter (hoch-)sensibler Daten. Sie verlassen sich auf die Sicherheit der bereits von der Firma getroffenen Massnahmen.

- Die Hälfte der befragten Personen kümmert sich nicht um sensitive Daten und geht gar verantwortungslos mit Bank-Logins und Kreditkartendaten um. Eine Testperson hat ihr Verhalten angepasst, nachdem mehrere ihrer Konten gehackt und von Cyberkriminellen missbraucht wurden.
- Die Probanden vermuten, dass Personen, welche sich in einem spezialisierten Umfeld mit hochsensiblen Daten bewegen, vermutlich eher Verständnis für zusätzliche Arbeitsschritte aufgrund von Sicherheitsmassnahmen aufbringen und den Wert darin erkennen können.

Für die Autoren ergibt sich daher folgendes Fazit aus dem durchgeführten Experiment:

- Anwender, die nicht mit sensiblen Daten zu tun haben oder ihre bearbeiteten Daten selbst nicht als sensibel wahrnehmen, haben kein Verständnis für die spezielle Behandlung des Sicherheitsaspektes und den daraus resultierenden, zusätzlich notwendigen Schritten im Arbeitsprozess.
- Anwender, die mit sensiblen Daten arbeiten oder zumindest bestimmte bearbeitete Daten als schützenswert ansehen, sind eher bereit, für kritische Aktionen einen gewissen Zusatzaufwand in der Bedienung in Kauf zu nehmen. Diese Toleranz gilt jedoch ausschliesslich für diese sensitive Teilmenge der bearbeiteten Daten.

Bei sensitiven Daten wird eine technische Hürde von manchen sogar als hilfreich gesehen, da die Daten so nicht versehentlich behandelt werden und um sich die Sensitivität der Daten im Bewusstsein zu halten.

5.3.3 Validierung der Annahmen und nächste Schritte

Der Split-Screen Modus wird nicht weiterverfolgt, da sich dieser Modus im Experiment negativ auf die Benutzbarkeit ausgewirkt hat und keine der Testpersonen eine Notwendigkeit für den parallelen Betrieb von zwei Sicherheitskontexten sah. Damit verbunden werden momentan auch keine anderen Konzepte zur Fensterverwaltung weiter untersucht. Die grösste Hürde für die Benutzer liegt im Workflow für den Datentransfer zwischen den einzelnen Zonen. Der «Shared Folder» ist umständlich zu bedienen und einschränkend. Hier braucht es ein komfortableres Konzept. Dazu wird die Idee eines konsolidierten Dateisystems auf Host OS Ebene als am erfolgversprechendsten angesehen und weiterverfolgt. Hierbei wird mit den Auftraggebern erst die technische Machbarkeit der Idee abgeklärt. Basierend darauf wird schliesslich ein MVP Prototyp entwickelt und in einem nächsten Experiment getestet.

Weiterhin untersucht werden müssen auch potentielle Benutzergruppen und deren Anwendungsszenarien in ihren täglichen Arbeitsprozessen. Hier bestärkten die Resultate des Experiments die Annahme, dass vor allem Menschen, die im Rahmen ihrer Arbeitstätigkeit mit sehr sensitiven Daten in Berührung kommen einen Mehrwert in einem hochsicheren Betriebssystem sehen. Das Augenmerk bei der Rekrutierung von zukünftigen Testpersonen wird daher insbesondere auf diesem Aspekt ruhen.

Annahmen Tabelle gapfruitOS Simulation

	Annahme	Zutreffend	Weiterverfolgen	Bemerkungen
A1	Spezifische Benutzergruppe vorhanden	Ja	Ja	Akzeptanz & Verständnis bei getesteten Personen nicht vorhanden, weitere Abklärungen notwendig
A2	Split-Screen Modus nicht sinnvoll	Ja	Nein	Störend auf 15’ Monitor, allenfalls optional anbieten, wird nicht weiter untersucht
A3	Problematische Verschachtelung VM & Gastsystem-Fenster	Ja	Nein	Problem existiert im realen gapfruitOS eher nicht und reduziert sich bei Weglassen der Split-Screen Konfiguration, wird nicht weiter untersucht
A4	Verlust der Übersicht der jeweils zur Verfügung stehenden Dateien & Programme	Nein	Ja	Problem in Testszenario schwer nachweisbar, da sehr einfaches Set-up und nur wenig bearbeitete Dateien im Workflow, weitere Abklärungen notwendig

5.4 Experiment Interviews potentielle Anwender

Nach der Durchführung der Benutzertests im Rahmen des ersten Experiments [vgl. 5.3 Experiment gapfruitOS Simulation] bestätigte sich die Vermutung nach einer sehr spezifischen Benutzergruppe ein weiteres Mal. Obschon der erste Prototyp hauptsächlich die Idee hinter dem hochsicheren Betriebssystem, noch ohne jegliche Optimierungen zum Abbau von Hürden in der Bedienung, visualisierte, zeigte sich, dass die meisten Mitarbeitenden in gewöhnlichen Unternehmen weder ein Verständnis für die durch das Produkt zu lösende Problematik noch eine Toleranz für «künstlich» eingeführte Hürden in ihrem Arbeitsprozess haben. Aus diesem Grund wurden parallel zu weiteren Experimenten mit Usability Tests Personen aus dem eigenen Netzwerk für Interviews rekrutiert, die innerhalb ihrer Arbeitstätigkeit bewusst in unterschiedlichen Sicherheitskontexten agieren.

Für die Interviews konnten zu diesem Zeitpunkt zwei Personen gewonnen werden. Die Befragungen wurden als nicht standardisierte Interviews [22] geführt und setzten sich zum Ziel, möglichst konkrete Anwendungsszenarien für einen potentiell gewinnbringenden Einsatz des Produktes zu erheben. Nach einer kurzen Einführung mit Vorstellung des Projektes und Erläuterung des Konzeptes von gapfruitOS wurden die befragten Personen gebeten, ihren Arbeitsprozess und ihre Erfahrungen im Umgang mit unterschiedlichen Arbeitsumgebungen und Sicherheitskontexten genauer zu erläutern. Es sollte vor allem darum gehen, die Arbeitsprozesse und den Umgang mit den unterschiedlichen Umgebungen kennen und verstehen zu lernen.

5.4.1 Annahmen

A1 **Innerhalb von spezialisierten Berufsgruppen bzw. Arbeitsabläufen existieren sinnvolle Anwendungsfälle für ein hochsicheres Betriebssystem. Mitarbeiter von Unternehmen, die ihre Tätigkeit bereits heute in verschiedenen Arbeitsumgebungen durchführen oder bewusst in unterschiedlichen Sicherheitskontexten arbeiten, können durch ein klares Zonenkonzept unterstützt werden.**

A2 **Berufsgattungen, welche oft mit sehr sensitiven Daten arbeiten verstehen den Nutzen eines hochsicheren Betriebssystems und sind bereit bestimmte Hürden im täglichen Arbeitsprozess auf sich zu nehmen.**

5.4.2 Auswertung und Zusammenfassung der Resultate

Die Aussagen und die erhobenen Arbeitsabläufe aus den beiden geführten Interviews konnten von den Autoren direkt in potentielle Kontextszenarien und Benutzergruppen überführt werden. Folgende Berufsgruppen für das zu entwickelnde, hochsichere Betriebssystem wären demnach denkbar:

1. **Benutzergruppe Entwickler auf Systemen mit hochsensiblen Daten**
2. **Treuhänder mit Remote Desktop Arbeitsumgebung**

Eine nähere Beschreibung dieser Berufsgruppen findet sich im Anhang [vgl. Anhang 9.20 Potentielle Berufsgruppen und Nutzungskontext].

[22] C. Hauri und U. Suter, «Interviewtechnik». CAS Requirements Engineering 2016. Rapperswil: HSR Hochschule für Technik Rapperswil..

5.4.3 Validierung der Annahmen und nächste Schritte

Die evaluierten Arbeitsabläufe dieser potentiellen Benutzergruppen wurden von den Autoren in die Annahmen für zukünftige Experimente mit aufgenommen. Die erhobenen Pain Points flossen als Ideen in die weitere Ausgestaltung der interaktiven Prototypen mit ein. Die erhobenen Daten fanden ausserdem Einzug in die Ausarbeitung der Proto-Personas [vgl. 6.4 Proto-Personas im Projekt] für das zu entwickelnde Produkt.

Annahmen Tabelle potentielle Anwender

	Annahme	Zutreffend	Weiterverfolgen	Bemerkungen
A1	Anwendungsfälle bei spezialisierten Berufsgruppen	Ja	Ja	Potentielle Anwendungsfälle gefunden, neue Ideen für Produktfeatures, weitere Erhebungen im Rahmen der Experimente sinnvoll
A2	Nutzen bei Arbeit mit sehr sensitiven Daten	Ja	Ja	Keine Indizien zur Validierung bzw. zum Verwerfen während Interviews gefunden

5.5 Experimente Shared Filesystem & Programs

Wie sich im ersten Experiment gezeigt hat, ist der Datentransfer zwischen den unterschiedlichen Sicherheitskontexten eines der grössten Hindernisse im Umgang mit dem hochsicheren Betriebssystem. Durch die Trennung der verschiedenen Sicherheitskontexte in unterschiedliche Zonen über virtualisierte Gastsysteme ist der Zugriff auf benötigte Dateien oder Programme für den Benutzer komplexer. Da die Gastsysteme völlig voneinander isoliert sind, hat jedes ein eigenes Dateisystem und eigene Programme. Will der Anwender nun auf eine dieser Ressourcen zugreifen, muss er sich jeweils bewusst machen in welcher Zone er sich aktuell befindet und in welcher die benötigte Ressource effektiv liegt. Je nachdem muss er dann in eine andere Zone wechseln oder auch eine Datei zwischen den Zonen transferieren.

Erster Prototyp Dateimanager

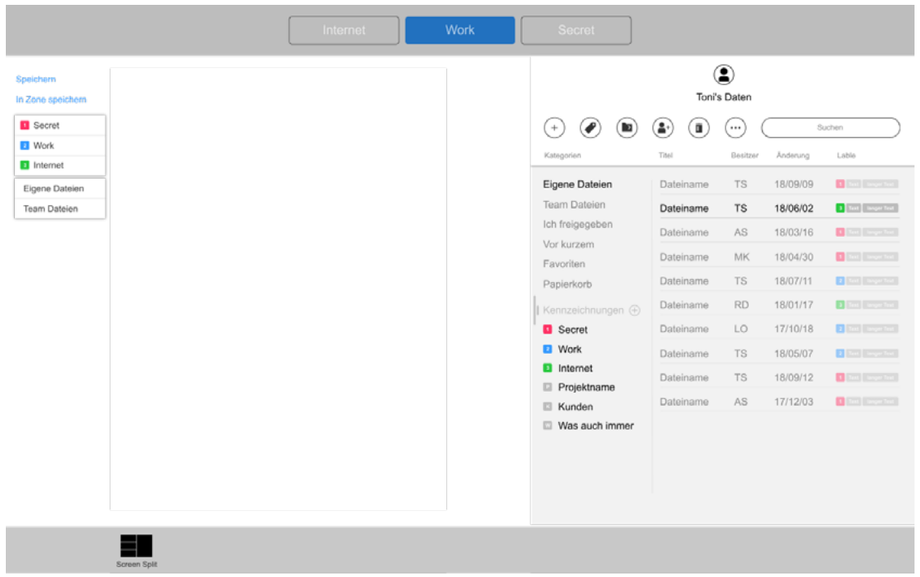


Abbildung 18: MVP Prototyp Variante für einen konsolidierten Dateimanager über alle Zonen

Unter anderem inspiriert durch das direkt im Gastsystem eingebundene Dateisystem des Hosts und die integrierten Programme bei Parallels [vgl. Anhang 9.5 Recherchen und Marktanalyse] entstand bei den Autoren die Idee für einen zonenübergreifenden Dateimanager und einen zonenübergreifenden App Launcher. Der konsolidierte Dateimanager ermöglicht es auf alle Dateien aus allen Zonen von einem einzigen Ort aus zuzugreifen. Dasselbe gilt auch für den zonenübergreifenden App Launcher. Das Öffnen einer Datei oder eines Programmes erfolgt immer nur in der zugeordneten Zone. In einem Workshop mit den Auftraggebern wurde die technische Machbarkeit abgeklärt und die initiale Idee weiter ausgearbeitet. Damit das grundsätzliche Sicherheitsparadigma der «Compartmentalisation» nicht verletzt wird, können diese zonenübergreifenden Komponenten nur auf Hostsystem-Ebene existieren.

Zu den folgenden getroffenen Annahmen wurden zwei Experimente mit unterschiedlichen Entwicklungsständen des MVP Prototyps durchgeführt. In der ersten Runde wurde eine Basisversion getestet, die für die zweite Runde mit den gewonnenen Einsichten verbessert und weiter ausgearbeitet wurde. Zusätzlich wurde die potentielle Benutzergruppe eingeschränkt und somit wurden die Probanden immer spezifischer.

Die verwendeten Testleitfäden mit Testszenarien und Fragebögen befinden sich im Anhang [vgl. Anhang 9.11 Leitfaden Experiment Shared Filesystem] und [vgl. Anhang 9.12 Leitfaden Experiment Shared Programs].

5.5.1 Annahmen

A1 Mit der Zusammenführung der unterschiedlichen Gast-Dateisysteme in einen zonenübergreifenden Dateimanager auf Hostsystem-Ebene werden die Anwender effizienter beim Auffinden ihrer Dateien. Ausserdem wird der notwendige Datentransfer zwischen unterschiedlichen Zonen vereinfacht. Dadurch wird der Benutzer in seinem Arbeitsprozess weniger eingeschränkt und kann komfortabler arbeiten.

A2 Durch das konsolidierte Dateisystem wird das Zonenkonzept für den Benutzer aufgeweicht. Daher müssen die Inhalte aus den unterschiedlich sicheren Zonen explizit ausgezeichnet werden. Der Anwender muss schnell und einfach erkennen können woher Dateien stammen und warum er allenfalls in der aktiven Zone nicht darauf zugreifen kann.

A3 Es muss jederzeit klar ersichtlich sein in welcher Zone sich ein Benutzer befindet, damit er versteht, welche Restriktionen bestehen und auf welche Ressourcen er innerhalb dieser Zone Zugriff hat.

A4 Dateien, die über den zonenübergreifenden Dateimanager geöffnet werden dürfen jeweils nur in der enthaltenden Zone geöffnet werden. Möchte der Anwender eine Datei in einer anderen Zone öffnen, muss er diese zuerst transferieren. Dieselbe Datei kann nur in einer einzigen Zone zur selben Zeit existieren.

A5 Eine zentrale Programmübersicht (App Launcher) analog dem konsolidierten Dateimanager bei der die jeweiligen Programme mit Zonenlabels versehen sind trägt zu einem besseren Verständnis bezüglich deren Verfügbarkeit in den jeweiligen Zonen bei. Werden bei der Programmwahl alle Applikationen aus allen Zonen an einem Ort angezeigt, erleichtert dies dem Benutzer anhand seines zu erledigenden Tasks aus jeder Situation direkt in das gewünschte Programm einzusteigen. Im Gegensatz zur Anzeige nur derjenigen Applikationen aus der jeweiligen Zone verhindert es zusätzliche Arbeitsschritte (Zonen Wechsel → Programm suchen → wenn falsche Zone gewählt, nächste Zone nach Programm absuchen).

A6 Dasselbe Programm kann in mehreren unterschiedlichen Zonen installiert sein. Zum Öffnen des Programmes in der gewünschten Umgebung muss analog zum Dateisystem bei jedem Programm zusätzlich die enthaltende Zone angezeigt werden, damit der Benutzer die gewünschte auswählen kann.

5.5.2 Auswertung und Zusammenfassung der Resultate

Die Rückmeldungen der Probanden, die Beobachtungen aus den Benutzertests sowie die verbesserungswürdigen Bereiche im Prototyp flossen direkt in die Annahmen für die folgenden Experimente und damit in die weitere Ausarbeitung der MVP Prototypen mit ein. Eine vollständige Aufstellung der Resultate findet sich im Anhang [vgl. Anhang 9.13 Auswertung Experimente Shared Filesystem & Programs]. Folgendes sind die wichtigsten Erkenntnisse aus den beiden Experimenten.

Prototyp und Zonenkonzept von gapfruitOS

- Der zonenübergreifende Dateimanager erleichtert den Umgang mit den über die verschiedenen Zonen verteilten Inhalten, da es nur einen «Topf» gibt, der alle Dateien beinhaltet. Dies stellt eine Erleichterung im Vergleich zu den isolierten Dateisystemen der unterschiedlichen Zonen dar.
- Im zonenübergreifenden Dateimanager kann über ein Label die Zonenzugehörigkeit der Datei verändert werden. Durch den Wegfall des dedizierten Transfer Ordners wird der Prozess zum Datentransfer massiv vereinfacht. Die Benutzerführung und die Kennzeichnungen im Prozess sind jedoch noch zu unklar und verwirrend.
- Die farbliche Auszeichnung der einzelnen Zonen ist gut unterscheidbar und intuitiv. Die Visualisierung der Zonenzugehörigkeit von Dateien im konsolidierten Dateimanager über die entsprechende Zonenfarbe ist einfach verständlich und auf einen Blick ersichtlich.
- Die Zonenzuteilung einer Datei wird von den Testteilnehmern gleichzeitig als eine Art Klassifizierung der Datei und damit auch als Leitlinie zum Umgang mit dem entsprechenden Inhalt angesehen. Dies impliziert jedoch einen eins-zu-eins Bezug zwischen der Anzahl Klassifizierungsstufen einer Firma und der Anzahl existierender Zonen. Diese Kopplung ist in der Praxis vermutlich nicht wünschenswert, da in diesem Fall zu viele Zonen existieren würden.
- Aufgrund technischer Rahmenbedingungen existieren Programme genau innerhalb eines Gastsystems. Ist dasselbe Programm auf mehreren Gastsystemen und damit in mehreren Zonen installiert, muss der Anwender beim Starten über den App Launcher zusätzlich die gewünschte Zone wählen. Der konsolidierte App Launcher ist deshalb für die meisten Testteilnehmer zu abstrakt und damit zu undurchsichtig.

Benutzergruppe von gapfruitOS

- Die Mehrheit der Testpersonen aus den beiden Experimenten, so wie vermutlich deren gesamte Berufsgattung, gehört nicht zur Benutzergruppe eines hochsicheren Betriebssystems. Diese Personen sehen ausser einer Erschwerung ihrer Arbeitsprozesse keinen Nutzen im Produkt.
- Die meisten der Probanden vertrauen auf die bestehenden Sicherheitsmassnahmen ihres Unternehmens bzw. der heute genutzten Systeme. Sie sehen keine Notwendigkeit für eine sicherere Lösung. Das Verständnis für die zugrunde liegende Problematik ist nicht gegeben und damit fehlt auch die Akzeptanz für ein derartiges Produkt.
- **Sollten diese Personen gezwungen sein mit einem hochsicheren Betriebssystem zu arbeiten, erwarten sie ein transparentes Zonenhandling vom System, so dass sie als Endbenutzer mit dem Zonenkonzept gar nicht erst in Berührung kommen.**

Neben den Rückmeldungen konnten in den auf die Benutzertests folgenden Interviews weitere Hinweise auf zwei potentielle Benutzergruppen eines hochsicheren Betriebssystems gefunden werden.

1. Benutzergruppe Legal Abteilung
2. Benutzergruppe Sound Producer

Eine nähere Beschreibung dieser Berufsgruppen findet sich im Anhang [vgl. Anhang 9.20 Potentielle Berufsgruppen und Nutzungskontext].

5.5.3 Validierung der Annahmen und nächste Schritte

Der Prozess zum Abspeichern bzw. Transferieren von Daten zwischen den Zonen muss optimiert werden. Die aktuelle Benutzerführung ist zu unklar und verwirrend für die Anwender. Zur Verbesserung sollen einfacher verständliche Kennzeichnungen und Benutzerbenachrichtigungen eingeführt und getestet werden. Mit tiefer Priorität wird ausserdem die Problematik des zonenübergreifenden App Launchers weiter analysiert und auf mögliche Lösungsansätze überprüft.

Weiterhin stellt sich die Frage nach einem sinnvollen Kriterium für die Aufteilung in Zonen. Wie viele Zonen sind sinnvoll und was genau ist der Unterschied zwischen den einzelnen Zonen. Soll nach ausgeführter Tätigkeit, nach Kontext wie privat/geschäftlich/etc. oder nach Klassifizierung der Daten geschnitten werden.

Die gewonnenen Erkenntnisse flossen direkt in die Annahmen für die folgenden Experimente mit ein. Bei der Rekrutierung von Teilnehmern für die nächsten Experimente liegt der Fokus weiterhin auf Berufsgruppen, die den bewussten Umgang mit sensitiven Daten pflegen. Damit versuchten die Autoren weitere reale Anwendungsszenarien zu erheben und potentielle Benutzergruppen zu identifizieren.

Annahmen Tabelle Shared Filesystem & Programs

	Annahme	Zutreffend	Weiterverfolgen	Bemerkungen
A1	Zonenübergreifender Dateimanager hilfreich	Ja	Ja	Von Probanden als einfach bedienbar und verständlich wahrgenommen, Prozess zum Datentransfer noch zu unklar, Konzept wird weiter ausgearbeitet
A2	Auszeichnung Zonenzugehörigkeit von Dateien via Label	Ja	Ja	Als intuitiv und einfach verständlich wahrgenommen, farbige Auszeichnung von Zonen funktioniert gut
A3	Visualisierung aktive Zone notwendig	Ja	Ja	Wichtig und hilfreich für Orientierung, Icons zur Unterscheidung eher verwirrend, Texte und Farben klarer und verständlicher, Konzept wird weiter ausgearbeitet
A4	Dateien in enthaltender Zone öffnen	Ja	Ja	
A5	Zonenübergreifender App Launcher	Nein	Nein	Nicht implizit klar, dass zonenübergreifend Programme angezeigt werden, weitere Ausarbeitung und Tests sinnvoll
A6	Dasselbe Programm kann in mehreren Zonen existieren	Nein	Nein	Von den meisten Teilnehmern nicht wirklich verstanden oder als zu kompliziert empfunden, aus technischer Sicht jedoch notwendig, weitere Ausarbeitung und Tests sinnvoll

5.6 Experimente Labeling & Notifications

Die letzten drei Experimente drehten sich hauptsächlich um die Verbesserung der Benutzerführung beim Transfer von Daten zwischen zwei Zonen. Mittels neu eingeführtem Notification Center und einfach verständlichen Inline-Benachrichtigungen soll der Benutzer klarer geführt und über durchgeführte oder anstehende Aktionen informiert werden. Innerhalb des Experiments werden dem Benutzer während der Abarbeitung der Testszenarien verschiedene Benachrichtigungen zum Arbeitsstand angezeigt und auf die gewünschte Wirkung überprüft.

Vor dem Transfer von Dateien zwischen verschiedenen Zonen kann gapfruitOS gemäss definierten Sicherheitsrichtlinien verschiedene Aktionen oder Prüfungen durchführen. Zum Transfer einer aus dem Internet heruntergeladenen Datei muss bspw. erst eine Virenprüfung durchgeführt werden, bevor diese in eine sichere Umgebung verschoben wird. Im Experiment werden daher verschiedene in den folgenden Annahmen definierte Aktionen beim Transfer zwischen den unterschiedlichen Zonen eingeführt und auf ihre Anwendbarkeit und Sinnhaftigkeit überprüft.

MVP Protoyp aus der achten Iteration mit Dateimanager und Benachrichtigungen

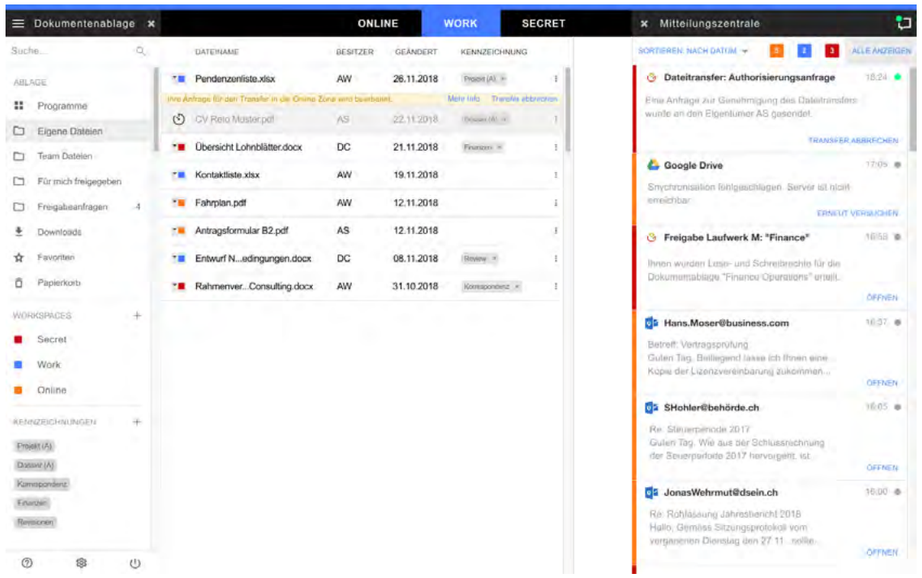


Abbildung 19: Konsolidierter Dateimanager mit offenem Notification Center

Da die Autoren in den vorausgehenden Experimenten die Bestätigung für die ursprüngliche Annahme einer spezifischen Benutzergruppe sahen, wurden die Auswahlkriterien für Testpersonen weiter verschärft. Die vergangenen Iterationen haben gezeigt, dass weitere Tests mit Personen ohne spezialisierte Anwendungsfälle im Umgang mit sensitiven Daten nicht sinnvoll sind. Daher wurden bei der Rekrutierung ausschliesslich Teilnehmer berücksichtigt, welche im Rahmen ihrer Arbeitstätigkeit explizit das Kriterium des Bearbeitens von sensitiven Daten erfüllen.

Die verwendeten Testleitfäden mit Testszenarien und Fragebögen befinden sich im Anhang [vgl. Anhang 9.14 - 9.16].

5.6.1 Annahmen

A1 Um die Kompromittierung einer sicheren Zone zu verhindern, müssen Dateien, die aus der unsicheren in die sichere Zone transferiert werden vom System auf Viren und andere Schädlinge überprüft werden. Erst wenn diese Prüfung erfolgreich ist, also keine Funde zutage liefert, darf eine Datei transferiert werden. Die Prüfung muss implizit im Hintergrund geschehen, so dass der Anwender nach Möglichkeit nichts davon mitkriegt und im Idealfall ohne Verzögerung weiterarbeiten kann. Soll jedoch bspw. eine aus dem Internet heruntergeladene Datei zur weiteren Bearbeitung in die sichere Arbeitszone transferiert werden muss der Prüfprozess dem Benutzer durch eine Fortschrittsanzeige im zonenübergreifenden Dateimanager angezeigt werden.

A2 Wird eine Datei vom Anwender in eine Zone mit hochsensiblen Daten verschoben, erfordert dies die Zustimmung einer verantwortlichen Person. Vor dem effektiven Transfer der Datei wird daher eine Anfrage an diese Person gesendet und die Datei erst nach erfolgter Bewilligung verschoben. Dem Anwender, der den Transfer initiiert muss dieser Genehmigungsprozess durch entsprechende Benachrichtigungen verständlich gemacht werden.

A3 Wird eine Datei von einer sicheren in eine unsichere Zone, bspw. zwecks Versands via E-Mail, transferiert, muss die Datei vom System automatisch verschlüsselt werden. Dies geschieht zur Sicherstellung, dass keine unautorisierten Zugriffe erfolgen bspw. falls die unsichere Zone unbemerkt durch einen Trojaner kompromittiert wurde, das E-Mail-Konto gehackt wurde oder die E-Mail auf einer unverschlüsselten Verbindung abgefangen wird.

A4 Ein konsolidiertes Notification Center auf Ebene Hostsystem hilft dem Benutzer laufende Vorgänge und ausstehende Aktionen beim sicheren Transfer von Dateien zwischen den Zonen an einer zentralen Stelle zu verwalten und schafft Verständnis für den Prozess.

A5 In einem konsolidierten Notification Center müssen ebenfalls Ereignisse aus den Gastsystemen angezeigt werden, damit der Anwender bei der Arbeit in einer Zone keine wichtigen Benachrichtigungen wie bspw. der Eingang einer wichtigen E-Mail aus einer anderen Zone verpasst und zeitnahe darauf reagieren kann.

A6 Zum Transferieren von Dateien wird im konsolidierten Dateimanager ein Label mit der gewünschten Zonenzugehörigkeit gesetzt. Die Änderung dieses Zonen-Labels startet schliesslich den Prozess zum Transfer der Datei. Zur Vereinfachung und Beschleunigung des Transferprozesses für den Benutzer wird ein dediziertes von gewöhnlichen Datei-Labels abgegrenztes Label eingeführt.

A7 Wird der App Launcher optisch klarer vom konsolidierten Dateimanager abgegrenzt werden sich die Anwender schneller zurechtfinden und Programme einfacher starten können. Die Zugehörigkeit von Programmen zu einer Zone müssen ausserdem klarer visualisiert werden.

A8 Beim Abspeichern eines in einer bestimmten Zone erstellten Dokumentes erwartet der Benutzer implizit, dass das Dokument automatisch innerhalb dieser Zone abgelegt wird. Eine erneute Eingabe der Speicher-Zone ist verwirrend und macht keinen Sinn, da das Dokument anschliessend immer noch im Textverarbeitungsprogramm in der ursprünglichen Zone angezeigt wird.

5.6.2 Auswertung und Zusammenfassung der Resultate

Da die letzten drei Experimente innerhalb eines sehr kurzen Zeitraums durchgeführt wurden, sind kleinere Verbesserung zwischen den User Tests jeweils direkt in den MVP Prototyp eingeflossen. Die Annahmen blieben grundsätzlich dieselben. Am Ende wurde eine Auswertung über alle drei Experimente mittels Affinity Diagramm vorgenommen. Eine vollständige Aufstellung der Resultate inkl. Affinity Diagramm findet sich im Anhang [vgl. Anhang 9.17 Auswertung Experimente Notifications]. Im Folgenden sind die wichtigsten Erkenntnisse aus den Experimenten zusammengefasst.

Zonenkonzept von gapfruitOS

- Die exakte Definition einer Zone ist für die meisten Probanden zu unscharf. Für technisch weniger versierte Personen sind die technischen Aspekte undurchschaubar während technischen Experten die exakte Definition und Abgrenzung (Zugriff auf Netzwerke; lokale Laufwerke vs. Netzwerk Shares; vordefinierte, für alle Zonen gleiche Ordnerstruktur vs. freie Ordnerstruktur; etc.) einer Zone fehlte. Dadurch entstanden zwangsweise eigene Interpretationen und Annahmen auf Seite der Testpersonen, die zu Verwirrungen während der Tests führten.

- Die Testpersonen verstanden den Unterschied zwischen den beiden sicheren Zonen «Work» und «Secret» nicht. Diejenigen Personen, welche mit sensiblen Daten arbeiten, bewegen sich im Rahmen ihrer Arbeitstätigkeit entweder in einer sicheren oder einer unsicheren Umgebung. In den allermeisten Fällen existieren daher sinnvollerweise nur zwei Zonen, eine unsichere zum Surfen im Internet und eine sichere zur Erledigung der restlichen Arbeiten. Ein Setup mit drei Zonen (wie es im Prototyp getestet wurde) macht vermutlich nur in Fällen Sinn, wo heutzutage eine Airgap Lösung eingesetzt wird.

- Die Idee hinter dem Zonenkonzept kommt bei Personen, die mit sensitiven Daten arbeiten gut an. Die Zonen bieten einen Rahmen zum Umgang mit den enthaltenen Daten und allenfalls deren Klassifizierung. Sie fördern die Awareness für sensible Daten und die damit verbundenen Gefahren. Für diese Personengruppe hat das Produkt vor allem Potential bei der Übernahme von mühsam manuell ausgeführten Arbeiten in Bezug auf das Handling sensitiver Daten, die aktuell in der Eigenverantwortung von Mitarbeitern liegen.

Datentransfer zwischen Zonen

- Der Prozess zum Transferieren von Daten über das Setzen eines dedizierten Zonenlabels ist einfach zu bewerkstelligen, gut verständlich und intuitiv. In einer Variante der getesteten Prototypen wurden Zonenlabels und persönliche, frei definierbare Labels kombiniert. Diese Kombination verwirrte die Testpersonen und wird wieder verworfen. Eine Funktion zum gleichzeitigen Transfer mehrerer Dateien fehlt.

- Ein Genehmigungsprozess beim Transferieren von Daten von einer unsicheren in eine sichere Zone ist kaum praktikabel, da der Administrationsaufwand für die autorisierende Person potentiell zu gross wird. In spezialisierten Fällen kann ein Genehmigungsprozess in die Gegenrichtung (sicher → unsicher) Sinn machen.

Existiert in einer Bank bspw. eine Zone, in welcher die Mitarbeiter Zugriff auf sensitive Finanzdaten haben, möchte der Arbeitgeber nicht, dass Mitarbeiter diese Daten frei aus dieser sicheren Zone kopieren und bspw. im Internet oder via E-Mail an Dritte weitergeben können.

- Eine Möglichkeit zum sicheren Teilen von Dateien zwischen sicheren Zonen verschiedener Mitarbeiter eines Unternehmens. Diese Funktionalität würde den Anwendern Zonentransfers und den Austausch von Dateien via unsicheres E-Mailing ersparen und so ihre Abläufe beschleunigen.

- Damit Benutzer in der Realität genügend flexibel arbeiten können, ist neben dem Verschieben von Dateien beim Datentransfer auch ein Kopieren zwischen den Zonen notwendig.

- Eine automatische Verschlüsselung von Daten beim Transfer von einer sicheren in eine unsichere Zone ist nur in symmetrisch aufgesetzten Systemen mit exakt derselben Zonenkonfiguration bei allen Beteiligten sinnvoll. Grundsätzlich macht die Verschlüsselung von E-Mails bzw. der angehängten Dateien Sinn, das bedeutet jedoch nicht, dass Dateien automatisch beim Zonenübergang verschlüsselt werden sollten.

Benachrichtigungen

- Ein Notification Center auf Ebene Hostsystem ist hilfreich beim Verständnis der ungewohnten Abläufe im neuen Produkt. Der im Prototyp simulierte Genehmigungsprozess beim Datentransfer bspw. kann so jedem verständlich gemacht werden. Die Problematik des Verständnisses warum diese Abläufe überhaupt notwendig sind, kann hingegen nicht über Benachrichtigungen gelöst werden.

- Benachrichtigungen müssen sparsam eingesetzt werden und für den Benutzer leicht verständliche, mit konkreten Handlungsoptionen angereicherte Inhalte transportieren. Unerwartete oder kryptische Benachrichtigungen werden im Arbeitsfluss oft zur störenden Nebensache und mit den Worten «das schaue ich mir später an» zur Seite geschoben.

Benutzergruppe von gapfruitOS

- Je sensitiver die von den Testpersonen bearbeiteten Daten sind, desto höher ist auch die Sensibilisierung dieser Personen auf die damit verbundenen Gefahren wie bspw. Cyberkriminalität. In vielen Fällen existiert in den entsprechenden Unternehmen bereits ein explizites Regelwerk zum Umgang mit diesen Daten. Es

existieren ausserdem automatisierte Mechanismen zur Durchsetzung bestimmter Massnahmen wie bspw. Kontrolle von E-Mails. Personen aus dieser Gruppe haben eine höhere Toleranz für und damit grössere Zustimmung zum entwickelten Produkt.

- Aus Security Perspektive wird das Konzept von den meisten Personen, die sich als Bearbeiter sensitiver Daten sehen, als sinnvoll empfunden. Die Praktikabilität im täglichen Einsatz und die Arbeitsgeschwindigkeit zur Erledigung der eigenen Aufgaben werden jedoch angezweifelt. Vor allem der (tendenziell oftmals) notwendige Zonentransfer erscheint zeitraubend und wird im Vergleich zu einem gewöhnlichen Betriebssystem als zu mühsam gewertet.
- Der Aufwand zur Einführung des Produktes wird als erheblich angesehen. Dabei wird angezweifelt wie viele Unternehmen sich so etwas antun würden, da bereits andere einfacher einzuführen und trotzdem relativ sichere Lösungen auf dem Markt sind.

Annahmen Tabelle Labeling & Notifications

	Annahme	Zutreffend	Weiterverfolgen	Bemerkungen
A.1	Anzeige Prüfprozess von Dateien bei Transfer Zone unsicher -> sicher	Ja	Ja	Information sinnvoll, wird aber von Testpersonen oft übersehen bzw. ignoriert, Sensibilisierung muss stattfinden
A.2	Genehmigungsprozess Vorgesetzter bei Transfer Zone sicher -> hochsensitiv	Nein	Ja	Bedürfnis existiert nur für sehr spezifischen Arbeitsprozess, verlangsamt ansonsten Prozess und führt zu unverhältnismässigem Admin Aufwand, Richtung eher umgekehrt Genehmigung für Transfer hochsensitiv -> unsicher
A.3	Automatische Verschlüsselung bei Transfer Zone sicher -> unsicher	Nein	Nein	Auto-Verschlüsselung macht nur in symmetrisch aufgesetzten Umgebungen Sinn, Anwendung evtl. für militärische Zwecke interessant
A.4	Notification Center auf Ebene Hostsystem	Ja	Ja	Hilfreich zur Anzeige Status von Transferoperationen und ähnliches, nur ausgewählte Benachrichtigungen und nicht überfluten
A.5	Konsolidierte Anzeige von Hostsystem und Gastsystem Benachrichtigungen	Nein	Ja	Unterschiedliche Meinungen bei Testpersonen, kein eindeutiges Pro oder Kontra, weitere Untersuchungen notwendig
A.6	Separates Zonenlabel für Transfer verwenden	Ja	Ja	Einfacher und verständlicher für Benutzerführung, führt zu Missverständnissen wenn gekoppelt mit anderen, persönlichen Labels
A.7	Klare Trennung App Launcher und Dateimanager	Ja	Ja	Verbesserung gegenüber vorherigen Experimenten, Problematik zu Verständnis welches Programm zu welcher Zone gehört besteht aber immer noch
A.8	Automatisches Speichern von Dateien in Zone wo erzeugt bzw. heruntergeladen	Bedingt	Ja	Aufgrund sicherheitskritischer Restriktionen vorgegeben, erscheint den meisten Teilnehmern logisch, mühsam erst herunterladen und dann transferieren

Bei den durchgeführten Experimenten konnten vier zusätzliche Berufsgruppen mit möglichen Anwendungsfällen für gapfruitOS identifiziert werden. Es handelt sich dabei um folgende:

1. **Benutzergruppe Human Resources**
2. **Benutzergruppe Anwalt**

3. **Benutzergruppe Bankangestellter**

4. **Benutzergruppe Mitarbeiter Kreditkartenunternehmen**

Eine nähere Beschreibung dieser Berufsgruppen findet sich im Anhang [vgl. Anhang 9.20 Potentielle Berufsgruppen und Nutzungskontext].

5.6.3 Nächste Schritte

Nach der Auswertung der letzten drei Experimente im Rahmen dieser Masterarbeit, werden die Erkenntnisse aus den durchgeführten Iterationen, die erarbeiteten Designansätze zu einem möglichen Interaktionskonzept sowie der Projektstand im Januar 2019 in Kapitel 6 Resultate und Bewertung festgehalten.

5.7 Eingesetzte Methoden während der Experimente

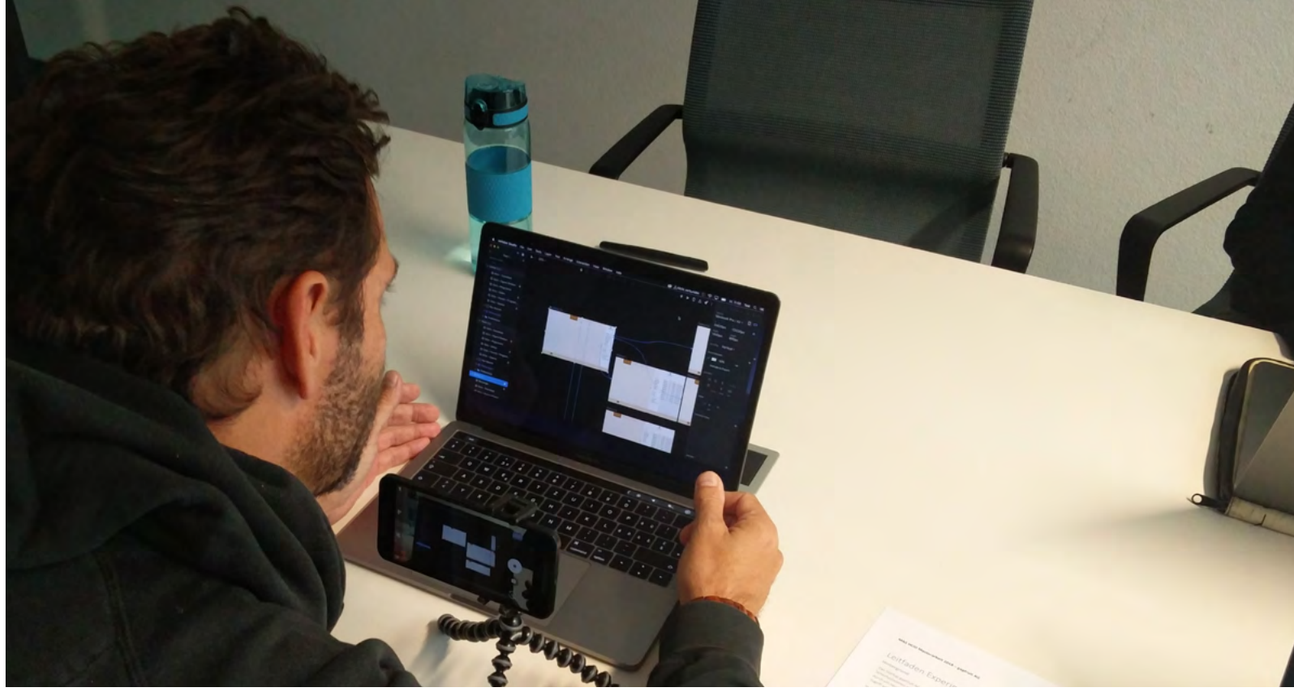
5.7.1 Collaborative Design

Zur Generierung von Ideen und zur Ausarbeitung verschiedener Lösungsansätze wurde die Methode des Collaborative Designs [30] aus dem Lean UX Prozess eingesetzt. Dabei wurden während des gesamten Projektes bei physischen Treffen Ideen für Interaktionskonzepte und Features gemeinsam am Whiteboard skizziert und anschliessend diskutiert. Diese Ideen flossen wiederum in die Prototypen der unterschiedlichen Teammitglieder mit ein.

Scribbles aus den Workshops Collaborative Design

Abbildung 20: Unterschiedliche Ansätze zum Umsetzen in der Prototyping-Phase

[30] J. Gothelf und J. Seiden, Lean UX - Applying Lean Principles to Improve User Experience, 16. Aufl. O'Reilly Media.



Insbesondere für die Ideation im Rahmen der Experimente «Shared Filesystem & Programs» wurden eine Art Remote Design Studio Runden durchgeführt. Alle Teammitglieder erstellten unabhängig voneinander erste Wire Frames mit ihren Ideen in digitaler Form. Bei gegenseitigen Vorstellungsrunden im Rahmen von Online Meetings wurden die Ideen schliesslich geteilt und diskutiert. Mit neuen Anregungen und Inspiration aus dem gemeinsamen Austausch iterierten die einzelnen Projektmitglieder erneut über ihren Prototyp und kamen so zu ausgereifteren Lösungsansätzen.

Reflexion zur Methode

Collaborative Design ist eine ausserordentlich effiziente und kreativitätsfördernde Methode. Die gemeinsame Diskussion über verschiedene Lösungsansätze führt praktisch immer zu neuen Ideen und unerwarteten Kombinationen von verschiedenen Aspekten aus verschiedenen Ansätzen. Am besten eignet sich dazu ein grosses Whiteboard. So können alle Ideen ohne Skrupel skizziert, verändert oder auch einfach wieder gelöscht werden. Die auf diese Weise entstandenen Lösungsansätze sind denjenigen, die im stillen Kämmerlein produziert werden, gemäss den Erfahrungen der Autoren meist überlegen. Effizient und kreativitätsfördernd ist auch der Prozess der individuellen Ideengenerierung, gemeinsamer Vorstellung und anschliessender Verfeinerung (divergieren – präsentieren – weiterentwickeln – konvergieren).

