INSTITUTE FOR NETWORKED SOLUTIONS

OST Eastern Switzerland University of Applied Sciences

Incident-Response für KMUs

Bachelorarbeit FS22

Studiengang Informatik
Ostschweizer Fachhochschule
Campus Rapperswil-Jona

Frühlingssemester 2022

Autoren:	Severin Grimm & Marco Martinez
Version:	8. Juni 2022
Betreuerin:	Prof. Dr. Nathalie Weiler
Experte:	Mike Günther (SwissSign AG)
Gegenleserin:	Prof. Dr. Mitra Purandare

Abstract

Einleitung

Kleinere und mittlere Unternehmen (KMUs) investieren viel Geld in die Digitalisierung ihrer Arbeitsprozesse und sind auf ihre digitale Infrastruktur angewiesen. Durch diese Digitalisierung erlangt eine Unternehmung auf dem Markt den wirtschaftlichen Vorteil, der zur Rentabilität nötig ist. Gerade diese Digitalisierung fördert die Attraktivität der KMUs gegenüber Cyberkriminellen.

Cyberkriminelle nehmen häufig KMUs ins Visier und scheuen nicht davor zurück, mit gestohlenen oder verschlüsselten Daten hohe Geldsummen zu erpressen. Wer den Forderungen nicht nachkommt, muss zahlreiche Systeme zurücksetzen oder unternehmenskritische Daten werden veröffentlicht. Oftmals erreichen Cyberkriminelle die Unternehmenssyteme durch Sicherheitslücken und bleiben dabei unentdeckt. Diese Angriffe können mit einfachen Massnahmen erschwert und von oft kostenlosen Sicherheitsapplikationen entdeckt werden.

Ziel

Das Ziel dieser Bachelorarbeit ist es, KMUs in der Planung, der Vorbereitung und der Abwicklung von Cyberangriffen zu unterstützen. Die KMUs werden entsprechend ihrer Grösse mit Anleitungen, Vorlagen und Applikationen ausgestattet. Die erarbeiteten Anleitungen und Vorlagen sind praxisnah, für IT-Fachkräfte eines KMUs leicht verständlich und schnell umzusetzen. Das interaktive Incident-Detection-Training festigt das durch die Anleitungen erlernte Fachwissen.

Ergebnisse

Die Ergebnisse dieser Bachelorarbeit sind in vier Bereiche aufgeteilt. Es wurden 4 Ergebnisformate gewählt, um eine möglichst breite Hilfestellung bieten zu können.

Anleitungen Es wurden technische Anleitungen für Sicherheits-‹Best Practices› in mehreren Bereichen erstellt. Diese reichen von konzeptionellen Vorgehensweisen bis hin zu konkreten Implementationen. Ausserdem wurden Anleitungen zur automatischen Installation und Verwendung einer Sicherheitsapplikation erstellt, welche KMUs hilft, Cyberangriffe zu entdecken.

Vorlagen Es wurden zwei Vorlagen zur Definition der Vorgehensweisen bei einem Cyberangriff erstellt. Die Vorlagen unterstützen KMUs darin, bei einem Cyberangriff effektiver reagieren zu können, da alle Prozessabläufe vorgegeben sind und dadurch Klarheit im Vorgehen herrscht.

Sicherheitsapplikation Es wurde eine automatische Installation inklusive Installations- und Benutzeranleitung für ein Sicherheitssystem erstellt. Dieses bringt Sichtbarkeit und Transparenz in die IT-Infrastruktur, mit welchem akutelle Ereignisse nachvollzogen werden können. Dadurch können Anomalien in der IT-Infrastruktur entdeckt und es kann darauf reagiert werden.

Incident-Detection-Training Mit dem Incident-Detection-Training können KMUs ihre IT-Fachkräfte in der Verwendung der Sicherheitsapplikation trainieren. Dies hilft KMUs, Angriffe frühzeitig zu erkennen.

Management-Summary

Ausgangslage

Die Incident-Response ist ein Bereich in der Informatik, der viel Fachwissen benötigt – Fachwissen welches in kleineren Unternehmen oftmals beschränkt zur Verfügung steht. Daher ist es schwierig, ein KMU in der Incident-Response zu trainieren. KMUs können sich vorbereiten um den gesamten Incident-Response-Prozess zu verbessern. Incidents können mit einem geregelten Prozess effektiver erkannt und eingedämmt werden.