Aufgrund der geographischen Distanz der Teammitglieder und der damit eingehenden eingeschränkten Anzahl gemeinsamer Arbeitstage sind viele Ideen direkt in inVision Studio bzw. Adobe XD umgesetzt worden. Im Gegensatz zur Whiteboard Variante ist dies natürlich weniger effizient und das Divergieren fällt schwerer, da der Aufwand grösser ist. Auch das Konvergieren und Konsolidieren der verschiedenen Designideen über Online Meetings hat eher schlecht funktioniert. Reale Treffen sind in jedem Fall effizienter, Missverständnisse lassen sich in Person einfach besser erkennen und bspw. mit einer Skizze ausräumen.

5.7.2 Prototyping und Usability Testing

Während der meisten Experimente wurden Usability Tests mit den Teilnehmern durchgeführt. Hierzu erarbeiteten die Autoren jeweils ein Testszenario mit mehreren Teilaufgaben. Parallel dazu wurden interaktive MVP Prototypen erstellt, um die Szenarien mit den Testpersonen durchspielen zu können. Grundsätzlich sollte den Probanden die Arbeitsweise in verschiedenen Sicherheitszonen und den dadurch notwendigen Transfer von Dokumenten zwischen den Zonen mittels Prototypen veranschaulicht werden. Dabei wurde in erster Linie Benutzerforschung betrieben um einerseits das Verständnis der zugrunde liegenden Problematik sowie die Anwendbarkeit dieses Zonenkonzepts auf reale Arbeitsabläufe verschiedener Berufsgruppen abzufragen. Nebenbei wurden zusätzlich verschiedene Ideen und Ansätze für ein mögliches Interaktionskonzept auf ihre Benutzbarkeit hin getestet.

Reflexion zur Methode

Eine grosse Herausforderung bei den Benutzertests im Rahmen der Experimente waren die stark eingeschränkten Freiheitsgrade in den erstellten, interaktiven MVP Prototypen. Ein Dateimanager oder App Launcher eines realen Betriebssystems bietet eine schier unüberblickbare Vielzahl von Interaktionsmöglichkeiten. Im täglichen Umgang mit einem Betriebssystem nutzt der Anwender diese mit einer Leichtigkeit und in einer Breite, die mit den gängigen Prototyping-Tools in einem interaktiven Prototyp niemals abgedeckt werden kann. Vermutlich aufgrund der vielen interaktiv anmutenden Elemente und den Gewohnheiten im Umgang mit dem eigenen Computer hatten viele der Probanden eine hohe Erwartung an die Fidelity des Prototyps. Viele klickten deshalb erst einmal munter drauf los und erwarteten vom Prototyp die entsprechende Reaktion für Interaktionen wie Selektion von Dokumenten, Scrollen, Kontext Menüs, etc.

Da nur ein schmaler Pfad durch den Prototyp funktionsfähig umgesetzt werden konnte und viele angezeigte Bedienelemente wenig oder keine Interaktionsmöglichkeiten boten, waren die meisten Teilnehmer irritiert und oftmals bereits von Beginn an verunsichert. Als Konsequenz daraus entstanden nur sehr schmale Testszenarien und es war schwer möglich, den Testpersonen ein richtiges Gefühl für die Funktionsweise des Systems zu vermitteln. Diese Hindernisse liessen sich durch eine sorgfältige Einführung und Erläuterung der Sachlage etwas abschwächen. Rückblickend wäre vermutlich bei der Einführung eine initiale Bedienung des Prototyps durch den Testleiter vernünftig gewesen. Der Proband hätte dann nach entsprechender Aufforderung erst einmal nur erläutert, was er auf dem Bildschirm sieht und wie er das Gesehene interpretiert. Erst nach dieser Phase wäre die Bedienung dann zwecks Durchführung der konkreten Aufgaben an den Probanden übergeben worden.

Eine weitere Schwierigkeit war die Rekrutierung der richtigen Teilnehmer für die Experimente. Da von den Auftraggebern aus keine konkrete Benutzergruppe bekannt war bzw. explizit alle mit dem Produkt adressiert werden sollten, wurde viel Test-Zeit mit Personen verbraucht, die nicht zur potentiellen Benutzergruppe eines derartigen Systems gehören. Daher konnten diese Personen auch keinen hilfreichen Input zur Ausarbeitung von konkreten Nutzungsszenarien und einem darauf basierenden Interaktionskonzept liefern. Durch die fehlende Einschränkung der Zielgruppe waren die Autoren gezwungen, ihre initiale Annahme einer sehr spezifischen Zielgruppe empirisch zu validieren, aufbauend darauf den Rekrutierungsprozess auf die neuen Erkenntnisse anzupassen und auf eine bestimmte Personengruppe einzuschränken. Aufgrund beschränkter zeitlicher Ressourcen und des

fehlenden Netzwerks in gewissen, potentiell relevanten Berufsgruppen wie bspw. Mitarbeiter von Atomkraftwerken oder anderen heiklen Infrastrukturbetrieben war es den Autoren dann auch nicht möglich, die gewünschte Breite zu erreichen um anschliessend einen sinnvollen und relevanten Satz von Personas zu definieren.

5.7.3 Standardfragebogen

Nach der Durchführung eines Benutzertests wurde grundsätzlich ein Standardfragebogen zur Bewertung der Usability des Prototyps eingesetzt. Dieser beinhaltete sowohl skalierte als auch offene Fragen [vgl. Anhang 9.11, 9.12, 9.16, 9.17] zur Erläuterung positiver und negativer Aspekte des Prototyps sowie zum Anbringen von Verbesserungsvorschlägen.

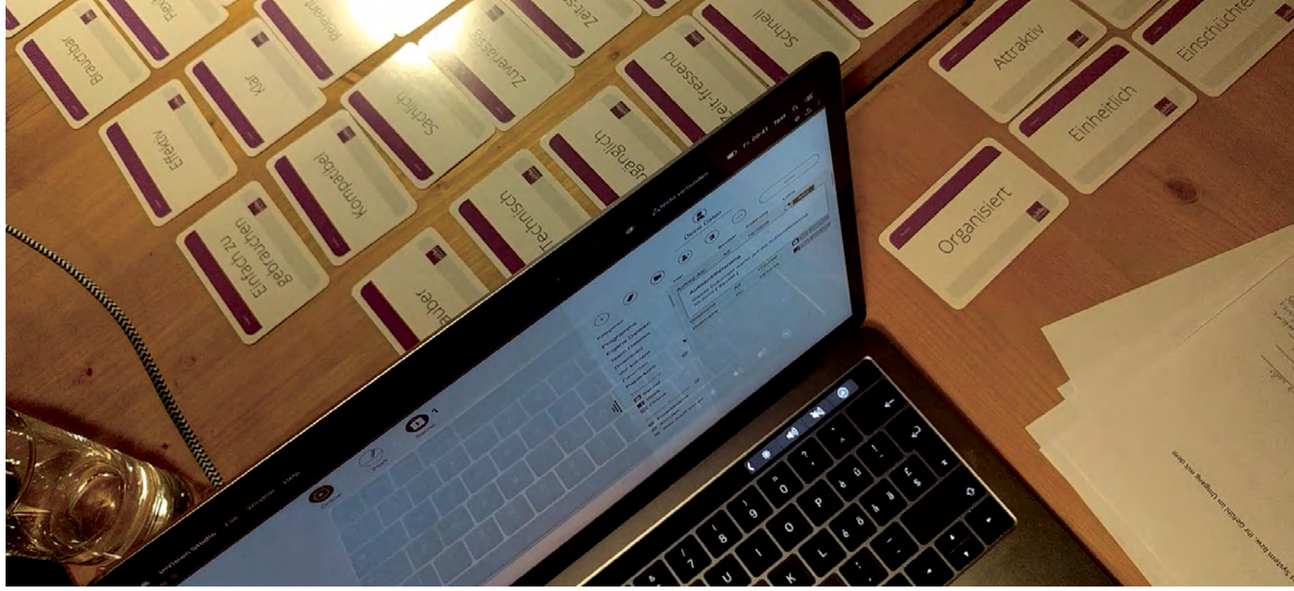
Reflexion der Methode

Der Standardfragebogen setzte einen einfachen aber konsequent gleichbleibenden Rahmen für das den Benutzertest abschliessende Interview. Auf diese Weise konnten strukturierte Daten erhoben und später einfacher ausgewertet werden. Die skalierten Fragen brachten im vorliegenden Projekt keinen wirklichen Mehrwert, da die Benutzer und ihr Verständnis der Problemstellung zu unterschiedlich waren. Für diejenigen Testpersonen, die bei ihrer Arbeitstätigkeit nicht bewusst sensitive Daten bearbeiten war das Zonenkonzept derart absurd, dass sie die notwendigen Interaktionen im Prototyp nicht nachvollziehen konnten. Auch die subjektive Wahrnehmung der Usability war bei den getesteten Berufsgruppen zu unterschiedlich, um vergleichbare Resultate zu produzieren. Die offenen Fragen hingegen leisteten wertvolle Hinweise auf den agierenden Benutzertyp sowie konkrete Hinweise auf die unterschiedlichen positiven und negativen Aspekte des Prototyps. Die strukturierten Antworten halfen den Autoren ausserdem bei der Auswertung der Testresultate.

5.7.4 Emotional Response Cards

Joey Benedeck und Trish Miner stellten 2002 mit ihren «Product Reaction Cards» [31] eine Methode vor, um die Begehrtheit (Desirability) von Produkten zu evaluieren. Die Idee dahinter war, die emotionale Antwort auf die Erfahrung im Umgang mit einem Produkt zu messen. Die «Product Reaction Cards» bestehen aus einem Satz von 118 physischen Karten mit verschiedenen Worten die Produktcharakteristiken beschreiben. Nach einem durchgeführten Usability Test wird die

[31] J. Benedek und T. Miner, «Measuring Desirability: New methods for evaluating desirability in a usability lab setting»..



Testperson gebeten, aus dem Kartensatz die fünf Worte auszuwählen, welche das Produkt am besten beschreiben [32].

Emotional Response Cards sind eine Abwandlung der oben beschriebenen Product Reaction Cards. Dabei wurden die ursprünglichen 118 beschreibenden Wörter auf 50 Ausdrücke reduziert, die jeweils Gegenteile sind oder gegenteilige Charakteristiken beschreiben, ähnlich dem Bipolar Emotional Response Test [33] [34] . Die Methode kann sehr einfach bspw. nach einem Usability Test eingesetzt werden und funktioniert gemäss folgendem Ablauf:

1. Kartensatz ungeordnet vor Probanden auslegen
2. Proband bitten diejenigen Worte zu wählen, welche das System bzw. das Gefühl im Umgang mit dem System am besten beschreiben
3. Die ausgewählten Worte vom Proband priorisieren und die Top 5 auswählen lassen
4. Durch den Probanden erklären lassen, warum genau diese Worte gewählt wurden

[32] «Using the Microsoft Desirability Toolkit to Test Visual Appeal». [Online]. Verfügbar unter: https://www.nngroup.com/articles/microsoft-desirability-toolkit/. [Zugegriffen: 17-Jan-2019]..

[33] «Emotional response cards: a simple user research tool / nForm / Blog». [Online]. Verfügbar unter: https://web.archive.org/web/20120531231540/http://nform.com/blog/2012/05/emotional-response-cards-simple-user-research-tool. [Zugegriffen: 17-Jan-2019].

[34] «Getting all emotional with BERT», UXM, 30-Juni-2010.

Während eines Experiments [vgl. Anhang 9.14 Leitfaden Experiment Notifications 1] wurde nach dem Benutzertest anstelle des Standardfragebogens die Methode der Emotional Response Cards angewendet. Die Teilnehmer wurden unmittelbar nach dem Test zu einem Tisch mit dem ausgelegten Kartensatz geführt und gebeten die entsprechenden Karten auszuwählen, welche ihre Emotionen und Eindrücke bei der Arbeit mit dem Prototyp am besten beschreiben. Dabei sollten die Probanden jeweils direkt während des Auswählens erläutern, warum sie gerade diese Karte gezogen hatten.

Reflexion zur Methode

Beim Abfragen der positiven und negativen Aspekte eines Prototyps mittels Standardfragebogen fällt es einigen Personen schwer, ihre Erlebnisse zu formulieren und in einen Kontext mit dem getesteten Produkt zu stellen. Die Karten mit den vordefinierten Worten helfen den Testpersonen konkrete Gefühle im Zusammenhang mit dem Benutzererlebnis während des Tests zu verbalisieren. Beim Durchgehen der ausgelegten Antwortkarten erinnert sich die Testperson unmittelbar an aufgetretene Emotionen zurück und kann diese einfacher zum Auslöser, einer bestimmten Situation oder eines bestimmten Eindrucks während des Tests, zurückverfolgen.

Die Methode ist leichtgewichtig, einfach einsetzbar und hat sehr gut funktioniert in der Praxis. Den meisten Probanden fiel es leicht Karten auszuwählen und eine Begründung für diese Wahl zu formulieren. Die Ausdrücke auf den gewählten Karten lenkten das Gespräch nicht nur über die verschiedenen positiven und negativen Aspekte des getesteten Prototyps sondern halfen auch den Benutzer und sein mentales Modell kennenzulernen. Tendenziell konnte über die Response Cards in der abschliessenden Diskussion ein breiteres Themenfeld abgedeckt und fundiertere Rückmeldungen der Testpersonen erhoben werden als mit dem in anderen Experimenten verwendeten Standardfragebogen.

5.7.5 Proto-Persona vs. Konventionelle (Design) Persona nach Cooper

In seinem Buch «The Inmates are Running the Asylum» [35] beschreibt Cooper Design Persona, die den Fokus auf Benutzerziele, aktuelles Verhalten, Schwierigkeiten und Herausforderungen legen. Design Personas basieren auf Daten aus Umfragen, Interviews, Fokusgruppen und intensiver Feldforschung und realen Menschen. Aus diesen Daten wird eine Hypothese über den Benutzer erstellt. Personas erzählen eine Geschichte und beschreiben warum Leute tun was sie tun. Sie helfen allen im Design- und Produktentwicklungsprozess involvierten Personen den Endbenutzer zu verstehen, sich mit ihm zu identifizieren und ihn immer im Kopf zu behalten.

Diese Art von Personas ist gut geeignet um Forschungseinsichten und Benutzerziele zu kommunizieren, bestimmte Benutzertypen zu verstehen und sich auf diese zu fokussieren. Sie helfen ein Produkt zu definieren und verhindern gleichzeitig die selbstreferenzielle Einflussnahme und das zurecht biegen der Benutzer. Derartige Persona-Evaluationen sind in der Regel aber zeitaufwendig und teuer.

Proto-Persona

Proto-Persona (auch provisorische Persona, Ad-Hoc Persona), basieren auf den Grundsätzen der konventionellen (Design) Personas. Sie werden dann eingesetzt, wenn wenig Zeit vorhanden, oder die Finanzierung nicht gewährleistet ist, um forschungsbasierte Personas erstellen zu können. Anstelle einer langen und kostenintensiven Research Phase starten Proto-Persona mit einer gut überlegten, erfahrungsbasierten Annahme. Sie sind die zum aktuellen Zeitpunkt bestmögliche Vermutung über die Benutzer und die Art der Benutzung eines Produktes. Proto-Persona werden im Verlauf des Projektes mit den neuen Erkenntnissen aus der fortlaufenden Benutzerforschung validiert oder verworfen beziehungsweise angepasst.

Daraus ergeben sich zwei grosse Vorteile:

1. **Die initiale Definition erfolgt sehr schnell**
2. **Ein iteratives Vorgehen wird forciert**

Im Lean UX Prozess beginnt alles bei einer Annahme, welche im Verlauf von Experimenten überprüft wird. So werden auch zur Benutzergruppe Annahmen getroffen und in Form so genannter Proto-Persona ausformuliert. Eine Proto-Persona beschreibt dabei bestimmte Attribute (Verhaltensbezogene und demografische Informationen, Pain Points und Bedürfnisse, mögliche Lösungsansätze) einer angenommenen Benutzergruppe und wird im Verlauf der durchgeführten Experimente an die effektiv erhobenen Benutzermerkmale angepasst oder auch verworfen. Das Ziel dabei ist, die Proto-Persona solange zu schärfen, bis sie eine real existierende und für das Produkt relevante Benutzergruppe abbildet. Die Methode wird in Kapitel 6.4 Proto-Personas im Projekt näher erläutert und die Anwendung im Kontext des Projektes dokumentiert.

[35] A. Cooper, The Inmates Are Running The Asylum, 1. Aufl. Sams - Pearson Education, 1999.

5.7.6 A/B Testing

A/B Testing ist eine Methode um zwei oder mehr relativ ähnliche Konzepte gegeneinander zu testen um herauszufinden, welche Variante das erwünschte Ziel effektiver erreicht [30]. Lean UX nutzt diese Technik, um die Gültigkeit von unterschiedlichen Design-Hypothesen zu überprüfen. Im Verlauf der Experimente wurde die Technik dazu eingesetzt, zwei leicht unterschiedliche Ansätze zum Transfer von Dateien zwischen Zonen, sowie zwei Varianten zum Wechseln der aktiven Zone gegeneinander zu testen [vgl. 6.1 - 6.2]. Das Szenario für den Benutzertest enthielt dazu zwei Teilaufgaben, welche jeweils mit einer Variante des Prototyps durchgespielt wurden. Somit konnten die Probanden die beiden unterschiedlichen Konzepte zum Zonenwechsel und Datentransfer direkt vergleichen und bewerten. Durch die entsprechenden Rückmeldungen nach den Tests war es den Autoren schliesslich möglich, die besseren Lösungsansätze zu bestimmen [vgl. 6 Resultate und Bewertungen].

Reflexion der Methode

Beim klassischen A/B Testing wird der einen Hälfte der Testgruppe Variante A und der anderen Variante B eines Designs vorgesetzt. Dabei wird ein quantitativ messbares Kriterium definiert, welches unmittelbar zwischen den Varianten verglichen werden kann. Dieser so genannte Key Performance Indicator kann bspw. die Anzahl Benutzer, welche einer Call-To-Action auf einer Webseite folgen sein. Somit kann A/B Testing im klassischen Sinne gemäss Jakob Nielsen nur für Projekte verwendet werden, die ein klares, entscheidendes Ziel haben, nämlich einen einzigen Key Performance Indicator [36]. Bei vielen Produkten existiert jedoch nicht nur ein ultimatives Ziel, das so einfach messbar ist. Um ein statistisch relevantes Resultat zu erhalten, muss ausserdem die Testgruppe genügend gross sein. In seiner Einordnung der Methode konstatiert Nielsen schliesslich, dass A/B Testing nie als erste oder einzige Methode zur Verbesserung einer Problemstellung eingesetzt werden sollte. Qualitative Beobachtungen sind schneller und generieren tiefere Erkenntnisse.

[30] J. Gothelf und J. Seiden, Lean UX - Applying Lean Principles to Improve User Experience, 16. Aufl. O'Reilly Media

[36] Putting A/B Testing in Its Place», Nielsen Norman Group. [Online]. Verfügbar unter: https://www.nngroup.com/articles/putting-ab-testing-in-its-place/. [Zugegriffen: 23-Jan-2019].

Da einerseits die Grösse der Testgruppe keine statistisch relevante Auswertung zuliess und andererseits das komplexe Konzept des Systems sowie der Stand des MVP Prototyps kein quantitativ messbares Kriterium zur eindeutigen Bestimmung der besseren Lösung zuliessen, waren die Autoren auf qualitatives Feedback der Testteilnehmer angewiesen. Dazu mussten jedoch die beiden Varianten des Prototyps im Rahmen eines Experiments in einen Kontext gestellt werden. Dieser direkte Vergleich ermöglichte es den Probanden, die in den meisten Fällen noch nie etwas von einem derartigen Zonenkonzept und der zugrunde liegenden Problematik gehört hatten, überhaupt erst die Designvarianten zu bewerten. Durch das so gewonnene qualitative Feedback konnten schliesslich unterschiedliche Designvarianten bewertet und wo sinnvoll weiter ausgearbeitet werden.

5.7.7 Affinity Diagram

Zu Beginn und zum Ende der Experimente wurden die Resultate aus den Experimenten mittels Affinity Diagram vertieft ausgewertet. Das erste Experiment [vgl. 5.3 Experiment gapfruitOS Simulation] sollte eine Baseline zur Entwicklung von Designhypothesen für die folgenden Experimente bieten. Mit den Rückmeldungen aus den letzten drei Experimenten [vgl. 5.6 Experimente Labeling & Notifications] wurde dann

eine erneute Bestandsaufnahme in Form eines Affinity Diagramms durchgeführt. Diese diente als Grundlage für die zum Abschluss der Arbeit beschriebenen Erkenntnisse [vgl. 6 Resultate und Bewertung].

Reflexion zur Methode

Affinity Diagram ist eine Art Allzweckwaffe zur Auswertung grosser Mengen von Sprachdaten und funktioniert hervorragend zur Identifikation zusammengehöriger Informationseinheiten. Die gesammelten Erkenntnisse konnten jedoch nicht direkt nach den Benutzertests durchgeführt werden, da die Anzahl der Testpersonen pro Tag zu hoch oder die Fahrzeit zwischen den einzelnen Testsorten zu lange war. Damit beanspruchte die Durchführung der Benutzertests im Rahmen eines Experiments jeweils den gesamten Tag. Aus diesem Grund konnte auch die Auswertung, entgegen der Empfehlung im Lean UX Prozess [30], nicht am selben Tag sondern erst ein paar Tage später durchgeführt werden. Zur Erstellung des Affinity Diagramms mussten daher alle Interviews bzw. aufgezeichneten Daten von den Autoren im Nachgang noch einmal durchgearbeitet werden. Durch die grosse Menge an gesammelten Daten mussten sich die Autoren ausserdem aufteilen, um alles bewältigen zu können. Dies führte einerseits zu einem Mehraufwand für die Auswertung und andererseits zu mehr Interpretationsspielraum, da viele nicht explizit aufgezeichnete Eindrücke vom Testtag bereits wieder verloren gegangen waren oder falsch rekonstruiert wurden.

[30] J. Gothelf und J. Seiden, Lean UX - Applying Lean Principles to Improve User Experience, 16. Aufl. O'Reilly Media

6 Resultate und Bewertung

Anhand der Storyline zum Transferieren von Dateien zwischen Sicherheitskontexten aus dem User Story Mapping Workshop [vgl. 2.2 Use Cases und User Story Mapping] wurden Testszenarien für die Benutzertests [vgl. Anhang 9.11 - 9.17] im Rahmen der Experimente definiert. Auf Basis dieser Testszenarien wurden mögliche Features für den interaktiven MVP Prototyp abgeleitet und als Designhypothese für den Benutzertest umgesetzt. Nach einem durchgeführten Testtag wurden im Team die jeweiligen Ergebnisse konsolidiert und in neue Annahmen formuliert. Diese Annahmen wiederum dienten als Grundlage für die nächste Iteration und flossen in die weitere Ausarbeitung des interaktiven MVP Prototyps.

In den folgenden Kapiteln wird die Entwicklung des interaktiven MVP Prototyps und der Proto-Personas dokumentiert. Anhand der durchgeführten Experimente [vgl. 5 Experimente] werden die getroffenen Designentscheidungen sowie die unterschiedlichen Ausbaustufen von MVP Prototyp und Proto-Personas aufgezeigt.

6.1 Resultate aus den Experimenten zu Zonen, Split Screen und Dateimanager

Mittels eines ersten Low-Fi Prototyps wurden dem Auftraggeber erste Ideenansätze zu seiner Fragestellung präsentiert:

A) **Zonen Wechsel: Wie soll der Benutzer zwischen verschiedene Zone wechseln können? Wie versteht der Benutzer, in welcher Zone er sich gerade befindet?** [vgl. Anhang 9.1 Protokolle]

B) **Arrangieren von VMs auf dem Desktop: Wie kann sich der Benutzer in den verschiedenen VM Fenstern der unterschiedlichen Zonen auf seinem Desktop organisieren? (Der Auftraggeber ist davon überzeugt, dass ein Split Screen Modus, also das Aufteilen von Screens für die einzelnen VM Fenster, die Lösung ist)** [vgl. Anhang 9.1 Protokolle]

C) **Organisieren der Daten: Wie kann der Benutzer seine Daten zwischen den verschiedenen Zonen organisieren?** [vgl. Anhang 9.1 Protokolle]

Diese Ideenansätze wurden im Prototyp auf eine visuell einfache Art wie folgt umgesetzt:

1. Ein Wechsel zwischen «Zone 1» und «Zone 2» wird über zwei Tabs simuliert. Jeder dieser Tabs stellt eine Zone dar und jede Zone eine eigene Desktopansicht. Wenn ein Benutzer zwischen diesen zwei Tabs (Zonen) hin und her wechselt, wird die zugehörige die Desktopansicht, welche jeweils eine eigene Zone simuliert, dargestellt.

2. Ein Split Screen Feature, welches mittels Overlay dem Benutzer verschiedene Layouts von Screen Einteilungen (Slices) zur Auswahl anzeigt. Auf dem Desktop wird die ausgewählte Einteilung zusätzlich über ein rotes Raster vorangezeigt. Wählt der Benutzer ein Layout, passen sich die offenen VM Fenster dieser neuen Einteilung an. Der Benutzer kann nun seine geöffneten VM Fenster innerhalb dieses Rasters verteilen. Das angewendete Raster kann im Nachhinein durch das manuelle Verschieben der Grenzen mittels Maus angepasst werden.

3. Ein Dateimanager, welcher Ablageordner, Programme und das Handling von Dateien zonenübergreifend zur Verfügung stellt und organisiert.

Die Idee dahinter ist, dass egal welche Sicherheitszone gerade aktiv ist (VM) der Benutzer:

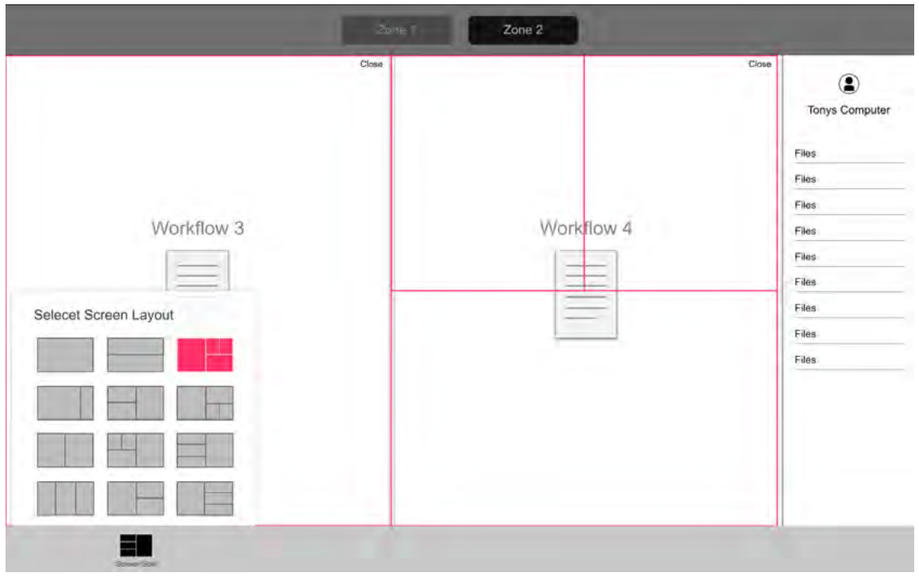
A) immer die gleiche Ordnerstruktur zur Verfügung hat,

B) immer die richtigen Programme zur Verfügung stehen (die firmeninterne Sicherheits- und Zugriffsregelung bestimmt, in welcher Zone und mit welchem Programm Daten geöffnet werden)

C) die Dateien, die geöffnet werden, sich immer in der richtigen Sicherheitszone öffnen, ohne dass der Benutzer einen Gedanken darüber verlieren muss: «Wo, in welcher Zone und mit welchem Programm darf ich diese Datei öffnen?»

6.1.1 Wire Frame Prototyp: Zonen Wechsel & Split Screen

Abbildung 21: Erster Ideen Prototyp



Nach einer intensiven Research Phase zu den Themen Desktop Metapher und alternative Konzepte, aber auch aus eigenen Erfahrungen mit dem Split Screen Modus in Windows, Mac OS und iOS, sind Zweifel am Nutzen dieser Funktionalität aufgekommen. Diese Zweifel bestätigten sich bereits in den ersten Interviews und Benutzertests [vgl. 5.3 Experiment gapfruitOS Simulation]. Innerhalb des Teams und im Gespräch mit dem Auftraggeber wurde beschlossen, die Split Screen Funktionalität nicht weiterzuverfolgen, da kein primärer Fokus zu erkennen war.

6.1.2 User Testing zu Zonen Wechsel & Datei Management

Die Konzepte Zonen Wechsel und Datei Management bilden das Grundkonzept der Interaktion von gapfruitOS. Daher sind sie in allen User Test Iterationen [vgl. 5 Experimente] zentrale Elemente der Prototypen und werden im Folgenden näher beschrieben.

Testszenario zu Zonen Wechsel und Datei Management

Die Testpersonen (TP) befinden sich in der Zone «Rot» und müssen ein Dokument mit dem Namen «Dateiname», welches in der Zone «Grün» abgelegt ist, im Dateimanager finden und mittels Doppelklick öffnen. Das geöffnete Dokument wird nun in die Zone «Rot» gespeichert [vgl. Anhang 9.11 - 9.12].

Da würde ich mir glatt drei weitere Monitore kaufen, bevor ich meine Arbeitsprozesse in einem Split Screen Modus durchführen würde.

Vinzent, Entwickler

Beispiele: Zonen Wechsel & Dateimanager (Iteration 2)

Abbildung 22: Übersicht Dateimanager geschlossen

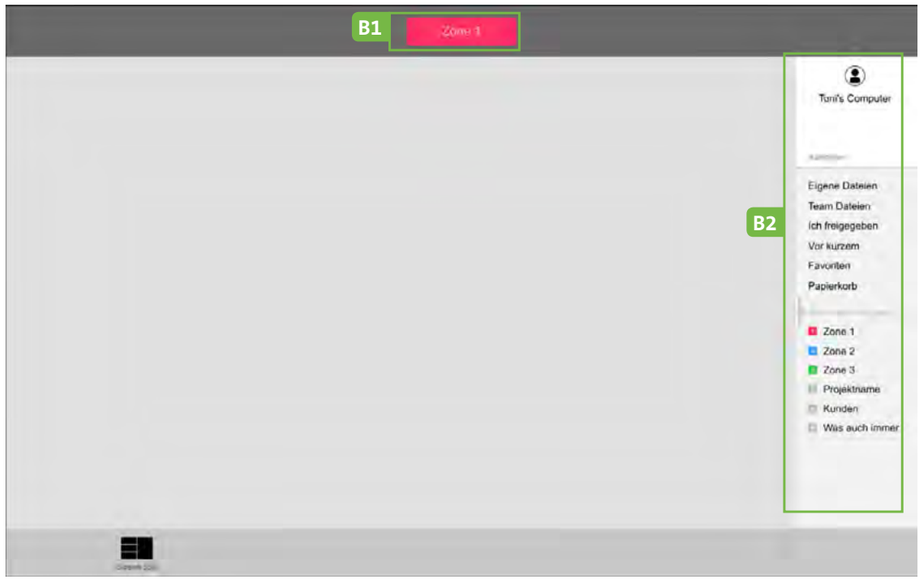


Abbildung 23: Übersicht Dateimanager offen

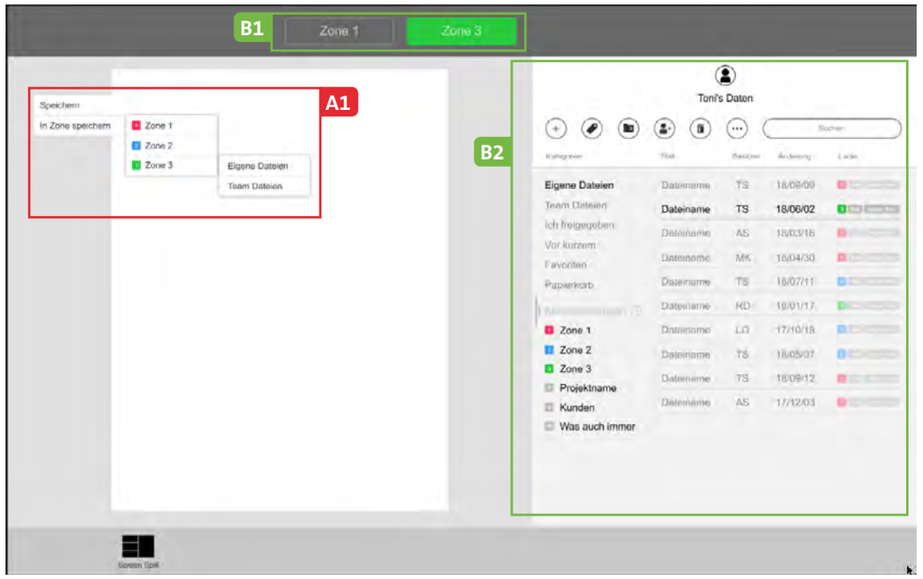


Abb 1, 2: Datei «Dateiname» im Dateimanager finden und unter neuem Label «Zone 1» abspeichern

A1: Das Label an dieser Stelle (in der VM) zu wählen wird nicht verstanden

B1: Die Zonen Tabs (Zonen Wechsel) werden sofort verstanden und genutzt, Unterscheidung mit Farbcode wird sehr positiv bewertet

B2: Der Übergreifende Dateimanager wird als solcher ebenfalls gut erkannt und genutzt

Erkenntnisse zu Zonen Wechsel & Datei Management

A1 Das Labeln von Zonen verwirrte die Benutzer an dieser Stelle. Sie gingen davon aus, dass ihr Dokument «Dateiname» automatisch unter der geöffneten Zone (3) gespeichert wird und erst danach die Zuteilung erfolge.

B1,B2 Der erste Entwurf (Prototyp) wurde von den Testpersonen bezüglich Zonen Wechsel und übergreifendem Dateimanager gut aufgenommen. Hier gilt es zu verfeinern und die unterschiedlichsten Inputs der Benutzer wie bspw. Farbgebungen, Verwendung von Icons u.a. in den kommenden Iterationen abzuholen.

6.2 Resultate aus den Experimenten zu Zonen Labeling und Notifications

Zusätzlich zur Idee eines zonenübergreifenden Dateimanagers wird den Auftraggebern ein Low-Fi Prototyp vorgestellt, der ein Konzept für ein Labeling der Zonen vorschlägt. Das heisst, einzelne Dateien können mit einem Zonen-Label versehen und darüber in der Zonenzugehörigkeit gesteuert werden. Für diesen Zonentransfer gelten vom Unternehmen definierte Regeln, die im Moment des Transfers durchgesetzt werden, bspw. ein Virencheck. Die Zonen-Labels erzwingen also die von den Unternehmen definierten Zugriffsregeln und -rechte, welche für die einzelnen Zonen gelten.

Abbildung 24: Skizze – Labeln von Zonen

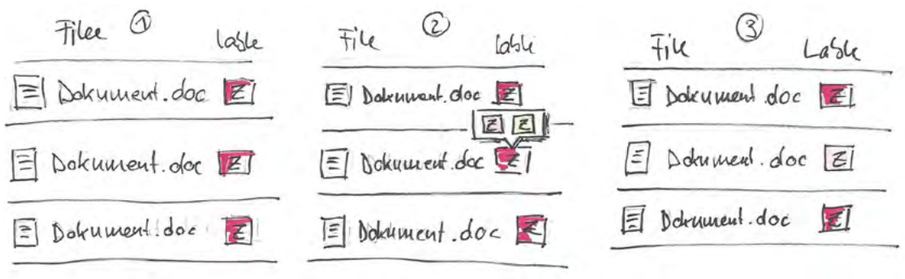


Abb 1: Die im Dateimanager enthaltenen Dateien sind mit einem Label für die Zone «Rot» markiert

Abb 2: Mit Klick auf das Label der Zone «Rot» wird dem Benutzer ein Pop-up mit weiteren, vom Unternehmen vordefinierten Zonen-Labels (in dieser Skizze «Zone Orange» und «Zone Gelb») zur Auswahl dargestellt

Abb 3: Indem der Benutzer ein anderes Label wählt (in dieser Skizze Label «Zone Orange»), wird die Datei in die neue Zone transferiert und damit passen sich die ZugriffsregelnLa dieser Datei der ausgewählten neuen Zone an.

Die Idee hinter diesem Labeling-Konzept für Zonen ist, dass Benutzer in gapfruitOS ihre Daten auf einfachste Art und Weise mit einer Zonenzugehörigkeit markieren können. Weiter müssen sie sich nicht darum kümmern, wie und wo ihre Dokumente physikalisch abgespeichert werden (in welchem der isolierten Dateisysteme der VMs). Das Betriebssystem soll das für die Benutzer im Hintergrund übernehmen.

6.2.1 User Testing zu Zonen-Label & Autorisierung (Iterationen 4 - 8)

Das Labeling-Konzept für Zonen wurde über vier Interationen mittels Prototypen und User Testings [vgl. 5 Experimente] validiert und verfeinert.

Testszenario zu Dateien mit Zonen-Label versehen

Die Testpersonen (TP) müssen ein Dokument «Auftrag.doc» welches in der «Online Zone» erstellt wurde, mit dem Label «Secret» für die sichere Zone versehen. Dabei haben sie zusätzlich noch die Möglichkeit, ein eigenes Label «Review» nach ihrer Wahl zu vergeben [vgl. Anhang 9.14 - 9.16].

Beispiel: Zonen Label & Autorisierung (Iteration 4)

Abbildung 25: Dateimanager Übersicht

Abb 1: Datei «Auftrag.doc» finden

A1: Icon Navigation verwirrt und lenkt ab

B1: Zonen-Label wird schnell gefunden und angeklickt

B2: Zonen-Label Workspace (Ordnung nach Zonen Labels) wird als solches erkannt

Abbildung 26: Persönliches Label setzen

Abb 2: Ein Wunschbegriff soll eingegeben und ein, in der Vergangenheit bereits gesetztes, persönliches Label, ausgewählt werden

A2: Icon Label wird von 2 TP nicht gesehen (verstanden), 3 TP wählen es an

A3: Bereits vorgegebene Auswahlen für Labels werden nicht erkannt

B3: Eingabe des eigenen Wunschbegriffs «Review» wird verstanden

Abbildung 27: Zonen Label zuweisen

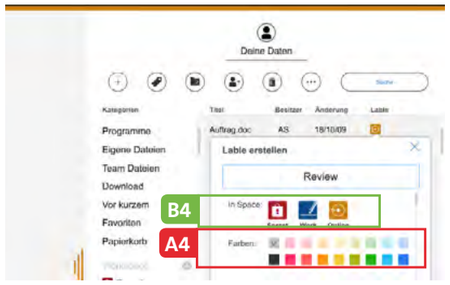


Abb 3: Auswahl der gewünschten Zone «Secret» und Farbe für persönliches Label «Review»

A4: Dass sich diese Farben auf das eigens gesetzte, persönliche Label beziehen wurde nicht erkannt

B4: Die richtige Zone wird mittels Label «Secret» ausgewählt

Abbildung 28: Notification Authentifizierung

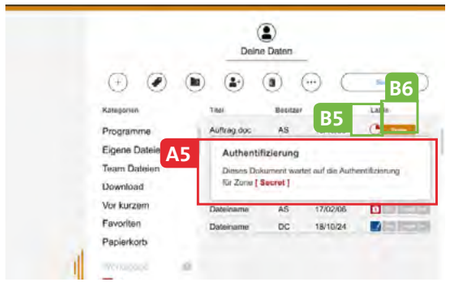


Abb 4: Benachrichtigung, dass die Autorisierung für den Transfer Zeit beansprucht

A5: Die Benachrichtigung wird von 2/3 TP nicht gelesen

B5: Die Veränderung bei Mouse-over des Icons Label zu einem Timer Icon wurde beachtet

B6: Das neue eigens gesetzte persönliche Label «Review» wurde erkannt

Abbildung 29: Prozessende Authentifizierung

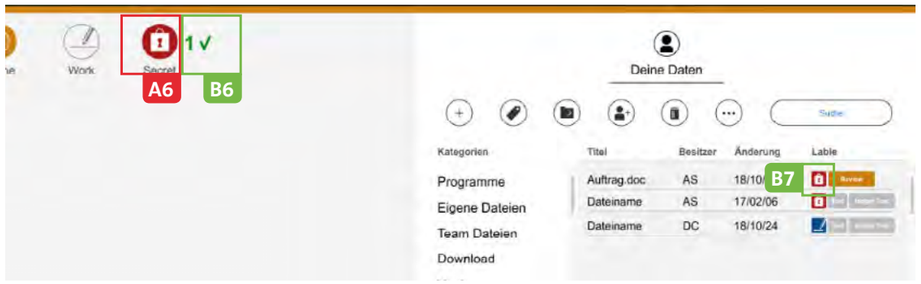


Abb 4: Benachrichtigung an Benutzer, dass die Autorisierung abgeschlossen ist

A6: Die Zonen Tabs zusätzlich mit Icons zu versehen wird gegenüber den Tabs nur mit Wortkennzeichnung weniger schnell wahrgenommen und als «fancy» (überflüssig) abgetan.

B6: Das Aktualisieren des Timer Icons auf Zone «Secret» Label wurde beachtet.

B6: Die Rückmeldung direkt bei der Zonen Beschriftung (Desktop Secret) wurde ebenfalls schnell erkannt.

Erkenntnisse zu Zonen-Label & Autorisierung (Iteration 4)

A1 Die Icons in der Navigation zusätzlich mit Text unterstützen damit sie besser verstanden werden oder zur Förderung der Übersichtlichkeit ganz weglassen.

A2 Das Label-Icon in der Navigation zusätzlich mit Text unterstützen damit es besser verstanden wird oder zur Förderung der Übersichtlichkeit ganz weglassen.

A3 Im Overlay «Labels erstellen» die bereits vorhandene Labels mit einem Übertitel bspw. «Bereits genutzte Labels» beschriften damit diese als solche erkannt werden.

A4 Wenn die Farben der persönlichen Labels einen Schritt vorher, bei der Texteingabe der Wunschlabels, gewählt werden können, ist die Zugehörigkeit dieser zum persönlichen Label gegeben.

A5 Indem das Overlay «Information Authorisation» explizit bestätigt oder geschlossen werden muss, werden die TPs den Text lesen müssen.

A6 Die Zonen Tabs, wie in vorangegangener Prototyp Version, nur mit Wörtern kennzeichnen.