Mithilfe von Vorlagen und Anleitungen sollen sich KMUs besser vor Cyberangriffen schützen können. Alle Dokumente sollen für IT-Fachkräfte leicht verständlich sein. Die Massnahmen in den Anleitungen können ohne grosses initiales Investement umgesetzt werden. Dabei wird auch der Fokus darauf gelegt, dass die Lösung so wenig aufdringlich wie möglich ist.

Vorgehen

Um die Schwelle zur Umsetzung der Ergebnisse dieser Bachelorarbeit für KMUs möglichst gering zu halten, wurde Wert darauf gelegt, kostengünstige und unkomplizierte Wege für eine Erhöhung der IT-Sicherheit zu definieren. Es wurden Anleitungen und Vorlagen für die technische und organisatorische Incident-Response ausgearbeitet, welche KMUs helfen, sich auf Incidents vorzubereiten. In den technischen Anleitungen werden empfohlene Vorgehensweisen und teilweise Implemetationen aufgezeigt. In der organisatorischen Vorbereitung werden Prozessvorlagen und Abläufe für ein strukturiertes Vorgehen im Falle eines Incidents vorgegeben, welche KMUs in ihr Unternehmen einbinden können. Zusätzlich werden Trainings für IT-Fachkräfte erstellt, um Incidents in der IT-Infrastruktur entdecken zu können.

Die Anleitungen wurden mit Informatikstudierenden und KMUs validiert. Mit zehn Informatikstudierenden wurde die Benutzeranleitung der Sicherheitsapplikation validiert, indem ein Training durchgeführt worden ist. Zwei KMUs haben sich alle Anleitungen und Implementationen angeschaut und durchgeführt.

Ergebnisse

Sicherheitsapplikation Es wurde eine automatische Installation inklusive Installations- und Benutzeranleitung für ein Sicherheitssystem erstellt. Dieses bringt Sichtbarkeit und Transparenz in die IT-Infrastruktur, mit welchem akutelle Ereignisse nachvollzogen werden können. Dadurch können Anomalien in der IT-Infrastruktur entdeckt und es kann darauf reagiert werden.

Prozessvorlagen Die Vorlagen zum Incident-Response-Plan helfen KMUs, einen definierten Prozess für einen Incident festzulegen. In der Vorlage werden Rollen und Zuständigkeiten definiert, welche an Mitarbeitende zu verteilen sind. Durch eine Priorisierungsmatrix werden Incidents klassifiziert und anhand dieser eskaliert. Zusätzlich werden die Kontaktdaten aller benötigten Parteien an einem zentralen Ort verwaltet. Dieser Prozess ermöglicht eine effektivere Reaktion auf einen Incident, um den Schaden zu minimieren.

Security-Best-Practices Die Security-Best-Practices beinhalten Sicherheitsvorschläge und empfohlene Vorgehensweisen für einen breiten Bereich der IT-Infrastruktur. Es wurden insgesamt sieben Bereiche abgedeckt. Die einzelnen Best Practices reichen von konzeptionellen Vorgehensweisen bis zu konkreten Implementationen. Mithilfe dieser Best Practices kann kostengünstig ein hoher Sicherheitsstandard in der IT-Infrastruktur erreicht werden.

Incident-Detection-Training Mit dem Incident-Detection-Training können IT-Fachkräfte von KMUs hinsichtlich der Erkennung von und der Reaktion auf Incidents trainiert werden. Dies wird mit einem automatischen Cloud-Deployment in Microsoft Azure aufgesetzt, welches das Verhalten eines Sicherheitssystems simuliert. Darin können IT-Fachkräfte Anomalien entdecken und Gelerntes anwenden.

1. Aufgabenstellung BA Incident Response für KMUs

1.1. Ausgangslage

Die Simulation von Cyber Security Angriffe hilft Angriffe besser verstehen und die Reaktion auf reale Angriffe zu verbessern. Die Durchführung ist allerdings in der Realität sehr aufwendig und wird deshalb in KMUs nicht eingesetzt. In dieser Arbeit soll ein Konzept entwickelt werden, wie Incident Response Awareness in einem KMU umgesetzt werden kann. Das Konzept wird mittels eines Prototypen validiert.

Die Bachelorarbeit soll dabei helfen die organisatorischen Grundlagen für eine erfolgreiche Incident Abwicklung besser in kleinen und mittleren Unternehmen zu etablieren.

1.2. Aufgabe und erwartete Resultate

Die Aufgabe erarbeiten die beiden OST-Studierenden Severin Grimm und Marco Martinez im Frühlingssemester 2022.

Die folgenden Resultate werden in der Arbeit erwartet:

- Einarbeitung in die Aufgabenstellung und Eingrenzung der Aufgabe
- Erstellung des Konzeptes
- Umsetzung des Konzeptes inklusive einer Validierung
- Dokumentation der Arbeit inklusive Vorgehen und kritische Bewertung der getroffenen Entscheide

1.3. Hinweise

Als Start wird empfohlen sich eine Übersicht über den Incident Management Prozess zu verschaffen:

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im IT Grundschutz Kompendium in dem Abschnitt DER.2.1. eine öffentlich zugängliche Beschreibung zur Abwicklung von Sicherheitsvorfällen dokumentiert. Diese folgt und erweitert dem (kostenpflichtigen) ISO/IEC Standard 27035:2016.

Eine gute Zusammenfassung vom ISO/IEC Standard gibt es auf der open ISO Seite eine kompakte Beschreibung.

Anerkennungen

Prof. Dr. Nathalie Weiler Wir möchten uns bei Prof. Dr. Nathalie Weiler herzlich Bedanken für die gute Betreuung. Die Freiheit innerhalb des Projektes und die sehr kompetente Wegleitung, sowie die stets guten Inputs.

Studenten Wir Danken allen Studenten, die in der Validierung sich die Zeit genommen haben am Incident-Detection-Training teilzunehmen.

KMUs Ein speziellen Dank an die KMUs, die sich die Zeit genommen haben und alle Dokumente durchgearbeitet haben. Vielen Dank auch für das viele präzise Feedback welches uns erreicht hat. Wir konnten sehr von den guten Vorschlägen, wie auch von den Verbesserungsvorschlägen profitieren und dadurch ein hoffentlich noch kompletteres Produkt erzielen.

Inhaltsverzeichnis

Teil I.

Technischer Bericht

KAPITEL 1

Scope

Dieses Kaptiel ist zur Erklärung gängier Fachwörter, welche in dieser Arbeit benutzt wurden.

Cybersecurity

Die Cybersecurity ist ein Bereich der Informatik, welcher sich mit dem absichern und schützen von IT-Infrastrukturen beschäftigt. Cybersecurity ist der englische Begriff für Informationssicherheit.

Cybersecurity-Event

Ein Cybersecurity-Event ist ein Vorfall, welcher eine mögliche Verletzung der Cybersecurity bedeuten kann. Event ist der englische Begriff für Ereignis.

Cybersecurity-Incident

Ein oder mehrere Cybersecurity-Events, welche Unternehmensressourcen kompromittiert haben. Jeder Cybersecurity-Incident ist ein Cybersecurity-Event. Nicht jeder Cybersecurity-Event ist ein Cybersecurity-Incident. Incident ist der englische Begriff für Vorfall.

Incident-Response

Vorgehen, um Cybersecurity-Incidents zu mitigieren oder zu lösen. Darunter fällt das Herstellen des normalen operativen Betriebs. Response ist der englische Begriff für Antwort/Reaktion.

Incident-Response-Team

Team von Cybersecurity Spezialisten, welche die Geschädigten unterstützen, um den normalen Betrieb herzustellen. Incident-Response-Teams werden häufig in Form eines CERT[1] oder CSIRT[2] betrieben.

Incident-Detection-Training

Das Incident-Detection-Training ist in dieser Arbeit ein Training, welches IT-Fachpersonen darin schult, einen Cybersecurity-Incident zu erkennen und erste Gegenmassnahmen einzuleiten. Detection ist der englische Begriff für Erkennung.

[1] https://en.wikipedia.org/wiki/Computer_emergency_response_team
[2] https://www.csirt.org/

KAPITEL 2

Einleitung

2.1. Motivation

Die meisten KMUs benutzen eine digitale Infrastruktur. Der fordernde Markt und die Konkurrenz machen die Vorteile einer guten IT-Infrastruktur unentbehrlich. Die Stabilität jeder IT-Umgebung in einem KMU ist zentral. Ist die Stabilität nicht zu gewährleisten, steht ein KMU vor enormen wirtschaftlichen Problemen, da gewinnbringende Arbeiten nicht mehr erledigt werden können.