Beispiele: Zonen Label & Autorisierung (Iteration 7)

Abbildung 30: Dateimanager Übersicht

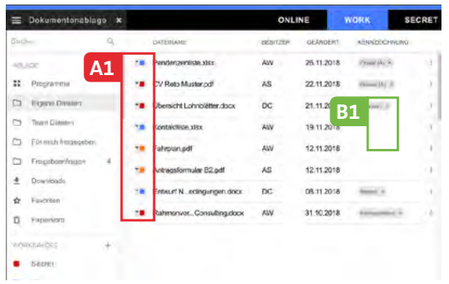


Abb 1: Zonen-Labels im Dateimanager als solche erkennen

A1: Das Zonen-Label wurde nicht als solches erkannt

B1: Die Trennung der persönlichen Labels von den Zonen-Labels wird als einfacher und übersichtlicher empfunden

Abbildung 32: Zonen Label

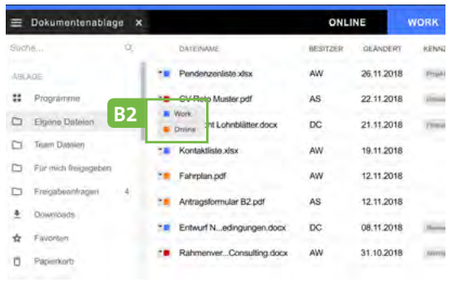


Abb 2: Ein Zonen-Label muss der Datei zugewiesen werden

B2: Die Beschriftung der Zonen mit Wort anstelle von Icons wird schneller erkannt

Abbildung 32: Rückmeldung Autorisierung

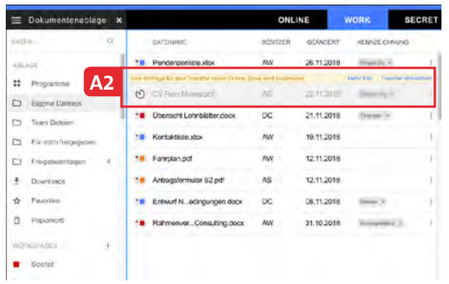


Abb 3: Systemrückmeldung, dass die Autorisierung Zeit beansprucht

A2: Die Meldung zur Autorisierung wurde nicht von allen PTs erkannt (gelesen)

Abbildung 33: Quittieren der Autorisierung

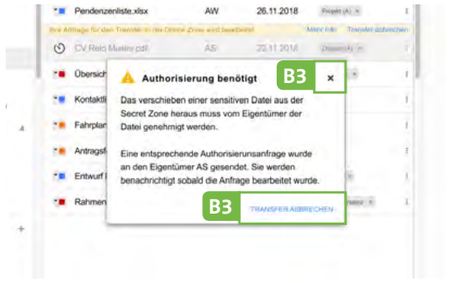


Abb 4: Overlay Autorisierung muss geschlossen oder der Prozess abgebrochen werden

B3: Dadurch, dass die Benutzer die Autorisierung mittels «schliessen» oder «Abbrechen» quittieren müssen, lesen sie die Informationen auf dem Overlay

Abbildung 34: Mitteilungszentrale

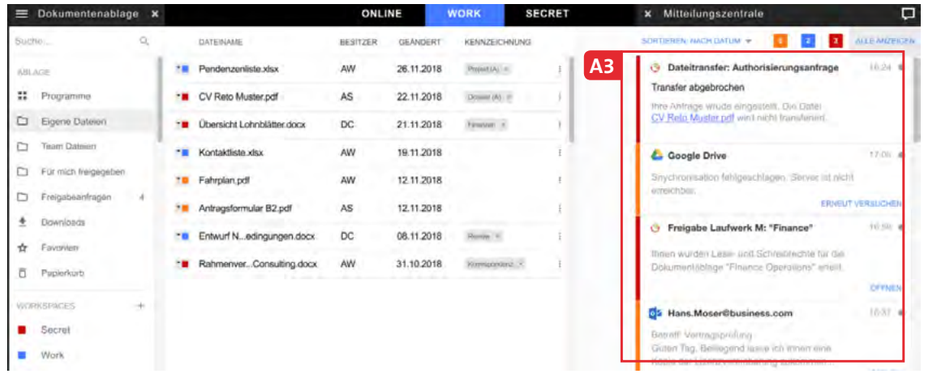


Abb 5: Zonen Informationen in der Mitteilungszentrale beachten und verarbeiten
A3: Die Mitteilungen in der Zentrale wurde nicht beachtet (erkannt)

Erkenntnisse zu Zonen Label & Autorisierung (Iteration 8)

A1 Damit die Zonen-Labels besser erkannt werden, müssen diese wieder grösser gemacht und die Interaktion zur Funktion dahinter, deutlicher visualisiert werden.

A2 Durch eine deutlichere Unterscheidung der Standard Systemrückmeldungen, wird die Meldung zur notwendigen Autorisierung von den Benutzern schneller erkannt.

A3 Wenn die Mitteilungen des Host- und der Gastsysteme getrennt werden, ist den Benutzer klar, ob es sich um relevante Systeminformation handelt oder ob bloss Mails zu beantworten sind.

6.3 Empfehlungen aus den Experimenten

6.3.1 Split Screen

«*Nice to have*» ist die Antwort der Probanden «*aber ich benutze diese Funktion selten*». Die Probanden kennen die Funktion ***Split Screen*** u.a. auch von den Apple iPads, iMacs und Windows Betriebssystemen, nutzen diese dort aber nur in seltenen Fällen bspw. zur Fotoarchivierung oder für Schularbeiten um Daten und Texte von einem Fenster ins andere zu kopieren. Dabei nutzen sie nur den 2-Split Modus. In ihrem täglichen Arbeitsalltag empfinden sie diese Funktion aber eher als hinderlich, da es sie in ihrer Arbeitsweise einschränkt oder gar zusätzlichen Arbeitsaufwand bedeutet. Sie müssten je nach Arbeitstask, die Fenster ständig neu anpassen und positionieren. In einem Betrieb der mit statischen Fensteransichten, bspw. zum Überwachen von Börsendaten, arbeitet, kann ein solche Split Screen Funktion jedoch durchaus eine Berechtigung haben.

6.3.2 Icons

Obwohl Standard Icons für ***Labels*** (A2) und Toolbars, welche auch in den OS der Bigplayer anzutreffen sind, gewählt wurden, waren die Bedeutungen dieser Icons und deren Funktion nicht von allen Testpersonen erkannt worden. Einzelne Wörter hingegen (bspw. Programme, Eigene Dateien, usw.) sind ohne Nachdenken von der TP erkannt und schnell benutzt worden. Auf der Website der Nielsen Norman Group [37] findet sich dazu folgende Aussage:

> «*Es gibt einige Symbole, die von Benutzern allgemein anerkannt werden. Die Symbole für Zuhause, Drucken und die Lupe für die Suche sind solche Fälle. Außerhalb dieser Beispiele sind die meisten Symbole für Benutzer nach wie vor mehrdeutig, da sie mit unterschiedlichen Bedeutungen über verschiedene Schnittstellen hinweg verbunden sind.*»

Die Autoren hegen dazu eine nicht verifizierte Hypothese, dass, geschuldet der zunehmenden mobilen Entwicklung mit immer kleineren Geräten, ein Überfluss an Icons existieren könnte? Mit der Zunahme von Informationen in einer immer mobileren Welt mit kleineren, mobilen Geräten, sind Icons für die Interaktion unerlässlich. Diese Entwicklung bedeutet daher, mehr Informationen (Icons) auf engem Raum wie bspw. die zahlreichen und bunten App-Icons auf Mobile Phones. Es kann sein, dass wir heute durch diese Zunahme von Icons an einen Punkt gestossen sind, an welchem diese Übersättigung mit Icons kontraproduktiv ist und Benutzer anfangen diese zu ignorieren?

«Es wäre spannend, diese Hypothese, separat in einem weiteren Projektverlauf, zu verfolgen.»

Wem in den vergangenen Jahren aufgefallen ist, dass in Desktopanwendungen der grossen Player wie Adobe, Apple und Mircrosoft (Word) bspw. das X-Icon (Fenster schliessen) durch die Wörter «close» oder «schliessen» ersetzt worden ist, kann durchaus darauf schliessen, dass dies nicht von ungefähr passiert. Gut möglich, dass wir uns in einer Zeit bewegen, in welcher die Benutzer aufgrund von Übersättigung den Icons immer weniger Beachtung schenken. Designer werden daher möglicherweise in Zukunft wieder vermehrt «Worte» anstelle von Icons für Interaktionen verwenden.

[37] https://www.nngroup.com/articles/icon-usability/

6.3.3 Farben

Die gewählte Farbzuweisung der Zonen

Online Zone = **Orange** (Achtung)

Work Zone = **Blau** (Vertrauen)

Secret Zone = **Rot** (Gefahr von Verlust)

wurde von den Probanden von Anfang an akzeptiert und richtig verstanden. Die Probanden nahmen die Bedeutung der Farben genau so wahr. Eine mögliche Alternative zu Blau sahen einige Probanden auch in Grün (Gut) für die Work Zone.

Die konsistente Einhaltung der Farbführung über das ganze Betriebssystem hinweg (Zonen, Dateien-Labels) erwies sich als sehr sinnvoll und nützlich. Für die Anwender war jederzeit klar ersichtlich, welche Dateien welcher Zone angehören. Werden die individuelle Aufteilung in Zonen und deren Bedeutung (Zugriffs- und Systemrechte) in der jeweiligen Firma mittels einer Schulung an die Mitarbeiter kommuniziert, ist den Benutzern auch klar, welche Rechte sie in welcher Zone mit welcher Datei haben.

6.3.4 Dateimanager

Ein absolutes No-go für die Probanden eines derartigen Systemkonzepts wäre, wenn sie sich in ihrem Alltag zusätzlich noch mit den verschiedenen, isolierten Ordnerstrukturen der unterschiedlichen VMs (Windows, Linux) auseinandersetzen müssten. Demzufolge ist die Idee des zonenübergreifenden Dateimanagers in den Prototypen sehr gut angekommen und wurde in seiner Funktion verstanden und akzeptiert. Die Ablage von Daten in einer vorgegebenen und reduzierten Ordnerstruktur wird begrüsst und als deutlicher Mehrwert empfunden: «Das Betriebssystem soll sich um den richtigen Ablageort und die Rechte meiner Daten kümmern».

6.3.5 Benachrichtigungen

3 TPs haben mit der Mouse-over Funktion «gespielt» und das Overlay «Rückmeldung Autorisierung» (A5) bis zu fünfmal ein- und ausgeblendet ohne dabei zu realisieren, dass ihnen mit diesem Overlay eine wichtige Information angezeigt wird. Die TPs haben den direkt vor Ihren Augen stehenden Text nicht bewusst wahrgenommen und damit auch nicht gelesen.

In einem derart komplexen Betriebssystem lassen sich Notifikationen zur Benutzerinformation und zur Steigerung des Verständnisses kaum vermeiden. Allerdings zeigte sich, dass die Benutzer kein Verständnis für Wartezeiten- und andere Sicherheitsnotifikationen im Betriebssystem in ihrem Arbeitsablauf akzeptieren. Philipp Murkowsky, Inhaber von Puzzle ITC, fasste das in seinem Vortrag am World Usability Day 2018 an der HSR Rapperswil [38] wie folgt zusammen:

«*Wir können nicht davon ausgehen, dass alle Benutzer unter Anleitung die Systeme verstehen. Wir müssen daran arbeiten, dass Systeme nicht mit Usability Design sicherer werden, sondern in ihrem strategischen Design*».

Laut Murkowsky leben Industrien wie die Luftfahrt oder die Maschinen Industrie nach dem Prinzip: Fehlerfreie System bauen – Nur eben, die IT Industrie nicht.

6.3.6 Zonen

Bei den im Rahmen der Experimente interviewten Probanden hat sich deutlich gezeigt, dass in den Firmen dieser Personen, ein Zwei-Zonen-Konzept «Secret» und «Online» ausreichend ist. Die Testpersonen, welche bei ihrer Tätigkeit mit hochsensitiven Daten zu tun haben, arbeiten zu 80%-90% nur auf hochsicheren Systemen (Secret Zone) auf welcher die Daten nicht verschoben (Daten werden nicht Kopiert), sondern der Zugriff mittels Zugriffsrechten gesteuert wird.

Während der gesamten Projektdauer ist es den Autoren nicht gelungen, Personen zu befragen, welche eine Konfiguration mit mehr als zwei Zonen benötigen würden, bspw. Mitarbeiter einer Behörde oder eines Atomkraftwerks. Es ist gut möglich, dass in einem derart spezialisierten Umfeld eine Konfiguration mit mehr als zwei Zonen sinnvoll sein kann. Aus diesem Grund existiert weiterhin die Proto-Persona «Martin BEAMTER» [vgl. 6.4.5 Erste mögliche Projekt Proto-Personas], welche dringend weiter untersucht werden sollte.

[38] Aussage von Philipp Murkowsky, Puzzle ITC am WUD2018 – https://www.youtube.com/watch?v=VeyjKz3NDKE&feature=youtu.be

Startups scheitern unter anderem auch daran, dass für die angebotenen Produkte und Dienstleistungen kein Marktbedarf besteht. Personas bieten eine schnelle Möglichkeit, ein Produkt durch gezielte Kundenorientierung zu überprüfen.

Die Autoren

6.4 Proto-Personas im Projekt

Das Kreieren von Personas hilft Unternehmen, ein Benutzererlebnis aus Sicht der Benutzer spürbar, sichtbar und kommunizierbar zu machen. Personas vermitteln Unternehmen Verständnis und knüpfen an die Bedürfnisse ihrer Kunden an, um fundierte Entscheidung treffen zu können.

Insbesondere wenn es sich um ein Startup handelt, welches die richtigen Zielkunden finden möchte aber wenig Budget hat oder der Glaube an User Centered Design fehlt, sind Proto-Personas ein guter Weg um Benutzer zu verstehen und sich anhand der erstellten Benutzeranforderungen zu orientieren. Für sie sind Protopersonen der beste Weg, um voranzukommen.

6.4.1 Proto-Personas nach Lean UX

Mit Augenmerk auf die Ausgangslage im vorliegenden Projekt wobei

A) **der Auftraggeber der Ansicht ist, dass sein Produkt für alle Benutzer (von Inhaber einer Metallwerkstatt bis hin zur Kanzlei) Anklang findet und deshalb keine Zeit in die Evaluationsphase von Personas investiert werden soll und**

B) **es ihm zusätzlich an den nötigen Ressourcen möglicher Testkunden, Benutzer und/oder Firmen fehlt,**

C) **die Autoren, mangels Punkt A) und B) nicht das nötige Domänenwissen aufbauen konnten,**

scheint das Vorgehen Proto-Persona nach Lean UX geeignet zu sein.

Vorgehen

Erste Annahmen zu Proto-Personas wurden im gesamten Team, parallel zur Durchführung des User Story Mappings [vgl. 2.2 Use Cases und User Story Mapping] im Rahmen von Brainstormings beschrieben. Später flossen die Erkenntnisse aus den Experteninterviews und den durchgeführten Experimenten mit ein. Dabei wurden die möglichen Zielgruppen und deren Auswirkung auf die Entwicklung von gapfruitOS heftig diskutiert.

Die nach wie vor gültige Annahme ist, dass potentielle Benutzer eines solchen sicheren Betriebssystems in ihrem Arbeitsumfeld mit hochsensitiven Daten zu tun haben müssen.

Die Auftraggeber haben die Vision, dass Benutzer ihres Systems parallel in mehreren Zonen gleichzeitig in einer Art Split Screen Konfiguration arbeiten möchten. Die Autoren hinterfragten diese Theorie und stellten die Annahme auf, dass eine derartige Konfiguration nicht sinnvoll einsetzbar ist. Erst ab einer bestimmten, minimalen Monitorgrösse oder Monitoranzahl kann die parallele Anzeige von Zonen sinnvoll sein. Auf einem Tablet oder kleinen 13-Zoll Monitor ist eine Split Screen Konfiguration sehr unangenehm für den Anwender. Daher steht für die Definition der Proto-Personas auch das verwendete Arbeitsgerät im Fokus.

In der Folge werden erste nicht validierte Charakterisierungen der Proto-Personas stichwortartig beschrieben:

- **Der Bundesbeamte**
  Arbeitet in einem Kernkraftwerk und muss gegen Angriffe von Aussen abgesichert werden, hat bei seinen täglichen Arbeitsroutinen strenge Vorschriften einzuhalten, bewegt sich neben gewöhnlichen administrativen Aufgaben in hochsensitiven Steuer- und Kontrollnetzwerken, ist jederzeit auf absolut zuverlässige und korrekte Daten angewiesen, die Infrastruktur darf unter keinen Umständen ausfallen
  Arbeitsumfeld: eher stationär
  Arbeitsgeräte: eher Personal Computer

- **Der Entwickler**
  Arbeitet in einem Unternehmen mit sehr sensitiven Daten, klinkt sich in wichtige produktive Systeme zwecks Analyse- und Wartungsarbeiten ein, arbeitet in unterschiedlichen Entwicklungs- und Testumgebungen, muss öfter neue Entwicklungs- und Testumgebungen aufsetzen oder existierende zurücksetzen, interagiert dadurch mit verschiedenen Ansichten von Screens und VMs, muss sensitive Test- oder Live-Daten innerhalb der entsprechenden Sicherheitskontexte halten
  Arbeitsumfeld: Stationär und unterwegs
  Arbeitsgeräte: Laptop

- **Der Banker**
  Arbeitet mit hochsensiblen Kundendaten (Steuer- und Finanzoptimierung, Bankgeheimnis, Rechtliches, länderübergreifende Regularien, usw.), nicht alle Daten dürfen kopiert werden oder den Laptop, die Bank oder das Land verlassen
  Arbeitsumfeld: eher stationär
  Arbeitsgeräte: Laptop

- **Der Anwalt**
  Arbeitet mit hochsensiblen Kundendaten wie Finanzen, Steuern, Scheidungen, usw., Daten sind digital wie physisch vorhanden,
  Arbeitsumfeld: viel unterwegs (Aktenkoffer, Laptop, etc.)
  Arbeitsgeräte: Laptop und/oder Personal Computer

- **Der Versicherungsberater**
  Arbeitet mit sensitiven Kundendaten (Versicherungen, Anlagen, Steuern, Finanzen, usw.) in einer Agentur oder im eigenen Standortbüro,
  Arbeitsumfeld: hauptsächlich stationär mit gelegentlichen Kundenbesuchen
  Arbeitsgeräte: Tablet und/oder Laptop und/oder Personal Computer

6.4.2 Erste grobe Persona-Skizzen nach Lean UX

Abbildung 35: Proto-Persona «Versicherungen»

Abbildung 36: Proto-Persona «Bundesbetriebe»

Abbildung 37: Proto-Persona «Kanzlei»

Abbildung 38: Proto-Persona «Banken»

Abbildung 39: Proto-Persona «Design»

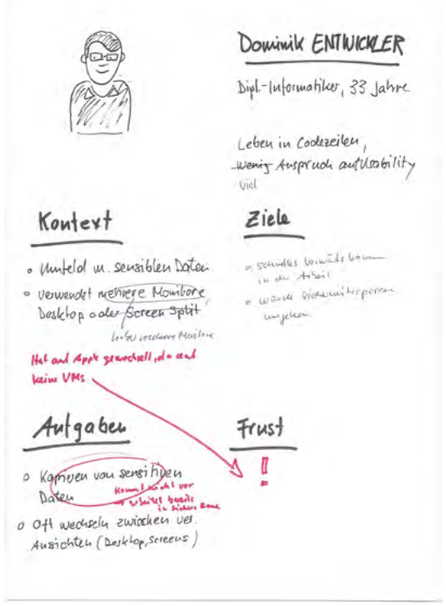


Abbildung 40: Proto-Persona «Entwicklung»

[vgl. Anhang 9.19 Skizzen Proto-Personas]

Diese Proto-Personas werden als mögliche Zielgruppe für weitere Evaluationen verwendet. Sie werden über den weiteren Projektverlauf mittels Experimenten gemäss Lean UX im Rahmen von User Tests und Interviews auf ihren Wahrheitsgehalt hin überprüft und wo notwendig verworfen bzw. angepasst und verfeinert.

Über die Dauer von 12 Tagen wurden 6 Experimente mit 19 Benutzertests und 21 Interviews mit potentiellen Anwendern durchgeführt. Dabei zeichneten sich die folgenden Benutzermerkmale ab.

6.4.3 Evaluierte Proto-Persona Typen

Proto-Persona – Typ 1

Gut die Hälfte der befragten Probanden (Entwickler, UX Designer, Sozialarbeiterin) appellieren an den «gesunden Menschenverstand» und gehen primär davon aus, dass sie als Person keine lohnenden Ziele für Angriffe sind. Sie vermuten, dass die aktuellen Bigplayer wie Apple oder Microsoft bereits das nötigste unternehmen, um ihre Benutzer gegen Angriffe von Aussen zu schützen. In ihren Unternehmen haben diese Probanden kaum mit sensitiven Daten zu tun. Bezüglich Klassifizierung und Zugriff auf Daten verlassen sich die meisten auf die von ihrem Unternehmen konfigurierten Rollen und Zugriffsberechtigungen auf Server Shares.

Evaluierte Benutzermerkmale

- Weder Verständnis noch Akzeptanz für zonenbasiertes Arbeiten vorhanden
- Würden Sicherheitsregeln bei sich anbietender Möglichkeit umgehen
- Benutzung nur wenn von ihrem Unternehmen vorgeschrieben

Sensible Daten sollten nie in unsicheren Zone landen – genau darum gelten sie ja als sensibel!

Florian, Data Science

Proto-Persona – Typ 2

Probanden die bereits in einem Umfeld mit erhöhten Sicherheitsvorkehrungen wie bspw. In einer Bank, Kanzlei, Legal Abteilung von Unternehmen, Treuhandbüro, usw. arbeiten, sind gegenüber gapfruitOS aufgeschlossener. Sie verstehen und akzeptieren den Sicherheitsaspekt hinter diesem OS. In Ihren Unternehmen arbeiten sie teilweise bereits auf Lösungen die einen ähnlichen Workflow vorschreiben bzw. mehrere unterschiedliche Sicherheitskontexte beinhalten.

- **Anwalt:** Bewältigt seine komplette Klienten- und Mandatsverwaltung (inkl. Mailverkehr mit Empfangen/Senden) aus der, vom Anwaltsverband vorgegebenen, sicheren Cloudlösung Avotime [39] heraus.
- **Legal Abteilung Zühlke:** Das Erfassen und Kontrollieren von Verträgen umfasst 80% dieser Arbeitstätigkeit. Sie wird direkt auf einem sicheren Server, mit Zugriffsregelung, geleistet. Die Verträge werden oft noch via E-Mail ausgetauscht, was unsicher und somit nicht optimal ist.
- **Bank Data Science, Legal & Compliance:** Kundendaten liegen auf streng kontrollierten, physisch abgekoppelten Servern und werden (aus rechtlichen Gründen aber auch wegen vielen Zugriffen innerhalb der Firma) nicht verschoben oder kopiert. Für den Zugriff auf diese Daten muss ein langwieriger Prozess «Access Right Approval» durchlaufen werden. In diesen Prozess sind weitere +/- 50 Kontrollmitarbeiter involviert. Dieser Genehmigungsprozess dauert rund drei Wochen.

Validierte Benutzermerkmale

- Unternehmen haben bereits integrierte Sicherheitssysteme
- Akzeptanz und Verständnis für systemrelevante Sicherheitsregelungen sind vorhanden
- Arbeitstätigkeit wird zu 80% bis 100 % in sicherer Zone ausgeführt
- Zwei-Zonen-Konzept: Bereits heute basiert die Arbeit auf einem Wechsel zwischen sicherem und unsicheren Kontext

[39] https://www.infocall.ch/index.php/software/madabawin/2-uncategorised/59-avotime

- Eine sichere Sharing-Funktion zum Teilen von Daten innerhalb eines Teams und zwischen Mitarbeitern ist erwünscht
- Sicherheitskonzept und Umgang mittels Schulung (Einführung) erlernbar

P**roto-Persona – Typ 3**

Bundesangestellter Kernenergie: Dieser Proband konnte trotz Anstrengungen in dieser Zeit, aus sicherheitstechnischen Gründen eines Atomkraftwerks, nicht akquiriert bzw. befragt werden. Die Autoren hegen aber die Annahme, dass es sich bei dieser Proto-Persona um eine zukünftige Persona (Primär) handeln könnte. Diese Annahme ist davon abhängig, wie sehr sich gapfruitOS System in Richtung derartiger Speziallösungen entwickeln möchte.

Nicht validierte Benutzermerkmale:

- Arbeiten in mehr als zwei Zonen
- Strenge Sicherheitsvorkehrungen, Gerätschaft komplett von der Aussenwelt (Internet, Mail, u.a.) getrennt
- Akzeptanz für «Sicherheit vor System Usability»

6.4.4 Empfehlung Proto-Persona

Zum jetzigen Projektstand kann keine eindeutige Empfehlung bezüglich Fokussierung auf eine Proto-Persona ausgesprochen werden. Basierend auf den im vorliegenden Bericht erarbeiteten Annahmen sollte sich das Projektteam gapfruit AG bei der Weiterentwicklung ihres gapfruitOS, die unter Kapitel 6.4.5 Erste mögliche Projekt Proto-Personas erwähnten Proto-Personas vertiefter verfolgen und weitere Benutzerforschung in diesem Bereich betreiben.

6.4.5 Erste mögliche Projekt Proto-Personas

Basierend auf den erwähnten Annahmen, können folgende zwei Proto-Persona Typen adressiert werden:

Proto-Persona Typ 2 – Anna-Marie LEGAL

Firmen wie bspw. Banken, Kanzleien, Treuhandbüros, Legal Abteilungen, u.a. nutzen bereits 2-Zonen Konzepte, basierend auf Remote Desktop Lösungen oder abgesicherten Servern/Cloudlösungen mit Zugriffsrechtsteuerung im Einsatz. Zum

Abbildung 41: Erste Projekt Proto-Persona «Legal» und «Bundesbeamter»

jetzigen Projektstand konnten die befragten Probanden keinen eindeutigen Mehrwert von gapfruitOS zu den bestehenden Konzepten erkennen.

Entscheidend wird sein, ob sich gapfruitOS in Zukunft als 2-Zonen Konzept oder gar als Lösung, in der die Sicherheitskontexte auf einzelnen nativen Apps basieren (sogar über die Cloud?), durchsetzen möchte? In diesem Fall wird für gapfruitOS die Proto-Persona Typ 2 ins Zentrum rücken, da diese Lösung dem heutigen State of the Art der Entwicklung und der Akzeptanz der Benutzer (ähnlich Mobile Apps) aus Usability Sicht, am nächsten steht. Für diese Proto-Persona sollte zusätzlich die Möglichkeit einer Team-Sharing-Funktion näher betrachtet werden.

Proto-Persona Typ 3 – Martin BEAMTER

Die zweite Möglichkeit ist, dass sich gapfruitOS auf spezialisierte Unternehmungen konzentriert. Unternehmen, die ganz spezifische und personalisierte Anforderungen für ein hochsicheres Betriebssystem haben. Zwar wäre gapfruitOS dann nicht mehr «Main Stream» aber die Ursprungsidee von gapfruitOS – ein Mehrzonen Konzept (> 2 Zonen) – kann für hoch spezialisierte Anwendungsfälle interessant sein. In diesem Fall wird es eher die Proto-Persona Typ 3, welche aber erst noch erforscht, validiert und verifiziert werden muss. Bei einem derart spezialisierten Persona Typ ist ein Contextual Iquiriy, ein benutzerzentrierter Design Prozess welcher in den 90er Jahren von Karen Holzblatt & Hugh Beyer [40] , entwickelt wurde, unabdingbar.

6.4.6 Reflexion Proto-Personas

Im Berufsalltag ist oft eine negative Einstellung gegenüber des Konzepts Persona zu spüren. Persona wären im Vergleich zu ihrem Nutzen zeitaufwendig und teuer. Für Projekte in einer derart spezialisierten und hoch komplexen Domäne mit vielen Unbekannten, macht sich die Investition in das Konzept Proto-Persona zwecks Benutzerforschung aber ausbezahlt.

Vom Projektstart und über eine längere Projektdauer, sind sich die Autoren und die Auftraggeber uneinig darüber, was der eigentliche Fokus des Projekts und auch von gapfruitOS sein soll. Erst über das Konzept Proto-Persona basierend auf Annahmen in Kombination mit Benutzertests, wurden erste mögliche Szenarien sichtbar und Probleme spürbar gemacht. Es verhalf dem Projektteam – zwar in kleinen Schritten und erst beinahe am Ende der Projektzeit – doch noch zu einem gemeinsamen Fokus zu gelangen.

[40] H. Beyer und K. Holtzblatt, Contextual Design: Defining Customer-Centered Systems, 1. Aufl. Morgan Kaufmann.

A) **Mittels Experten Interviews wird ein unabhängiges Domänenwissen aufgebaut und die Sichtweise (Aussensicht) von potentiellen Unternehmen und Benutzern werden spürbar**

B) **Die kontinuierliche Weiterentwicklung der Proto-Personas identifiziert mögliche potentielle Benutzer und deren Needs & Painpoints skizzenhaft.**

Im aktuellen Projektstand zeigt sich, dass grundlegende Annahmen nicht allzu weit weg von den erarbeiteten Erkenntnissen lagen. Erkenntnisse, die sonst über langwierige Befragungen und Beobachtungen entstehen. Entscheidend im Umgang mit Proto-Personas ist die Bereitschaft, jegliche getroffenen Annahmen auch ändern zu wollen und nicht bei den ersten Definitionen hängen zu bleiben.

6.5 Fazit und Projektstand im Januar 2019

Die Untersuchungen haben gezeigt, dass ein derartiges Betriebssystem trotz der offensichtlichen Notwendigkeit von vielen der untersuchten Testpersonen im Rahmen ihrer Arbeitstätigkeit nicht akzeptiert wird. Dies liegt einerseits an der fehlenden Sensibilisierung auf die Problematik der Cyberkriminalität und anderseits am fehlenden Bewusstsein, wie sensitiv die eigenen, bearbeiteten Daten eigentlich sind. Viele der befragten Testpersonen bearbeiten gar keine sensitiven oder keine als sensitiv wahrgenommenen Daten. Viele Probanden vertrauen auf die getroffenen Sicherheitsmassnahmen des eigenen Unternehmens und sehen keinen Handlungsbedarf. Andere kümmern sich überhaupt nicht Datensicherheit und sensitive Daten.

Eine weitere Problematik besteht laut Aussagen aus den Experten-Interviews [vgl. 2.3 Interviews mit Subject Matter Experts] bei den Kosten für die Einführung eines solchen Produktes bei KMUs oder Grossunternehmen. Diese dürften «exorbitant» sein und damit die Einführung gar nicht erst rechtfertigen, da die Kosten von Schäden als tendenziell geringer eingeschätzt werden als die unternehmensweite Einführung eines neuen Systems.

Aufgrund der fehlenden Fokussierung auf eine bestimmte Benutzer- oder Berufsgruppe war es für die Autoren im Verlauf des Projektes nicht möglich, konkrete und validierte Benutzergruppen und Anwendungsszenarien eines hochsicheres Betriebssystems wie gapfruitOS zu erheben. Im Rahmen der durchgeführten Experimente konnten jedoch Berufsgruppen, die potentiell zur Benutzergruppe eines hochsicheren Systems gehören, sowie deren Anwendungskontext [vgl. Anhang

9.20 Berufsgruppen und Nutzungskontext] eruiert werden. Auf Basis dieser erhobenen Daten wurden schliesslich die Proto-Personas [vgl. 6.4 Proto-Personas im Projekt] entwickelt. Diese Proto-Personas basieren noch auf Annahmen und sollten im Anschluss an dieses Projekt weiter untersucht und validiert werden. Zusammen mit den erhobenen Berufsgruppen bilden sie einen ersten, jedoch noch unvollständigen Rahmen für eine mögliche Zielgruppe des Produktes.

Die im Rahmen der Experimente entwickelten Prototypen, insbesondere der zonenübergreifende Dateimanager und das Labeling-Konzept für die Zonenzugehörigkeit von Dateien bieten interessante Ansätze für ein Interaktionskonzept [vgl. 6.1 - 6.2]. Bei den durchgeführten Benutzertests wurden diese Ideen grundsätzlich gut aufgenommen und als intuitiv und einfach verständlich beurteilt. Es darf jedoch nicht vergessen werden, dass es sich hierbei, wie bei den Proto-Personas, lediglich um Ansätze mit vielen Annahmen handelt. Die Prototypen dürfen in diesem Sinn nicht als fertiges Interaktionskonzept angesehen werden. Zum Projektende existieren so beim konsolidierten Dateimanager auch noch drei grosse, nicht untersuchte Bereiche:

1. **Wie intuitiv und einfach zu bedienen ist ein zonenübergreifender Dateimanager wenn anstatt der in den Prototypen dargestellten 15-20 Dateien plötzlich mehrere hundert Dateien existieren?**
2. **Wie geht man mit dem Aspekt um, dass jedes Gastsystem zusätzlich einen eigenen Dateimanager mitbringt, der jedoch nur auf das eigene isolierte Gastsystem Zugriff hat? Kann/soll/muss dieser einfach deaktiviert werden?**
3. **Wie nimmt ein Benutzer einen vollen Desktop eines Gastsystems mit Programm-Verknüpfungen und allenfalls wild herumliegenden Dateien innerhalb einer Zone wahr? Innerhalb der Prototypen waren die Desktops der Gastsysteme vollständig leer. Kann/soll/muss das im echten System auch so funktionieren um die Übersicht zu wahren?**

7 Reflexion

In diesem Kapitel wird die Projektarbeit der vergangenen neun Monate reflektiert. Als erstes wird auf das Vorgehen nach Lean UX Prinzipien eingegangen. Im weiteren Verlauf folgt die Reflektion von Organisation und Planung innerhalb des Projektes. Anschliessend werden der Wissensaufbau und die inhaltliche Erarbeitung durchleuchtet sowie die gefällten Entscheidungen nochmals kritisch hinterfragt. Zuletzt folgt die persönliche Reflexion der Autoren zu ihrer Zusammenarbeit.

7.1 Reflexion Lean UX

Lean UX steht in direktem Widerspruch zu Alan Coopers Goal-Directed Design, indem es den Ansatz verfolgt Annahmen zu definieren und diese mit potentiellen Benutzern zu testen. Alan Cooper bezieht in seinem Artikel [26] ganz klar Stellung und erklärt, dass «Prototyping und Testing» nie Teil seiner Methoden war. Er spricht sich sogar explizit dagegen aus. Aus seiner Sicht verkommt die Entwicklung eines Interaktionskonzepts dabei zu einer Designer-centered Angelegenheit und verfehlt damit die ursprüngliche Intention des User-centered Designs. Die Autoren stimmen dieser Ansicht nicht uneingeschränkt zu und meinen, dass dieser Prototyping-Ansatz gerade im Startup Bereich oder bei der Entwicklung von sehr komplexen Produkten durchaus sinnvoll sein kann. Bei vielen Projekten sind die vom zu lösenden Problem betroffenen Benutzergruppen unmittelbar bekannt, bspw. bei der Entwicklung einer firmenintern genutzten Software oder einer Anwendung, die von einer bestimmten Berufsgruppe eingesetzt wird. In diesem Fall ist eine ausgedehnte User Research Phase durchaus angebracht.

Im Falle eines Startups hingegen beginnt alles mit einer möglicherweise neuartigen, im Idealfall sogar grossartigen Idee zur Lösung eines potentiell bei einer unbekannten Zielgruppe bestehenden Problems. Die Problemstellung ist dabei in den wenigsten Fällen vollumfänglich untersucht und die potentielle Benutzergruppe damit nicht im Detail bekannt oder wie im vorliegenden Projekt eine blosse Vermutung. Aufgrund der beschränkten finanziellen Mittel und einer möglichst kurzen Time-to-Market besteht also meist keine Möglichkeit für einen aufwendigen,

[26] A. Cooper, «The Endless Battle», Alan Cooper, 22-Okt-2017

vorgeschalteten Forschungsprozess. Auch bei etablierten Unternehmen werden diese Aspekte immer wichtiger, fast niemand kann oder will sich heutzutage einen langwierigen Forschungsprozess vor der Umsetzung leisten. Erschwerend kommt hinzu, dass bei einer neuartigen Produktidee oder auch der Entwicklung eines komplexen Produkts unmöglich alle Anforderungen im Voraus erhoben werden können. In der Praxis zeigt sich immer wieder, dass Anforderungen über die Dauer der Entwicklung so gut wie nie stabil bleiben. Sie verändern sich zuweilen gravierend durch die über den Entwicklungsprozess gewonnene Erfahrung. Auch die genaue Art der zukünftigen Nutzung des Produktes ist schwierig vorauszusagen. Aus diesem Grund erscheint den Autoren der dogmatische, beinahe wasserfallartige Prozess von Cooper (Benutzerforschung → Anforderungen → Design) zu unflexibel in bestimmten Situationen.

Lean UX formalisiert den «Prototyping und Testing» Prozess und ermöglicht es, parallel Benutzerforschung und Ideation zu betreiben. Die initial formulierten Benutzergruppen eines Produktes basieren dabei auf mehr oder minder validen Annahmen. Je valider diese Annahmen sind, desto relevanter sind die Resultate aus den Experimenten. Hier lauert aber bereits der erste grosse Stolperstein von Lean UX. Sind die initialen Annahmen zur Benutzergruppe falsch, führen die Experimente im besten Fall zu irrelevanten Erkenntnissen, im schlimmsten zu komplett falschen Annahmen zu Benutzergruppe und Features für die folgenden Experimente. Daher ist aus Sicht der Autoren auch hier eine vorgeschaltete Research Phase sinnvoll, um die Benutzergruppe einzuschränken oder zumindest einen Fokus auf eine bestimmte Personen-/Berufsgruppe zu lenken. Die Research Phase muss jedoch nicht so ausgedehnt und abschliessend sein, wie von Goal-directed Design gefordert. Lean UX beleuchtet diese Thematik jedoch nicht und bietet damit auch keinerlei Hilfestellung für einen sinnvollen Startpunkt in die Experimente. Aus Sicht der Autoren wäre es also eine gute Idee, erst nach einer vorgeschalteten Benutzerforschung mit einigermassen validen Annahmen zu den Benutzergruppen in die Experimente einzusteigen.

Dies war im vorliegenden Projekt jedoch nur beschränkt möglich, da es von den Auftraggebern explizit keine Fokussierung auf eine bestimmte Zielgruppe gab. Einzig die vorgängig durchgeführten Experteninterviews gaben erste Leitplanken und zeigten bereits in die Richtung einer sehr spezifischen Benutzergruppe. Trotzdem wurden die Probanden für die ersten Benutzertests gemäss Wunsch der Auftraggeber willkürlich ausgesucht. Hierbei zeigte sich jedoch rasch, dass die meisten dieser Testteilnehmer nicht zur Zielgruppe des Produktes gehören. Damit waren jedoch auch die Erkenntnisse in Bezug auf die effektive Benutzergruppe, das Design und den Kontext des Produktes wenig relevant.

In einem derartigen Fall kann Lean UX oder allgemein ein Lean-Ansatz leicht als Ausrede benutzt werden, um die beiden aus Sicht der Autoren wichtigsten Aspekte, die Erhebung von konkreten Benutzergruppen und deren Nutzungskontext zu vernachlässigen oder gar ganz wegzulassen. Werden Proto-Personas nicht ganz genau als das angesehen was sie in Wirklichkeit sind, nämlich reine Annahmen, und konsequent mit den neu gewonnenen Erkenntnissen weiterentwickelt oder verworfen, werden zwangsläufig auch alle folgenden Experimente irrelevante bzw. falsche Erkenntnisse liefern. Nur mit der inkrementellen Weiterentwicklung der Proto-Personas wird es möglich, die Benutzergruppe einzugrenzen und schliesslich auch die richtigen Personen zur Durchführung der Experimente zu rekrutieren. Dabei bleibt jedoch eine wichtige Frage zu klären, ab welchem Zeitpunkt (Anzahl Zustimmungen oder Absagen) kann eine Annahme als validiert und damit als Wahrheit betrachtet werden. Insbesondere wenn zu Beginn der Experimente mit falschen bzw. aufgrund von fehlendem User Research nicht relevanten Benutzern getestet wird. Während des Projekts entstanden viele Diskussionen und auch unterschiedliche Interpretationen, welche Teile des Lösungsansatzes noch auf Annahmen basierten und welche bereits validiert sind.

Lean UX erscheint im ersten Moment sehr einfach in der Durchführung. Eine konsequente Anwendung der Prinzipien erfordert jedoch Erfahrung und permanentes Hinterfragen der getroffenen Annahmen. Analog den Enabling und Exploitation Practices für die agile Softwareentwicklung von Martin Fowler [41], können bei Lean UX nicht einfach die angenehmen Aspekte ausgenutzt werden, ohne die notwendigen Voraussetzungen dafür zu schaffen. Man muss sich also jederzeit exakt bewusst sein, welche Artefakte auf Annahmen basieren und darf nichts als gegeben ansehen, das weder validiert noch getestet ist. Während der Arbeit im Projektstress ist dieser Aspekt ausserordentlich schwierig im Auge zu behalten und bereitete den Autoren viele Probleme.

Innerhalb der zur Verfügung stehenden Projektzeit war es den Autoren dann auch nicht möglich bis zum Punkt von validierten Benutzergruppen und Anwendungsszenarien vorzudringen. Das Feld für potentielle Benutzergruppen konnte zwar im

[41] "Is Design Dead?," martinfowler.com. [Online]. Available: https://martinfowler.com/articles/designDead.html. [Accessed: 28-Jan-2019].

Verlauf der Experimente immer weiter eingegrenzt werden, jedoch ging viel Zeit für Tests mit für das Produkt nicht relevanten Benutzergruppen verloren. Am Ende konnten so auch nicht Personen aus allen potentiell relevanten Berufsgruppen für die Experimente rekrutiert werden. Erst damit wäre es möglich geworden, einen Fokus auf die vielversprechendsten Benutzergruppen zu legen und das Produkt entsprechend auszugestalten. Damit bleibt am Ende ein offenes, unvollständiges Feld von erhobenen, potentiell validen Benutzergruppen mit unterschiedlichem Potential für die spätere Nutzung des zu entwickelnden Produktes.

Damit ist Lean UX bei Weitem kein Patentrezept zur Entwicklung eines erfolgreichen Produktes. Wird es richtig angewendet kann es helfen, gute von schlechten Ideen zu unterscheiden und mit äusserst geringem Aufwand (sowohl zeitlich als auch finanziell) herauszufinden, welche Ansätze sich zur weiteren Ausarbeitung lohnen. Gleichzeitig wird die Benutzergruppe geschärft und somit auch der Anwendungskontext des Produktes immer klarer. Mit diesen erhobenen Daten werden auch die getroffenen Annahmen im Verlauf der Entwicklung zutreffender und können auf eine stabile Basis gestellt werden. Voraussetzung ist jedoch ein vernünftiger Startpunkt, insbesondere in Bezug auf die fokussierte Zielgruppe. Ansonsten bleibt es eine Frage der Ideologie, ob man Lean UX (sprich Prototyping und Testing) für einen validen Ansatz hält. Prinzipien aus dem Lean-Ansatz wurden implizit auch bereits im CAS Studiengang Requirements Engineering eingeführt [42]. Gemäss Insider Informationen soll Lean UX in den nächsten Jahren auch explizit Einzug in den Unterricht erhalten.

Schlussendlich ergibt sich für die Autoren folgendes Fazit aus dem Vorgehen nach Lean UX:

[42] T. Steimle, “HCI Technik - Einführung in User Research.” 2016.

Positiv	Negativ
Sinnvoller Ansatz wenn sowohl Problem- als auch Lösungsraum im Voraus nicht vollständig bekannt sind [43]	Schwierigkeit die richtigen Testpersonen zu rekrutieren, um relevante Erkenntnisse zu gewinnen
Probleme oder Ideen für Lösungsansätze lassen sich anhand von Prototypen viel einfacher kommunizieren und diskutieren, konkrete Varianten mindern Missverständnisse und unterschiedliche Interpretationen	Unterscheidung zwischen echten Erkenntnissen und Pseudo-Erkenntnissen aus Experimenten mit nicht relevanten Benutzergruppen
Sobald sich eine konkrete Benutzergruppe identifiziert und stabilisiert hat, bringen die Experimente schnelle und hochwertige Erkenntnisse zur Definition der Anforderungen und damit zur Ausarbeitung eines detaillierten Interaktionsdesigns	Valide Messkriterien zur Bewertung, ob eine Annahme gültig ist, sind schwierig zu definieren, insbesondere bei derart komplexen Produkten wie das vorliegende, oft ist man nur auf Rückmeldungen aus den Interviews oder auf Beobachtungen aus den Benutzertests angewiesen
Es können viele verschiedene Ideen schnell und mit minimal nötigem Aufwand getestet und gegeneinander verglichen werden	Permanentes Bewusstsein um die Existenz der aktuell bestehenden Annahmen notwendig
	Schwierigkeit herauszufinden wann eine Annahme wirklich validiert ist
	Designer-centered Ansatz vermeiden indem Ideen für Lösungsansätze bereits als Lösungen verkauft werden
	Jede Designentscheidung in einem Prototyp ist eine Hypothese, dabei ist es schwierig nur den Teil auszugestalten, der explizit als Hypothese formuliert wurde und geprüft werden soll

[43] B. at WordPress.com, “10 things I’ve learnt about lean startup,” We Love Lean – Lean startups, design, happiness and everything in between, 01-May-2013.