Mit der fortschreitenden Digitalisierung nehmen die Risiken zu. Cyberkriminalität tritt gehäuft auf und es werden auch KMUs gezielt angegriffen.

Für KMUs gibt es alternativ die Möglichkeit, die verursachten Kosten eines Cyberangriffes auf eine dritte Partei zu übertragen. Dies ist in Form einer Cyberversicherung möglich. KMUs bekommen von Versicherungen ein Anforderungsprofil, welches sie erfüllen müssen, um sich für eine Cyberversicherung zu qualifizieren. Viele Punkte solcher Anforderungen widerspiegeln sich in dieser Arbeit.

2.2. Aktuelle Situation

KMUs investieren viel Geld in die Digitalisierung ihrer Arbeitsprozesse. Die Sicherheit der Infrastruktur wird dabei oftmals vernachlässigt. Gründe dafür sind fehlendes Know-how im Bereich der Cybersicherheit, der Kostenfaktor oder die Einstellung, dass nur grosse Unternehmen betroffen sind.

Gemäss einer Umfrage der ENISA vom Juni 2021, befürchten 80 % der befragten KMUs, dass ein Cybersecurity-Incident innerhalb einer Woche nach Auftreten des Problems schwerwiegende negative Auswirkungen auf ihr Unternehmen haben würde. Weiterhin gaben 57 % an, dass sie höchstwahrscheinlich in Konkurs gehen oder ihr Geschäft aufgeben würden.[1]

Häufig ist für KMUs unklar, wie die Prozesse und Vorgehensweisen zu gestalten sind, wenn ein Cybersecurity-Incident auftritt. Die Vorbereitung auf Incidents ist häufig dürftig oder inexistent. Ohne Vorkehrungen ist das Reagieren auf einen Cybersecurity-Incident allerdings schwierig und fordert mehr Ressourcen.

[1] [Ann21]

2.3. Ziel

Beim Auftreten eines Incidents zählt jede Minute. Um die Zeit zwischen einem Incident und der entsprechenden Response möglichst klein zu halten, ist es essenziell, einen vordefinierten Ablauf zu verfolgen. Nur gute Planung kann die Responsezeit verkürzen und folglich den Schaden möglichst minimal halten.

In jedem Fall ist es wirtschaftlicher, einen Cybersecurity-Incident zu verhindern, wie zu behandeln. Das Ziel dieser Bachelorarbeit ist es, KMUs in der Planung von und der Vorbereitung auf Cybersecurity-Incidents zu unterstützen. Ausserdem sollen mittels einem interaktiven Incident-Detection-Training das Gelernte gefestigt und die Erkennung von Incidents verbessert werden.

2.3.1. Incident-Response Prozess

KMUs sollen mit dem erarbeiteten Konzept dieser Bachelorarbeit in der Lage sein, sich auf einen Ernstfall vorbereiten zu können. Dies beinhaltet den organisatorischen und technischen Teil der Incident-Response. Für den organisatorischen Teil werden Vorlagen für Prozesse erarbeitet, welche KMUs benutzen können. Im technischen Teil werden die Installation und die Verwendung von Open-Source-Programmen erklärt, welche für die Incident-Response benutzt werden können.

2.3.2. Incident-Detection-Training

Ein Security-Information-and-Event-Management (SIEM) System im Einsatz zu haben, hilft, mögliche Angriffe entdecken zu können. Die Meldungen und Vorfälle in einem SIEM-System müssen angeschaut, interpretiert und bewertet werden können.

Um die Verwendung des SIEM-Systems zu trainieren, wurde ein interaktives Incident-Detection-Training erstellt. Mit diesen sollen Informatik-Mitarbeitende aus KMUs trainiert werden, Incidents tatsächlich zu erkennen und die nötigen Schritte einzuleiten.

2.4. Einschränkungen

2.4.1. Arten von Incident-Responses

Proaktive Incident-Response

Der beste Schutz vor den Auswirkungen eines Incidents ist es, diesen gar nicht auftreten zu lassen. Es lässt sich nicht jeder Incident verhindern, aber die Anzahl von Incidents kann neben der technischen Vorbereitung auch durch Schulungen von Mitarbeitenden im Unternehmen minimiert werden. In dieser Bachelorarbeit wird darauf verzichtet, Schulungen für nichttechnische Mitarbeitende zu erstellen.