7.2 Projektreflexion

7.2.1 Organisation und Planung

Bereits vor dem Projektstart besprachen wir die Zusammenarbeit. Die 300 Projektstunden verteilten wir, mit Vorbehalt, auf gemeinsame Arbeitstage über die gesamte Projektdauer. Die Ferien waren dabei ausgeklammert. Mit dem Freitag konnte ein gemeinsamer, wöchentlicher Arbeitstag gefunden werden. Diese klare Abmachung sollte sicherstellen, dass die nötigen Arbeitsstunden gewährleistet werden können und der Organisationsaufwand für Termine reduziert wird.

Bei den ersten zwei Treffen mit den Stakeholdern im Mai 2018 wurde für uns spürbar, dass verschiedene Ansichten und Erwartungen hinter dem Ziel dieser Projektarbeit schlummerten. Die Auftraggeber gingen unausgesprochen davon aus, dass sie in Kürze ein Interaktionskonzept und Visual Designs (für bevorstehende Verkaufspräsentationen) erhalten würden und drängten uns bald zur Entwicklung erster Prototypen und Visual Designs. Wir wiederum versuchten mittels zeitintensiven Präsentationen aufzuzeigen, warum wir das Projekt nach erlerntem UCD Vorgehen durchführen möchten und dass wir dabei auch an Auflagen seitens der Hochschule gebunden sind. Dieser anhaltende Umstand führte im Juli 2018 beinahe zu einem Projektabbruch von unserer Seite her.

Dieser unglücklichen Ausgangslage geschuldet, investierten wir fast einen Drittel der wertvollen Projektzeit für Diskussionen und Überzeugungspräsenstationen gegenüber den Auftraggebern. Die finale Konsequenz daraus war ein Wechsel des Vorgehens und eine komplette Neuplanung, da das ursprünglich gewählte Vorgehensmodell plötzlich nicht mehr passte.

Im Team sind wir uns heute einig, dass wir bereits im Vorfeld, in der Phase der Projekteinreichung, das Projekt und den damaligen Projektstand beim Auftraggeber sauber hätten abklären sollen. Damit wäre uns auch bewusst geworden, wie gross und umfangreich dieses Vorhaben tatsächlich war und welche Auswirkung dies auf unsere bevorstehende Masterarbeit haben kann. Uns wäre bewusst geworden, dass die Entwicklung eines Interaktionskonzepts für ein hochsicheres Betriebssystem wie gapfruitOS vermutlich den vorgegebenen Projektrahmen und die Projektdauer von neuen Monaten sprengen würde. Mit diesem Bewusstsein hätten wir wahrscheinlich ein anderes Projekt oder von Anfang an einen anderen Vorgehensprozess für die Arbeit gewählt und unsere Projektziele auf den User Research beschränkt. Wir gingen zudem davon aus, dass es dem Auftraggeber klar ist, um was es in dieser Masterarbeit geht und wurden von der eher abgeneigten Einstellung gegenüber den erlernten Designprozessen nach UCD Vorgehen überrascht. Mit dieser Erfahrung würden wir heute bereits im Vorfeld der Projektabklärungen, einen kleinen Vortrag über Sinn & Zweck dieser Masterarbeit und die Anforderungen der HSR lancieren, um so alle Stakeholder abzuholen und Missverständnisse bezüglich unserer Arbeit aus dem Weg zu räumen.

7.2.2 Aufbau Domänewissen

Selbst die technisch versierten Autoren unter uns hatten ihre liebe Mühe, den Einstieg in die Domäne zu finden. Da sich das Projekt zu Beginn nur in Codezeilen und den Köpfen der Stakeholder abspielte und wir aufgrund der Geheimhaltung weder Konkurrenzprodukte noch Contextual Inquiry mit bereits bestehenden Benutzern «von ähnlichen Systemen» durchführen konnten, erschwerte uns den Einstieg in dieses Thema über einen längeren Zeitraum. Wir wurden einfach nicht warm. Durch diese Unsicherheit auf unserer Seite merkten wir zunehmend, dass die Auftraggeber versuchten, uns mit ihrer Denkweise zu beeinflussen und zu steuern. Mittels Online Recherchen versuchten wir uns in diese viel beschriebene aber unbestimmte Thematik einzulesen. Erst als wir aus Eigeninitiative Interviews und Diskussionen mit Experten aus der IT Security Branche führten, kam langsam Licht in das unbekannte Thema und das Volumen unserer Projektarbeit wurde deutlicher.

Die Methode Experteninterviews für Untersuchungen einzusetzen erwies sich als Goldwert. Durch den persönlichen Kontakt mit Spezialisten aus der Branche war es uns möglich, einen direkten und unabhängigen Zugang zu Unternehmen und deren Sichtweise bezüglich Usability und Sicherheit zu erhalten. Die Experten zeigten uns auch weitere, aus Sicht der Unternehmen relevante Einflüsse wie bspw. Kosten-Nutzen Verhältnis, Einführung, Umrüsten, u.s.w. bei der Beschaffung neuer Systeme in Betrieben auf. Diese Sicht konnten wir vom Auftraggeber nicht erhalten.

Zu diesen halbstrukturierten Interviews mit einem Leitfaden zu erscheinen half uns die Zügel in der Hand zu behalten, liess uns jedoch genügend Flexibilität auf Besonderheiten und Spezialitäten der Experten einzugehen und individuelle Informationen zu erfragen. Als ungeübte Protokollanten und der Komplexität des Themas geschuldet, haben wir bald auf die Aufzeichnung von Audio und Video (wenn erlaubt) umgestellt. Die anschliessende Transkription ist zwar aufwendiger, hat sich in unserem Projekt aber als sehr sinnvoll erwiesen, da wir über den gesamten Projektverlauf immer wieder auf verschiedene Stellen der Aufnahmen zurückgreifen mussten. Zudem liegt die Aufmerksamkeit damit voll und ganz bei den interviewten Personen und Gesprächen.

7.2.3 Teamarbeit

Wie in unserer Arbeitswelt üblich hatten wir in dieser Team Konstellation auch sehr kritische Momente zu bewältigen. Mit einer offenen Dialogkultur konnten wir die meisten Hürden meistern.

Den im Bericht erwähnten Projektabbruch hätten wir als eine grosse Stärke unseres Teams gewertet. Wie im wirklichen Leben auch, müssen unangenehme Entscheidungen, sofern sie begründet sind, getroffen werden. Damals im Juli 2018 wurde uns das Ausmass des Projekts und die daraus resultierenden Auswirkungen auf die uns zur Verfügung stehende Projektdauer bewusst. Unsere Auftraggeber und das Projekt selbst war noch nicht soweit fortgeschritten, dass die Problemstellung als Thematik für ein Masterarbeit im vorliegenden Rahmen passte. Nach unseren Einschätzungen hätte zu diesem Zeitpunkt eine gross angelegte Marktanalyse mit einer umfassenden User Research Phase stattfinden sollen. Bei einem Vorhaben mit der Komplexität dieses Betriebssystems müssten dazu vermutlich mindestens 3 Jahre investiert werden. Für uns bedeutete dies, dass wir nach neun Monaten Arbeit gerade mal erste «mögliche» Einsatzgebiete eines solchen Systems lokalisieren konnten.

Seit Beginn dieser Masterarbeit existierten unter uns zudem unterschiedliche Auffassungen, wie die anfallenden Arbeiten unter uns aufgeteilt werden sollten. Die Frage: «Ist die Masterarbeit dazu da, dass sich jeder noch etwas selber «erfinden» soll oder sollen die Aufgaben nach den Stärken der Autoren aufgeteilt werden?» konnte über die Projektdauer nicht zufriedenstellend geklärt werden. Innerhalb des Projekts wirkte sich das sogar zunehmend so aus, dass Aufgaben angenommen wurden (für die eine andere Person vermutlich geeigneter gewesen wäre) aber am Ende des Tages nichts geliefert wurde. Das führte auch dazu, dass Lieferobjekte aus Aufgaben anders als vorher abgesprochen innerhalb des Teams abgeliefert wurden. Solche Momente waren unnötige Belastungen in einem sowieso schon schwierigen Projektverlauf und raubten zusätzlich Zeit durch unnötige Diskussionen, die wir besser anderweitig hätten einsetzen können. Vor allem aber verminderte es eine fokussierte Projektsicht. Auch wir werden in einem nächsten Projekt, bewusst klare Aufgabenteilungen vornehmen, so wie wir es zum Ende hin, beim Schreiben dieses Berichtes, tatsächlich getan haben.

7.2.4 Schlusswort

Am Ende des Tages durften wir, allen Schwierigkeiten zum Trotz, eine sehr spannende und lehrreiche Zeit erleben mit vielen interessanten Personen und Themen in einem uns unbekannten Gebiet. Leider erst jetzt ganz am Ende des Projektes fühlen wir uns in der Thematik Usable Security langsam angekommen und bedauern beinahe das Projektende. Es fühlt sich so an, als ob nach dem Abschluss einer mühsamen Vorarbeit das Projekt gapfruitOS von nun an endlich auf der von uns erarbeiteten Basis fokussiert und richtig vorwärts gehen könnte.

8 Referenzen und Literatur

8.1 Bücher und Publikationen

[1] «Angriffsvektor», Wikipedia. 17-Feb-2014.

[2] «Security through compartmentalisation», 2004.

[3] «What is a Distributed Denial-of-Service (DDoS) attack?», Cloudflare. [Online]. Verfügbar unter: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/. [Zugegriffen: 26-Dez-2018].

[4] Differences between a GPOS (Normal OS) and an RTOS (Real Time OS)», Electronic Circuits and Diagrams-Electronic Projects and Design, 12-Juni-2012. [Online]. Verfügbar unter: http://www.circuitstoday.com/gpos-versus-rtos-for-an-embedded-system. [Zugegriffen: 20-Juli-2018].

[5] «Hardening (computing)», Wikipedia. 31-Dez-2018.

[6] «Trojanisches Pferd (Computerprogramm)», Wikipedia. 30-Sep-2018.

[7] «Virtualisierung und Software für virtuelle Maschinen».

[8] «IDC Studie zu Next Gen Endpoint Security in deutschen Unternehmen: Gefahr erkannt, aber nicht gebannt». [Online]. Verfügbar unter: https://idc.de/de/ueber-idc/press-center/64840-idc-studie-zu-next-gen-endpoint-security-in-deutschen-unternehmen-gefahr-erkannt-aber-nicht-gebannt. [Zugegriffen: 25-Juli-2018].

[9] M. Zacher, «Next Gen Endpoint Security in Deutschland 2017».

[10] «iX extra: Endpunkt-Sicherheit», März 2014.

[11] «Human Error Accounts for Over 95% of Security Incidents, Reports IBM», The Duo Security Bulletin. [Online]. Verfügbar unter: https://duo.com/blog/human-error-accounts-for-over-95-percent-of-security-incidents-reports-ibm. [Zugegriffen: 20-Juli-2018].

[12] «Whitepaper Angriffsziel Endpoint», 2010.

[13] C. Cooper, «The rise and rise of Cybercrime as a Service», CSO Online, 27-Juli-2017. [Online]. Verfügbar unter: https://www.csoonline.com/article/3205253/data-breach/the-rise-and-rise-of-cybercrime-as-a-service.html. [Zugegriffen: 20-Juli-2018].

[14] McAfee, «Economic Impact of Cybercrime 2017», Februar 2018, S. 28.

[15] Cybersecurity Ventures und S. Morgan, «2017 Cybercrime Report».

[16] Ponemon Institute und Accenture, «Cost of Cybercrime Study 2017».

[17] T. Steimle und D. Wallach, Collaborative UX Design, 1. Aufl. dpunkt, 2018.

[18] Problem Statement. [Online]. Verfügbar unter: http://collaborative-uxdesign.com/scoping/problem-statement. [Zugegriffen: 10-Jan-2019].

[19] «Desktop Neo – rethinking the desktop interface for productivity.»

[20] «The Design Sprint — GV». [Online]. Verfügbar unter: http://www.gv.com/sprint/. [Zugegriffen: 01-Jan-2019].

[21] J. Knapp, J. Zeratsky, und B. Kowitz, Sprint: How to solve big problems and test new ideas in just five days.

[22] C. Hauri und U. Suter, «Interviewtechnik». CAS Requirements Engineering 2016. Rapperswil: HSR Hochschule für Technik Rapperswil.

[23] C. Hübscher, «Skript Vorgehensmodelle: User Centered Design 1». CAS Requirements Engineering 2016. Rapperswil: HSR Hochschule für Technik Rapperswil.

[24] C. Hübscher, «Skript Vorgehensmodelle: User Centered Design 2». CAS Interaction Design 2017 Rapperswil: HSR Hochschule für Technik Rapperswil.

[25] A. Cooper, R. Reimann, D. Cronin, und C. Noessel, About Face, Fourth Edition

[26] A. Cooper, «The Endless Battle», Alan Cooper, 22-Okt-2017

[27] J. Gothelf und J. Seiden, Lean UX - Applying Lean Principles to Improve User Experience, 16. Aufl. O'Reilly Media.

[28] C. Hübscher, «Slides Vorgehensmodelle: User Centered Design Grundlagen». CAS Requirements Engineering 2016. Rapperswil: HSR Hochschule für Technik Rapperswil.

[29] «Oracle VM VirtualBox». [Online]. Verfügbar unter: https://www.virtualbox.org/. [Zugegriffen: 15-Jan-2019]

[30] J. Gothelf und J. Seiden, Lean UX - Applying Lean Principles to Improve User Experience, 16. Aufl. O'Reilly Media.

[31] J. Benedek und T. Miner, «Measuring Desirability: New methods for evaluating desirability in a usability lab setting».

[32] «Using the Microsoft Desirability Toolkit to Test Visual Appeal». [Online]. Verfügbar unter: https://www.nngroup.com/articles/microsoft-desirability-toolkit/. [Zugegriffen: 17-Jan-2019].

[33] «Emotional response cards: a simple user research tool / nForm / Blog». [Online]. Verfügbar unter: https://web.archive.org/web/20120531231540/http://nform.com/blog/2012/05/emotional-response-cards-simple-user-research-tool. [Zugegriffen: 17-Jan-2019].

[34] «Getting all emotional with BERT», UXM, 30-Juni-2010.

[35] A. Cooper, The Inmates Are Running The Asylum, 1. Aufl. Sams - Pearson Education, 1999.

[36] «Putting A/B Testing in Its Place», Nielsen Norman Group. [Online]. Verfügbar unter: https://www.nngroup.com/articles/putting-ab-testing-in-its-place/. [Zugegriffen: 23-Jan-2019].

[37] https://www.nngroup.com/articles/icon-usability/

[38] Aussage von Philipp Murkowsky, Puzzle ITC am WUD2018 – https://www.youtube.com/watch?v=VeyjKz3NDKE&feature=youtu.be

[39] https://www.infocall.ch/index.php/software/madabawin/2-uncategorised/59-avotime

[40] H. Beyer und K. Holtzblatt, Contextual Design: Defining Customer-Centered Systems, 1. Aufl. Morgan Kaufmann.

[41] "Is Design Dead?," martinfowler.com. [Online]. Available: https://martinfowler.com/articles/designDead.html. [Accessed: 28-Jan-2019].

[42] T. Steimle, "HCI Technik - Einführung in User Research." 2016.

[43] B. at WordPress.com, "10 things I've learnt about lean startup," We Love Lean – Lean startups, design, happiness and everything in between, 01-May-2013.

8.2 Abbildungsverzeichnis

9 Anhang

Kick-Off Protokoll - MT 2018/19 - Gruppe 08

Projekt:	Security focused OS
Datum:	04. Mai 2018
Ort:	Baarerstrasse 135, 6300 Zug
Anwesende:	Auftraggeber (gapfruit AG), Christian Heusser, Aaron Wyder, Adrian Schmid, Daniel Crvelin

Produktbezogene Themenpunkte

Allgemein

- Mitarbeiter von gapfruit AG haben in der Vergangenheit bereits ein ähnliches Produkt entwickelt
- Sichere OS werden praktisch immer nur zusammen mit Hardware verkauft, gapfruit AG will nur OS ohne Hardware verkaufen
- Ziel von gapfruit AG: “sicheres OS für alle (nicht nur für Regierungen und Behörden)”
- Zielpublikum von gapfruit AG sind Firmen
- Erste Testkunden stammen aus Energie- und Finanzbranche

Security-Aspekte

- 2015 Schaden durch Cybercrime: 3 Billionen $
- 2016 Schaden durch Cybercrime: 6 Billionen $
- schwächstes Glied in der Kette ist immer der Mensch

MVP und Release

- MVP Release geplant für Ende Juli 2018
- First Release geplant für Mai 2019
- MVP testen mit bisher zwei Testkunden
- MVP beinhaltet:
    - Host OS mit 2 Guest OS => zwei Sicherheitszonen: “Work Zone” und “Internet Zone”
    - Benutzer kann zwischen Zonen switchen
    - Benutzer kann in Fullscreen Modus schalten

Projektbezogene Themenpunkte

Probanden

Eine angeheizte Diskussion löste das Thema User Research aus, insbesondere der Zugang zu Kunden. Der Auftraggeber steht in Kontakt mit Unternehmen die als Pilotkunden fungieren, zieht es jedoch vor, diese aus dem User Research herauszuhalten. Als Alternative stellt gapfruit AG Probanden aus dem Kreise der Bekanntschaft zur Verfügung.

Vorgehen

Ein weiterer Eindruck, der aus dem Gespräch mitgenommen wurde, war die starke Tendenz des Auftraggebers sein Augenmerk bereits auf die Lösung zu legen. Dies sorgte beim Projektteam insofern für Argwohn, da wesentliche Phasen einer nutzerzentrierten Entwicklung ausgeklammert wurden. Es war deutlich ersichtlich, dass die GUI Gestaltung im Zentrum seines Interesses stand, ohne diese jedoch auf die Basis erhobener Nutzeranforderungen zu stellen, sondern vielmehr auf die von eigenen Mutmassungen, die sich aus dem Konzept Ihres Produktes ableiteten.

Marktanalyse und Know-how Transfer MT 2018/19 - Gruppe 08

Projekt:	Security focused OS
Datum:	24. Mai 2018
Ort:	Baarerstrasse 135, 6300 Zug
Anwesende:	Auftraggeber (gapfruit AG), Christian Heusser, Aaron Wyder, Adrian Schmid, Daniel Crvelin

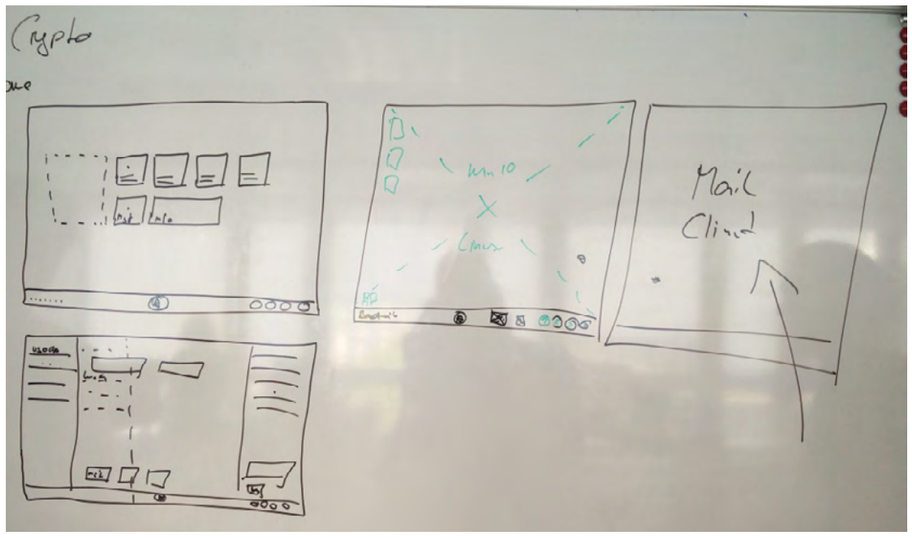
Allgemein

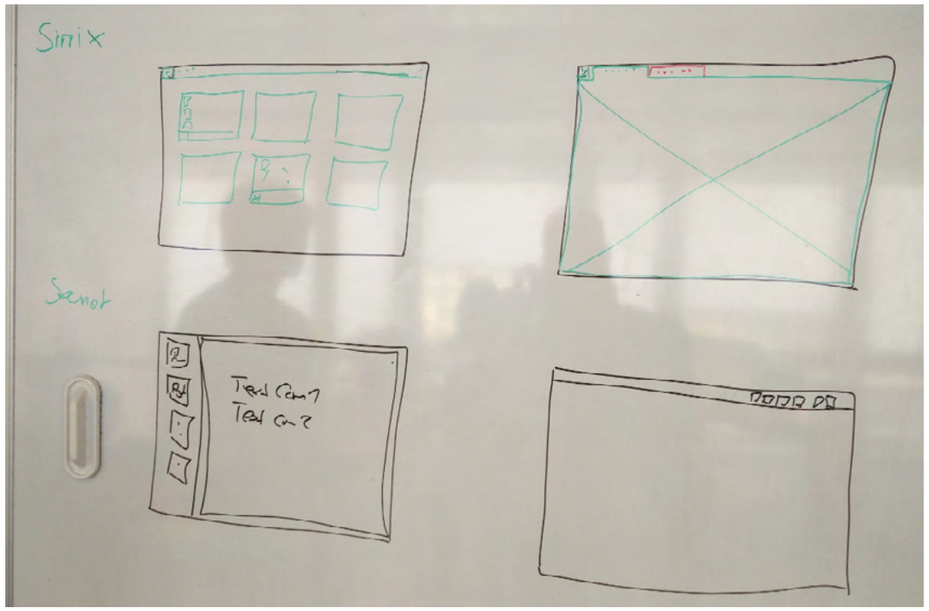
- gapfruit OS basiert auf Microkernel-Architektur mit beliebig vielen virtualisierten Gastsystemen und später auch nativen Apps (= Compartements = Sicherheitskontexte = Aktivitäten)
- Ein derartiges Konzept existiert bisher nur für Behörden und Regierungen und wird nicht im Business-Kontext eingesetzt

Ähnliche Produkte und andere Hersteller

Hard- und Software für Regierungen & Behörden (nicht einsehbar für Projektteam):

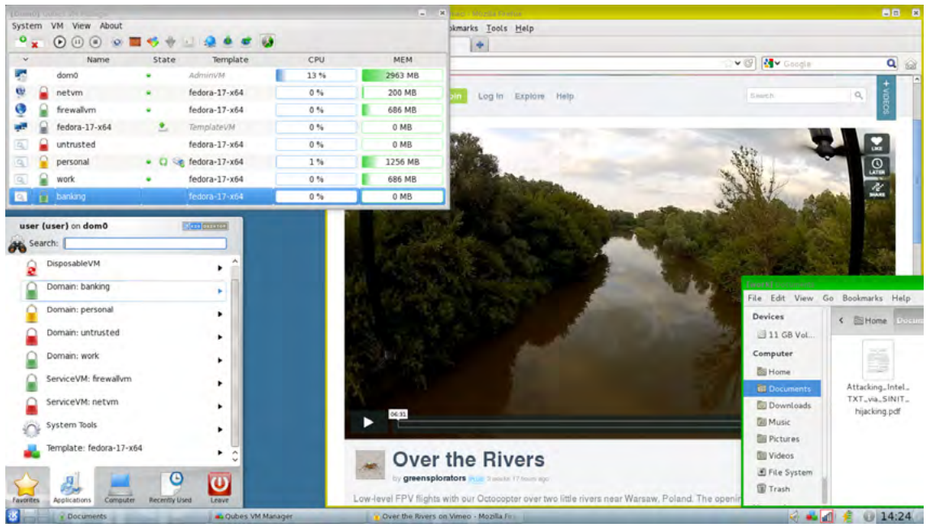
- Crypto cOffice (kein Datentransfer zw. Zonen möglich)
- Secunet SINA (kein Datentransfer zw. Zonen möglich) --> Webseite
- Sirrix TrustedDesktop (kein Datentransfer zw. Zonen möglich) --> Webseite
- General Dynamics --> Webseite
- Genua Security Laptop cyber-top --> Webseite





Open Source (Community-driven):

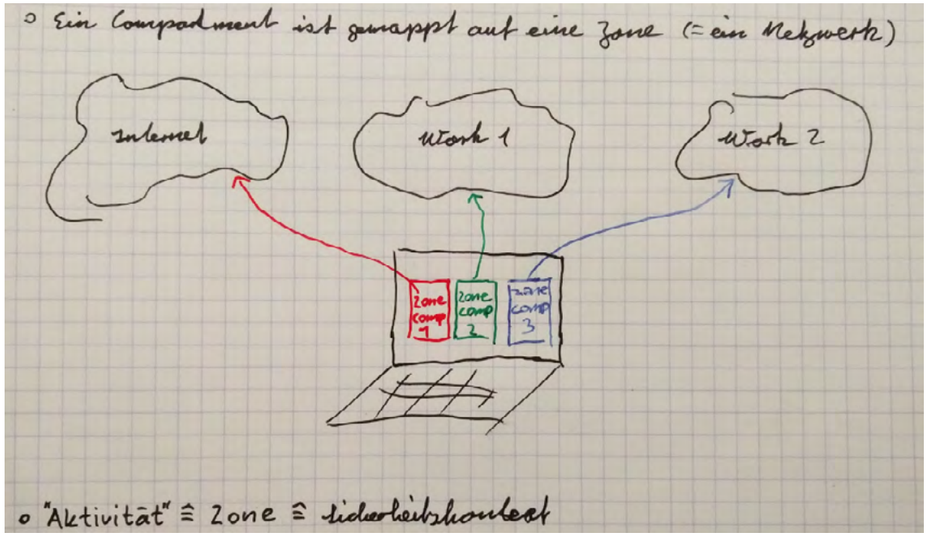
- Qubes OS (Datentransfer zw. Zonen möglich, aber sehr umständlich, technisch orientiert und für Laien praktisch unverständlich)



Quelle: Wikipedia

MVP und Release

- MVP Release geplant für Ende Juli 2018
- First Release geplant für Mai 2019
- MVP testen mit bisher zwei Testkunden
- MVP beinhaltet:
  - Host OS mit 2 Guest OS => zwei Sicherheitszonen: “Work Zone” und “Internet Zone”
  - Benutzer kann zwischen Zonen switchen
  - Benutzer kann Daten zwischen Zonen austauschen
  - Benutzer kann in Fullscreen Modus schalten



Nächste Schritte

- Nutzungs-Szenarien ausarbeiten
- Interviews mit Security Spezialisten

Coaching Protokoll - MT 2018/19 - Gruppe 08

Projekt:	Security focused OS
Datum:	08. Juni 2018
Ort:	Förrlibuckstrase 181, 8005 Zürich
Anwesende:	Christian Heusser (Coach), Aaron Wyder, Adrian Schmid, Daniel Crvelin

Vorbemerkung

Aus dem bisherigen Verlauf des Projektes haben sich erhebliche Problemzonen manifestiert, die ein ordnungsgemäßes Fortführen des Projektes ins Stocken gebracht haben. Diese zwingen das Projektteam dazu ihren Fokus auf die Erarbeitung eines Massnahmenkatalogs zur Bewältigung dieser Schwierigkeiten zu legen. Im Folgenden ein kurzer Überblick der Problemstellungen mit denen sich Projektteam konfrontiert sieht:

- Auftraggeber kann dem Projektteam keinen Zugang zu potentiellen Anwendern stellen und nimmt die Position ein; „Alle Personen sind die Zielgruppe“
- Auftraggeber teilt nicht die gleiche Auffassung bezüglich der Notwendigkeit einer eingehenden User Research Phase und stellt den Mehrwert einer solchen in Frage.
- Nach 2 mit dem Auftraggeber durchgeführten Workshops, stellen 3 sehr generische Anwendungsfälle das einzige handfeste Ergebnis dar. Dabei handelt es sich um:
    - Navigation zwischen den unterschiedlichen Sicherheitskontexten (das sich im Wesentlichen auf ein Screen-Switch Feature zwischen den VM‘s beschränkt)
    - Datentransfer zwischen den unterschiedlichen Sicherheitskontexten (Kopieren über eine Zwischenablage, mit automatisiertem Viren-Scan)
    - System-Benachrichtigungen (Notifications) an den User über die unterschiedlichen Sicherheitskontexte hinweg.

Die Meinungsverschiedenheiten in Bezug auf Vorgehen und Prioritäten sorgen zunehmend für ein angespanntes Klima zwischen Projektteam und Auftraggeber. Darüber hinaus stellt sich dem Projektteam die Frage, ob die bisher identifizierten Anwendungsfälle ausreichend für den Umfang einer Masterarbeit sind. Daher wurde folgende Agenda zur Begutachtung mit dem Coach zusammengestellt:

- Definition Interaktionskonzepte (https://creativschmid.myDS.me:10003/d/f/436740252690817135)
- Dokumentation identifizierter Projektrisiken (https://creativschmid.myDS.me:10003/d/f/436740253649215603)
- Skizzierung möglicher Optionen für das weitere Projektvorgehen:
    1. Annahme Kunde werden nicht validiert, ohne Research, direkt in UI-Designphase
    2. Annahme Kunde durch Validierung von Ziel-, Nutzergruppen und Kontextszenarien erheben, durch z. Bsp.: Interviews, Affinity Diagram Clustern
    3. Wie Punkt 2 mit zusätzlichem User Research für Persona (Aufwand) (https://creativschmid.myDS.me:10003/d/f/436740253638729841)

Traktanden

1. Positionierung gegenüber Auftraggeber

Diskussionspunkte:

- Wie ist damit umzugehen wenn das eine oder andere mögliche Szenario mit dem Kunde eintreffen sollte (bspw. Abbruch der Zusammenarbeit)
    - Christian erzählt über andere (ähnliche) Projektabläufe
    - Schulanforderung an die MAS Projektarbeit (in einem genannten Szenario) muss Christian erst über Markus klären
    - Es herrscht zu diesem Zeitpunkt Unstimmigkeit innerhalb des Projektteams in Bezug auf das weitere Vorgehen.
- Team verzettelt sich, weil keine Vorgaben und keine Ziele für das Team ersichtlich sind
- Im schlechteren Fall soll das Projektziel, unabhängig vom Kundenziel, durch das Projektteam neu definiert werden.

Fazit, Beschlüsse:

- Team erarbeitet für das bevorstehende Eskalationsmeeting eine Präsentation. Darin enthalten ist:
    - warum wir nicht nur auf Basis von Annahmen des Auftraggebers fortfahren können
    - verfeinerter Projektplan mit Lieferobjekten
    - Wichtigkeit eines Vorgehens nach UCD (und dessen Stellenwert für das Projektteam in Bezug auf die Masterarbeit
    - Ausschnitte/erste Erkenntnisse aus den Interviews aufzeigen

2. Experten-Interviews

Diskussionspunkte:

- Um auch Input aus unvoreingenommenen Quellen einzuholen, hat sich das Projektteam entschieden halb-strukturierte Interviews mit IT-Security Experten durchzuführen. Das Projektteam erhofft sich, aus diesen Gesprächen neue Perspektiven zu erhalten, die mögliche Anhaltspunkte für einen Ausweg aus der gegenwärtigen Situation bieten.

Fazit, Beschlüsse:

- Interviews werden mit 2 IT-Spezialisten des Unternehmens Zühlke und einem IT-Fachexperten der Skyguide durchgeführt
- Erstellung eines Interview-Leitfadens

Coaching Protokoll - MT 2018/19 - Gruppe 08

Projekt:	Security focused OS
Datum:	27. Juli 2018
Ort:	Wiesenstrasse 5, 8952 Schlieren
Anwesende:	Christian Heusser (Coach), Aaron Wyder, Daniel Crvelin
Entschuldigt:	Adrian Schmid,

Vorbemerkung

Die im nachfolgenden aufgeführten Traktanden gingen aus einer mit dem Auftraggeber durchgeführten Revision des Projektauftrags hervor. Anlass zu dieser Begutachtung und Reflexion mit dem Auftraggeber gaben Erkenntnisse die das Projektteam aus Interviews mit IT-Spezialisten und Sicherheitsexperten gewonnen hatte. Aus deren Ausführungen ging hervor, dass es sich bei vorliegendem Produkt um ein sehr technisch ausgeprägtes Nischenprodukt handle, dessen potentielle Anwendergruppe aus sehr dedizierten Personen bestehe. Da bereits von Seiten Auftraggeber kein Zugang zu potentiellen Anwendern gestellt werden konnte (siehe Coaching Protokoll vom 08.Juni), sah sich das Projektteam mit der prekären Situation konfrontiert, keinen ausreichenden User Research betreiben zu können. Zumindest nicht im Rahmen der bis dahin ausgelegten Aufgabenbeschreibung.

Die Bedenken wurden dem Auftraggeber vorgelegt. In der Folgediskussion kamen Aspekte der Produktvision zur Sprache, die Einblicke in die langfristige Zielsetzung des Auftraggebers bot. Diese Vision führt weg von virtualisierten Gastsystemen hin zu nativen Apps mit einem jeweils eigenen, abgetrennten Sicherheitskontext. Im Rahmen dieser Vision stellt der Auftraggeber auch die Tauglichkeit der derzeit immer noch allgegenwärtigen Desktop-Metapher in Frage. Als Präzedenz führt er Interaktionsparadigmen an, die sich aufgrund der in jüngster Vergangenheit weit verbreiteten Anwendung von mobilen Endgeräten (Smartphones und Tablets) fest etabliert haben. Aus diesen neu gewonnenen Einblicken gehen die nachfolgend aufgeführten Diskussionspunkte hervor.

Traktanden

---

1. Verlagerung des Projektfokus und Anpassung der Aufgabenstellung

Diskussionspunkte:

- Darlegung der revidierten Aufgabenstellung:
  - Analyse der Praktikabilität einer Desktop-Metapher in Bezug auf Arbeitsweisen des heutigen Arbeitsalltags, mit Blick auf das vom Produkt unterstütze zonenbasierte Konzept.
  - Aspekte technischer Limitationen und Wirtschaftlichkeit werden im weiteren Projektverlauf ausgeklammert.

Fazit, Beschlüsse:

- Mit dem Auftraggeber detaillierter erörtern, warum dieser die bestehende Desktop Metapher hinterfragt.
- Mögliche Hypothesen für Projekt:
  - Mit herkömmlicher Desktop Metapher ist Sec OS Konzept unverständlich zum Bedienen → Validität Testen
  - Veränderte Arbeitsabläufe durch Sicherheitskonzept (Zonen/Aktivitäten Wechsel für unterschiedliche Tätigkeiten) ist mit gängiger Desktop Metapher nicht zufriedenstellend lösbar, daher hinterfragen und neue Konzepte einführen.
- Potentielle Schwierigkeit für neue Konzepte: die Leute haben sich bereits so stark an bestehendes gewöhnt, dass neues möglicherweise nicht akzeptiert wird → Wie testen, um diesen Effekt zu minimieren?
  - Wichtigkeit eines Vorgehen nach UCD (und dessen Stellenwert für das Projektteam in Bezug auf die Masterarbeit
  - Ausschnitte/erste Erkenntnisse aus den Interviews aufzeigen

---

2. Wechsel des Vorgehensmodells

Diskussionspunkte:

- Wechsel des Vorgehensmodells von Goal Directed Design zu Lean-UX
  - Die Änderung des Projektfokus zieht eine drastische Verlagerung der Zielgruppe nach sich, von zu Beginn sehr spezifische, kleine und schwer zugängliche Zielgruppe zu offen und mit allen testbar (positiver Effekt → Hallway Test)
  - Dieses Vorgehen ergänzt sich ausserdem mit demjenigen des Auftraggebers → Lean Start-Up. Daraus können sich mögliche Synergien ergeben.
  - Um Konzepte in schneller Abfolge erzeugen und testen zu können erscheint ein hypothesen-getriebenes Vorgehen zum gegenwärtigen Zeitpunkt des Projektstandes zielführender, im Vergleich zu der Durchführung ausgedehnter Phasen des GDD Modells.

Fazit, Beschlüsse:

- Für das weitere erfolgreiche Projektvorgehen ist es wichtig:
  - keine unverifizierten Behauptungen im Raum stehen zu lassen.
  - nicht nur Annahmen treffen und es dabei belassen, sondern diese auch testen und validieren
- Begründung für den Wechsel des Vorgehensmodells muss Eingang in den Bericht finden und dort nachvollziehbar erläutert werden.
- Eine nachvollziehbare Erläuterung muss auch im Hinblick auf die Erarbeitung der Proto-Personas und deren Verfeinerung zu Personas erfolgen. Bspw. wie erfolgte deren Auswahl und nach welchen Kriterien wurde in Primäre-, Sekundäre- und Non-Personas unterteilt.
- Recherche ausweiten auf die Analyse von Non-Desktop Betriebssysteme wie bspw. iOS 11 (Split-Screen, File Management).

---

3. Allgemeines

Tipps für Projektbericht:

- Methoden begründen warum eingesetzt, pro/contra von Alternativen
- Begründung für Wechsel von Goal Directed Design zu Lean UX begründen

Auftraggeber Meeting «Research Desktop Metapher» Protokoll - MT 2018/19 - Gruppe 08

Projekt:	Security focused OS
Datum:	17. August 2018
Ort:	Baarerstrasse 135, 6300 Zug
Anwesende:	Sid Hussmann, Roman Iten, Christian Kielmann, Adrian Schmid, Daniel Crvelin, Aaron Wyder
Entschuldigt:	-

Vorbemerkung

Auf die Anpassung des Projektauftrags folgte eine Neuausrichtung des Teams und eine Änderung des Vorgehensmodells von Goal directed Design zu Lean UX. Im Rahmen des neuen Fokus auf die Desktop-Metapher wurde Forschung zu alternativen bzw. innovativen Konzepten zur Umsetzung des hochsicheren Betriebssystems vorgenommen. Die Resultate aus den Untersuchungen wurden gemäss den Paradigmen von Lean UX in Annahmen zum Umgang von Anwendern mit dem Betriebssystem überführt. Aus diesen Annahmen erstellten das Team unabhängig voneinander erste Wireframes und generierte unterschiedliche Ideen für Prototypen.

Sowohl die Resultate aus der Forschung wie auch die Wireframes wurden dem Auftraggeber präsentiert und kontrovers diskutiert. Aus diesen ersten Sketches konnte der Fokus weiter geschärft und die Marschrichtung für die nächsten Iterationen festgelegt werden.

Traktanden

---

1. Einstieg und offene Fragen

Fragen:

Auf welche Endgeräte konzentriert sich gapfruit OS?

Antwort: Von Tablets „aufwärts“, keine Mobiltelefone, Touch Bedienung ist ein Thema

Was ist die Motivation von gapfruit die klassische Desktop Metapher zu hinterfragen?

Antwort: Kein prinzipielles Hinterfragen, aber neue Ideen und Alternativen zu Bestehendem untersuchen und zur Optimierung verwenden wo sinnvoll; gapfruit OS mit Host und beliebig vielen virtuellen Gastsystemen bzw. Apps führt zu weiterer Hierarchie Stufe => OS in OS = Inception

---

2. Präsentation der Forschungsergebnisse und Prototypen

Diskussionspunkte:

- Prinzip Sandboxing wie in sicherer Mobile Messaging App „Signal“, werden bspw. Bilder versendet sind diese nicht ohne weiteres im Dateisystem des Mobile Betriebssystems verfügbar, sondern nur innerhalb der App Sandbox. Will der Anwender das Bild ausserhalb des App Kontextes weiterverwenden, muss er es explizit „herunterladen“ und im Dateisystem des Betriebssystems abspeichern.
- Limitationen der bestehenden Desktop Metapher im Vergleich zum realen, physischen Arbeitstisch
  - Dateisystem bei der Desktop-Metapher, inspiriert vom Aktenschrank, erlaubt es Dokumente hierarchisch mit beliebig tiefer Verschachtelung abzulegen. In der physikalischen Realität ist ein Aktenschrank in einem Aktenschrank eher unüblich
- Braucht es überhaupt noch eine Unterscheidung zwischen Apps und Files?
- Tagging auch für Klassifikation von Dateien verwenden
  - mittels Policies und manuell
- Aktivitäten vs. Zonen => vermutlich sind Aktivitäten oft zonenübergreifend, bspw. Internet Recherche
- Gute Ansätze aus den Prototypen:
  - vorgegebene Screen Split Patterns via Button einfach Auswählen und herstellen
  - Auswahl der Screen Split Patterns adaptiv (responsive) zu Monitorgrösse, wenn mehrere Screens für jeden eine eigene Konfiguration wählbar
  - System merkt sich Position der Apps innerhalb des Screen-Split-Patterns und stellt diese auf die selbe Weise beim erneuten Öffnen wieder her
  - Möglichkeit meist genutzte App direkt in Split Area zu öffnen falls mehr Areas als offene Apps aktiv sind

Fazit, Beschlüsse:

- Priorität und Fokus auf Window und File Management legen
- Konzepte von Tiling Window Manager weiterverfolgen
  - automatisches Arrangieren von Fenstern
  - vorgegebene/konfigurierbare Layouts für Fenster Arrangement
  - welche Layouts machen auf welchen Auflösungen bzw. Gerätegrössen Sinn
  - adaptive Layouts, je nach Grösse des Monitors, was muss bspw. beim Anschliessen eines externen Monitors geschehen, etc.
- Tagging Konzepte für File Management weiterverfolgen
  - Ideen für kombiniertes Dateisystem aus allen VMs ausarbeiten, Ziel: möglichst flache Hierarchie, kein mühsames Hin- und Her-Kopieren von Dateien zwischen Dateisystemen der unterschiedlichen VMs
  - Möglichkeiten für automatisches, allenfalls intelligentes Tagging von Dateien ausloten
  - Klassifizierung von Dateien abhängig von Zone bzw. konfigurierten Policies innerhalb der Zonen oder manuelle Klassifizierung
  - Effekt der Klassifizierung auf die Behandlung der jeweiligen Dateien innerhalb des Dateisystems

---

4. Präsentation gapfruit OS Prototyp

- Präsentation des aktuellen Entwicklungsstandes von gapfruit OS
- Prototyp hat ein Control Center und kann Apps bzw. virtuelle Maschinen im Full- und Split-Screen-Modus auf jeweils voller Höhe darstellen
- Noch kein Sicherheitsmerkmal eingebaut

---

3. Allgemeines und nächste Schritte

- Ideen für Prototypen konsolidieren und weiter ausarbeiten
- Testszenario erstellen und Probanden für erste User Tests rekrutieren
- A/B Testing planen für gapfruit OS Fake mit Standard-Konzepten vs. Prototyp
- Workshop zum Thema „File Tagging” durchführen (Vorbereiten Konzept Synology NAS und andere Tagging File Manager)

Coaching Protokoll - MT 2018/19 - Gruppe 08

Projekt:	Security focused OS
Datum:	25. August 2018
Ort:	Oberseestrasse 10, 8640 Rapperswil
Anwesende:	Chri Hübscher, Adrian Schmid, Daniel Crvelin, Aaron Wyder
Entschuldigt:	-

Traktanden

1. Besprechung Projektsituation (Wechsel auf Lean UX)

Diskussionspunkte:

- Konkrete und detaillierte Use Cases mit allen Spezialfällen Datentransfer/Klassifizierung, was geht, was nicht, wie kann das dem Benutzer verständlich gemacht werden, Navigation über VM Grenzen
  - Was geschieht, wenn File aufgrund Klassifizierung nicht transferiert werden darf?
  - Was geschieht, wenn File nicht sicher ist und nicht transferiert werden darf?
  - Wie funktioniert der Virencheck bzw. wie wird dieser dem Benutzer verständlich gemacht?
- Fragestellung des Projektes ist ein riesen Thema und gibt locker genügend her für eine Masterarbeit
- Proto-Persona sind okay, es muss aber klar argumentiert werden warum es keine andere Möglichkeit gab:
  - Gültig wenn wir argumentieren, dass keine Unterstützung durch Auftraggeber, daher nicht möglich User Research gemäss gewöhnlichem Persona Ansatz durchzuführen (Cooper, Goodwin)
  - Muss für Zuhörer/Leser klar werden, Fragen vorwegnehmen und klar präsentieren
  - Im Bericht erwähnen, dass es uns bewusst ist, dass man eigentlich anders vorgehen müsste --> Empfehlung an den Auftraggeber die Proto-Persona zu validieren
  - Bei Resultaten "Delta" beschreiben, nicht mit richtigen User getestet
  - Ist nur Simulation, Empfehlung an Auftraggeber für Tests mit realen Usern danach
- Empfehlung Cognitive Walkthrough mit UX-Experten durchführen um verschiedene Ansätze bezüglich Window/File Handling zu testen
  - Dani --> UX-Champion
  - Adi --> UX Menschen Swisscom
  - Aaron --> Markus F.
- Bei Lean UX ist es wichtig saubere Hypothesen aufzustellen, zu priorisieren und diese dann zu prüfen
  - Annahmen basierend auf User Ziele definieren, mit Blick auf das Interaction Design
- Lean UX Teil mit MVP können wir nicht leisten --> keine Implementation, nur Prototyp
  - Muss gut erläutert werden
  - Nur bis Stufe MVP Prototyp
  - Hypothesen und Annahmen Teil wird vor allem verwendet
- Analysieren was es schon gibt und adaptieren
  - Virenscanner, Quarantäne, etc.
  - Existierende VMs, Parallels, Virtualbox, VM Ware, etc.
  - File Tagging
- Idee: Leute, die bereits im Virtualisierungsbereich gearbeitet haben interviewen
  - Betreibern Webseite mprove.de
  - Anbieter von Remote Desktop Umgebungen für Treuhänder (Martin A.)