Reaktive Incident-Response

KMUs verfügen intern meist nicht über das Know-how, um Incidents selbstständig zu bewältigen. Daher wird sich der reaktive Teil dieser Bachelorarbeit auf die Erkennung von Incidents beschränken. Für die Bewältigung von schwerwiegenden Incidents wird ein Team aus Spezialisten benötigt, welches extern eingekauft werden muss.

2.4.2. Formen und Grössen von KMUs

Diese Bachelorarbeit beschränkt sich auf KMUs, welche nicht Teil des Techniksektors sind. Es gibt Aspekte, die ebenso für Technikunternehmen gelten und übernommen werden könnten; es wird allerdings beabsichtigt, nicht auf diese einzugehen. Wird im Folgenden also von KMUs gesprochen, sind KMUs ausserhalb des Techniksektors gemeint.

KMUs können unterschiedlich aufgestellt sein, je nach Grösse und Tätigkeitsgebiet. Die Grösse der KMUs wurde vom ENISA[2]-Standard übernommen und leicht angepasst.

Die Einteilung beinhaltet drei Kategorien: Mikro KMU, Kleine KMU und Mittlere KMU.

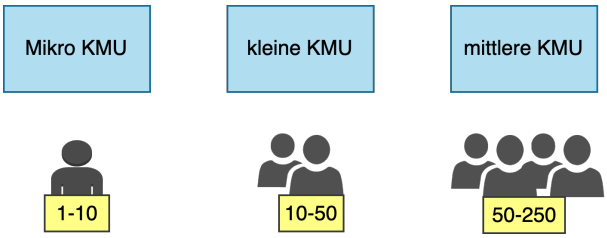


Abbildung 2.1.: KMU Grössentabelle

Zusätzlich wird bei allen KMUs mit zehn und mehr Mitarbeitenden vorausgesetzt vorausgesetzt, dass diese mindestens eine technikaffine Person beschäftigen, welche die Konzepte umsetzen kann.

[2][Ann21]

KAPITEL 3

Methodik

3.1. Übersicht

Die Landschaft der Cybersecurity ist gross und komplex. Es gibt unzählige Komponenten, welche sich – auch in ihrer Funktionsweise – voneinander unterscheiden.

Bei einem Cybersecurity-Incident ist die Zeit essenziell. Daher werden Spezialisten mit Fachwissen im Bereich der Incident-Response benötigt. Dieses Fachwissen ist in einem KMU in den meisten Fällen nicht vorhanden und ein Person mit solchem Fachwissen zu beschäftigen ist wirtschaftlich nicht tragbar. Daher wird in der Praxis nicht versucht, direkt auf Vorfälle zu reagieren, sondern es wird darauf abgezielt, Vorfälle zu verhindern. Die Incident-Response überlässt man dann einem Team aus Incident-Response-Fachpersonen, das KMU unterstützt in einem Vorfall die Incident-Responder.

Aus den vorhergehenden Gründen wurde sich im Rahmen dieser Arbeit dazu entschieden, KMUs dabei zu unterstützen, sich auf einen Incident vorzubereiten oder diesen zu verhindern. Die Dokumente sind nicht auf die eigentliche Incident-Response, welche von Fachleuten durchgeführt wird, ausgelegt. In dieser Arbeit wird zwischen zwei Vorbereitungen unterschieden: der technischen Vorbereitung und der organisatorischen Vorbereitung.

3.1.1. Technische Vorbereitung

Die technische Vorbereitung besteht aus gezielten Massnahmen, welche in Hard- oder Software umgesetzt werden können.

In dieser Arbeit gibt es spezifische Empfehlungen und Anleitungen, wie solche Vorbereitungen vorgenommen werden können.

3.1.2. Organisatorische Vorbereitung

Die organisatorische Vorbereitung besteht aus gezielten Massnahmen, welche in Geschäftsprozessen umgesetzt werden können.

Dies kann ein administrativer Prozess sein oder ein Dokument wie ein Kontaktformular.