Fazit, Beschlüsse:

- Nicht gesamte Metapher hinterfragen, da bereits 30 Jahre Forschung auf diesem Gebiet existieren und wir damit nicht "mithalten" können im Rahmen der Arbeit, stattdessen gewisse Konzepte hinterfragen und aus bestehenden Ideen bessere Möglichkeiten suchen
  - Mehr auf bestehende Lösungen abstützen anstatt gesamte Desktop Metapher hinterfragen
  - Was können wir an bestehenden Lösungen noch verbessern bzw. Wie kombinieren im Rahmen unseres Projekts
  - Vor- und Nachteile evaluieren, evtl. Cognitive Walkthrough mit UX Experten
- Problematiken im Bericht hervorheben die hauptsächlich zur Hinterfragung bestehender / festgefahrener Konzepte aus der Desktop Metapher geführt haben:
  - Window Management "Inception"
  - File Management Problematik, pro VM ein abgetrenntes File Management
- Besprochene Punkte mit Christian Heusser durchgehen und weiter wie geplant
  - Sind uns bewusst bezüglich existierendem Research und Herausforderungen
  - Anzahl Use Cases --> komplex und anspruchsvoll
  - CC an Coach und Chri Hübscher

Coaching Protokoll - MT 2018/19 - Gruppe 08

Projekt:	Security focused OS
Datum:	31. August 2018
Ort:	Wiesenstrasse 5, 8952 Schlieren
Anwesende:	Christian Heusser (Coach), Adrian Schmid, Daniel Crvelin, Aaron Wyder
Entschuldigt:	-

Traktanden

1. Retrospektive Meeting mit Chri Hübscher

Diskussionspunkte:

- Diskussion über Stand und Meeting mit Chri

Fazit, Beschlüsse:

- Weiter wie geplant unter Berücksichtigung der besprochenen Punkte

2. Weiteres Vorgehen

Diskussionspunkte:

- Fragebogen mit Mitarbeitern / Kollegen über Nutzungsszenarien Computer im täglichen Arbeitsalltag (Aufgaben, parallele Interaktion mit verschiedenen Tools, Security Affinität)
- Wichtig User Tests starten und in iterativen Lean UX Prozess gelangen: Think – Make – Check
- sollte Kunde den Tests, bzw. den Testresultaten widersprechen und sich für schlechtere / andere Design Variante entscheiden als User Tests ergeben existieren zwei Möglichkeiten, entweder Kundenwunsch respektieren und in Bericht begründen oder andere Richtung einschlagen mit Risiko, dass Auftraggeber nicht mitzieht
- A/B Testing als Methode ausprobieren um verschiedene Ansätze gegeneinander abzuwägen
- Bewährtes Vorgehen bei Dokumentation von Methoden aus anderen Arbeiten, erleichtert Lesefluss und nimmt Fragen warum bestimmte Methoden angewendet wurden vorweg:
  - Methode beschreiben
  - Alternativen aufzählen
  - Begründung warum diese Methode angewendet wurde
- Methoden die vom Projektteam angewendet / ausprobiert werden wollen im Vornherein sammeln
- Research über Konkurrenz, Desktop Metapher, Window Management und File Management unbedingt in Bericht mit aufnehmen (nicht Anhang), bspw. als Einführung um den Kontext zu setzen und dem Leser zu erklären, was es mit dem Ganzen überhaupt auf sich hat
- **Wichtig**: Bei Entscheidung für Lean UX als Grund nicht nur Kunde nennen, sondern eigene Gründe anführen, wieso das sinnvoll ist in der aktuellen Situation
- **Idee**: Kontakt zu Lean Startup Experten (David Griesbach) von HSLU via Christian Heusser möglich
- **Idee**: Dokumentation der einzelnen Experimente auch in Lean UX Zyklus aufnehmen
- **Offene Fragen**:
  - Interessiert Split Screen überhaupt jemanden bei virtualisierten Gastsystemen in unmittelbarer Zukunft?
  - Möglicherweise erst bei zukünftigen virtualisiertem App Konzept interessant?

Fazit, Beschlüsse:

- Erstes Experiment durchführen, Fake gapfruit OS mit Benutzern testen in KW 36
- Quantitative Umfrage zu den Aufgaben und Nutzungsszenarien auf dem PC von Mitarbeitern in KW 37 starten

Auftraggeber Meeting «Ergebnisse Experiment Virtual Box» Protokoll - MT 2018/19 - Gruppe 08

Projekt:	Security focused OS
Datum:	05. Oktober 2018
Ort:	Baarerstrasse 135, 6300 Zug
Anwesende:	Sid Hussmann, Roman Iten, Pirmin Duss, Adrian Schmid, Daniel Crvelin, Aaron Wyder
Entschuldigt:	-

Traktanden

1. Präsentation Resultate aus Experiment «Virtual Box»

Diskussionspunkte:

- Diskussion über Experiment und Realitätsnähe zu geplantem Produkt
- Diskussion der Richtung für die Entwicklung der weiteren Prototypen
- Von Projektteam angedachte Richtung „Shared File System“ ist sinnvoll
  - evtl. sogar neue Marktchance für Produkt entdeckt im Sinne einer neuartigen, einfachen Zusammenführung von lokalen und Cloud Dateisystemen wie bspw. OneDrive, Google Drive, Dropbox, etc. mit einer benutzerfreundlichen Handhabung
- Paradigmenänderung in Bezug auf Nutzung der unterschiedlichen Dateisysteme der einzelnen virtuellen Maschinen
  - Einführung eines übergeordneten, konsolidierten File Managers auf Host System Ebene
  - Startpunkt für auszuführende Arbeiten nicht mehr Gastsystem, sondern Dokument aus dem konsolidierten Host System File Manager

Fazit, Beschlüsse:

- Vision macht Sinn für Auftraggeber, Projektteam kann Prototypen in angedachte Richtung entwickeln und testen
- Hinweis von Auftraggeber: Nicht zu stark durch potentielle technische Restriktionen einschränken lassen und Vision weiterentwickeln, bei der Umsetzung wird dann halt möglicherweise nur ein Teil umgesetzt werden können

2. Weiteres Vorgehen

Diskussionspunkte:

- Festlegen weiterer Testpersonen aus dem Bekanntenkreis der gapfruit AG für weitere Experimente und Benutzertests mit den entwickelten Prototypen
- Fokus vor allem auf Personen, die im Rahmen ihrer Arbeit potentiell mit sensitiven Daten oder Sicherheitsaspekten zu tun haben

Fazit, Beschlüsse:

- Planung der nächsten Experimente als fixe Tage bei den Firmen der Projektteilnehmer (Swisscom, Swiss Re und Zühlke) mit möglichst verschiedenen Berufsgruppen
  - Nach Möglichkeit min. vier Probanden pro Tag
- Paralleles Aufgleisen von Terminen mit den ausgewählten Testpersonen der gapfruit AG
  - Nach Möglichkeit zwei Testtage, einer in Zürich einer in Luzern je nach Standort der Testpersonen

Coaching Protokoll - MT 2018/19 - Gruppe 08

Projekt:	Security focused OS
Datum:	19. Oktober 2018
Ort:	Förrlibuckstrasse 181, 8005 Zürich
Anwesende:	Christian Heusser (Coach), Adrian Schmid, Daniel Crvelin, Aaron Wyder
Entschuldigt:	-

Traktanden

---

1. Präsentation Resultate aus Experiment «Virtual Box»

Diskussionspunkte:

- Vorstellung Experiment und durchgeführte Auswertung mit gefundenen und weiterzuverfolgenden Punkten für die kommenden Prototypen
- Diskussion über Findings
  - Anmerkung Coach: Kommen gute Punkte raus, Diskussionen werden spannend
- Möglichkeiten und Ideen zur Durchführung weiterer Experimente
  - A/B Testing als gute Methode vorgeschlagen, da Benutzer einfacher vergleichen bzw. sich eine Meinung bilden können, wenn zwei konkrete Ansätze vorgestellt werden, das Feedback wird konkreter

Fazit, Beschlüsse:

- A/B Testing für kommende Experimente einplanen

---

2. Vorstellen & Durchführung Experiment «Shared File System»

Diskussionspunkte:

- Durchführung des Experiments «Shared File System» mit Coach Christian Heusser

Fazit, Beschlüsse:

- Benutzerführung im Prototyp optimieren, zwei wichtige Fragestellungen klären
  - Wann braucht es welche Benachrichtigungen im Prozess?
  - Wie kann die Kommunikation in welcher Sicherheitszone sich der Benutzer befindet bzw. in welche Zone er sich begeben muss um bestimmte Aktionen ausführen zu dürfen optimiert werden?

---

3. Weiteres Vorgehen

Diskussionspunkte:

- Richtung des Projektes macht Sinn, nach langer Ungewissheit und Schwierigkeiten mit Richtungsfindung positive Entwicklung
- Input Coach: Da Lean UX als Vorgehen gewählt und Zeit langsam dem Ende entgegen geht besser mehr Zeit auf Iterationen gemäss Vorgehensmodell investieren, als zusätzlich quantitative Umfrage starten (im Idealfall beides tun)
- Input Coach: Für Projektteam mit schwierigem Projekt ist Reflexion äusserst wichtig
  - Erfahrungen und Entscheidungen dokumentieren
  - Schwierigkeiten und Meinungsverschiedenheiten bezüglich Projektfokus und Vorgehen mit Auftraggeber aufzeigen
  - Lean UX als Vorgehensmodell kritisch hinterfragen, da viele Paradigmen nicht dem klassischen UCD Prozess entsprechen und am Ende tendenziell eine Empfehlung steht und keine verifizierte Nutzergruppe und Szenarien
  - Gefühlte Änderung des Mindset auf Auftraggeber-Seite evtl. auch als Erfolg für gelebten UX Prozess zu werten?

Fazit, Beschlüsse:

- Fokus auf möglichst viele kurze und agile Iterationen gemäss Lean UX legen
- Ab jetzt Fokus tendenziell auf das Erledigen der Masterarbeit legen
  - Auftraggeber auf dem Laufenden halten, nicht mehr viel Zeit mit Diskussionen und Workshops zubringen (nächste Auftraggeber Präsentation evtl. erst am Ende der Arbeit)
  - Abschluss der Arbeit als unmittelbares Ziel für Projektteam

Coaching Protokoll - MT 2018/19 - Gruppe 08

Projekt:	Security focused OS
Datum:	30. November 2018
Ort:	Förrlibuckstrasse 181, 8005 Zürich
Anwesende:	Christian Heusser (Coach), Adrian Schmid, Aaron Wyder
Entschuldigt:	Daniel Crvelin

Traktanden

---

1. Aktueller Stand und erarbeitete Resultate

Diskussionspunkte:

- Erarbeitete Resultate & Entscheidungen der letzten 8 Wochen:
  - Window Management verworfen und Fokus auf File Management gelegt
  - File Manager weiter ausgearbeitet und Notifications in den Ablauf eingeführt
  - User Tests bzw. Experimente gemäss Lean UX über 5 Iterationen mit insgesamt 24 Probanden durchgeführt
- Vorstellung aktueller Stand des Prototyps in zwei verschiedenen Varianten die nebeneinander mit Probanden getestet wurden
  - Farben für Zonen mit Probanden diskutiert und Meinungen abgefragt
  - Diskussion über Drag & Drop als Möglichkeit für Zonentransfer von Dateien
  - Diskussion über Labeling-Konzept und potentielle Schwierigkeiten bei der angedachten Vereinigung von Zonenlabels und persönlichen Labels, die Verwendung zusätzlicher Farben für persönliche Labels könnte die Wirkung der Zonenfarben konterkarieren
- Schwierigkeit nach wie vor, für Benutzer sinnvolles und verständliches Szenario innerhalb des Zonenkonzepts zu definieren
  - Technische Rahmenbedingungen vs. Benutzersicht bzw. -bedürfnisse
  - Breite und Flexibilität des Systems erlauben eine unüberblickbare Fülle von möglichen Konfigurationen bzw. Abläufen innerhalb des Zonenkonzepts
  - Das durchlaufene Szenario im Prototyp macht je nach Benutzergruppe mehr oder weniger Sinn

Fazit, Beschlüsse:

- Szenarien müssen aus Benutzersicht Sinn machen und verständlich sein, auch im Hinblick auf den Bericht und die Präsentation
- Wichtig: Designentscheidungen auf die Auswertung von User Feedback stützen und damit begründen

---

2. Inhalt Bericht

Diskussionspunkte:

- Input Coach: Zitat aus Benutzertest «Was heisst schon Sicherheit, Sicherheit gibt es nie» als Aufhänger verwenden
  - Als Diskussionsgrundlage für Präsentation?
  - Als Ausgangslage um das Narrativ für den Bericht rundherum aufzubauen?
- Input Coach: Ein Kapitel für die Zusammenarbeit mit Kunde einbauen
  - Wie hat sich der Prozess der Zusammenarbeit entwickelt bzw. verändert?
  - Hat UCD bzw. unsere Arbeit den Mindset des Kunden allenfalls verändert?
- Input Coach: Reflexion insbesondere in unserem Fall sehr wichtig, vor allem auch eine kritische Auseinandersetzung mit Lean UX
- Input Coach: Zur Dokumentation von eingesetzten Methoden kurze Zusammenfassung, allenfalls Alternativen und warum ausgewählt
- Lean UX als Methode findet langsam Einzug im Studiengang (für Arbeit evtl. ein Jahr zu früh)
  - Buch «Collaborativ UX Design» von Toni Steimle
  - Chri Hübscher stellt Unterricht um und entwickelt seinen neuen Lehrplan um Lean herum
- Referenzen im Bericht müssen einfach auffindbar sein, bpsw. auf Anhang etc.

Fazit, Beschlüsse:

- Lean UX darf ausführlicher dokumentiert werden, da im Studiengang bisher nicht allzu präsent
- Abkürzungen im Bericht ausschreiben und Glossar für technische Begriffe einführen
  - Glossar als Marginalien wäre hilfreich, Vereinfachung für Leser da Projekt sehr technischer Natur
- Technische Tiefe/Komplexität von Bericht zum aktuellen Zeitpunkt ist in Ordnung
  - Nach Möglichkeit vereinfachen und Leser nicht überfordern
  - Besser strukturieren und verständlich bleiben für nicht Techies
- Annahmen oder konzeptuelle Entscheidungen zum Design durch Projektteam ebenfalls dokumentieren
  - Keine Taskbar in Windows Gastsystem wie in Prototyp designt?
  - Keine Shortcuts und Files auf Windows Desktop?
  - etc.
- Good Practice: Ideen bzw. Ansätze die nur gestreift aber nicht weiterverfolgt wurden ebenfalls kurz dokumentieren, Empfehlungen für Zukunft beschreiben und warum nicht weiterverfolgt (bspw. auf einer Doppelseite)
  - Gut geeignet zum Verständnis und Nachverfolgen durch den Leser
  - Weiterverfolgte Ideen ebenfalls begründen
- Good Practice: Konkrete Reflexionen zu Abschnitten bzw. Kapiteln einfügen, wird gerne gesehen und liest sich gut

---

3. Weiteres Vorgehen

Diskussionspunkte:

- Sinnvollen Abschluss für Projekt finden, wann aufhören, was ist der Endpunkt für die vorliegende Arbeit
  - Erkenntnisse aus „letztem“ Benutzertest dokumentieren
  - Erkenntnisse in Prototyp einarbeiten und allenfalls noch einmal testen
- Prototyp sieht konzeptuell vernünftig aus
  - Funktioniert gut mit cleanem Design und aktuell leerem Platzhalter für Gastsystem
  - Was geschieht, wenn bspw. Gastsystem Desktop mit grossem Durcheinander (Taskbar, Shortcuts, Files, etc.) angezeigt wird?

- Wäre Konzept in einem derartigen Fall immer noch clean und einfach verständlich?
- Ansonsten konzeptuelle Anforderungen für aktuelles Design definieren und dokumentieren, wie bspw. keine Taskbar und keine Inhalte auf Desktop von Gastsystem erlaubt

- Die Design-Ideen im Prototyp visuell klarer formulieren
  - Varianten des Prototyps konsolidieren
  - Platzhalter für Gastsystem mit Inhalt füllen (aktuell nur weisse Fläche im Prototyp)

Fazit, Beschlüsse:

- Die beiden Varianten des Prototyps konsolidieren und die Erkenntnisse aus den Benutzertests einarbeiten
  - Nach Möglichkeit noch einmal kurz testen
- Designfrage nach „Desktop-Inhalt Gastsystem“ klären
  - Wichtige Design-Frage, sollte beantwortet werden im Hinblick auf Präsentation und vor allem mündliche Prüfung
  - Bestenfalls Varianten mit gewöhnlichem Desktop-Inhalt (Taskbar, Shortcuts, Files, etc.) und ohne gegeneinander testen und damit Entscheidung auf stabiles Fundament stellen
  - Falls nicht mehr getestet werden kann unbedingt als nächste Schritte in Bericht aufnehmen und dokumentieren, bspw. als nicht angegangene Probleme

Szenario Anwaltskanzlei

Julia ist Anwältin in einer kleinen Kanzlei mit drei Anwälten. Sie will ungestört arbeiten und dabei nicht von Ransomware, Phishing und Staatstrojaner gehindert werden. Sie hat mal gehört, dass man die Webcam abkleben sollte, weil Hacker über einen Trojaner sie beobachten könnte. Da sie gerne mit ihren Freundinnen Katzenvideos austauscht, klickt sie auf einen Link, den sie per Email mit dem Titel „Das lustigste Katzenvideo, das du je gesehen hast“ bekommen hat. Über den Link lädt sie sich unbemerkt eine Ransomware auf ihren Rechner. Dadurch wird die gesamte Festplatte verschlüsselt, so dass sie weder den Rechner starten kann noch Zugriff hat auf ihre Daten. Da sie kurz vor dem Abschluss von ihrem bisher grössten Projektes war zahlt sie die Summe mit der Hoffnung, dass sie dadurch wieder an ihre Daten kommt. Leider vergebens. Der Schaden ist immens. Sowohl für sie, die gesamte Kanzlei und vor allem für die Klienten des Riesen-Projektes. Zum den Schaden zu beheben gibt die Anwaltskanzlei mehrere Zehntausend Franken aus.
Mit NyanOS kann sie ihre wertvollen Akten einfach und sicher von Internetrecherchen im Darknet und ihren privaten Katzenvideos trennen. Auch der Dateiserver der Kanzlei, die Mail-Kommunikation mit ihren Kollegen und ihre Backup-Festplatte wird von NyanOS transparent geschützt. NyanOS schützt auch ihr Notebook, wenn sie es zum Arbeiten nach Hause oder ins Gericht mit nimmt. Wenn man den Berichten in den Medien folgt, dann sieht man, dass es nur eine Frage der Zeit ist bis man Opfer von Cyberkriminalität wird. Durch den Einsatz von NyanOS wäre der Angriff ins Leere gelaufen und die Anwaltskanzlei hätte viel Geld und Mühe gespart. Der Aufkleber über der Webcam hat nicht wirklich viel geholfen. Aber auch hier hat NyanOS eine Lösung: Man kann sie sicher deaktivieren.

Szenario Grossbank

Robert arbeitet als Investment-Banker bei einer Schweizer Grossbank. Er und sein Chef wollen verhindern, dass Transaktionen manipuliert werden, Kundendaten leaken oder die Produktivität durch Ransomware beeinträchtigt wird. Das Leaken von Kundendaten basiert heute auf Vertrauen zum Mitarbeiter. Da es diesbezüglich noch keine Lösung gab, sind in den letzten Jahren mehrere Bestände solcher Daten in die falschen Hände gelangt. Robert bekommt von einem alten Studienkollegen einen USB Stick mit Fotos und Filmen aus der Studienzeit. Der USB Stick ist verseucht. Beim Einstecken wird unbemerkt ein Trojaner auf seinem Rechner installiert. Durch diesen Trojaner hat der Angreifer Zugriff auf alles was er mit seinem Computer macht: Kann Passwörter abfangen, in Roberts Namen Emails versenden, Transaktionen tätigen, Kundendaten stehlen etc. Ausserdem verbreitet er sich im Intranet auf verschiedenen Rechner der gesamten Firma. Da es sich um einen neuen Trojaner handelt, entdeckt die Antiviren Software erst Monate später die Malware. Der finanzielle Schaden geht in die Millionen. Der Imageschaden ist immens.
NyanOS trennt die Core-Banking-Applikation von den Mails der Kunden und diese wiederum von seiner Marktrecherche in Onlineportalen, Zeitungen und soziale Netzwerken. NyanOS sichert den Zugriff auf Transaktionen und sensible Mails auch beim Arbeiten von Zuhause und bei Kundenbesuchen transparent. Es verhindert zudem, dass heikle Informationen von Robert massenhaft exportiert und als Steuer-CD verkauft werden.
Mit NyanOS wäre der Trojaner in dem Compartment isoliert gewesen, wo der USB Stick reingereicht wurde und der Schaden wäre begrenzt gewesen. Dadurch hätte die Firma sehr viel Geld gespart. Geleakte Kundendaten ziehen Imageschäden und letztlich Umsatzeinbussen und sogar Strafzahlungen nach sich.

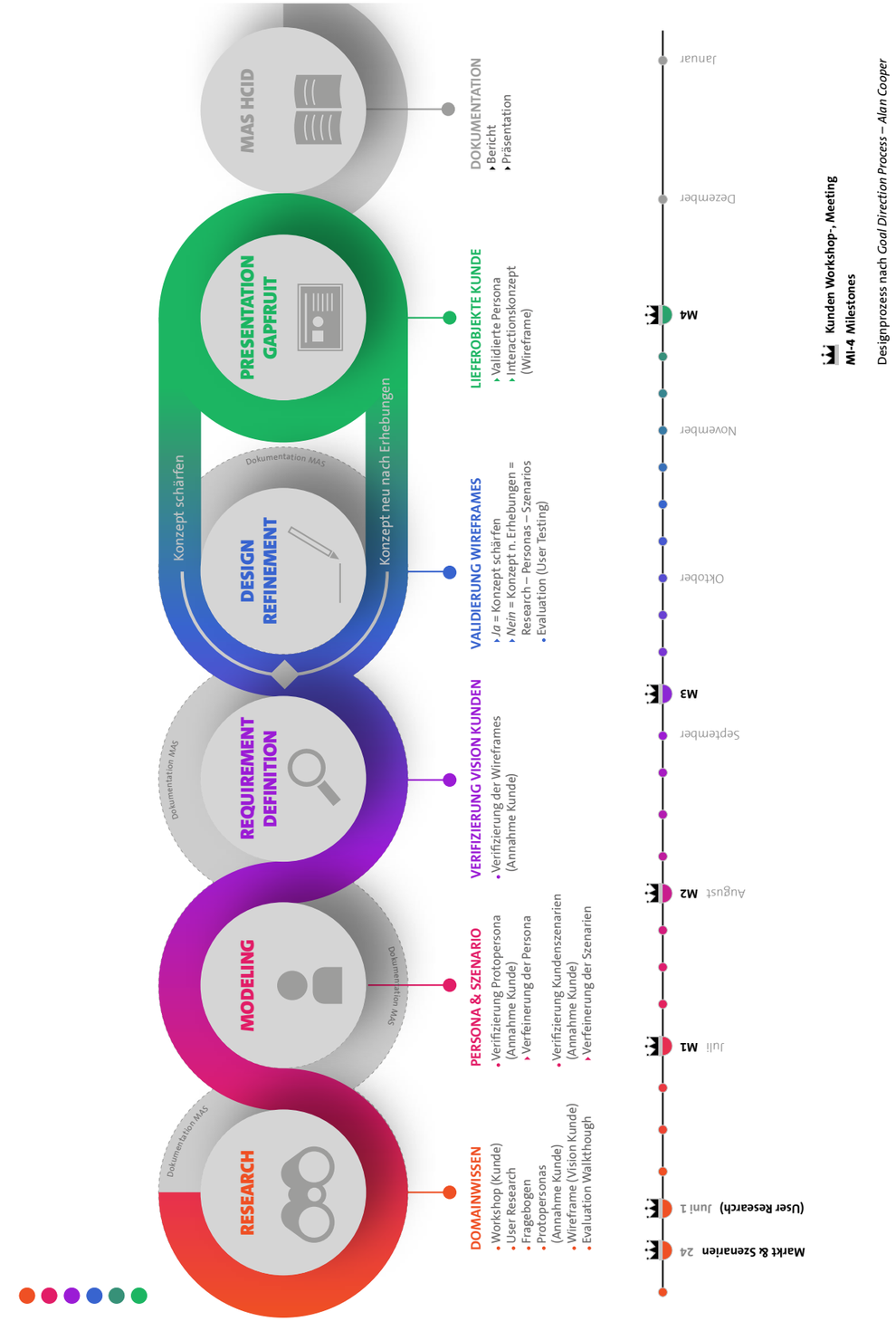
Szenario Kantonsverwaltung

Nora hat die Verantwortung für die IT einer Kantonsverwaltung. Sie will sicherstellen, dass der Datenschutz eingehalten wird und trotzdem produktiv gearbeitet werden kann. Hochgeheime Polizeiakten dürfen auf keinen Fall an die Öffentlichkeit gelangen. NyanOS erlaubt es ihr, verschiedenen Zonen für das polizeiliche Informationssystem, die Steuerveranlagung und den Surfzugang ins Internet einzurichten und per Policy festzulegen wie Daten transferiert werden dürfen. Dadurch, dass Mitarbeiter mehrere Zonen auf einem Gerät benutzen können, wird das Umgehen des Systems durch frustrierte Benutzer verhindert. Gleichzeitig wird mit NyanOS verhindert, dass Daten unberechtigt deklassifiziert werden und sich Malware von einer Zone in die nächste verbreitet.

Szenario Auslandskorrespondent

Thomas ist Auslandskorrespondent einer grossen Tageszeitung. Er will sicherstellen, dass die korrupte Polizei in dem Land nicht an seine Informanten herankommt. Damit er mobil ist, hat er ein Notebook, mit welchem er alles mögliche macht. Er recherchiert im Internet, kommuniziert mit der Redaktion, speichert sein Geld in seinem Bitcoin Wallet. Durch eine driveby Attacke auf einer Webseite, die er besucht wird der Rechner durch die Spionage-Malware FinFisher komprimittiert. Dadurch haben die Angreifer Zugriff auf sämtliche Daten auf dem Rechner und können in seinem Namen Fake-News produzieren. Ausserdem werden seine Informanten entlarvt, was zu deren Verurteilung und mehrjährige Haftstrafen führt. Mit NyanOS sind seine Notizen auch dann sicher, wenn er abseits der Netzabdeckung offline arbeitet und seine Redaktion nur sporadisch per E-Mail mit Artikeln versorgt. Er kann sich ausserdem potentiell gefährliche Seiten des Regimes anschauen, ohne sein Arbeitsinstrument und sein Bitcoin Wallet zu gefährden.

9.3 Projektplanung

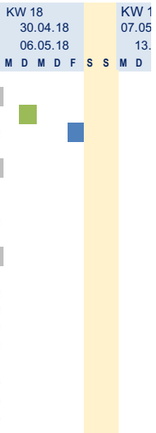


HCID Master Thesis 2018/19 - Projektplan

Projekt	Gruppe
Security focused OS	**G08**

Projektteam (PT)	Coach (CH)	Auftraggeber (AG)
Aaron Wyder (AW), Adrian Schmid (AS), Daniel Crvelin (DC)	**Christian Heusser**	**gapfruit AG**

Nr	Aktivität	Artefakt	Wer	Wann
1	**Kick-off**			
	Vorbereitung Kick-Off Meeting mit Auftraggeber	Leitfaden	PT	
	Kick-off Meeting mit Aufftaggeber		PT, CH, AG	04.05.18
2	**Planung, Vorbereitung**			
	Team-Meeting (Wrap-up Kick-off und Grobplanung)	High-Level Projektplan	PT	KW
	Update Projektbeschrieb		PT	KW 19
	Meeting mit Auftraggeber: Besprechung Grobplan und Projektbeschrieb		PT, AG	14.05.18
3	**Domänenrecherche**			
	Vorbereitung Workshop	Leitfaden	PT	KW 20
	Workshop "Problemstellung", "Vision", "Konkurrenzprodukte"		PT, AG	24.05.18
	Team-Telco (Wrap-up Worskshop, nächste Schritte)		PT	30.05.18
	Worskshop "Szenarien"	User Story	PT, AG	01.06.18
	Team-Meeting (Wrap-up Workshop, nächste Schritte)		PT	08.06.18
	Vorbereitung Experten-Interviews	Fragebogen	PT	KW 23
	Durchführung Experten-Interview "Zühlke"		PT	14.06.18
	Team-Meeting		PT	22.06.18
	Durchführung Experten-Interview "Skyguide"		PT	02.07.18
	Meeting mit Auftraggeber (Projektreview)		PT, AG	06.07.18
	Meeting mit Auftraggeber (Projektreview)		PT, AG	13.07.18
3	**Analyse**			
	Team-Meeting (Feinplanung, nächste Schritte)	Projektplan	PT	21.07.18
	Team-Meeting / Coach Sitzung		PT, CH	27.07.18
	Annahmen deklarieren u priorisieren		PT	KW 30
	Hypothesen u. Messindikatoren definieren		PT	KW 31
	Ideation		PT	KW 32
	Meeting mit Auftraggeber		PT, AG	17.08.18
4	**Evaluation - Iteration 1**			
	Probanden rekrutieren (Anzahl 3 für KW 36)		PT	KW 33-35
	Test Case erstellen, MVP vorbereiten		PT	KW 33
	Test Case erstellen, MVP vorbereiten		PT	KW 34
	Test Case erstellen, MVP vorbereiten		PT	KW 35
	Testen und Ergebnisse dokumentieren		PT	KW 36
	Testergebnisse auswerten und konsolidieren		PT	KW 37
5	**Evaluation - Iteration 2**			
	Probanden rekrutieren (Anzahl 3 für KW 40)		PT	KW 38-40
	Test Case anpassen/definieren, MVP anpassen/vorbereiten		PT	KW 38
	Test Case anpassen/definieren, MVP anpassen/vorbereiten		PT	KW 39
	Test Case anpassen/definieren, MVP anpassen/vorbereiten		PT	KW 40
	Testen und Ergebnisse dokumentieren		PT	KW 41
	Testergebnisse auswerten und konsolidieren		PT	KW 42
6	**Evaluation - Iteration 3**			
	Probanden rekrutieren (Anzahl 3 für KW 46)		PT	KW 43-45
	Test Case anpassen/definieren, MVP anpassen/vorbereiten		PT	KW 43
	Test Case anpassen/definieren, MVP anpassen/vorbereiten		PT	KW 44
	Test Case anpassen/definieren, MVP anpassen/vorbereiten		PT	KW 45
	Testen und Ergebnisse dokumentieren		PT	KW 46
	Testergebnisse auswerten und konsolidieren		PT	KW 47
7	**Evaluation - Iteration 4**			
	Probanden rekrutieren (Anzahl 3 für KW 51)		PT	KW 48-50
	Test Case anpassen/definieren, MVP anpassen/vorbereiten		PT	KW 48
	Test Case anpassen/definieren, MVP anpassen/vorbereiten		PT	KW 49
	Test Case anpassen/definieren, MVP anpassen/vorbereiten		PT	KW 50
	Testen und Ergebnisse dokumentieren		PT	KW 51
	Testergebnisse auswerten und konsolidieren		PT	KW 52



Lieferergebnisse
- Validierte Hypothesen
- Personas
- Informtationsarchitektur
- Prototyp (MVP)

9.4 Risikoliste

Projektrisiken

Nr	Risiko	Auswirkungen	A	E	RQ	Verantw.	Massnahmen bei Risikoeintritt	Bemerkungen
#1	Kein Zugang zu konkreten Unternehmen/Testkunden und kein Fokus auf konkrete Zielgruppen zwecks User Research seitens Auftraggeber vorhanden	- Fokus und gemeinsames Verständnis kann nicht aufgebaut werden - User Research nach klassischem UCD Vorgehen ist nicht möglich - Rekrutierung von Testteilnehmern ist sehr aufwendig - Zeitverlust oder falsche Erkenntnisse mit nicht relevanten Personengruppen - Zugang zu spezialisierten Berufsfeldern nicht möglich	6	6	36	alle	- Mehr Zeit für die Rekrutierung von Personen zwecks Benutzerforschung einplanen - Eigenständige Rekrutierung von TPs aus Branchen der potentiellen Zielgruppe die ev. einen Bedarf für ein Security-OS haben könnten (bspw. Finanz, Anwälte, Treuhänder, Energiesektor, Cloud Anbieter) - Interviews mit Domänenexperten führen um Erkenntnisse bezüglich Zielgruppe zu erlangen - Aktivitäten innerhalb der Projektzeit exklusiv auf User Research beschränken	**Risiko ist eingetroffen**; anstelle der exklusiven Beschränkung auf User Research wurde, in Abhängigkeit von Risiko #2, das Vorgehensmodell in Absprache mit den Coaches von UCD auf Lean UX geändert
#2	Auftraggeber unterstützt UCD Vorgehen nicht und erwartet UI Mock-Ups und Visual Design	- Fokus und gemeinsames Verständnis kann nicht aufgebaut werden - Potentiell erarbeitete Interaktionskonzepte haben keine Grundlage - Vorgehensmodell muss angepasst werden - Bruch mit Auftraggebern im schlimmsten Fall	6	3	18	alle	- Dialog mit Auftraggeber suchen und Wichtigkeit von UCD Vorgehen sowie Verpflichtungen gegenüber HSR klar hervorheben - Projektthema auf eigene Faust weiterverfolgen oder Projektabbruch mit kompletter Neuorientierung	**Risiko ist eingetroffen**; Projektabbruch stand im Raum, wurde aber in Abhängigkeit mit Risiko #1 zugunsten einer Änderung des Vorgehensmodells verworfen
#3	Aufgabenstellung zu technisch für Autoren	- Autoren verstehen Problemstellung und Lösungsansatz nicht korrekte und interpretieren - Es kann kein gemeinsames Domänenverständnis aufgebaut werden - Beim Austausch entstehen gravierende Missverständnisse über Lösungsansätze die auf impliziten Annahmen basieren	3	3	9	Aaron	- Enger Dialog mit Auftraggebern, regelmässige Statusmeetings und Knowhow Transfer - Technische Machbarkeit von Ideen mit Auftraggeber abklären	Knowhow-Transfer und Workshops mit Auftraggebern wurden durchgeführt, Risiko konnte dadurch teilweise abgefedert werden, jedoch blieben bei den Autoren viele Unsicherheiten bei wichtigen technischen Feinheiten bestehen
#4	Wenig aussagekräftige oder falsche Erkenntnisse aus Experimenten mit potentiell wenig relevanten Anwendern des Systems	- Grundlagen für Benutzergruppen und Nutzungsszenarien sind falsch - Interaktionskonzept wird auf Basis falscher Grundlagen ausgearbeitet	6	1	6	alle	- Getroffene Annahmen permanent hinterfragen - Rekrutierung von Testpersonen fortlaufen mit neuen Erkenntnissen einschränken und so versuchen immer näher an die reale Zielgruppe zu rücken	Neues Risiko, welches vor allem durch den Einsatz von Lean UX aufgekommen ist, konnte aufgrund der Experteninterviews und dem erhobenen Wissen im Rahmen der Experimente mitigiert werden

Produktrisiken

Nr	Risiko	Auswirkungen	A	E	RQ	Verantw.	Massnahme bei Risikoeintritt und Bemerkungen	Bemerkungen
#1	Produkt wird von potentiellen Endbenutzern nicht akzeptiert (Unverständnis für Problemstellung oder zu grosse Einschränkung im Arbeitsprozess)	- Produkterfolg bleibt aus - Es können keine Benutzergruppen und Anwendungsszenarien erhoben werden	6	3	18	alle	- Einschränkung der Zielgruppe bei Auftraggeber einfordern - Erste Versionen explizit für spezifische Workflows spezialisierter Benutzergruppen entwickeln	Risiko besteht weiterhin und wird für die zukünftige Entwicklung von gapfruit OS äusserst relevant, die Entscheidung für eine Eingrenzung der Zielgruppe liegt bei den Auftraggebern

A Auswirkung: klein = 1, mittel = 3, gross = 6
E Eintrittswahrscheinlichkeit: klein = 1, mittel = 3, gross = 6
RQ Risiko quantifiziert: A x E

Recherche und Marktanalyse

Betriebssysteme mit einer ähnlich sicheren Architektur wie das vom Auftraggeber entwickelte System existieren zurzeit beinahe ausschliesslich für Behörden und Regierungen. Diese Systeme basieren ebenfalls auf dem Prinzip der «Compartmentalisation». Die Produkte sind jedoch nicht öffentlich zugänglich und werden nur bei Demonstrationen durch die Hersteller beispielsweise auf einschlägigen Messen vorgeführt. Somit waren diese Systeme für das Projektteam nicht direkt test- und analysierbar. Alle Informationen zu diesen geschlossenen Systemen stammen ausschliesslich vom Auftraggeber und wurden wie erläutert in diese Arbeit übernommen [vgl. Kap.: Geschlossene Systeme für Behörden und Regierungen].

In den folgenden Kapiteln werden neben den für das Projektteam nicht zugänglichen Systemen noch weitere interessante Produkte analysiert und für die vorliegende Arbeit eingeordnet.

Geschlossene Systeme für Behörden und Regierungen

Eine Reihe von Herstellern ist bereits mit ähnlichen Systemen wie das von den Auftraggebern entwickelte auf dem Markt. Obwohl aufgrund der Bedrohungslage und der durch Cyberkriminalität verursachten Schäden [vgl. Kap.: Kontext der Arbeit] der Einsatz derartiger Produkte für viele marktorientierte Unternehmen sinnvoll wäre, werden diese Systeme in der Privatwirtschaft praktisch gar nicht eingesetzt. Dies mag hauptsächlich daran liegen, dass die Produkte nur bedingt für den täglichen Gebrauch in den meisten Unternehmen geeignet sind.

Funktionsweise

Die grundsätzliche Funktionsweise ist allen Systemen gemeinsam. Ein minimales Hostsystem bietet die Plattform für verschiedene virtuelle Maschinen welche die unterschiedlichen Sicherheitskontexte wie bspw. «Internet Zone» oder «Work Zone» implementieren. Die meisten dieser Systeme erlauben keinen Datentransfer zwischen den Sicherheitskontexten. Bei vielen unserer täglichen Aufgaben im Arbeitsumfeld ist jedoch exakt dieser Datenaustausch essentiell, so müssten beispielsweise bei einer Internetrecherche Dokumente in der «Internet Zone» heruntergeladen und in der «Work Zone» weiterverarbeitet werden können.

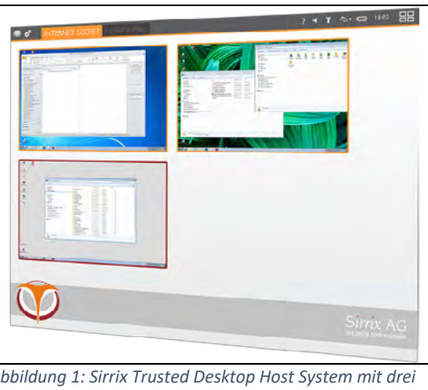


Abbildung 1: Sirrix Trusted Desktop Host System mit drei unterschiedlichen Sicherheitskontexten [Quelle: sirrix]

Abbildung 2: SINA OS Host System mit sechs unterschiedlichen Sicherheitskontexten [Quelle: secunet]

Als Beispiele für Hersteller und Produkte können die folgenden aufgeführt werden:

- Crypto AG: cOffice [1]
- Secunet AG: SINA (Sichere Inter-Netzwerk Architektur) [2]
- Sirrix AG: TrustedDesktop [3]
- Genua GmbH: Security Laptop cyber-top [4]
- General Dynamics [5]

Eignung für den Einsatz beim Endbenutzer

Die Sicherheitsrestriktionen und die Notwendigkeit für unterschiedliche Tätigkeiten in unterschiedlichen Zonen agieren zu müssen haben grobe Abweichungen vom gewohnten Umgang mit dem Computer zur Folge. Der nahtlose Arbeitsfluss und die gute Usability der gängigen Betriebssysteme werden durch die strikte Separierung der verschiedenen Sicherheitszonen auf diesen hochsicheren Systemen unterbunden. Daher werden diese speziellen Betriebssysteme heutzutage auch nur von Institutionen mit ausserordentlich sensiblen Daten, wie bspw. Regierungen oder Militärs, eingesetzt.

Qubes OS von der Open Source Community

Die einzige breiter verfügbare Alternative zu den eingangs erwähnten, geschlossenen Systemen [vgl. Kapitel «Geschlossene Systeme für Regierungen und Behörden»] bietet die Open Source Community mit Qubes OS [6]. Qubes OS funktioniert ebenfalls nach dem Prinzip der Sicherheit durch «Compartmentalisation».

Funktionsweise

Qubes OS erlaubt es verschiedene virtuelle Maschinen, so genannte «Qubes» oder auch «Domänen», mit unterschiedlichen Betriebssystemen (Linux und Windows 7) aufzusetzen. Eine einzelne Domäne repräsentiert einen eigenständigen, isolierten Sicherheitskontext. Hierbei kann beispielsweise wiederum ein getrennter Kontext für die «Internet Zone» und einer für «Work Zone» geschaffen werden, wobei die Arbeitsumgebung komplett vom Internet getrennt wird.

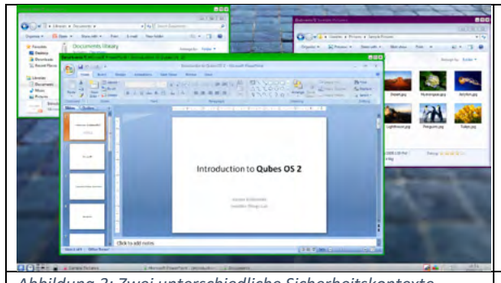


Abbildung 3: Zwei unterschiedliche Sicherheitskontexte implementiert durch Windows VMs in Qubes OS

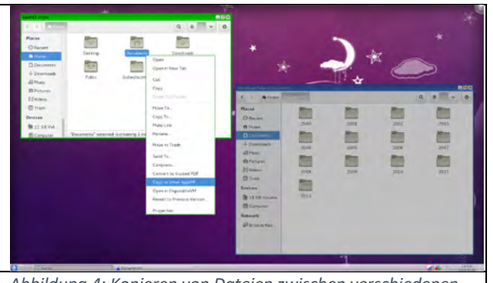


Abbildung 4: Kopieren von Dateien zwischen verschiedenen Sicherheitskontexten mit Qubes OS

Alle offenen Anwendungen aus derselben Domäne werden durch einen Rahmen mit derselben charakteristischen Farbe unterschieden. Auf diese Weise erkennt der Benutzer jederzeit, in welchem Sicherheitskontext die aktive Applikation läuft. Im Gegensatz zu den meisten der vorgestellten

geschlossenen Systeme bietet Qubes OS die Möglichkeit Daten über einen dedizierten Kopier-Service von einem Sicherheitskontext in einen anderen zu kopieren.