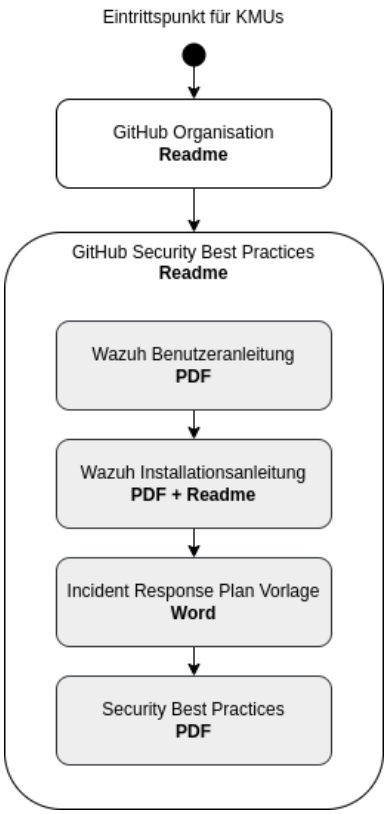
3.2. Struktur

Es ist ein Ziel, mit der Struktur des Produktes eine begleitende Wirkung zu erzeugen. Der Anwender bekommt nicht bloss Dokumente, sondern wird mit einem roten Faden durch die Arbeit geführt und erhält die Informationen Schritt für Schritt in einer Reihenfolge, welche den Einstieg erleichtern soll. Die Dokumente sollen dabei im PDF-Format vorliegen, wenn sie von den KMUs nicht editiert werden müssen. Sofern das Dokument zu editieren ist, wird es als Word-Datei zur Verfügung gestellt.

Für die Veröffentlichung wird eine kostenlose Online-Lösung evaluiert. GitHub bietet eine Platform für viele Open-Source-Projekte. Zudem gilt GitHub als Standard zur Veröffentlichung derartiger Projekte Daher ist es naheliegend, auch das Produkt der Bachelorarbeit ‹KMU Incident-Response› auf GitHub zu veröffentlichen.

3.2.1. Veröffentlichung

Es wurde eine Dachorganisation[a] namens ‹KMU-Incident-Response› auf GitHub erstellt. Es besteht ein roter Faden durch alle Dokumente, welchem IT-Mitarbeitende eines KMUs folgen können. Diese Organisation[b] ist auch der Einstiegspunkt für Anwender.



Unter der Gruppe wurden vier Repositorys erstellt.
Im Repository[c] ‹KMU-Security-Best-Practices› sind alle Konzepte in Dokumentform abgelegt. Diese sind entweder mit Word erstellt oder mit LaTeX geschrieben und als PDF verfügbar. Ein GitHub-Workflow hilft, die LaTeX-Dokumente zu kompilieren, Word-Dokumente hochzuladen und bei einem Tag einen Release zu erstellen. Im GitHub-Release ist die letzte offizelle Version der Dokumente. Diese Version wird auch an allen Orten referenziert und gilt als ‹aktueller Stand›.
In zwei weiteren Repositorys wurde eine Wazuh-Installation für KMUs vorbereitet. Wazuh ist eine Sicherheitsapplikation und wird zu einem späteren Zeitpunkt weitererklärt. Ein Repository beherbergt den Wazuh-Installer und ein zweites beherbergt zusätzlich benutzerdefinierte Regeln. Die Regeln wurden vom Repository ossec-sysmon geforkt und weiterentwickelt. Dazu wurde auch ein automatische Installation dieser Regeln für Wazuh entwickelt und im selben Repository abgelegt.
Im letzten Repository wurde das README für die Organisation abgelegt. Das ist per Konvention im ‹.github›-Repository.

[a] https://github.com/KMU-Incident-Response
[b] https://github.com/KMU-Incident-Response
[c] https://github.com/KMU-Incident-Response/KMU-Security-Best-Practices

Übersicht über die Struktur der Organisation:

Repositorybezeichnung	Beschreibung
KMU-Security-Best-Practices	Dieses Repository beinhaltet alle Dokumente für die Installation des SIEM Systems Wazuh, die Vorlagen für ein Incident-Response Plan und die Security Best-Practices.
KMU-Basis-Logging	Dieses Repository beinhaltet alle Installationsdateien für das SIEM-System.
ossec-sysmon	Dieses Repository beinhaltet alle Regeln und Konfigurationen für das SIEM-System.
.github	Dieses Repository beinhaltet das Readme auf der Organisationsseite auf GitHub.