Eignung für den Einsatz beim Endbenutzer

In einem Selbstversuch wurde Qubes OS auf dem Rechner eines Teammitglieds installiert und getestet. Installation und Konfiguration des Systems setzen ein tiefes technisches Verständnis voraus. Auch in der täglichen Nutzung sind häufig Anpassungen an der Konfiguration notwendig. Für Nutzer ohne Expertise im Umgang mit Linux Systemen und deren Funktionsweise ist das kaum zu bewerkstelligen. Aufgrund der schlechten Usability von Qubes OS wird ausserdem die Arbeit in unterschiedlichen Sicherheitskontexten und der erforderliche Datentransfer mühselig und anstrengend. Da die Nutzung des Systems selbst einen Anwender mit Fachkenntnissen immer wieder vor Rätsel stellte, wurde im Folgenden auch von einem Nutzertest mit Qubes OS abgesehen.

Herkömmliche Virtualisierungslösungen am Beispiel Parallels

Virtualisierung findet auch ausserhalb der IT-Sicherheit breite Anwendung, beispielsweise in der Softwareentwicklung. Eine virtuelle Maschine mit dem Gastsystem muss hierbei nur einmal komplett mit Entwicklungsumgebung, Tools und Testdaten aufgesetzt werden. Danach kann diese ganz einfach kopiert und an die Entwickler verteilt werden. Das verwendete Betriebssystem (Hostsystem) der einzelnen Entwickler ist dabei zweitrangig. Solange die genutzte Virtualisierungssoftware für die jeweilige Plattform (Windows, Linux, Mac OS, etc.) zur Verfügung steht, kann die virtuelle Maschine genutzt werden. Anhand der Virtualisierungssoftware Parallels [7], welche es unter anderem ermöglicht Windows auf einem Mac laufen zu lassen, sollen die Möglichkeiten aktueller Virtualisierungstechnologie aufgezeigt werden.

Funktionsweise

Es existieren verschiedene Arten von Virtualisierung [8]–[10]. Parallels funktioniert nach dem Prinzip der Desktop Virtualisierung. Als Ausgangslage wird ein installiertes Betriebssystem wie beispielsweise Windows, das so genannte Hostsystem, vorausgesetzt. Die einzelnen virtuellen Maschinen setzen auf einer Abstraktionsschicht, dem Hypervisor, über dem Hostsystem auf. Der Hypervisor abstrahiert und regelt den Zugriff auf die reale Hardware und reicht diese zur Nutzung in die Gastsysteme weiter. Nach dem Erstellen einer neuen virtuellen Maschine über die Management Konsole von Parallels, kann darin ein neues Betriebssystem, auch Gastsystem genannt, installiert werden. Die einzelnen virtuellen Maschinen stellen dabei mehr oder minder isolierte (Sicherheits-)Kontexte dar.

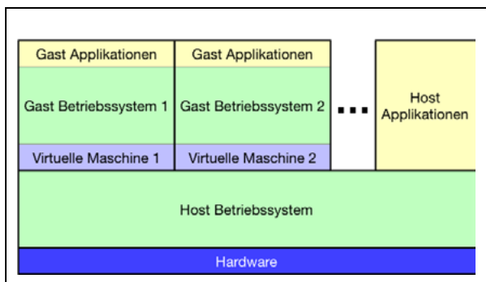


Abbildung 5: Funktionsweise der Desktop Virtualisierung

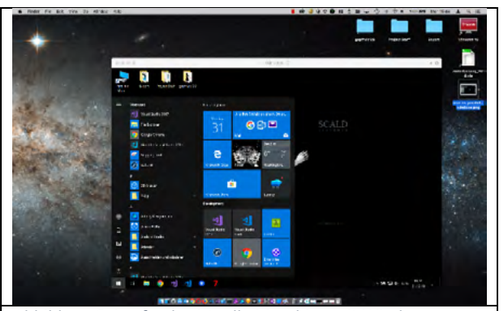


Abbildung 6: Laufende virtuelle Maschine mit Windows Gastsystem in Parallels

Eignung für den Einsatz beim Endbenutzer

Virtualisierung ist eine ausgereifte Technologie, die nicht aus der IT Welt wegzudenken ist. Sie kommt in unzähligen Bereichen und Anwendungsgebieten zum Einsatz. Die weit verbreitete, anhand von Parallels untersuchte Desktop Virtualisierung erfüllt nicht gewünschten Anforderungen an die Sicherheit. Da die virtuellen Maschinen mit den Gastsystemen oberhalb eines unsicheren Hostsystems wie bspw. Windows aufsetzen, kann keine effektive Isolation der einzelnen Sicherheitskontexte gewährleistet werden. Aus Security-Perspektive ist sie daher absolut ungeeignet für die Problemstellung, welche mit dem Produkt gapfruit OS gelöst werden soll.

Interessante Aspekte

Die einfache Bedienbarkeit von Parallels sowie die beinahe nahtlose Integration der Gastsysteme mit dem Hostsystem sollen als Ausgangspunkt und als Inspirationsquelle beim Interaktionsdesign von gapfruit OS dienen. Im Folgenden werden daher die interessantesten Aspekte von Parallels im Zusammenhang mit dem Projektauftrag hervorgehoben.

Integriertes Dateisystem

Das Dateisystem des Host-Betriebssystem wird auf dem Gastsystem automatisch als Netzlaufwerk eingebunden. Auf diese Weise kann der Benutzer ganz einfach auf alle Daten des Hosts zugreifen. Weiter können ebenfalls Daten im Kontext des Gastsystems erzeugt und direkt auf dem Host-Dateisystem abgelegt werden. Für den Benutzer entfällt dadurch ein mühseliges hin- und her-kopieren von Dateien zwischen Host und Gast.

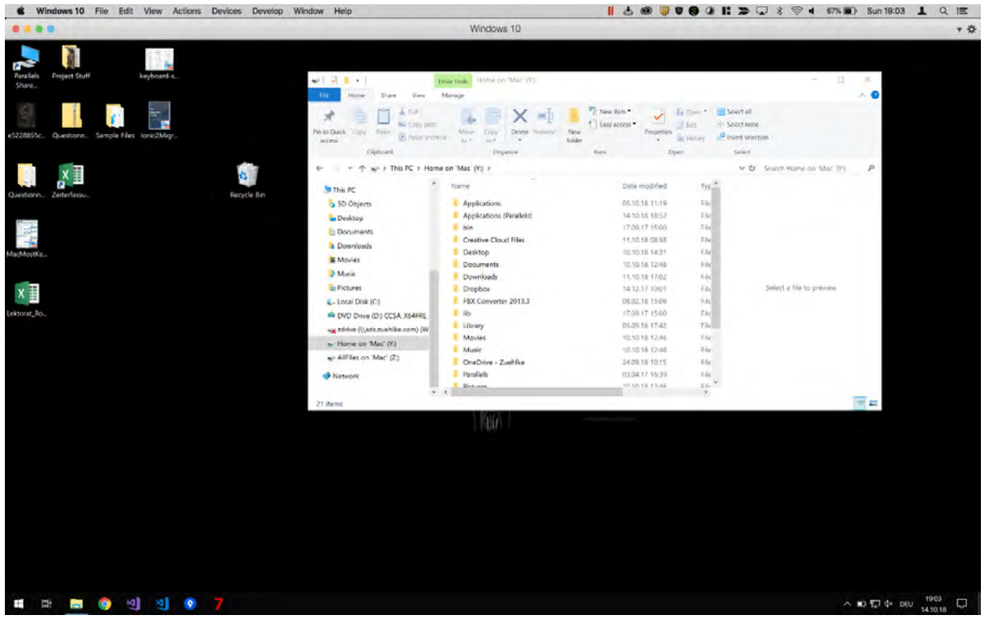


Abbildung 7: Dateisystem des Host-Betriebssystem wird auf dem Gast als Netzlaufwerk eingebunden

Integrierte Programme

Die installierten Programme des Gastsystems können direkt via Hostsystem aufgerufen werden, auch ohne vorgängig die virtuelle Maschine zu starten. Umgekehrt ist es ebenfalls möglich im Kontext des Gastsystems beispielsweise über das Windows Startmenü Programme des Hosts zu starten. Auf diese Weise kann unabhängig vom aktuellen Arbeitskontext jederzeit sehr einfach die benötigte Anwendung aufgerufen werden.

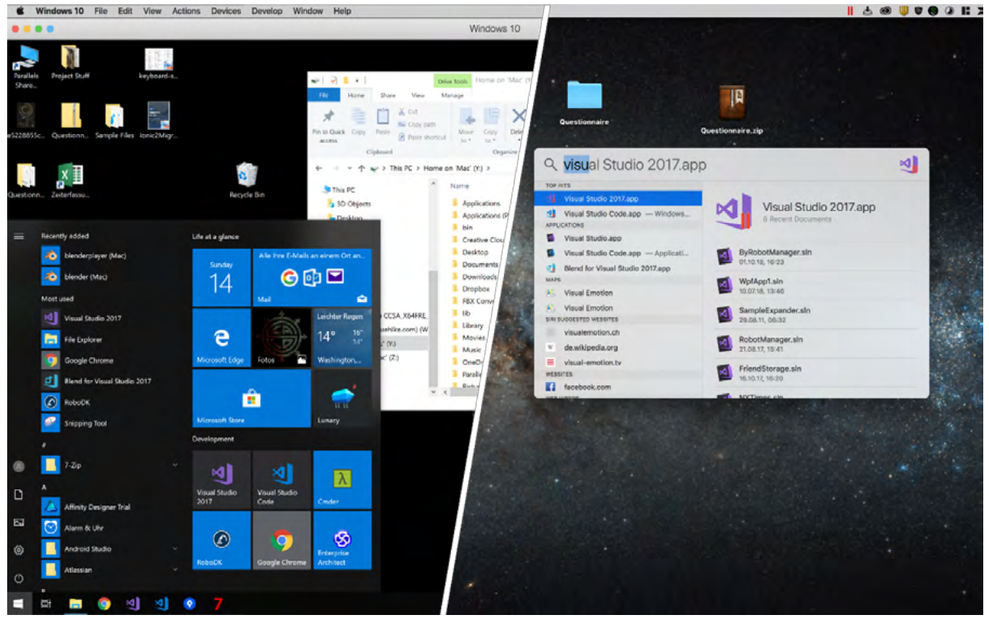


Abbildung 8: Integrierter Zugriff innerhalb Gast-/Host-Betriebssystem auf die installierten Programme des jeweils anderen

Coherence Mode

Der so genannte Coherence Mode von Parallels erlaubt es ein Gastsystem ohne Desktop zu betreiben. Die offenen Anwendungen Gastsystems erscheinen neben den nativen Applikationen im Mac OS Dock und der Benutzer kann komfortabel zwischen ihnen umschalten. Das Startmenü von Windows erscheint ebenfalls als Icon auf dem Dock und kann von dort aus geöffnet werden. Als Resultat verhält sich die VM und die zugehörigen Applikationen genau wie native Mac OS Anwendungen.

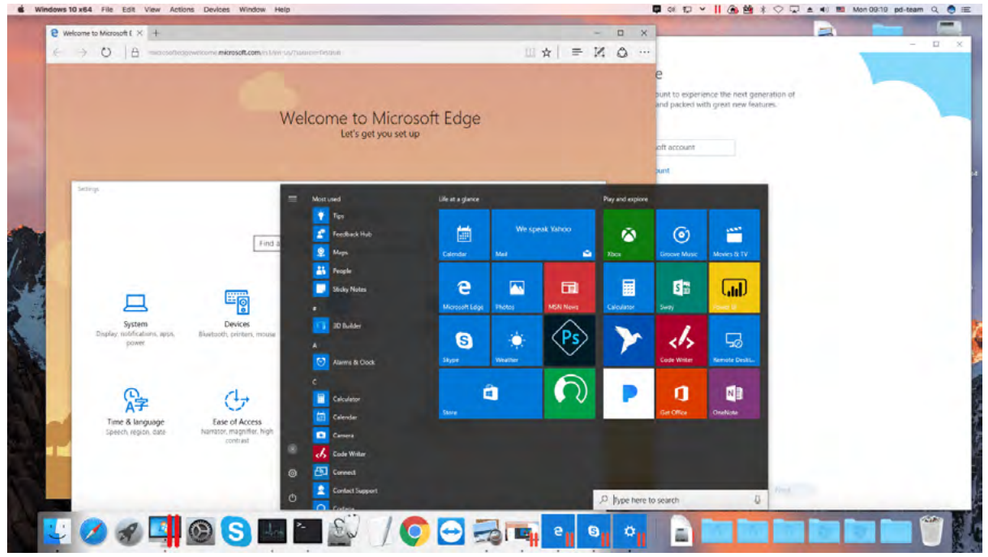


Abbildung 9: Parallels Coherence Mode Mac OS Desktop mit Windows Startmenü und Applikationen, Windows VM läuft ohne Desktop [11]

Windows Sandbox

Windows Sandbox ist ein neues Feature, welches mit einem der nächsten grossen Windows 10 Updates eingeführt wird. Es steht aktuell als Preview Build 18305 [12] für Entwickler und Administratoren zur Verfügung. Windows Sandbox erlaubt es, eine temporäre Desktop Umgebung aufzusetzen, um nicht vertrauenswürdige Software in einem isolierten Kontext vor dem effektiven Einsatz zu testen. Installierte Software, auch unabsichtlich mitinstallierte Viren oder Malware, bleibt in der Sandbox der temporären Umgebung und kann das normale Betriebssystem nicht kompromittieren. Nach dem Schliessen der temporären Desktop Umgebung werden alle zugehörigen Dateien und installierten Programme permanent gelöscht. [13]

Funktionsweise

Über die Windows Features in oben erwähntem Preview Build kann Windows Sandbox nachinstalliert werden. Danach kann über das Start Menü via Windows Sandbox Applikation eine neue Sandbox erzeugt werden. Die zu installierende Software kann mittels Drag & Drop in die Sandbox kopiert und anschliessend ganz normal installiert werden. Nach der Installation kann die Software auf Herz und Nieren überprüft werden.

Windows Sandbox setzt ebenfalls auf Virtualisierungstechnologie auf. Eine Sandbox funktioniert also grundsätzlich nach demselben, im vorangehenden Kapitel [vgl. Kapitel «Herkömmliche Virtualisierungslösungen am Beispiel Parallels»] beschriebenen Prinzip. Es ist eine schnelle und komfortable Art zum Aufsetzen einer virtuellen Maschine, welche beim Ausschalten wieder komplett gelöscht wird.

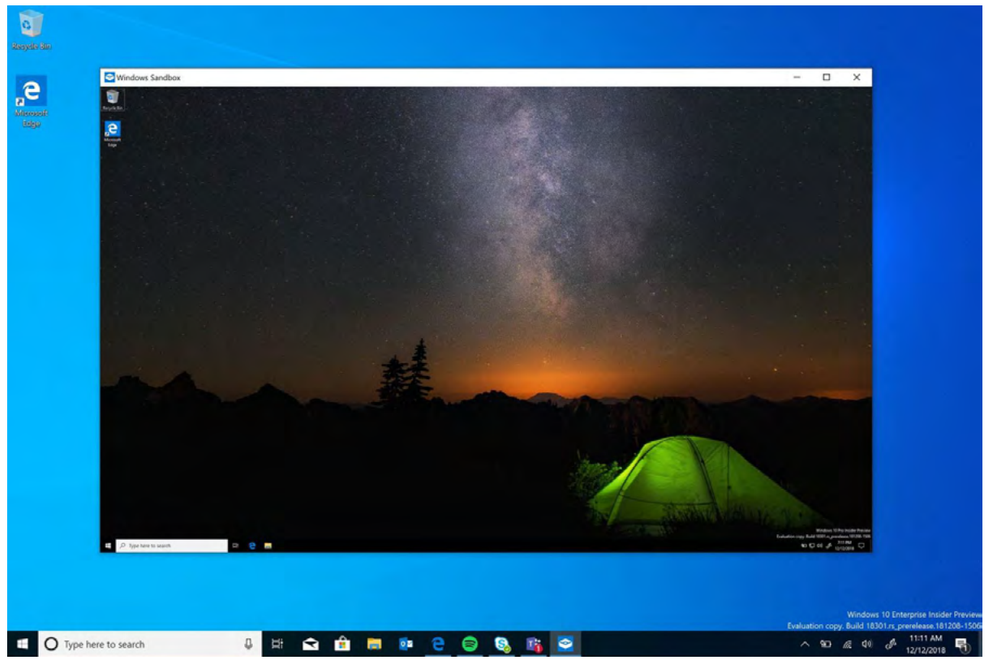


Abbildung 10: Windows 10 Preview Build mit laufender Windows Sandbox [13]

Eignung für den Einsatz beim Endbenutzer

Eine Windows Sandbox eignet sich wie oben beschrieben zum Aufsetzen einer temporären Testumgebung, jedoch aufgrund ihrer flüchtigen Natur nicht für den dauerhaften Betrieb im Arbeitsalltag. Damit schränkt sich der Benutzerkreis drastisch auf technische Administratoren bzw. Expertenbenutzer ein. Ausserdem bleibt das grundsätzliche Problem von virtuellen Maschinen, die auf einem unsicheren Hostsystem aufsetzen bestehen [vgl. Kapitel «Herkömmliche Virtualisierungslösungen am Beispiel Parallels»]. Damit wäre Windows Sandbox ebenfalls ungeeignet zur Lösung der mit gapfruit OS adressierten Problematik.

Andere Security Tools

Es existiert eine Vielzahl weiterer Security Tools wie bspw. Bromium oder Sandboxie, die ebenfalls nach dem Sandboxing Prinzip funktionieren.

Funktionsweise Bromium

Bromium isoliert Benutzertasks wie bspw. E-Mail Attachments, Links oder Datei Downloads in so genannte Micro Virtual Machines. Micro VMs sind für den jeweiligen Task zugeschnittene, minimale virtuelle Maschinen. Sie beinhalten jeweils nur genau die Funktionalität, welche zur Ausführung des Tasks notwendig ist. Für jeden Task wird eine solche Micro VM erzeugt und der Task anschliessend darin ausgeführt. Potentiell vorhandene Malware kann nicht aus dieser Micro VM ausbrechen und das Hostsystem kompromittieren. Nach Abschluss des Tasks wird die virtuelle Maschine wiederum aufgelöst. [14], [15]

Funktionsweise Sandboxie

Sandboxie erzeugt unter Verwendung von Virtualisierungstechnologie eine isolierte Umgebung zur Ausführung von Applikationen. Dadurch kann das unterliegende Hostsystem durch die ausgeführten Anwendungen nicht modifiziert und damit nicht kompromittiert werden. Auf diese Weise können beispielsweise nicht vertrauenswürdige Anwendungen in einer sicheren Umgebung getestet werden. Sandboxie erlaubt es aber auch das Surfen im Internet oder Senden und Empfangen von E-Mails in diesem sicheren Kontext zu betreiben. [16], [17]

Eignung für den Einsatz beim Endbenutzer

Aufgrund der beschriebenen Problematik mit dem unsicheren Hostsystem genügen auch diese Tools nicht den gesetzten Anforderungen zu einer wirklich sicheren Lösung.

Literaturverzeichnis

[1] «crypto AG». [Online]. Verfügbar unter: https://www.crypto.ch/en. [Zugegriffen: 18-Sep-2018].

[2] secunet S. N. AG, «SINA Clients | secunet», *secunet AG*. [Online]. Verfügbar unter: https://www.secunet.com/de/produkte/sina-clients/. [Zugegriffen: 19-Sep-2018].

[3] «TrustedDesktop | Sirrix Aktiengesellschaft». [Online]. Verfügbar unter: https://www.sirrix.com/content/pages/trusteddesktop_en.htm. [Zugegriffen: 18-Sep-2018].

[4] «Security Laptop cyber-top | genua GmbH». [Online]. Verfügbar unter: https://www.genua.de/loesungen/security-laptop-cyber-top.html. [Zugegriffen: 18-Sep-2018].

[5] «General Dynamics», *General Dynamics*. [Online]. Verfügbar unter: https://www.gd.com/. [Zugegriffen: 18-Sep-2018].

[6] «Qubes OS: A reasonably secure operating system», *Qubes OS*. [Online]. Verfügbar unter: https://www.qubes-os.org/. [Zugegriffen: 18-Sep-2018].

[7] «Parallels: Mac & Windows Virtualization, Remote Application Server, Mac Management Solutions», 21-Aug-2018. [Online]. Verfügbar unter: https://www.parallels.com/. [Zugegriffen: 28-Okt-2018].

[8] Admin, «The Different Types of Virtualization in Cloud Computing – Explained». [Online]. Verfügbar unter: https://www.redswitches.com/blog/different-types-virtualization-cloud-computing-explained/. [Zugegriffen: 26-Dez-2018].

[9] «What is Virtualization & Its Types?», *Chronicloop*, 02-Okt-2017. .

[10] «Weighing hosted, bare-metal, OS and hybrid server virtualization», *SearchServerVirtualization*. [Online]. Verfügbar unter: https://searchservervirtualization.techtarget.com/tip/Weighing-hosted-bare-metal-OS-and-hybrid-server-virtualization. [Zugegriffen: 26-Dez-2018].

[11] «Windowed, Full Screen or Coherence view mode». [Online]. Verfügbar unter: https://www.parallels.com/blogs/view-modes-parallels-desktop/. [Zugegriffen: 25-Dez-2018].

[12] «Announcing Windows 10 Insider Preview Build 18305 | Windows Experience Blog». [Online]. Verfügbar unter: https://blogs.windows.com/windowsexperience/2018/12/19/announcing-windows-10-insider-preview-build-18305/. [Zugegriffen: 27-Dez-2018].

[13] «Windows Sandbox», *TECHCOMMUNITY.MICROSOFT.COM*, 19-Dez-2018. [Online]. Verfügbar unter: https://techcommunity.microsoft.com/t5/Windows-Kernel-Internals/Windows-Sandbox/ba-p/301849. [Zugegriffen: 23-Dez-2018].

[14] «Advanced Malware Protection with Application Isolation», *Bromium*. [Online]. Verfügbar unter: https://www.bromium.com/. [Zugegriffen: 23-Dez-2018].

[15] «Bromium», *Wikipedia*. 16-Sep-2018.

[16] «Sandboxie - Sandbox software for application isolation and secure Web browsing». [Online]. Verfügbar unter: https://www.sandboxie.com/. [Zugegriffen: 23-Dez-2018].

[17] «Sandboxie», *Wikipedia*. 15-Okt-2018.

MAS HCID Masterarbeit 2018

Leitfaden Interview

Halbstrukturiertes Interview, Juni 2018

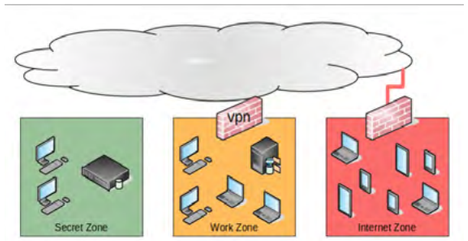
Security vs. Usability – Barrierefreiheit in einem hochsicheren Betriebssystem

Name Interviewperson

Bezeichnung/Position

Persönliche Sicht auf heutige Gefahren in der IT-Security:

Einleitung



- UX Team stellt sich vor (Name, Funktion, Aufgaben)
- Vorstellung Projekt und Produkt gapfruit OS

Kontext-Fragen

(Vertiefen mit Fokus-Fragen, wenn passend)

a) Warum geschieht es trotz technischer Sicherheitsvorkehrungen, dass sensible Daten gestohlen werden und Unternehmen und Privatpersonen durch digitale Angriffe geschädigt werden können?
b) Sind die heute existierenden Lösungen technisch unzureichend oder zu komplex für Benutzer?
c) Was gehört zu den grössten Sicherheitsrisiken der heutigen IT Welt?
d) Besteht für das Thema Sicherheit in der IT Nachholbedarf? Warum?

Fokus-Fragen

1) Warum werden Betriebssysteme wie Windows, Mac OS X, etc. trotz Sicherheitslücken in Unternehmen mit sensiblen Daten eingesetzt?

- Was sind alternative Betriebssysteme, die mehr Schutz versprechen?

2) Welche technischen Massnahmen sind Ihnen bekannt um bestehende Betriebssysteme gegen "Angriffe von aussen" zu schützen?

- Sind diese vielversprechend?
- Werden diese Techniken von Benutzern verstanden/akzeptiert?
- Welche Einschränkungen entstehen dadurch für einen Nutzer in Bezug auf seine tägliche Anwendung?
  - Warum? Auf welche Weise?

3) Sind Nutzer von «sicheren» Systemen sich der Risiken und Konsequenzen bei Verletzung der Sicherheitsvorgaben bewusst?

- Wie klären sie Ihre Mitarbeiter in Bezug auf den Umgang mit sensiblen Daten auf?
- Wie fördern Sie das Bewusstsein Ihrer Mitarbeiter für das Thema IT-Sicherheit generell?

4) Sind hochsichere Betriebssysteme die auf «Virtualization» und «Compartmentalization» basieren ein Thema für Ihr Unternehmen? Welche Vorteile gegenüber «normalen» Betriebssystemen bringen diese Konzepte?

- Was bedeutet es für die Mitarbeiter (Nutzer) mit einem solchen spezialisierten Sicherheitskonzept arbeiten zu müssen (Usability)?
- Sind diese Konzepte als hochsichere Betriebssysteme anzusehen?
- Können Sie sich solche hochsicheren Betriebssysteme in der privaten Nutzung vorstellen?

5) **Warum werden «sichere» Betriebssysteme wie Qubes OS nicht häufiger in Unternehmen und im Privaten eingesetzt, um sensible Daten zu schützen?**

6) **Gibt es Ihrer Meinung nach einen Bedarf an einem neuen, sicheren Betriebssystem?**

- Auch im privaten Bereich?
- Was müsste ein sicheres Betriebssystem (Benutzer/Administratoren) bieten, um erfolgreich in Ihrem Unternehmen (oder bei Privatpersonen) eingesetzt werden zu können?

7) **Können «Thin Clients» mit Remote Desktop Umgebungen (Citrix, etc.) oder andere Cloud Lösungen bestehende Sicherheitslücken minimieren?**

- Wie schätzen Sie ihre Relevanz in Bezug auf IT Sicherheit ein?
- Welche Grenzen haben derartige Systeme?
- Für wie zukunftsträchtig halten Sie solche Systeme?

8) **Wie werden sensible Daten bei Ihnen gehandhabt?**

- Werden diese speziell klassifiziert oder an speziellen Orten abgelegt?
- Wurden bereits sensible Daten versehentlich/absichtlich weitergegeben oder waren für Unbefugte einsehbar?

9) **Was wäre für Sie (in einer idealen Welt) ein erstrebenswertes, sicheres IT System/Betriebssystem?**

- Welche Tools, Techniken und Massnahmen müssten eingeführt werden?
- Auf was würden Sie setzen?

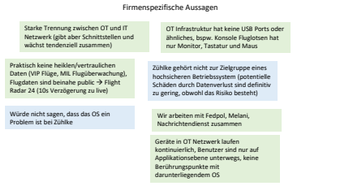
Fallbeispiele

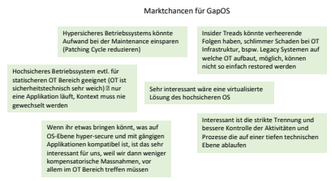
1) Sind Ihnen konkrete Beispiele bekannt, wie Benutzer bewusst oder unbewusst, bestehende Sicherheitsmechanismen aushebeln?
2) Warum denken Sie tun Benutzer das?
3) Sehen Sie eine technische Lösung für dieses Vorgehen?

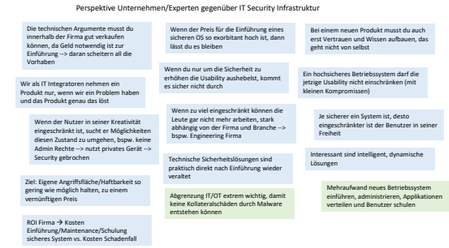
Mitnahme

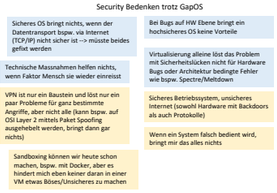
- Was nehmen wir mit grob zurückspiegeln

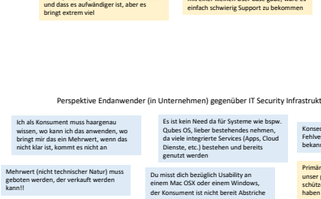
9.7 Auswertung Interviews Subject Matter Experts

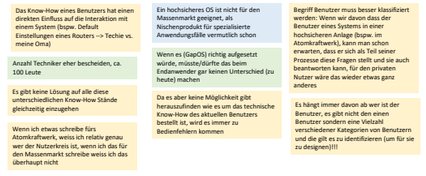


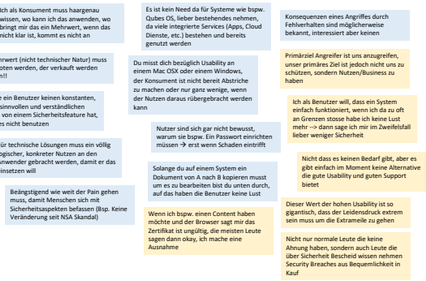


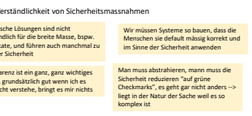


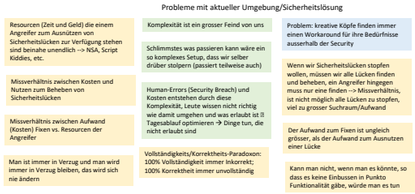


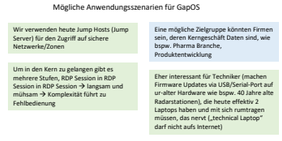










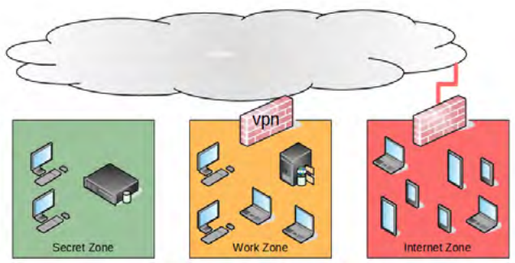


Leitfaden Experiment 1 – gapfruit OS Simulation

Einführung

Die heutzutage verwendeten Betriebssysteme wie bspw. Windows, Linux oder OSX sind über viele Jahre hinweg gewachsen und sind aufgrund ihrer Architektur nicht sicher. Über Fehler und Schwachstellen im System kann ein Angreifer durch Einschleusen von Schadsoftware bspw. via E-Mail Anhang das gesamte Betriebssystem komplett übernehmen.

Aus Unternehmenssicht existieren unterschiedliche Sicherheitskontexte, die meist durch separate, unabhängige Netzwerke getrennt sind. Dabei gibt es zum Beispiel ein Netzwerk für hochsensible, geheime Daten. Auf dieses haben nur wenige Personen Zugriff. Es ist durch den so genannten «Air Gap» physisch vom Internet und anderen internen Netzwerken getrennt. Neben dieser sensiblen Zone existiert häufig ein weiteres internes Netzwerk mit Intranet und anderen firmenspezifischen Diensten. Daneben benötigen die Mitarbeiter aber auch Zugang zum Internet für Recherchen und die Kommunikation nach aussen.



Die Firma gapfruit AG, entwickelt nun sicheres Betriebssystem für die gleichzeitige Arbeit in den unterschiedlichen Sicherheitskontexten auf einem einzigen Computer. Das Produkt ermöglicht unter anderem, dass der Benutzer zeitgleich auf öffentliche Informationen im Internet zugreifen kann, ohne dabei die interne Infrastruktur des Unternehmens zu gefährden.

Ablauf

Nach wenigen Einstiegsfragen und einer kurzen Einleitung ins Thema schauen wir uns den Prototyp an. Dabei versetzt du dich in eine bestimmte Alltagssituation und beurteilst aus dieser Perspektive die Applikation. Zum Schluss fassen wir das Gesehene und Erlebte zusammen und der Testleiter stellt dir einige Fragen zu den Erfahrungen mit dem Prototyp. Der Test dauert maximal 45 Minuten.

Bitte denke daran…

Du kannst nichts falsch machen. Der präsentierte Prototyp ist nicht vollständig und der Testleiter unterstützt dich, falls du an eine Grenze stösst. Das zu erstellende Betriebssystem ist noch im Entstehungsprozess und der Prototyp simuliert den aktuellen Wissensstand. Bitte „denke laut“ und äussere jederzeit frei und offen deine Meinung: Alle deine Gedanken sind wertvoll!

stiegsfragen

1. Wie alt bist du?

   _____

2. Als was arbeitest du?

   _____

3. Wie viel Erfahrung im Umgang mit dem Computer hast du?

   _____

4. Wie oft und wozu nutzt du einen Computer (Desktop/Notebook)?

   _____

5. Welche Geräte (z.B. Desktop, Laptop, Tablets etc.) benutzt du am häufigsten in deinem privaten sowie beruflichen Alltag?

   _____

6. Hat sich dein Verhalten in der Computernutzung seit Einführung von Smartphones und Tablets verändert?

   _____

7. Hast du bei deiner Arbeit mit (hoch-)sensiblen Daten zu tun? Falls ja, um welche Art von Daten handelt es sich dabei?

   _____

8. Bist du mit den Gefahren von Cyberkriminalität vertraut und wirkst ihnen aktiv entgegen?

   _____

Aufgaben

Du bist Mitarbeiter/in in einer Firma für Computersicherheit. Es ist Freitagmorgen du kommst verschlafen ins Büro und startest deinen Computer.

1 News

Um richtig wach zu werden surfst du als erstes deine Lieblingsseite http://heise.de für Neuigkeiten aus der IT Branche an. Ein Artikel erregt deine Aufmerksamkeit, da du gerade gestern mit deinem Arbeitskollegen über eben dieses Thema diskutiert hast. Kurz entschlossen kopierst du den Link zum Artikel und sendest ihn zusammen mit einer kurzen Nachricht per E-Mail an deinen Kollegen adrian.schmid@hsr.ch.

2 Zusammenfassung Bedrohungslage

Beim Versenden des Artikels via E-Mail bemerkst du eine neu eingetroffene E-Mail. Ein Kollege ist für die nächsten Wochen krankgeschrieben und bittet dich seine Aufgaben in dieser Zeit zu übernehmen. Konkret sollst du eurem gemeinsamen Vorgesetzten eine Zusammenfassung über die aktuelle Bedrohungslage im Bereich der Cyberkriminalität zukommen lassen. Detaillierte Anweisungen dazu stehen in der E-Mail (hcid_secos@outlook.com).

Hallo liebe Testperson

Infolge eines Unfalls falle ich für die nächsten Wochen leider aus. Ich müsste bis heute Abend für Daniel noch die wichtigsten Eckdaten der aktuellen Studien zum Thema Cyberkriminalität zusammenfassen. Es wäre herzallerliebst, wenn du mich in dieser Angelegenheit vertreten könntest. Folgendes müsste dazu erledigt werden:

1. *Dokumente als Quelle der Zusammenfassung herunterladen*
   McAfee: https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html
   Accenture: https://www.accenture.com/us-en/insight-cost-of-cybercrime-2017
   Cybersecurity Ventures: https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf

2. *Mail mit den wichtigsten Eckdaten aus den Berichten erstellen (zufällig irgendwelche Kennzahlen aus dem jeweiligen Bericht kopieren und in E-Mail einfügen)*

3. *Berichte an E-Mail anhängen und an daniel.crvelin.gonzalez@hsr.ch senden*

Herzlichen Dank und frohes Schaffen

3 Organisation Abschiedsfest

Ein langjähriger Arbeitskollege tritt seine letzte Arbeitswoche in eurem Unternehmen an. Aus diesem Anlass organisiert deine Abteilung ein Abschiedsfest. Du bist verantwortlich den Flyer mit der Einladung für den heutigen Abend zu erstellen. Da du nicht mehr allzu viel Zeit hast, suchst du dir im Internet ein paar lustige, animierende Bilder und packst diese zusammen mit untenstehenden Eckdaten in ein Word Dokument. Da du noch einen Aufhänger für den Event brauchst, suchst du im Internet nach einem passenden Zitat und schreibst das ebenfalls auf den Flyer. Das erstellte Dokument legst du schliesslich in deiner Dropbox/Google Drive/etc. ab um in der Mittagspause beim Kopierladen um die Ecke ein paar Flyer drucken zu lassen.

Eckdaten: Beginn: Freitag, 07. September 16:00 | Ende: offen | Ort: Förrlibuckstrasse 181, Terrasse 5. Stock | Specials: Grilladen, Gin Tasting und Guggen-Musik inkl. gratis Gehörschutz

Fragebogen zum Experiment

1. Es war einfach die Aufgaben durchzuführen

   ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
   (stimme überhaupt nicht zu) (stimme voll zu)

2. Ich wusste jederzeit was ich im aktuellen Schritt tun konnte um die Aufgabe zu erfüllen

   ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
   (stimme überhaupt nicht zu) (stimme voll zu)

3. Der Prototyp hat so funktioniert, wie ich mir das vorgestellt habe

   ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
   (stimme überhaupt nicht zu) (stimme voll zu)

4. Was hat dir bei der Arbeit mit dem Prototyp am besten gefallen?

5. Was hat dir bei der Arbeit mit dem Prototyp am wenigsten gefallen?

6. Was würdest du am Prototyp ändern? Wie?

7. Ist dir sonst noch etwas aufgefallen?

Weitere Kontext-Fragen

1. Hast du jederzeit gewusst wo du dich befindest (in welchem Sicherheitskontext) und was du darin tun konntest/durftest?
2. Wie hat das Wechseln zwischen den Anwendungen funktioniert?
3. Wie hat der Split Screen für die Erfüllung der Aufgaben funktioniert?
4. Wie empfindest du den Dateiaustausch zwischen den unterschiedlichen Sicherheitskontexten?
5. Verstehst du den Sinn bzw. die Notwendigkeit der Massnahmen zur Erhöhung der Sicherheit?
6. Inwiefern bist du bereit für die Sicherheit auf einen gewissen Bedienkomfort zu verzichten?

Auswertung Experiment gapfruit OS Simulation

Für die Probanden war insbesondere der Datentransfer zwischen den unterschiedlichen Sicherheitszonen zu umständlich. Alle Dateien immer via «Shared Folder» zwischen den Zonen hin und her zu schieben war für die meisten Testpersonen nicht akzeptabel und zu ineffizient im täglichen Arbeitsprozess. Die fehlende Clipboard Funktionalität zum einfachen Kopieren von Textinhalten bewegte eine Teilnehmerin beinahe zum Abbruch des Benutzertests. Keine der Testpersonen konnte sich vorstellen, täglich so arbeiten zu müssen. Die meisten würden für sich Umgehungslösungen in der einen oder anderen Form suchen. Bereits während der Durchführung des Experiments, haben mehrere Benutzer nach Workarounds gefragt bzw. gesucht, um nur in einer einzigen Zone arbeiten zu müssen. Auch das permanente Wechseln zwischen den Sicherheitszonen empfinden die Probanden als mühsam. Es hindert sie bei der Erreichung ihres Primärziels, der effektiven und effizienten Abwicklung ihrer Arbeitsaufgaben.

Keine der befragten Personen hat im Rahmen ihrer Arbeit mit hochsensiblen Daten zu tun oder versteht sich als Bearbeiter derartiger Daten. Es gibt in der Firma zwar klassifizierte, nicht für die Öffentlichkeit bestimmte Daten, diese werden jedoch von den Probanden innerhalb der Firmenrichtlinien bearbeitet und damit ist das Thema für sie erledigt. Die meisten der befragten Probanden waren sich allerdings darin einig, dass Personen, welche sich in einem spezialisierten Umfeld mit hochsensiblen Daten bewegen, vermutlich eher Verständnis für zusätzliche Arbeitsschritte aufgrund von Sicherheitsmassnahmen aufbringen und den Wert darin erkennen können. Grundsätzlich gilt also folgendes:

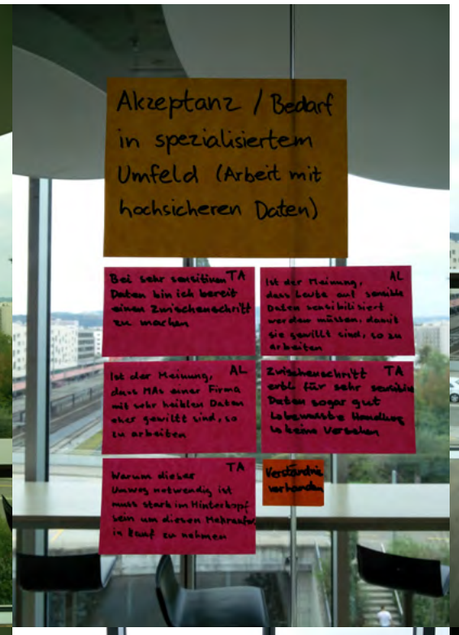
- Anwender, die nicht mit sensiblen Daten zu tun haben oder ihre bearbeiteten Daten selbst nicht als sensibel wahrnehmen, haben kein Verständnis für die spezielle Behandlung des Sicherheitsaspektes und den daraus resultierenden, zusätzlich notwendigen Schritten im Arbeitsprozess.
- Anwender, die mit sensiblen Daten arbeiten oder zumindest bestimmte bearbeitete Daten als schützenswert ansehen, sind eher bereit, für kritische Aktionen einen gewissen Zusatzaufwand in der Bedienung in Kauf zu nehmen. Diese Toleranz gilt jedoch ausschliesslich für diese sensitive Teilmenge der bearbeiteten Daten. Bei der Bearbeitung von sensitiven Daten wird eine technische Hürde von manchen sogar als hilfreich und wünschenswert wahrgenommen, da die Daten somit nicht versehentlich kopiert bzw. unsachgemäss behandelt werden (evtl. auch um sich die Sensitivität der Daten immer wieder bewusst zu machen).

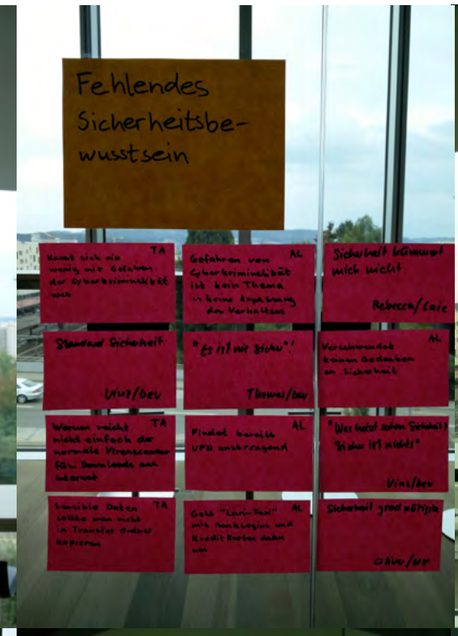
Etwa die Hälfte der Benutzer gab auch ohne Umschweife zu, sich nicht um die Datensicherheit zu kümmern oder gar verantwortungslos mit sensiblen Daten wie Banklogins und Kreditkartendaten umzugehen. Ein Benutzer erklärte, dass er erst seit einem Hack sein Verhalten angepasst hat und nicht mehr überall dasselbe Standard-Passwort verwendet. Von einem Betriebssystem wird grundsätzlich erwartet, dass Sicherheit transparent gelöst ist. Der gewöhnliche Benutzer will sich nicht mit Sicherheitsfunktionen auseinandersetzten und delegiert die Verantwortung implizit ans System. Insbesondere nicht technische Benutzer kennen weder die Gefahren, noch verfolgen sie eine Strategie, um Risiken zu vermindern. Tendenziell gilt: Je grösser das technische Knowhow, desto höher die Bereitschaft zur Risikoverminderung und zur Ergreifung von Gegenmassnahmen.

Window Management scheint eher ein Nebenschauplatz und eine Frage des persönlichen Geschmacks zu sein. So nutzen bspw. einige Anwender virtuelle Desktops und andere nicht. Es gibt bereits viele gute Ansätze in den unterschiedlichen Betriebssystemen wie Mac OS und Windows 10 die für den Anwendungszweck sinnvoll kombiniert werden können. Der permanente Split-Screen Modus fand jedoch keine Anhänger. Für die meisten Probanden war der 15-Zoll Monitor zu klein, um sinnvoll im Split-Screen Modus arbeiten zu können. Zumeist waren die Testpersonen auch der Ansicht, dass sie auf dem kleinen Monitor nicht beide Zonen parallel betreiben oder alternativ die Zonen jeweils auf einen separaten, physischen Monitor auslagern möchten. Gäbe es die Möglichkeit eine Zone zu minimieren und mit der anderen im Fullscreen Modus zu arbeiten, würde diese auf dem kleinen Monitor genutzt werden.

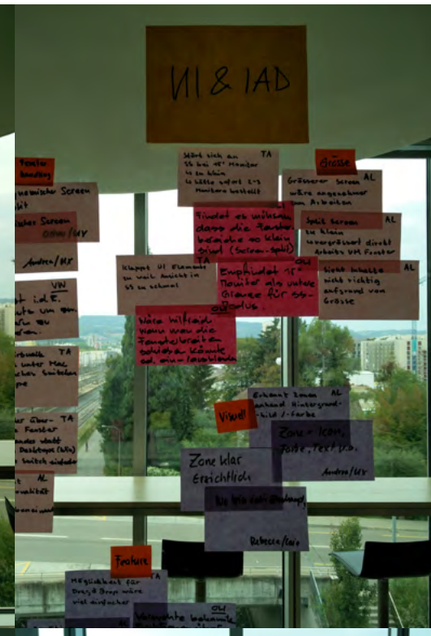
Eine zusätzliche Schwierigkeit des Testsetups bestand in den doppelt verschachtelten Fenstern, VM-Fenster vs. untergeordnete Gastsystem-Applikationsfenster. Mehrere Testpersonen verklickten sich und minimierten statt des gewünschten Gastsystem-Applikationsfensters das gesamte VM-Fenster. Ein möglicher Lösungsansatz, der von einem Probanden genannt wurde, könnte der so genannte «Seamless Mode» sein. Dabei verschwinden die VM-Fenster vom Desktop und es existieren nur noch die Gastsystem-Applikationsfenster nebeneinander, fast wie in einem gewöhnlichen Betriebssystem.

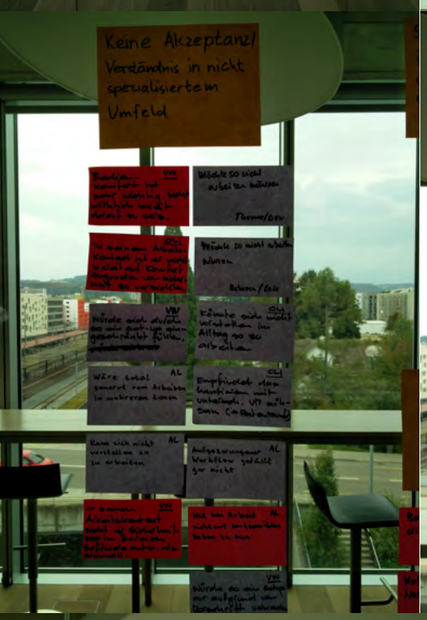

Workarounds für erzwungene Arbeitsweise

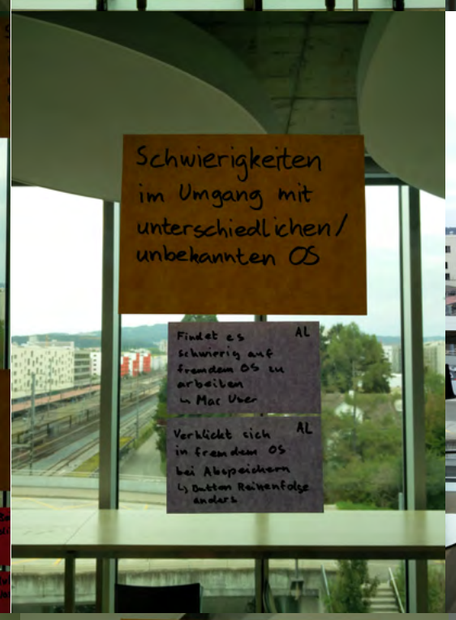

Akzeptanz / Bedarf in spezialisiertem Umfeld (Arbeit mit hochsicheren Daten)

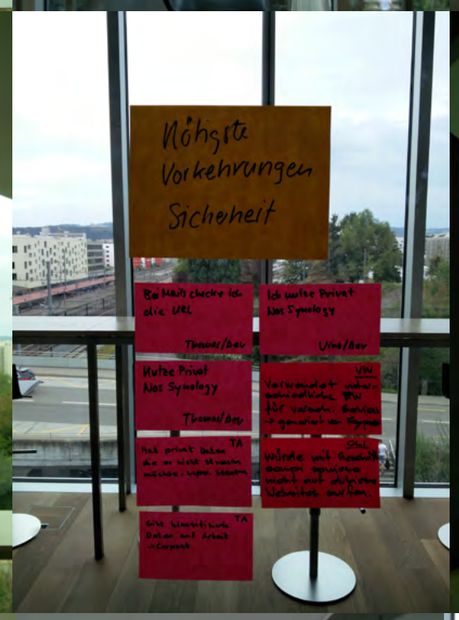

Fehlendes Sicherheitsbewusstsein


Workarounds für erzwungene Arbeitsweise

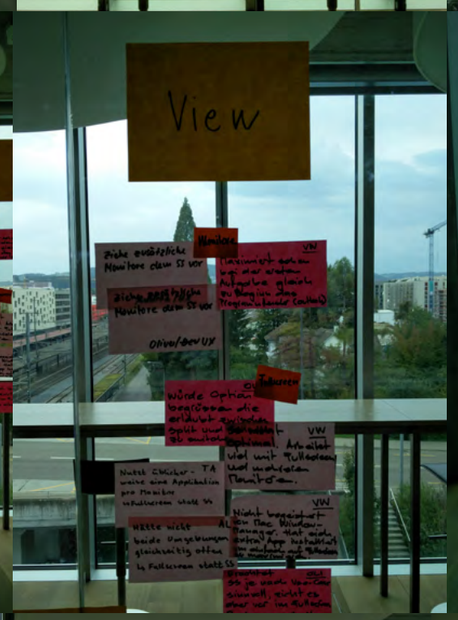

VI & IAD

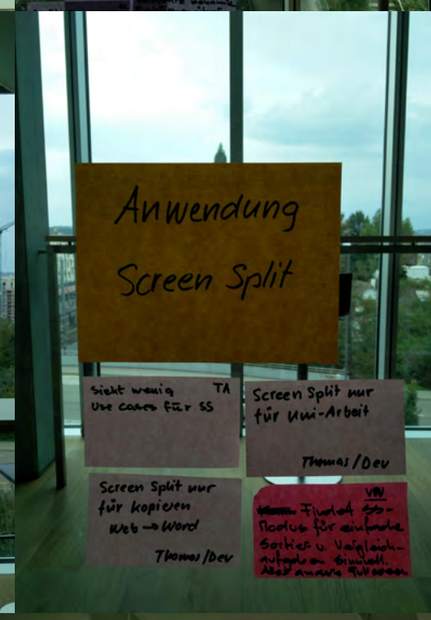

Keine Akzeptanz/ Verständnis in nicht spezialisiertem Umfeld

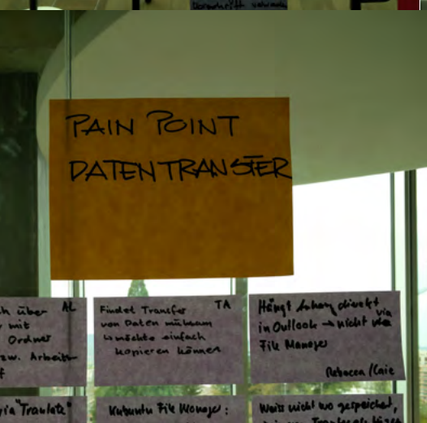

Schwierigkeiten im Umgang mit unterschiedlichen/ unbekannten OS

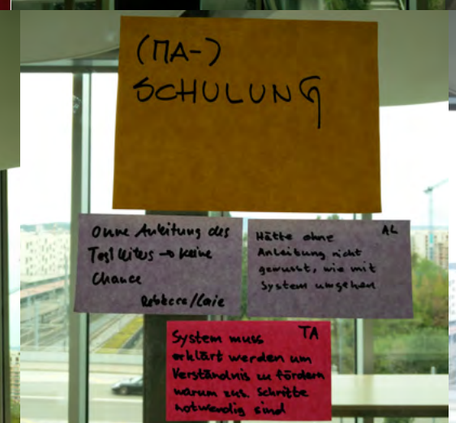

Nötigste Vorkehrungen Sicherheit

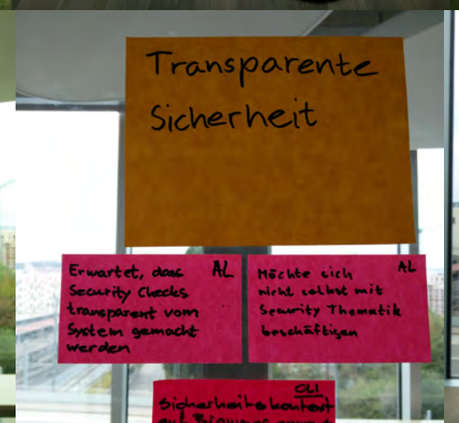

VI & IAD
View

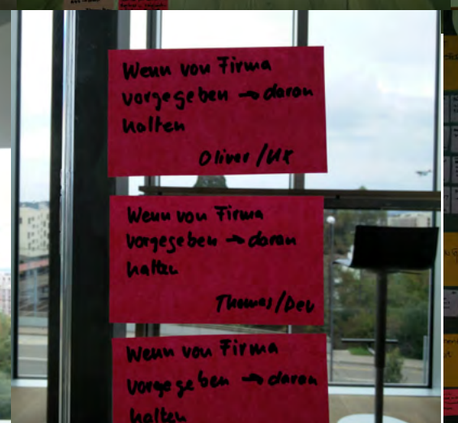

View


Anwendung Screen Split


PAIN POINT DATENTRANSFER


(MA-) SCHULUNG


Transparente Sicherheit




VI & IAD
View

MAS HCID Masterarbeit 2018 – gapfruit AG

Leitfaden Experiment 2 – Shared Filesystem

Hintergrund

Das Startup gapfruit AG entwickelt ein Endpoint System für die gleichzeitige Arbeit in unterschiedlichen Sicherheitszonen auf einem einzigen Computer. Die strikte Separierung der Zonen auf dem Endpoint wird durch ein neues Betriebssystem auf mittels «Virtualization» und «Compartmentalization» (=Kontrollierter Zugriff auf Daten und Hardware-Ressourcen in den jeweiligen Zonen) sichergestellt.

In unserer Projektarbeit führen wir regelmässige Testverfahren mit Testpersonen zu der von gapfruit AG zu erstellender Applikation, durch. Dabei möchten wir herausfinden, was du an dieser Applikation gut oder schlecht findest und ob deine Wünsche und Bedürfnisse damit erfüllt werden können oder nicht.

Ablauf

Nach wenigen Einstiegsfragen und einer kurzen Einleitung ins Thema Sicherheit und Filemanagement schauen wir uns die Applikation an. Dabei versetzt du dich in eine bestimmte Alltagssituation und beurteilst aus dieser Perspektive die Applikation. Der Testleiter stellt dir jeweils pro Handlung einige Fragen.
Am Ende fassen wir das Gesehene und Erlebte zusammen. Der Test dauert maximal 45 Minuten.

Bitte denke daran…

Du kannst nichts falsch machen. Die präsentierte Applikation ist ein Prototyp. Das bedeutet hauptsächlich, dass die Applikation noch in einem Entstehungsprozess ist. Bitte „denke laut“ und sagen jederzeit frei und offen deine Meinung: Alle deine Gedanken sind wertvoll!

Aufgaben

Der dir vorgelegte Prototype zeigt dir einen Filemanager (FM). Dieser FM beinhaltet die drei Sicherheitszonen **Internet, Work, Secret.** Die Zone **«Secret»** kannst du in diesen Prototypen aber nicht aktive nutzen.

Anleitungszenario 1 – Neues Word Dokument erstellen

1) In unseren Prototypen möchtest du ein neues Word Dokument erstellen und bearbeiten (in dem du auf das Dokument klickst).
2) Nach dem bearbeiten des Dokuments speicherst du dieses Worddokument in deinen Ordner «Eigene Dateien» unter deiner «Secret» Zone (Space).
3) Zum Schluss möchtest du dein soeben erstelltes Dokument noch mit dem Label «Methoden» versehen.

Anleitungszenario 2 – Download Word Dorkument aus dem Internet

1) In unseren Prototypen möchtest du eine Word Dokument aus dem Internet runterladen
2) und in deiner Arbeitsumgebung bearbeiten.
3) Nach der Bearbeitung speicherst du diese Worddokument in deinem Space «Secret» in deinem Ordner «Eigene Dateien»
4) und versiehst das Dokument mit dem Label «**Methoden**».

Beobachtungen Experiment

Benutzertest und Interview, Oktober 2018

Filemanagement – Barrierefreiheit in IT-Security Betriebssystemen

Name Interviewperson

_____

Bezeichnung/Position

_____

Alter

_____

Erfahrung im Umgang mit Computer

_____

Anmerkung an die Testleiter: Der Proband hat jeweils mehrere Möglichkeiten diese Aufgaben zu bewältigen. Es interessiert uns welcher Weg der Proband wählt.

Fragebogen zum Experiment Filemanagement

1. Es war einfach die Aufgaben durchzuführen

   ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
   (stimme überhaupt nicht zu) (stimme voll zu)

2. Ich wusste jederzeit was ich im aktuellen Schritt tun konnte um die Aufgabe zu erfüllen

   ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
   (stimme überhaupt nicht zu) (stimme voll zu)

3. Der Prototyp hat so funktioniert, wie ich mir das vorgestellt habe

   ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
   (stimme überhaupt nicht zu) (stimme voll zu)

4. Was hat dir bei der Arbeit mit dem Prototyp am besten gefallen?

   _____

5. Was hat dir bei der Arbeit mit dem Prototyp am wenigsten gefallen?

   _____

6. Was würdest du am Prototyp ändern? Wie?

   _____

7. Ist dir sonst noch etwas aufgefallen?

   _____

MAS HCID Masterarbeit 2018 – gapfruit AG

Leitfaden Experiment Shared Programs

Hintergrund

Das Startup gapfruit AG entwickelt ein Endpoint System für die gleichzeitige Arbeit in unterschiedlichen Sicherheitszonen auf einem einzigen Computer. Die strikte Separierung der Zonen auf dem Endpoint wird durch ein neues Betriebssystem mittels «Virtualization» und «Compartmentalization» (=Kontrollierter Zugriff auf Daten und Hardware-Ressourcen in den jeweiligen Zonen) sichergestellt.

In unserer Projektarbeit führen wir regelmässige Benutzertests mit Testpersonen zu der von gapfruit AG zu erstellender Applikation, durch. Dabei möchten wir herausfinden, was du an dieser Applikation gut oder schlecht findest und ob deine Wünsche und Bedürfnisse damit erfüllt werden können oder nicht.

Ablauf

Nach wenigen Einstiegsfragen und einer kurzen Einleitung ins Thema Sicherheit und Filemanagement schauen wir uns die Applikation an. Dabei versetzt du dich in eine bestimmte Alltagssituation und beurteilst aus dieser Perspektive die Applikation. Der Testleiter stellt dir jeweils pro Handlung einige Fragen.
Am Ende fassen wir das Gesehene und Erlebte zusammen. Der Test dauert maximal 45 Minuten.

Bitte denke daran…

Du kannst nichts falsch machen. Die präsentierte Applikation ist ein Prototyp. Das bedeutet hauptsächlich, dass die Applikation noch in einem Entstehungsprozess ist. Bitte „denke laut" und äussere jederzeit frei und offen deine Meinung: Alle deine Gedanken sind wertvoll!

Einverständnis- und Geheimhaltungserklärung

Ich bin damit einverstanden, dass die Videoaufnahmen aus dem Test zu internen Auswertungszwecken verwendet werden können. Weiter erkläre ich mich einverstanden damit,

☐ dass die Aufnahmen für schulische Zwecke verwendet werden können
☐ sowie von gapfruit AG (in Ausschnitten oder als Ganzes) intern genutzt, aber nicht unbeteiligten Dritten zugänglich gemacht werden dürfen.

Ich verpflichte mich das hier Erlebte und Gesehene, vertraulich zu behandeln.

Ort, Datum: Unterschrift:

Aufgaben

Der dir vorgelegte Prototype zeigt dir einen Filemanager (FM). Dieser FM beinhaltet die drei Sicherheitszonen **Internet, Work, Secret.** Die Zone **«Secret»** kannst du in diesen Prototypen aber nicht aktiv nutzen.

Anleitungszenario 1 – Neues Word Dokument erstellen

1) In unseren Prototypen möchtest du ein neues Word Dokument erstellen und bearbeiten (in dem du auf das Dokument klickst).
2) Nach dem Bearbeiten des Dokuments speicherst du dieses Worddokument in deinen Ordner «Eigene Dateien» unter deiner «Secret» Zone (Space).
3) Zum Schluss möchtest du dein soeben erstelltes Dokument noch mit dem Label «Methoden» versehen.

Anleitungszenario 2 – Download Dokument aus dem Internet

1) In unseren Prototypen möchtest du ein Dokument aus dem Internet herunterladen
2) und in deiner Arbeitsumgebung bearbeiten.
3) Nach der Bearbeitung speicherst du dieses Word Dokument in deinem Space «Secret» in deinem Ordner «Eigene Dateien»
4) und versiehst das Dokument mit dem Label «**Methoden**».

Fragebogen zum Experiment

1. Es war einfach die Aufgaben durchzuführen

   ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
   (stimme überhaupt nicht zu) (stimme voll zu)

2. Ich wusste jederzeit was ich im aktuellen Schritt tun konnte um die Aufgabe zu erfüllen

   ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
   (stimme überhaupt nicht zu) (stimme voll zu)

3. Der Prototyp hat so funktioniert, wie ich mir das vorgestellt habe

   ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
   (stimme überhaupt nicht zu) (stimme voll zu)

4. Was hat dir bei der Arbeit mit dem Prototyp am besten gefallen?

5. Was hat dir bei der Arbeit mit dem Prototyp am wenigsten gefallen?

6. Was würdest du am Prototyp ändern? Wie?

7. Ist dir sonst noch etwas aufgefallen?

Kontext-Fragen

1. Bist du mit den Gefahren von Cyberkriminalität vertraut und wirkst ihnen aktiv entgegen?
2. Hast du bei deiner Arbeit oder privat mit (hoch-)sensiblen Daten zu tun? Falls ja, um welche Art von Daten handelt es sich dabei?
3. Resultieren aus deiner Arbeit mit (hoch-)sensiblen Daten spezielle Nutzungsszenarien bzw. Arbeitsabläufe im Umgang mit diesen Daten? Wenn ja, welche?
4. Resultieren aus deiner Arbeit andere spezifische Nutzungsszenarien bzw. Arbeitsabläufe welche durch das Zonenkonzept tangiert werden? Wenn ja, welche?

Auswertung Experimente Shared Filesystem & Programs

Die farbliche Unterscheidung der einzelnen Zonen wurde als gut erkennbar und intuitiv beurteilt. Die Zonenzugehörigkeit im konsolidierten Dateimanager über ein Label mit der entsprechenden Zonenfarbe wurde ebenfalls als einfach verständlich und logisch wahrgenommen. Für die Probanden wurde dadurch direkt klar, welches File wie klassifiziert ist. Bei der Frage welche Farbe für welche Zone sinnvoll ist (rot = sicher vs. rot = unsicher vs. rot gar nicht verwenden, da für Leute mit Farbsehstörungen problematisch), waren sich die Teilnehmer allerdings uneinig.

Die Zonenzuteilung einer Datei wurde von den meisten gleichzeitig als eine Art Klassifizierung von Dateien angesehen und damit auch als Leitlinie zum Umgang mit den entsprechenden Inhalten. Momentan ist es jedoch schwierig zu beurteilen, ob dieser eins-zu-eins Bezug in der Realität vernünftig ist. Es würde nämlich bedeuten, dass es für jede existierende Klassifizierungsstufe in einem Unternehmen eine eigene Zone geben müsste. Das ist in der Praxis vermutlich nicht wünschenswert, da in diesem Fall zu viele Zonen existieren würden. Die Frage nach der sinnvollsten Aufteilung in Zonen kam während der Tests ebenfalls auf, wie viele Zonen sind sinnvoll und was genau ist der Unterschied zwischen den einzelnen Zonen. Insbesondere ein Teilnehmer fragte sich, ob nach ausgeführter Tätigkeit oder nach Kontext wie privat/geschäftlich/etc. geschnitten werden sollte. Hierbei könnte man ebenfalls die Klassifizierung der Daten als Kriterium anfügen.

Der zonenübergreifende Dateimanager kam mehrheitlich positiv an, da es nur einen «Topf» gibt, wo alle Dateien drin liegen. Für die Benutzer stellte dies eine Erleichterung im Vergleich zu den isolierten Dateisystemen der unterschiedlichen Zonen dar. Eine zusätzliche Möglichkeit zum Filtern nach Zonen wurde jedoch gefordert und als hilfreich angesehen. Obwohl die Benutzerführung und die Kennzeichnungen im Prozess als noch zu unklar angesehen wurden, konnte der Datentransfer auf diese Weise ebenfalls erleichtert werden. Hauptgrund hierfür war, dass die Anwender nicht mehr den Umweg über einen dedizierten Transfer Ordner gehen mussten. Der Dateimanager war für einige jedoch noch zu überladen und zu wenig übersichtlich. Die Integration des App Launchers in den Dateimanager funktionierte eher schlecht und die meisten Probanden fanden den Ort zum Starten von Programmen erst nach einem Hinweis durch den Testleiter. Der App Launcher war zu wenig klar abgegrenzt vom Dateimanager und wurde daher oft gar nicht als solcher erkannt.

Eine technische Restriktion des Systems bringt eine weitere Verständnisschwierigkeit für den App Launcher mit sich. Programme existieren genauso wie Dateien genau innerhalb eines Gastsystems. Das bedeutet, wenn ein Programm gestartet wird, öffnet sich dieses immer innerhalb der Zone, in welcher es installiert ist. Ist dasselbe Programm auf mehreren Gastsystemen und damit in mehreren Zonen installiert, muss der Anwender beim Starten über den App Launcher zusätzlich die gewünschte Zone wählen. Dies war für die meisten Teilnehmer zu abstrakt und unverständlich. Nach einer Erläuterung schien es den meisten zwar einleuchtend, jedoch zu kompliziert. Damit konnte die Sinnhaftigkeit und Benutzbarkeit eines zonenübergreifenden App Launchers nicht abschliessend geklärt werden. Die meisten Anwender gaben auf Nachfrage an, zu erwarten, dass im App Launcher nur die jeweils in der aktiven Zone verfügbaren Programme angezeigt werden.

Auch während dieser beiden Experimenten zeigte sich wiederum bei einer Mehrheit der Testpersonen, dass sie (so wie vermutlich auch ihre gesamte Berufsgattung) nicht zur Benutzergruppe eines hochsicheren Betriebssystems gehören. Etwa die Hälfte der Teilnehmenden sahen ausser einer

Auswertung Experimente Shared Filesystem & Programs

Die farbliche Unterscheidung der einzelnen Zonen wurde als gut erkennbar und intuitiv beurteilt. Die Zonenzugehörigkeit im konsolidierten Dateimanager über ein Label mit der entsprechenden Zonenfarbe wurde ebenfalls als einfach verständlich und logisch wahrgenommen. Für die Probanden wurde dadurch direkt klar, welches File wie klassifiziert ist. Bei der Frage welche Farbe für welche Zone sinnvoll ist (rot = sicher vs. rot = unsicher vs. rot gar nicht verwenden, da für Leute mit Farbsehstörungen problematisch), waren sich die Teilnehmer allerdings uneinig.

Die Zonenzuteilung einer Datei wurde von den meisten gleichzeitig als eine Art Klassifizierung von Dateien angesehen und damit auch als Leitlinie zum Umgang mit den entsprechenden Inhalten. Momentan ist es jedoch schwierig zu beurteilen, ob dieser eins-zu-eins Bezug in der Realität vernünftig ist. Es würde nämlich bedeuten, dass es für jede existierende Klassifizierungsstufe in einem Unternehmen eine eigene Zone geben müsste. Das ist in der Praxis vermutlich nicht wünschenswert, da in diesem Fall zu viele Zonen existieren würden. Die Frage nach der sinnvollsten Aufteilung in Zonen kam während der Tests ebenfalls auf, wie viele Zonen sind sinnvoll und was genau ist der Unterschied zwischen den einzelnen Zonen. Insbesondere ein Teilnehmer fragte sich, ob nach ausgeführter Tätigkeit oder nach Kontext wie privat/geschäftlich/etc. geschnitten werden sollte. Hierbei könnte man ebenfalls die Klassifizierung der Daten als Kriterium anfügen.

Der zonenübergreifende Dateimanager kam mehrheitlich positiv an, da es nur einen «Topf» gibt, wo alle Dateien drin liegen. Für die Benutzer stellte dies eine Erleichterung im Vergleich zu den isolierten Dateisystemen der unterschiedlichen Zonen dar. Eine zusätzliche Möglichkeit zum Filtern nach Zonen wurde jedoch gefordert und als hilfreich angesehen. Obwohl die Benutzerführung und die Kennzeichnungen im Prozess als noch zu unklar angesehen wurden, konnte der Datentransfer auf diese Weise ebenfalls erleichtert werden. Hauptgrund hierfür war, dass die Anwender nicht mehr den Umweg über einen dedizierten Transfer Ordner gehen mussten. Der Dateimanager war für einige jedoch noch zu überladen und zu wenig übersichtlich. Die Integration des App Launchers in den Dateimanager funktionierte eher schlecht und die meisten Probanden fanden den Ort zum Starten von Programmen erst nach einem Hinweis durch den Testleiter. Der App Launcher war zu wenig klar abgegrenzt vom Dateimanager und wurde daher oft gar nicht als solcher erkannt.

Eine technische Restriktion des Systems bringt eine weitere Verständnisschwierigkeit für den App Launcher mit sich. Programme existieren genauso wie Dateien genau innerhalb eines Gastsystems. Das bedeutet, wenn ein Programm gestartet wird, öffnet sich dieses immer innerhalb der Zone, in welcher es installiert ist. Ist dasselbe Programm auf mehreren Gastsystemen und damit in mehreren Zonen installiert, muss der Anwender beim Starten über den App Launcher zusätzlich die gewünschte Zone wählen. Dies war für die meisten Teilnehmer zu abstrakt und unverständlich. Nach einer Erläuterung schien es den meisten zwar einleuchtend, jedoch zu kompliziert. Damit konnte die Sinnhaftigkeit und Benutzbarkeit eines zonenübergreifenden App Launchers nicht abschliessend geklärt werden. Die meisten Anwender gaben auf Nachfrage an, zu erwarten, dass im App Launcher nur die jeweils in der aktiven Zone verfügbaren Programme angezeigt werden.

Auch während dieser beiden Experimenten zeigte sich wiederum bei einer Mehrheit der Testpersonen, dass sie (so wie vermutlich auch ihre gesamte Berufsgattung) nicht zur Benutzergruppe eines hochsicheren Betriebssystems gehören. Etwa die Hälfte der Teilnehmenden sahen ausser einer

MAS HCID Masterarbeit 2018 – gapfruit AG

Leitfaden Experiment – Notifications 1

Hintergrund

Das Startup gapfruit AG entwickelt ein Endpoint System für die gleichzeitige Arbeit in unterschiedlichen Sicherheitszonen auf einem einzigen Computer. Die strikte Separierung der Zonen auf dem Endpoint wird durch ein neues Betriebssystem mittels «Virtualization» und «Compartmentalization» (=Kontrollierter Zugriff auf Daten und Hardware-Ressourcen in den jeweiligen Zonen) sichergestellt.

In unserer Projektarbeit führen wir regelmässige Experimente mit Testpersonen zu der von gapfruit AG zu erstellender Applikation, durch. Dabei möchten wir herausfinden, was Sie an diesem System gut oder schlecht finden und ob Ihre Wünsche und Bedürfnisse damit erfüllt werden können oder nicht.

Ablauf

Nach wenigen Einstiegsfragen und einer kurzen Einführung ins Thema Sicherheit und ins Konzept des Systems schauen wir uns den Prototyp an. Dabei versetzen Sie sich in eine bestimmte Alltagssituation und beurteilen aus dieser Perspektive die Applikation. Der Testleiter stellt Ihnen jeweils pro Handlung oder am Ende des Experiments einige Fragen. Zum Schluss fassen wir das Gesehene und Erlebte zusammen. Der Test dauert maximal 45 Minuten.

Bitte denken Sie daran…

Sie können nichts falsch machen. Die präsentierte Applikation ist ein Prototyp. Das bedeutet hauptsächlich, dass die Applikation noch in einem Entstehungsprozess ist. Bitte „denken Sie laut“ und äusseren Sie jederzeit frei und offen Ihre Meinung: Alle Ihre Gedanken sind wertvoll!

Einverständnis- und Geheimhaltungserklärung

Ich bin damit einverstanden, dass die Videoaufnahmen aus dem Test zu internen Auswertungszwecken verwendet werden können. Weiter erkläre ich mich einverstanden damit,

☐ dass die Aufnahmen für schulische Zwecke verwendet werden können
☐ sowie von gapfruit AG (in Ausschnitten oder als Ganzes) intern genutzt, aber nicht unbeteiligten Dritten zugänglich gemacht werden dürfen.

Ich verpflichte mich das hier Erlebte und Gesehene, vertraulich zu behandeln.

Ort, Datum: Unterschrift:

Aufgaben

Der Ihnen vorgelegte Prototyp zeigt ein Betriebssystem. Dieses Betriebssystem umfasst die drei Sicherheitszonen **Internet**, **Work** und **Secret**. Die Zonen sind strikt getrennt und so abgesichert, dass bei der Kompromittierung einer Zone, bspw. durch einen Virus, die übrigen ohne Gefahr weiterbenutzt werden können. Zwischen den Zonen können Daten kontrolliert ausgetauscht werden.

Die Zone **«Internet»** fungiert als Tor nach draussen und wird für alle potentiell unsicheren Aktivitäten verwendet. Aus dieser Zone kann uneingeschränkt auf das Internet zugegriffen, Dateien heruntergeladen oder E-Mails mit Anhängen versendet und empfangen werden. Auch der Zugriff auf unsichere Speichermedien wie bspw. USB-Sticks, externe Festplatten und ähnliches ist möglich.

Die Zone **«Work»** wird als hauptsächliche Arbeitsumgebung verwendet. Hier sind alle Applikationen zur Erledigung der täglichen Arbeitsaufgaben installiert. Die Zone bietet ausserdem Zugriff auf firmeninterne Dienste wie Intranet oder Fileserver zur Datenablage. Ein Zugriff auf das freie Internet ist nicht möglich.

Die Zone «**Secret**» dient als Ablageort für sehr sensitive Daten wie bspw. spezifisches, wettbewerbsentscheidendes Firmen Knowhow, heikle Kunden- und Personendaten, Verträge oder ähnliches.

Anwendungsszenario 1 (Dani) 1 – Neues Word Dokument erstellen

Sie haben soeben an einem externen Workshop zum Thema Cybersicherheit und Umgang mit sensiblen Daten teilgenommen. Ihre Notizen aus der Veranstaltung möchten Sie auch Ihren Kollegen gerne zur Verfügung stellen. Dazu erstellen Sie ein neues Word Dokument mit einer Zusammenfassung aus dem besuchten Workshop. Anschliessend soll das erstellte Dokument in der «Work Zone» unter «Eigene Dateien» abgespeichert werden.

Hinweis: Im Prototyp müssen Inhalte nie von Hand eingetippt werden, durch einen Klick auf das Dokument erscheint der Inhalt.

Für Proband nicht sichtbar: Während des Erstellens des Word Dokuments trifft eine Benachrichtigung über eine neue, wichtige Mail in der «Internet Zone» ein. Die Mail beinhaltet den dringenden Auftrag, ein weiteres, an die E-Mail angehängtes Word Dokument zu überprüfen und mit Anmerkungen zu versehen. Dazu muss dieses heruntergeladen und in die «Work Zone» transferiert werden.

Testleiter: Wenn der Proband nicht auf die Mail Benachrichtigung reagiert aktiv nachfragen und auf «wichtige E-Mail» hinweisen. E-Mail Szenario ersetzt ursprüngliche Aufgabenstellung

Anwendungsszenario 2 (Adi) – Dokument in Work Zone transferieren

Das im Szenario 1 in den «Download Ordner» heruntergeladene Dokument [Auftrag.doc] soll nun mit dem eigenen Label [Review] und dem vordefinierten Label Zone [Secret] versehen werden. Danach wird es zur Kontrolle geöffnet und wieder geschlossen.

Emotional Response Cards

1. Wählen Sie diejenigen Worte, welche das System bzw. Ihr Gefühl im Umgang mit dem System am besten beschreiben
2. Priorisieren Sie die gewählten Worte
3. Wählen Sie die Top 5
4. Warum haben Sie diese Worte ausgewählt?

Gewählte Begriffe/Erläuterungen:

_____

_____

_____

_____

_____

_____

_____

Kontext-Fragen & Nutzungsszenarien

1. Farben und Zonen --> Zusammenhang? → *konkret nachfragen*
2. Varianten Zonenswitch vergleichen --> A/B Testing? → *konkret nachfragen*
3. Sind Sie mit den Gefahren von Cyberkriminalität vertraut und wirkst ihnen aktiv entgegen?
4. Haben Sie bei Ihrer Arbeit oder privat mit (hoch-)sensiblen Daten zu tun? Falls ja, um welche Art von Daten handelt es sich dabei?
5. Resultieren aus Ihrer Arbeit mit (hoch-)sensiblen Daten spezielle Nutzungsszenarien bzw. Arbeitsabläufe im Umgang mit diesen Daten? Wenn ja, welche? → *User Story Mapping*
6. Resultieren aus Ihrer Arbeit andere spezifische Nutzungsszenarien bzw. Arbeitsabläufe welche durch das Zonenkonzept tangiert werden? Wenn ja, welche? → *User Story Mapping*

MAS HCID Masterarbeit 2018 – gapfruit AG

Leitfaden Experiment – Notifications 2

Hintergrund

Das Startup gapfruit AG entwickelt ein Endpoint System für die gleichzeitige Arbeit in unterschiedlichen Sicherheitszonen auf einem einzigen Computer. Die strikte Separierung der Zonen auf dem Endpoint wird durch ein neues Betriebssystem mittels «Virtualization» und «Compartmentalization» (=Kontrollierter Zugriff auf Daten und Hardware-Ressourcen in den jeweiligen Zonen) sichergestellt.

In unserer Projektarbeit führen wir regelmässige Experimente mit Testpersonen zu der von gapfruit AG zu erstellender Applikation, durch. Dabei möchten wir herausfinden, was Sie an diesem System gut oder schlecht finden und ob Ihre Wünsche und Bedürfnisse damit erfüllt werden können oder nicht.

Ablauf

Nach wenigen Einstiegsfragen und einer kurzen Einführung ins Thema Sicherheit und ins Konzept des Systems schauen wir uns den Prototyp an. Dabei versetzen Sie sich in eine bestimmte Alltagssituation und beurteilen aus dieser Perspektive die Applikation. Der Testleiter stellt Ihnen jeweils pro Handlung oder am Ende des Experiments einige Fragen. Zum Schluss fassen wir das Gesehene und Erlebte zusammen. Der Test dauert maximal 45 Minuten.

Bitte denken Sie daran…

Sie können nichts falsch machen. Die präsentierte Applikation ist ein Prototyp. Das bedeutet hauptsächlich, dass die Applikation noch in einem Entstehungsprozess ist. Bitte „denken Sie laut“ und äusseren Sie jederzeit frei und offen Ihre Meinung: Alle Ihre Gedanken sind wertvoll!

Einverständnis- und Geheimhaltungserklärung

Ich bin damit einverstanden, dass die Video-/Audioaufnahmen aus dem Test zu internen Auswertungszwecken verwendet werden können. Weiter erkläre ich mich einverstanden damit,

☐ dass die Aufnahmen für schulische Zwecke verwendet werden können
☐ sowie von gapfruit AG (in Ausschnitten oder als Ganzes) intern genutzt, aber nicht unbeteiligten Dritten zugänglich gemacht werden dürfen.

Ich verpflichte mich das hier Erlebte und Gesehene, vertraulich zu behandeln.

Ort, Datum: Unterschrift:

Walkthrough Aufgaben

Der Ihnen vorgelegte Prototyp zeigt ein Betriebssystem. Dieses Betriebssystem umfasst die drei Sicherheitszonen **Internet**, **Work** und **Secret**. Die Zonen sind strikt getrennt und so abgesichert, dass bei der Kompromittierung einer Zone, bspw. durch einen Virus, die übrigen ohne Gefahr weiterbenutzt werden können. Zwischen den Zonen können Daten kontrolliert ausgetauscht werden.

Die Zone **«Internet»** dient als Tor nach aussen und wird für alle potentiell unsicheren Aktivitäten verwendet. Aus dieser Zone kann uneingeschränkt auf das Internet zugegriffen, Dateien heruntergeladen oder E-Mails mit Anhängen versendet und empfangen werden. Auch der Zugriff auf unsichere Speichermedien wie bspw. USB-Sticks, externe Festplatten und ähnliches ist möglich.

Die Zone **«Work»** wird als hauptsächliche Arbeitsumgebung verwendet. Hier sind alle Applikationen zur Erledigung der täglichen Arbeitsaufgaben installiert. Die Zone bietet ausserdem Zugriff auf firmeninterne Dienste wie Intranet oder Fileserver zur Datenablage. Ein Zugriff auf das freie Internet ist nicht möglich.

Die Zone «**Secret**» dient als Ablageort für sehr sensitive Daten wie bspw. spezifisches, wettbewerbsentscheidendes Firmen Knowhow, heikle Kunden- und Personendaten, Verträge oder ähnliches.

Anwendungsszenario 1 (Dani) 1 – Neues Word Dokument erstellen

Sie haben soeben an einem externen Workshop zum Thema Cybersicherheit und Umgang mit sensiblen Daten teilgenommen. Ihre Notizen aus der Veranstaltung möchten Sie auch Ihren Kollegen gerne zur Verfügung stellen. Dazu erstellen Sie ein neues Word Dokument mit einer Zusammenfassung aus dem besuchten Workshop. Anschliessend soll das erstellte Dokument in der «Work Zone» unter «Eigene Dateien» abgespeichert werden.

Hinweis: Im Prototyp müssen Inhalte nie von Hand eingetippt werden, durch einen Klick auf das Dokument erscheint der Inhalt.

Für Proband nicht sichtbar: Während des Erstellens des Word Dokuments trifft eine Benachrichtigung über eine neue, wichtige Mail in der «Internet Zone» ein. Die Mail beinhaltet den dringenden Auftrag, ein weiteres, an die E-Mail angehängtes Word Dokument zu überprüfen und mit Anmerkungen zu versehen. Dazu muss dieses heruntergeladen und in die «Work Zone» transferiert werden.

Testleiter: Wenn der Proband nicht auf die Mail Benachrichtigung reagiert aktiv nachfragen und auf «wichtige E-Mail» hinweisen. E-Mail Szenario ersetzt ursprüngliche Aufgabenstellung

Anwendungsszenario 2 (Adi) – Dokument in Work Zone transferieren

Das aus der E-Mail von Szenario 1 heruntergeladene Dokument soll zur Bearbeitung nun in die «Work Zone» transferiert und mit Anmerkungen versehen werden. Danach wird es abgespeichert und mit dem Label «Review» versehen.

Fragebogen zum Experiment

1. Es war einfach die Aufgaben durchzuführen

   ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
   (stimme überhaupt nicht zu) (stimme voll zu)

2. Ich wusste jederzeit was ich im aktuellen Schritt tun konnte um die Aufgabe zu erfüllen

   ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
   (stimme überhaupt nicht zu) (stimme voll zu)

3. Der Prototyp hat so funktioniert, wie ich mir das vorgestellt habe

   ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
   (stimme überhaupt nicht zu) (stimme voll zu)

4. Was hat dir bei der Arbeit mit dem Prototyp am besten gefallen?

5. Was hat dir bei der Arbeit mit dem Prototyp am wenigsten gefallen?

6. Was würdest du am Prototyp ändern? Wie?

7. Ist dir sonst noch etwas aufgefallen?

Kontext-Fragen & Nutzungsszenarien

1. Bist du mit den Gefahren von Cyberkriminalität vertraut und wirkst ihnen aktiv entgegen?

2. Hast du bei deiner Arbeit mit (hoch-)sensiblen Daten zu tun? Falls ja, um welche Art von Daten handelt es sich dabei?

3. Was wären die Konsequenzen/der Schaden bei einem Datenleck oder Verlust dieser Daten?

4. Resultieren aus deiner Arbeit mit (hoch-)sensiblen Daten spezielle Nutzungsszenarien bzw. Arbeitsabläufe im Umgang mit diesen Daten? Wenn ja, welche? Bitte detailliert und Schritt für Schritt ausführen. → *User Story Mapping*

5. Resultieren aus deiner Arbeit andere spezifische Nutzungsszenarien bzw. Arbeitsabläufe welche durch das Zonenkonzept tangiert werden? Wenn ja, welche? Bitte detailliert und Schritt für Schritt ausführen. → *User Story Mapping*

MAS HCID Masterarbeit 2018 – gapfruit AG

Leitfaden Experiment – Notifications 3

Hintergrund

Das Startup gapfruit AG entwickelt ein Endpoint System für die gleichzeitige Arbeit in unterschiedlichen Sicherheitszonen auf einem einzigen Computer. Die strikte Separierung der Zonen auf dem Endpoint wird durch ein neues Betriebssystem mittels «Virtualization» und «Compartmentalization» (=Kontrollierter Zugriff auf Daten und Hardware-Ressourcen in den jeweiligen Zonen) sichergestellt.

In unserer Projektarbeit führen wir regelmässige Experimente mit Testpersonen zu der von gapfruit AG zu erstellender Applikation, durch. Dabei möchten wir herausfinden, was Sie an diesem System gut oder schlecht finden und ob Ihre Wünsche und Bedürfnisse damit erfüllt werden können oder nicht.

Ablauf

Nach wenigen Einstiegsfragen und einer kurzen Einführung ins Thema Sicherheit und ins Konzept des Systems schauen wir uns den Prototyp an. Dabei versetzen Sie sich in eine bestimmte Alltagssituation und beurteilen aus dieser Perspektive die Applikation. Der Testleiter stellt Ihnen jeweils pro Handlung oder am Ende des Experiments einige Fragen. Zum Schluss fassen wir das Gesehene und Erlebte zusammen. Der Test dauert maximal 45 Minuten.

Bitte denken Sie daran…

Sie können nichts falsch machen. Die präsentierte Applikation ist ein Prototyp. Das bedeutet hauptsächlich, dass die Applikation noch in einem Entstehungsprozess ist. Bitte „denken Sie laut“ und äusseren Sie jederzeit frei und offen Ihre Meinung: Alle Ihre Gedanken sind wertvoll!

Einverständnis- und Geheimhaltungserklärung

Ich bin damit einverstanden, dass die Video-/Audioaufnahmen aus dem Test zu internen Auswertungszwecken verwendet werden können. Weiter erkläre ich mich einverstanden damit,

☐ dass die Aufnahmen für schulische Zwecke verwendet werden können
☐ sowie von gapfruit AG (in Ausschnitten oder als Ganzes) intern genutzt, aber nicht unbeteiligten Dritten zugänglich gemacht werden dürfen.

Ich verpflichte mich das hier Erlebte und Gesehene, vertraulich zu behandeln.

Ort, Datum: Unterschrift:

Walkthrough Aufgaben

Der Ihnen vorgelegte Prototyp zeigt ein Betriebssystem. Dieses Betriebssystem umfasst die drei Sicherheitszonen **Internet**, **Work** und **Secret**. Die Zonen sind strikt getrennt und so abgesichert, dass bei der Kompromittierung einer Zone, bspw. durch einen Virus, die übrigen ohne Gefahr weiterbenutzt werden können. Zwischen den Zonen können Daten kontrolliert ausgetauscht werden.

Die Zone **«Internet»** dient als Tor nach aussen und wird für alle potentiell unsicheren Aktivitäten verwendet. Aus dieser Zone kann uneingeschränkt auf das Internet zugegriffen, Dateien heruntergeladen oder E-Mails mit Anhängen versendet und empfangen werden. Auch der Zugriff auf unsichere Speichermedien wie bspw. USB-Sticks, externe Festplatten und ähnliches ist möglich.

Die Zone **«Work»** wird als hauptsächliche Arbeitsumgebung verwendet. Hier sind alle Applikationen zur Erledigung der täglichen Arbeitsaufgaben installiert. Die Zone bietet ausserdem Zugriff auf firmeninterne Dienste wie Intranet oder Fileserver zur Datenablage. Ein Zugriff auf das freie Internet ist nicht möglich.

Die Zone «**Secret**» dient als Ablageort für sehr sensitive Daten wie bspw. spezifisches, wettbewerbsentscheidendes Firmen Knowhow, heikle Kunden- und Personendaten, Verträge oder ähnliches.

Hinweis: Im Prototyp müssen Inhalte nie von Hand eingetippt werden, durch einen Klick auf das Dokument erscheint der Inhalt.

Anwendungsszenario 1 – Dokument transferieren (Rolle: Beantragender Mitarbeiter)

Du möchtest die Datei «CV Reto Muster.pdf» per E-Mail versenden. Die Datei enthält sensitive Informationen und ist daher in der Secret-Zone unter «Eigene Dateien» abgelegt. Um das Dokument per E-Mail versenden zu können, musst du die Datei zunächst in die Online-Zone transferieren.

Anwendungsszenario 2 – Transfer autorisieren (Rolle: Autorisierender Mitarbeiter)

Ein Arbeitskollege von dir hat den Transfer der Datei «CV Reto Muster.pdf» in seine Online-Zone initialisiert. Da die Datei in der Secret-Zone abgelegt ist, musst du als Eigentümer der Datei den Transfer autorisieren.

Anwendungsszenario 3 – Verschlüsselung prüfen (Rolle: Beantragender Mitarbeiter)

Deine Anfrage für den Dateitransfer wurde vom Eigentümer der Datei genehmigt. Du kannst die E-Mail jedoch noch nicht versenden, da du noch auf weitere Informationen wartest, welche dem E-Mail Schreiben beigefügt werden müssen. Du möchtest allerdings vorab schon prüfen, ob die Datei aufgrund des Transfers in die Online-Zone, korrekt verschlüsselt wurde.

Anwendungsszenario 4 – Dokument in Work Zone transferieren

Das in Szenario 1 in den «Download Ordner» heruntergeladene Dokument [Auftrag.doc] soll nun mit dem eigenen Label [Review] und dem vordefinierten Label Zone [Secret] versehen werden. Danach wird es zur Kontrolle geöffnet und wieder geschlossen.

Kontext-Fragen & Nutzungsszenarien

1. Bist du mit den Gefahren von Cyberkriminalität vertraut und wirkst ihnen aktiv entgegen?

2. Hast du bei deiner Arbeit mit (hoch-)sensiblen Daten zu tun? Falls ja, um welche Art von Daten handelt es sich dabei?

3. Was wären die Konsequenzen/der Schaden bei einem Datenleck oder Verlust dieser Daten?

4. Resultieren aus deiner Arbeit mit (hoch-)sensiblen Daten spezielle Nutzungsszenarien bzw. Arbeitsabläufe im Umgang mit diesen Daten? Wenn ja, welche? Bitte detailliert und Schritt für Schritt ausführen. → *User Story Mapping*

5. Resultieren aus deiner Arbeit andere spezifische Nutzungsszenarien bzw. Arbeitsabläufe welche durch das Zonenkonzept tangiert werden? Wenn ja, welche? Bitte detailliert und Schritt für Schritt ausführen. → *User Story Mapping*

6. Was sind deiner Meinung nach die schwerwiegendsten Probleme von Unternehmen im Umgang mit (hoch-)sensiblen Daten?

7. Könnte ein Konzept wie das im Prototyp vorgestellte helfen, Probleme im Umgang mit (hoch-)sensitiven Daten zu mindern?

8. Siehst du einen konkreten Nutzen, allenfalls für eine bestimmte Branche oder einen bestimmten Berufszweig, in der Anwendung eines Systems, wie im Prototyp vorgestellt? Insbesondere im Hinblick auf das komplexere Handling und die zusätzlich notwendigen Arbeitsschritte. Falls ja/nein, was müsste man ändern/verbessern?

9. Sind dir konkrete Anwendungsszenarien von Unternehmen bekannt, die mit (hoch-)sensiblen Daten agieren? Wenn ja, welche? → *User Story Mapping*

10. Sind dir konkrete Nutzungsszenarien bzw. Arbeitsabläufe von Unternehmen bekannt, bei welchen ein derartiges Zonenkonzept eingesetzt werden könnte? → *User Story Mapping*

9.17 Auswertung Experimente Notifications

Auswertung Experimente Labeling & Notifications 1-3

Es stellte sich heraus, dass die Definition einer Zone für die meisten Probanden in den Experimenten zu unscharf war. Die Autoren schafften es oft nicht, die notwendigen Erläuterungen adressatengerecht an die jeweilige Testperson zu übermitteln. Für technisch weniger versierte Personen waren die technischen Aspekte oft undurchschaubar während technischen Experten die exakte Definition und Abgrenzung (Zugriff auf Netzwerke; lokale Laufwerke vs. Netzwerk Shares; vordefinierte, für alle Zonen gleiche Ordnerstruktur vs. freie Ordnerstruktur; etc.) einer Zone fehlte. Dadurch entstanden zwangsweise eigene Interpretationen und Annahmen auf Seite der Testpersonen, die zu Verwirrungen während der Tests führten. In den Interviews nach dem Benutzertest brachten einige Teilnehmer diese Problematik implizit oder wie im Falle der teilnehmenden Security Experten auch ganz explizit zur Sprache.

Für viele war der Umstand, dass im Prototyp drei Zonen existierten (Online, Work und Secret) unbegreiflich. Dabei stellte sich für die Probanden vor allem die Frage nach dem Unterschied zwischen der «Work» und «Secret» Zone und welche Tätigkeiten denn in welcher dieser Zonen ausgeführt werden sollten. Die meisten Testpersonen, welche mit sensiblen Daten arbeiten, gaben an, im Rahmen ihrer Arbeitstätigkeit in diesem potentiellen Setup grösstenteils in der «Secret» Zone zu arbeiten. Dies führte zur Erkenntnis, dass in den meisten Fällen sinnvollerweise nur zwei Zonen existieren, eine unsichere zum Surfen im Internet und eine sichere zur Erledigung der restlichen Arbeiten. Gemäss Aussage eines IT Security Spezialisten mach ein Setup mit drei Zonen nur in Fällen Sinn, wo heutzutage eine Airgap Lösung eingesetzt wird.

Der Prozess zum Transferieren von Daten über das Setzen des entsprechenden Zonenlabels im zonenübergreifenden Dateimanager war für die meisten Probanden einfach zu bewerkstelligen und wurde als gut verständlich und intuitiv deklariert. In einer Variante der getesteten Prototypen wurden Zonenlabels und persönliche, frei definierbare Labels kombiniert. Diese Kombination verwirrte die Testpersonen und wurde daher im Verlauf der Experimente wieder verworfen. Ein dediziertes Zonenlabel funktionierte bei den Tests wesentlich besser. Daneben kam auch die Frage nach einer Möglichkeit zum gleichzeitigen Transfer mehrerer Dateien auf. Diese Funktion war im Prototyp nicht vorgesehen und sollte daher ergänzt werden.

Gapfruit OS kann beim Transferieren von Daten zwischen den Zonen je nach definierten Regeln verschiedene Prüfungen durchführen. Im Prototyp existierte die Regel, dass beim Verschieben einer Datei in die «Secret» Zone ein Genehmigungsprozess angestossen wird. Sobald ein Benutzer diesen Prozess startet, erhält eine autorisierte Person eine Anfrage zur Genehmigung des Datentransfers. Erst nach erfolgter Genehmigung erscheint die Datei in der neuen «Secret» Zone. Für viele Probanden war trotz der Bemühungen zur Verbesserung der Benutzerführung nicht klar, warum und in welchem Fall eine derartiger Genehmigungsprozess angestossen wird. In den Interviews mit den Testteilnehmern zeigte sich ausserdem, dass ein Genehmigungsprozess, um Daten von aussen in die sichere Zone zu bringen, kaum praktikabel sein dürfte. Aufgrund der potentiellen Masse an Anfragen würde der Administrationsaufwand für die autorisierende Person viel zu gross werden.

In spezialisierten Fällen wäre jedoch ein Genehmigungsprozess in die andere Richtung, von der sicheren/geheimen in die unsichere Zone, sinnvoll. Existiert in einer Bank bspw. eine Zone, in welcher die Mitarbeiter Zugriff auf sensitive Finanzdaten haben, möchte der Arbeitgeber nicht, dass Mitarbeiter

diese Daten frei aus dieser sicheren Zone kopieren und bspw. im Internet oder via E-Mail an Dritte weitergeben können. In so einem Fall macht oben beschriebener Genehmigungsprozess durchaus Sinn. Der interviewte Bankmitarbeiter gab jedoch an, dass in einer Bank sensible Daten im Normalfall die sichere Umgebung gar nie verlassen dürfen.

In diesem Zusammenhang stellte sich auch die Frage, ob Dateien beim Transfer verschoben oder kopiert werden. Im Prototyp war nur ein Verschieben skizziert, in der Realität müssten jedoch beide Möglichkeiten gegeben sein, damit die Benutzer genügend flexibel arbeiten können. Von einigen Probanden wurde auch die Wichtigkeit einer Sharing Funktionalität innerhalb sicherer Zonen hervorgehoben. Diese Funktionalität würde den Anwendern Zonentransfers und den Austausch von Dateien via unsicheres E-Mailing ersparen und so ihre Abläufe beschleunigen.

Als weitere Annahme war im Prototyp eine Funktionalität zur automatischen Verschlüsselung von Daten beim Transfer in die unsichere Zone umgesetzt. Die Grundidee dahinter war, dass Daten aus der sicheren Zone in der unsicheren Zone permanent auf unautorisierten Zugriff gefährdet sind. Für die meisten Benutzer war diese implizite Verschlüsselung jedoch unverständlich und unerwartet. Diese Funktionalität macht ausserdem gemäss Aussagen des IT Security Spezialisten aus technischer Sicht nur in symmetrisch aufgesetzten Systemen mit exakt derselben Zonenkonfiguration bei allen Beteiligten Sinn. Wird diese Datei nämlich versendet, müsste auf der Gegenseite eine entsprechende Konfiguration zum automatischen Entschlüsseln vorherrschen. Ansonsten können die Daten gar nicht erst gelesen werden. Grundsätzlich macht die Verschlüsselung von E-Mails bzw. der angehängten Dokumente Sinn, das bedeutet jedoch nicht, dass Dateien automatisch beim Zonenübergang verschlüsselt werden sollten.

Das neu eingeführte Notification Center auf Ebene Hostsystem wurde von den Probanden positiv aufgenommen. Die angezeigten Benachrichtigungen im simulierten Genehmigungsprozess halfen den Benutzern beim Verständnis der Abläufe im System, bspw. warum sie nach einer Transfer Anfrage nicht unmittelbar im Prozess weiterarbeiten können. Zum Verständnis warum dieser Genehmigungsprozess überhaupt notwendig ist, trugen die Benachrichtigungen hingegen wenig bei. Oft zu beobachten war auch die Tatsache, dass Benachrichtigungen ignoriert oder überlesen werden. Insbesondere wenn sich die Testperson auf die unmittelbare Erledigung einer Testaufgabe konzentriert, werden unerwartete Benachrichtigungen zur störenden Nebensache oder mit den Worten «das schaue ich mir später an» zur Seite geschoben.

Die Idee hinter dem Zonenkonzept kam bei vielen Teilnehmern gut an. Es bietet ihnen einen Rahmen zum Umgang mit den enthaltenen Daten und allenfalls deren Klassifizierung. Mehrere Probanden waren ausserdem der Auffassung, dass die unterschiedlichen Zonen zusätzlich die Awareness für sensible Daten und die damit verbundenen Gefahren fördern. Das System hat weiterhin das Potential sicherheitsrelevante, mühsam manuell ausgeführte Aufgaben zu übernehmen, die aktuell in der Eigenverantwortung von Mitarbeitern liegen. In den getesteten Prototypen waren die unterschiedlichen Zonen für die Probanden übersichtlich dargestellt und das Umschalten intuitiv möglich. Die farbliche Auszeichnung von Zone und zugehörigen Dateien funktionierte sehr gut und wurde problemlos verstanden. Die seit Einführung bestehende Problematik mit dem zonenübergreifenden App Launcher [vgl. Kapitel «Experiment Shared Files & Programs»] konnte hingegen nicht gelöst werden. Dass Programme ebenfalls ein Zonenlabel besitzen und damit in einer spezifischen Zone geöffnet werden ist für die meisten zu technisch.

Zum Einsatz eines hochsicheren Betriebssystems wie gapfruit OS herrschten auch während dieser Experimente verschiedene Meinungen vor. Aus Security Perspektive wurde das Konzept von den meisten Probanden als sinnvoll empfunden. Insbesondere ein Teilnehmer hob die Wichtigkeit hinter einem derartigen Produkt hervor, da seine Firma in jüngster Zeit vermehrt Ziel von Cyberattacken war. Mit dem Zonenkonzept kann eine kompromittierte Zone einfach neu aufgesetzt werden, ohne dass andere sichere Zonen davon betroffen sind. Die Praktikabilität im täglichen Einsatz und die Arbeitsgeschwindigkeit zur Erledigung der eigenen Aufgaben wurden jedoch mehrmals angezweifelt. Vor allem der notwendige Zonentransfer erscheint zeitraubend und wird im Vergleich zu einem gewöhnlichen Betriebssystem als zu mühsam gewertet. In den getesteten Prototypen befand sich die E-Mail Anwendung immer in der unsicheren Zone, hier fürchteten einige Probanden zu viel Mehraufwand beim permanenten Transferieren der Mail-Anhänge in die sichere Arbeitszone. Es wäre natürlich auch denkbar, die E-Mail Anwendung direkt in der sicheren Arbeitszone zu betreiben. Damit erhöht sich allerdings die Gefahr für eine Kompromittierung über eine infizierte E-Mail.

Da ein erheblicher Aufwand zur Einführung des Systems notwendig ist, stellte sich auch hier wieder die Frage wie viele Unternehmen sich so etwas antun würden. Gemäss Aussage eines IT Security Experten existieren auch andere, relativ sichere Lösungen auf dem Markt, die einfacher einzuführen sind.

Bei den durchgeführten Experimenten konnten vier zusätzliche Berufsgruppen mit möglichen Anwendungsfällen für gapfruit OS identifiziert werden. Diese potentiellen Benutzergruppen und der zugehörige Anwendungskontext werden in Kapitel [«Resultate und Bewertung»] näher beschrieben. Es handelt sich dabei um folgende:

1. Benutzergruppe Human Resources
2. Benutzergruppe Anwalt
3. Benutzergruppe Bankangestellter
4. Benutzergruppe Mitarbeiter Kreditkartenunternehmen

9.18 Bilder –Auswertung Experimente Notifications

Hans VERSICHERUNG

Versicherungs Berater
46 Jahre

- ein fast Rentner
- konservativ
- Stationär mit Kundenbesuch

Kontext

- Sensitive Kundenmandate
- Versicherungen
- Beratung
- Mobile zwischen Agentur/Büro & Kunden
- Laptop/Tablet, Personal Computer

Ziele

9-5 Job

Aufgaben

- Versicherung verkaufen
- Beratung Versicherung/Anlagen
- Kunden/Firmen besuchen

Frust

- Keine Versicherung verkaufen
- Kompliziertes Vorschrift
- viel Autofahren
- Abwechselnd Gesellschaft

Martin BEAMTER

Ingenieur, 55 Jahre
Kernenergie

- Digital Immigrant, bequem,
- "Warum Neues, wenn Altes bewährt"
- Arbeitsmittel: eher Stationär

Kontext

- Routinierte Arbeitsabläufe
- vers. Sicherheits Zonen!
- Streng Reguliert
- Arbeiten mit Personal Computer

Ziele

- Geheimhaltung von Daten
- 9 to 5 Job
- Einfach im Alltag

Aufgaben

- Zahlen, Tabellen berechnen
- Daten (sensitive) zwischen vers. Sicherheits Zonen verschieben
- Stempeln

Frust

- kein Bezug zum Internet
- muss Sicherheits Zonen wechseln

Anita ANWÄLTIN

RA lic. iur., 38 Jahre

Vertraut der ihr Angebotenen Sicherheitslösung, Wenig Design/usability Affin

Kontext

- o Sensitive Kundendaten ✓
- o Verträge ✓
- o Steuerdaten ✓
- o Vertrauensumfeld ✓

Ziele

- o Verschwiegenheit ✓
- o Seriös ✓

Aufgaben

- o Betreuen/Bearbeiten sensitiven Kundenmandate
- o Kundenrechnung (im Minutentakt)

Nutzt SW von Anwaltverband !

↳ Cloud-Lösung (sicheren Server)

Frust

~~Frust~~

Macht alles (Mail, Dokument erstellen, Kunden Dossier) in der Cloud umgebung

Vorgegeben vom Anwaltsverband !

Peter BANK

Data Science & Compliance

41 Jahre

IT Background

Kontext

- o Sensitive Kundendaten ✓
- o Finanzen ✓
- o Steuern ✓
- o Geldwäsche/Schwarzgeld ✓

Ziele

- o Geheimhaltung
- o Freigabe von Daten

Spielt keine wesentliche Rolle in der Lösung

Aufgaben

- o Datenaustausch ü. Landesgrenzen
- o Datenaustausch innerhalb Team

Bank hat eigene Lösung basiert auf Zertifikaten von eigenem Server !!

Frust

- o Lange Wartezeiten für Freigabe !

Andrea UX

UX Designerin, 38 Jahre

- Hoher Anspruch an Usability,
- Freigeist, kreativ
- Mobil

Kontext

- Umfeld mit sensiblen Daten (Kunden)
- Abstimmprozesse
- UI Design
- Arbeit auf Laptop

Ziele

- gute/verständliche Usability
- Einfache & verständliche Prozesse

Aufgabe

- Abstimmprozesse begleiten
- UI & Usability
- Kunden beraten

Frust

- Viele Schnittstellen (technisch)

Dominik ENTWICKLER

Dipl.-Informatiker, 33 Jahre

Leben in Codezeilen,
~~wenig~~ Anspruch auf Usability
viel

Kontext

- Umfeld m. sensiblen Daten
- Verwendet ~~mehrere Monitore~~, Desktop ~~oder Screen Split~~
  lieber mehrere Monitore

Hat auf Apple gewechselt, da auf keine VMs

- Kopieren von sensiblen Daten — Kommt nicht vor — arbeitet bereits in sicherer Zone
- Oft wechseln zwischen verschiedenen Ansichten (Desktop, Screens)

Ziele

- Schnelles Vorwärtskommen in der Arbeit
- Wenig Sicherheitssperren umgehen

Aufgaben

Frust

!

Potentielle Berufsgruppen und Nutzungskontext

Berufsgruppe Entwickler auf Systemen mit hochsensiblen Daten

Ein Software Entwickler im Bankenumfeld bekommt vom Arbeitgeber einen konfigurierten Arbeitslaptop mit zwei unterschiedlichen Sicherheitskontexten. Die gewöhnliche Windows Installation dient hauptsächlich zur Erledigung der administrativen Aufgaben, dem Versenden von E-Mails und dem Surfen im Internet zwecks Online Recherche. Daneben existiert lokal eine speziell gehärtete, streng kontrollierte virtuelle Maschine mit der Entwicklungs- und Testumgebung für ein wichtiges Banking System. Diese virtuelle Maschine ist vollständig vom Netzwerk abgekoppelt und hat keinen Internet-Zugang.

Die Testumgebung enthält sehr sensitive Finanz- und Kundendaten. Aus diesem Grund ist es nicht erlaubt, Daten aus der virtuellen Maschine zu kopieren und auf das Hostsystem zu bringen. Umgekehrt muss es jedoch möglich sein, Code Snippets, Tutorials, Anleitungen oder ähnliche Dokumente aus Internetrecherchen in die sichere Entwicklungsumgebung zu bringen.

Pain Points mit der aktuellen Lösung:

- Häufiges Wechseln zwischen Host- und Gastsystem je nach ausgeführter Tätigkeit, bspw. bei einer Internet-Recherche
- Code Snippets oder Tutorials aus dem Internet in die sichere virtuelle Maschine mit der konfigurierten Entwicklungs- und Testumgebung bringen
- Keine Möglichkeit Daten aus der sicheren virtuellen Maschine nach aussen zu bringen, weil technisch verhindert durch den Arbeitgeber
- Verpassen von wichtigen Terminen oder E-Mails, da bei der Arbeit in der virtuellen Maschine keine Benachrichtigungen von Hostsystem ankommen
- Schlechte Performance der virtualisierten Entwicklungs- und Testumgebung

Berufsgruppe Treuhänder

Ein Cloud-Anbieter stellt den Mitarbeitern einer Treuhandfirma virtualisierte Windows Instanzen mit installierter Revisionssoftware zur Verfügung Die Treuhandfirma hat keine eigene IT-Abteilung und rüstet alle ihre Mitarbeitenden mit gewöhnlichen Windows Notebooks aus. Offline Arbeiten, administrative Aufgaben, E-Mail Empfang und Versand sowie Internetrecherchen oder der Zugriff auf benötigte Webapps werden über die lokale Windows Installation erledigt. Über eine gesicherte Internet-Verbindung können die Mitarbeitenden schliesslich via Remote Desktop auf die Windows Oberfläche in der Cloud zugreifen und mit der Revisionssoftware arbeiten. Alle kundenspezifischen Arbeiten und Daten sollten auf der sicheren Cloud Umgebung bearbeitet und abgespeichert werden.

Erstellt ein Mitarbeiter bspw. einen Jahresabschluss für einen Kunden, benötigt er aktuelle Informationen über dessen Unternehmen sowie die Jahreszahlen. Diese werden von den Firmen meist in Geschäftsberichten online publiziert. Der Mitarbeiter wechselt also auf die lokale Windows Instanz, informiert sich auf Seiten wie bspw. Moneyhouse, lädt sich den Jahresbericht von der Webseite des Kunden herunter und kopiert ihn via Drag & Drop in die Cloud Umgebung. Dort verknüpft er das Dokument in der Revisionssoftware mit dem entsprechenden Kunden.

Zur Besprechung von Jahresabschlüssen oder ähnlichem mit Kunden oder Partnern innerhalb der Treuhandfirma müssen Kundendaten und Geschäftsberichte oft auch offline zur Verwendung in Meetings oder Präsentationen vorliegen. Da die Remote Desktop Verbindung in die sichere Cloud Umgebung nur bei vorhandener Internetverbindung möglich ist, müssen die entsprechenden Daten aus der Cloud Umgebung heruntergeladen werden. Aus diesem Grund sind die Mitarbeiter der Treuhandfirma immer wieder gezwungen Sicherheitsbestimmungen zu verletzen und sensitive Daten auf die unsichere lokale Umgebung oder auch auf USB Sticks zu kopieren. In den Meetings werden die heruntergeladenen Dokumente besprochen und oft mit Anmerkungen versehen oder anderweitig weiterbearbeitet. Die Resultate müssen schliesslich wieder manuell in die Cloud Umgebung gebracht werden.

Pain Points mit der aktuellen Lösung

- Arbeiten mit der relativ langsamen Remote Desktop Umgebung
- Sensible Kundendaten können unkontrolliert aus der sicheren Cloud Umgebung kopiert und weiterverbreitet werden
- Zum Offline Arbeiten müssen Daten aus der sicheren Cloud Umgebung kopiert und auf der unsicheren lokalen Umgebung oder auf USB Sticks abgelegt werden
- Schlampiger Umgang mit den heruntergeladenen, sensitiven Kundendaten, die Daten bleiben nach der Nutzung/Weiterbearbeitung oft auf der unsicheren, lokalen Umgebung oder auf USB Sticks liegen da das eigentlich notwendige, manuelle Löschen vergessen geht
- Es fehlt eine sichere, omnipräsente Datenablage wie bspw. OneDrive, Mitarbeiter müssen sich immer manuell um die Synchronisation der Daten kümmern und diese zwischen den Umgebungen (Cloud/lokal) hin und her kopieren

Berufsgruppe Legal Abteilung eines Unternehmens

Die Arbeit der Legal Abteilung eines Unternehmens besteht darin Kundenverträge auf rechtliche Aspekte zu prüfen und die Sales-Verantwortlichen zu beraten. Dabei kann es sich einerseits um vom Unternehmen selbst erstellte oder von Kunden erhaltene Verträge für Dienstleistungen handeln. Die Aufgabe der Legal Abteilung besteht also in der Durchsetzung rechtlicher Aspekte innerhalb von Verträgen aber auch im Unternehmen ganz allgemein.

Aktuell existiert im Unternehmen eine Legal-Mailbox. Hierhin können die Mitarbeiter ihre Anfragen bzw. Verträge zwecks Prüfung und Beratung durch das Legal Team senden. Verträge enthalten oft sensitive Daten und sind daher als vertraulich oder sogar geheim eingestuft. Es gibt sogar Fälle, in denen nur bestimmte Mitarbeiter des Legal Teams Einsicht in Verträge erhalten dürfen. Die eingegangenen Dokumente werden dann von Mitarbeitern des Legal Teams zur Bearbeitung auf eine sichere Ablage kopiert. Danach werden die Inhalte geprüft und gegebenenfalls mit Anmerkungen versehen. Dabei können auch mehrere Mitarbeiter (gleichzeitig) an einem einzigen Dokument arbeiten. Nach Abschluss der Prüfung werden die eingegangenen Dokumente inklusiv Anmerkungen und Rückmeldungen per E-Mail zurück an die Antragsteller gesendet.

Pain Points mit der aktuellen Lösung

- E-Mail ist keine sichere Plattform, um sensitive Dokumente oder Verträge auszutauschen, eine sicherere Lösung wäre interessant
- Sensitive Dokumente und Verträge bleiben unter Umständen in der unsicheren Mailbox liegen

- Mitarbeiter können sensitive Dokumente auf unsicheren Umgebungen ablegen, bspw. um zu Hause weiterarbeiten zu können
- Die gleichzeitige Arbeit an einem Dokument durch unterschiedliche Mitarbeiter ist eine Herausforderung, sollte aber möglich sein

Berufsgruppe Sound Producer

Während eines Experiments tauchte eine weitere, für die Autoren durchaus überraschende potentielle Benutzergruppe auf. Eine der befragen Personen produziert in ihrer Freizeit Musik auf einem eigens dafür eingerichteten Studio PC. Die Installation und Konfiguration dieses Computers sind ausserordentlich fragil, da bspw. bei der unbedachten Installation eines Tools oder versehentlichen Änderung einer Einstellung die Soundproduktion nicht mehr korrekt funktionieren kann. Nach eigener Aussage behandelt die Person diesen Computer «wie ein rohes Ei». Trotzdem möchte sie nebenbei damit im Internet surfen. Eine spezielle, für die Soundproduktion optimierte und vom Internet abgekoppelte Zone könnte hier interessant sein.

Pain Points mit der aktuellen Lösung:

- Eine unbedachte Installation einer Software oder (unabsichtliche) Änderung der Konfiguration hat das Potential die Soundproduktion auf dem Computer zu verunmöglichen. Das Problem muss dann in mühsamer Kleinarbeit ausfindig und rückgängig gemacht werden.

Berufsgruppe Kommunikation und Eventorganisation eines Kreditkartenunternehmens

Zum Aufgabenbereich einer im Rahmen der Experimente befragten Person gehört die Kommunikation und Eventorganisation für Premiumkunden eines Schweizer Kreditkartenunternehmens. Innerhalb

dieser Tätigkeit arbeitet die Person mit sensiblen Personen-, Konto- und Kreditkartendaten von Kunden. Werden diese Daten von einem Mitarbeitenden bearbeitet, dürfen Sie nur auf speziell gesicherten Laufwerken auf einem zentralen Dateiserver des Unternehmens abgelegt werden. Entstehen im Arbeitsprozess trotzdem lokale Kopien dieser sensiblen Kundendaten müssen diese nach Gebrauch umgehend wieder gelöscht werden. Diese Löschung erfolgt manuell und in Eigenverantwortung des Mitarbeiters. Das lokale Dateisystem wird regelmässig durch einen automatisierten Scan Prozess auf Inhalte mit sensiblen Kundendaten überprüft. Verstösse bei Nichteinhaltung der Ablagerichtlinien werden gemeldet. Auch ausgehende E-Mails werden auf sensible Daten gescannt und können gegebenenfalls nicht versendet werden, bspw. wenn sie eine Kreditkarten-Nummer beinhalten.

Um eine Kommunikation, bspw. zur Organisation eines Events, an ein bestimmtes Kundensegment zu tätigen, benötigt der Mitarbeiter die entsprechenden Adressdaten. Um an diese Datensätze zu gelangen stellt er eine Anfrage mit den gewünschten Selektionskriterien an die Abteilung, welche das System mit allen Kundendaten verwaltet. Diese exportieren den entsprechenden Datensatz, der auch bspw. Kreditkartendaten enthält, als Excel-Liste, verschlüsseln die Datei und senden sie schliesslich via E-Mail zurück an den Antragsteller. Dieser lädt den verschlüsselten Anhang aus der E-Mail auf seinen lokalen Rechner, entschlüsselt die Datei mit der Adressliste und kopiert sie auf das sichere Netzlaufwerk. Die lokale Kopie der Datei sowie die E-Mail muss danach manuell wieder gelöscht werden. Derselbe Prozess gilt auch für Daten, die von den Kunden selbst kommen. Hierbei kann es sich bspw. um die Passdaten eines Teilnehmers für eine Eventteilnahme handeln.

Pain Points mit der aktuellen Lösung

- Viel Eigenverantwortung bei der vorgeschriebenen Handhabung von sensitiven Daten, insbesondere bei Stress ist es sehr anstrengend eine korrekte Arbeitsweise aufrecht zu erhalten
- System unterstützt nicht bei der Einhaltung der Ablagerichtlinien für sensitive Dateien
- Manuelles Löschen von temporär lokal abgelegten Dateien mit sensitiven Inhalten notwendig
- Buchungen von Dienstleistungen, die mittels Kreditkarte bezahlt werden sind nicht möglich via E-Mail, da E-Mails mit Kreditkartendaten beim Scan hängenbleiben und somit nicht versendet werden können

Berufsgruppe Anwalt

Der befragte Anwalt arbeitet nach demselben Prinzip wie die unter [Berufsgruppe Treuhänder] beschriebene Person. Über eine gesicherte Verbindung kann via Remote Desktop auf eine virtualisierte Windows Instanz zugegriffen werden. Innerhalb dieser Umgebung steht die benötigte Anwaltssoftware zur Verfügung. In dieser Software werden Kundendaten sowie Falldaten mit allen zugehörigen Dokumenten erzeugt und bearbeitet. Aus dieser Arbeitsweise ergeben sich damit grundsätzlich dieselben Abläufe und Pain Points wie bei der [Berufsgruppe Treuhänder].

Berufsgruppe Human Resources Abteilung eines Unternehmens

Die Human Resources Abteilung in einem Unternehmen bearbeitet hauptsächlich sensible Personendaten von Mitarbeitenden wie Gesprächsdaten, Lohndaten Gesundheitsdaten und Personaldossiers (Werdegang, CV, etc.). Vom Gesetz ist vorgeschrieben, dass auch innerhalb des HR Teams nur Mitarbeiter, welche im Rahmen ihrer Arbeitstätigkeit ein bestimmtes Dokument benötigen auch darauf zugreifen dürfen. So darf bspw. ein CV nicht einfach frei im Team verteilt werden. Es dürfen nur Leute Einsicht erhalten, die im spezifischen Recruiting Prozess involviert sind. Aktuell existiert im Unternehmen eine gesicherte Datenablage wo alle Personaldaten zentral abgelegt und verwaltet werden. Alle Personen aus dem HR Team haben uneingeschränkten Zugriff auf diese Datenablage und können somit auch alle Personaldaten einsehen. Der Zugriff ist rein auf Vertrauensbasis geregelt und das Unternehmen kann nicht sicherstellen, dass HR Mitarbeiter nur auf Personaldaten zugreifen, welche sie unmittelbar bearbeiten und damit von Gesetzes wegen auch für den Zugriff autorisiert sind.

Eingehende Personaldaten werden vom zuständigen Mitarbeiter immer auf der gesicherten Datenablage abgelegt. Geht beim HR Team ein physischer CV ein, wird dieser mittels Scanner digitalisiert und erst lokal auf einem Computer abgespeichert. Die entstandene Datei wird danach auf die Datenablage transferiert und muss manuell auf dem lokalen Computer gelöscht werden. Das physische Dokument wird schliesslich geschreddert. Ähnlich funktioniert der Prozess beim Eingang einer E-Mail in der HR Inbox. Der Anhang der E-Mail wird vom Mailserver heruntergeladen und auf die zentrale Datenablage kopiert. Am Ende werden alle lokalen Kopien, einschliesslich der E-Mail gelöscht. Diese manuellen Arbeiten liegen ebenfalls in der Eigenverantwortung der HR Mitarbeitenden. Theoretisch wären auch Kontrollen zur Durchsetzung der gesetzlichen Grundlagen durch das interne Quality Management Team oder Gesetzesvertreter möglich.

Pain Points mit der aktuellen Lösung

- Vertrauensbasis beim Zugriff auf sensitive Daten ist nicht optimal, es sollten nur autorisierte Personen in die jeweiligen Dokumente Einsicht nehmen können

- Manueller Prozess für Handling und Transfer von eingehenden Personaldaten mit viel Eigenverantwortung

Berufsgruppe Compliance im Bankenumfeld

Mitarbeiter im Bereich Compliance einer Bank sind dafür verantwortlich, dass die Kunden und Mitarbeiter der Bank Gesetze und Regeln einhalten. Sie treffen Vorkehrungen, dass die geltenden Rahmenbedingungen nicht verletzt werden indem sie bspw. Transaktionen auf Geldwäscherei überwachen. Hält sich eine Bank nicht an geltendes Recht oder verletzt ihre Aufsichtspflicht gibt es Bussen von Aufsichtsbehörden und der Finma. Um eine Überwachung zur Einhaltung der geltenden Rahmenbedingungen überhaupt zu ermöglichen, unterhält die Bank eine zentrale Datenbank, in welcher jegliche Bankbeziehungen von allen bestehenden Kunden zusammengeführt werden. Diese Datenbank enthält damit hochsensible Kunden- und Finanzdaten. Nur speziell autorisierte Mitarbeiter dürfen mit ihrem persönlichen Laptop über eine physische Netzwerkverbindung innerhalb der Räumlichkeiten der Bank (teilweise sogar nur auf bestimmten Stockwerken) auf diese Daten zugreifen. Ein Zugriff über WLAN oder von zu Hause aus ist nicht möglich. Der Zugriff auf sensible Daten ist für die Mitarbeiter grundsätzlich sehr restriktiv geregelt und sie erhalten nur Zugriff auf Inhalte, die zwingend für ihre Tätigkeit notwendig sind. Die persönlichen Laptops dürfen zum Surfen im Internet verwendet werden, jedoch sind bestimmte Seiten geblockt und es können keine eigenen Programme auf den Geräten installiert werden.

Um bestimmte Auskünfte über Bankkunden zu erhalten stellen Mitarbeiter aus anderen Abteilungen Anfragen an das Compliance Team. Ist jemand bspw. an den Beziehungen eines bestimmten Kunden X zur Bank interessiert, sendet diese Person eine entsprechende E-Mail an die Mitarbeiter des Compliance Teams. Beinhaltet die E-Mail zusätzlich ein Dokument mit der Erlaubnis der Legal Abteilung, dass der Antragsteller die gewünschten Daten des Kunden X einsehen darf, wird ein Compliance Mitarbeiter aktiv. Der Mitarbeiter loggt sich in die zentrale Kundendatenbank ein und exportiert die gewünschten Daten als Excel-Liste. Diese Liste legt der Compliance Mitarbeiter dann in einem geschützten Ordner auf einem Netzlaufwerk ab und schaltet nur den Antragsteller für den Zugriff frei. Je nach Menge der exportierten Daten ist auch ein Versand via E-Mail an den Antragsteller möglich. E-Mails werden vor dem Versand automatisch auf sensible Daten gescannt. Schlägt die Überprüfung an, ist entweder eine zusätzliche Bestätigung des Absenders oder eine Verschlüsselung der Inhalte notwendig, um die E-Mail versenden zu können. Es liegt also in der Eigenverantwortung des Senders sicherzustellen, dass sensible Daten in einer E-Mail verschlüsselt werden.

Pain Points mit der aktuellen Lösung

- Fehlende Freiheit auf persönlichem Laptop, keine Administrator Rechte zur Installation von Programmen und eingeschränkter Internetzugriff
- Zugriff auf sensible Kundendaten nur vor Ort und über physische Netzwerkverbindung
- Eigenverantwortung im Umgang mit hochsensiblen Daten (E-Mail Verschlüsselung, exportierte Daten nicht auf unsicherer Datenablage zurücklassen)

9.21 Stundenrapport

Arbeitszeiterfassung I Master Thesis 2018-19 I MAS HCID - HSR

Name	Vorname	Monat
Wyder	**Aaron**	**Januar**
Projekt	**Gruppe**	**Auftraggeber**
Secure Operating System	G08	gapfruit AG

Datum		Arbeits-beginn	Arbeits-ende	Arbeits-zeit	Bemerkungen
01.01.19	Di	14:00	17:00	3:00	Einzelarbeit: Dokumentation Interviews SMEs
02.01.19	Mi	13:00	18:00	5:00	Einzelarbeit: Dokumentation Interviews SMEs & potentielle
03.01.19	Do	13:00	18:00	5:00	Einzelarbeit: Dokumentation Experiment "Shared Programs"
04.01.19	Fr	9:00	11:00	2:00	Team: Synchronisation Bericht
05.01.19	Sa				
06.01.19	So	15:00	17:00	2:00	Team: Synchronisation Bericht
07.01.19	Mo				
08.01.19	Di	18:30	23:00	4:30	Team: Vorlagen Bericht und neue Struktur
09.01.19	Mi				
10.01.19	Do	12:00	17:00	5:00	Einzelarbeit: Kapitel Einführung in die Domäne
11.01.19	Fr	13:00	18:00	5:00	Teamarbeit: 1.5h Synch Bericht, Einzelarbeit: 3.5h Review Bericht
12.01.19	Sa	14:00	16:00	2:00	Einzelarbeit: Kapitel Experimente
13.01.19	So	13:00	18:00	5:00	Einzelarbeit: Kapitel Experimente & Review Bericht
14.01.19	Mo				
15.01.19	Di	21:30	23:30	2:00	Einzelarbeit: Kapitel Experimente
16.01.19	Mi	17:00	20:00	3:00	Einzelarbeit: Kapitel Experimente
17.01.19	Do	10:00	16:00	6:00	Teamarbeit: 1h Synch Bericht, Einlzelarbeit: 5h Kapitel Experimente
18.01.19	Fr	12:00	15:00	3:00	Einzelarbeit: Kapitel Experimente
19.01.19	Sa	18:00	18:30	0:30	Teamarbeit: Synch Call
20.01.19	So	12:00	19:00	7:00	Einzelarbeit: Kapitel Experimente
21.01.19	Mo	14:00	20:00	6:00	Teamarbeit: 3h Synch Bericht, Einzelarbeit 3h Resultate Berufsgruppen
22.01.19	Di	20:00	23:30	3:30	Einzelarbeit: Kapitel Resultate Berufsgruppen
23.01.19	Mi	20:00	23:30	3:30	Einzelarbeit: Kapitel Methoden und Reflexion
24.01.19	Do	16:00	22:00	6:00	Einzelarbeit: Kapitel Methoden und Reflexion, Methodik und Vorgehen
25.01.19	Fr	10:00	19:00	9:00	Einzelarbeit: Revision Bericht
26.01.19	Sa	12:00	21:30	9:30	Einzelarbeit: Revision Bericht
27.01.19	So	9:30	17:00	7:30	Einzelarbeit: Revision Bericht
28.01.19	Mo	15:30	21:15	5:45	Einzelarbeit: Abstract & Reflexion
29.01.19	Di	13:30	21:45	8:15	Einzelarbeit: Revision Bericht & Fazit
30.01.19	Mi				
31.01.19	Do				
			Monatstotal:	119:00	
			Gesamttotal:	483:45	

Arbeitszeiterfassung | Master Thesis 2018-19 | MAS HCID - HSR

Monat	Stunden September	Total Projektstunden
Januar 19	143:30:00	487:45:00

Name	Vorname	Gruppe	Projekt	Auftraggeber
Schmid	Adrian	G08	Security Focused OS	gapfruit AG

Datum	Startzeit	Endzeit	Dauer	Arbeitsweg	Arbeitsbeschreibung
03.01.18	11:00:00	15:30:00	4:30:00		Ich: Konzept & Bericht Vorwort
04.01.18	10:00:00	12:30:00	1:30:00		Team: Bericht Review, Stand & Konzept
	13:00:00	16:45:00	3:45:00		Ich: Konzept & Text Vorwort
05.01.18	7:30:00	16:00:00	8:30:00		Ich: Konzept & Text Vorwort, Protopersona
08.01.18	8:15:00	20:00:00	21:15:00		Ich: Text Protopersona (Skizzen, Grafiken)
09.01.18	9:00:00	16:30:00	7:30:00		Ich: Text Protopersona (Skizzen, Grafiken)
10.01.18	9:30:00	17:15:00	6:45:00		Ich: Konzept & Text Protopersona, Experimente
11.01.18	10:15:00	12:30:00	2:15:00		Ich: Konzept & Text Protopersona, Experimente
	13:00:00	15:00:00	2:00:00		Team: Bericht Synch
	15:00:00	17:45:00	2:45:00		Ich: Text Experimente
15.01.18	8:15:00	14:45:00	6:45:00		Ich: Text Experimente
	11:00:00	11:30:00	0:30:00		Ich: Admin (Christian)
16.01.18	9:00:00	17:45:00	8:45:00		Ich: Text Experimente, Revidieren Aaron
17.01.18	7:30:00	8:30:00	8:45:00		Team: Bericht Synch – Abgebrochen: Dani nicht geliefert (wieder)
	14:00:00	14:30:00	0:30:00		Ich: Admin
18.01.18	11:00:00	15:15:00	4:15:00		Ich: Text Experimente
	16:00:00	21:15:00	5:15:00		Team: Bericht Struktur(Swisscom) – Dani nicht geliefert
19.01.18	9:30:00	10:30:00	1:00:00		Ich: Admin (Christian)
	11:00:00	12:30:00	1:30:00		Team: Text Review Annette
	12:30:00	13:00:00	0:30:00		Ich: Admin (Christian)
	14:00:00	14:30:00	0:30:00		Ich: Admin (Christian)
20.01.18	9:30:00	19:00:00	9:30:00		Ich: Konzept & Gestaltung Bericht, Revidieren v. Texten
21.01.18	6:15:00	8:00:00	1:45:00		Ich: Revidieren v. Texten & Layout
	13:30:00	1:15:00	11:45:00		Ich: Revidieren v. Texten & Layout, Cover
23.01.18	5:30:00	8:00:00	2:30:00		Ich: Revidieren v. Texten & Layout, Cover
24.01.18	6:00:00	12:00:00	6:00:00		Ich: Revidieren, schreiben v. Texten & Layout
	15:30:00	18:30:00	3:00:00		Ich: Revidieren, schreiben v. Texten & Layout
25.01.18	6:00:00	10:00:00	5:00:00		Ich: Revidieren v. Texten & Layout, Cover
27.01.18	19:30:00	21:30:00	2:00:00		Ich: Revidieren v. Texten & Layout, Cover
29.01.18	6:00:00	9:00:00	3:00:00		Ich: Revidieren v. Texten & Layout, Cover

	Dauer	Arbeitsweg
Total Januar	143:30:00	0:00:00