Tabelle 3.1.: Struktur GitHub-Organisation

3.3. Anwendungsbereich

Der Anwendungsbereich der Konzepte konzentriert sich auf KMUs. KMUs können den Anwendungsbereich selbst definieren und aus relevanten Punkten in den Konzepten wählen.

Die Themen werden wie folgt je nach Grösse des Unternehmens empfohlen:

	Unternehmensgrösse		
Kategorie	Mikro	Klein	Mittlere
Geräteverschlüsselung	X	X	X
Antivirus (AV)	X	X	X
Backup	X	X	X
Updates	O	X	X
Firewall	O	X	X
Identity-and-Access-Management (IAM)		X	X
Local Administrator Password Solution (LAPS)		O	X
Security-Information-and-Event-Management (SIEM)			O

X = starke Empfehlung, O = Empfehlung

Tabelle 3.2.: Security-Anforderungen

3.4. Security-Information-and-Event-Management

Ein Security-Information-and-Event-Management (SIEM) System ist eine Software, die die Transparenz einer IT-Umgebung verbessert. Es verbessert die Erkennung von Bedrohungen, das Einhalten von Richtlinien und die Bewältigung von Cybersecurity-Events durch die Erfassung und Analyse von Echtzeit- und historischen Sicherheitsereignisdaten.

Ein SIEM-System ist in einem KMU vor allem nützlich, weil bei einem Incident das Zusammensuchen der Logdateien am meisten Zeit beansprucht. Ein SIEM-System hat alle nötigen Daten zentral an einem Ort und es kann schneller mit der eigentlichen Arbeit begonnen werden: dem Verstehen und Eindämmen des Vorfalls.

Ausserdem hilft ein SIEM-System, Anomalien in der IT-Infrastruktur zu entdecken um nötige Massnahmen einzuleiten. Solche Anomalien bleiben ohne zentrale Verwaltungsstelle von Logs eher unentdeckt.

3.4.1. Wazuh

Als SIEM wurde Wazuh ausgewählt. Wazuh eignet sich als SIEM für KMUs, da es Open-Source ist und alle Funktionen kostenlos verwendet werden können. Ausserdem ist die Installation auf Linux oder mit Docker möglich. Dies ermöglicht es, die Installation zu automatisieren. Somit können Hürden für KMUs reduziert werden und es fällt keine zusätzliche Last an. Eine genauere Beschreibung zum Aufbau von Wazuh befindet sich im Kapitel ‹Wazuh Übersicht›[1] im Anhang.

Für Wazuh wurde ein automatischer Installer erstellt, eine Installationsanleitung, eine Benutzeranleitung und ein Repository mit Regeln zur Entdeckung von Anomalien.

Installationsanleitung

Die Installationsanleitung beinhaltet die drei Themenbereiche, wie der Wazuh-Manager, die Wazuh-Agents und Sysmon installiert werden.

Wazuh-Manager

Die Installationsanleitung[2] für den Wazuh-Manager erklärt, wie der Manager automatisch mithilfe des Installers[3] auf einem Ubuntu-Server installiert wird.

Wazuh-Agent

Die Installationsanleitung[4] für die Wazuh-Agents erklärt, wie die Agents auf allen Clients in einem Unternehmen installiert werden können. Die Voraussetzung hierfür ist, dass das Unternehmen ein Active Directory im Einsatz hat, da die Agents über Group Policy Objects (GPO) installiert werden.

Sysmon

Sysmon wird auf den Windows-Clients benötigt, da die Wazuh-Regeln auf Sysmon-Logdateien zugreifen. Die Installationsanleitung für Sysmon legt dar, wie Sysmon auf allen Clients im Unternehmen installiert werden kann. Auch hier wird ein Active Directory vorausgesetzt, da Sysmon über GPO installiert wird.

Eine genauere Beschreibung zu Sysmon befindet sich im Kapitel Sysmon[5] im Anhang.

Sysmon für sich genommen loggt keine Events. Es braucht eine Konfiguration, welche Sysmon sagt, was genau in den Windows-Event-Log geschrieben werden soll. Das Schreiben einer solchen Konfiguration ist zeitintensiv und und geht daher über den Rahmen dieser Arbeit hinaus. Daher wurde eine bereits erstellte Konfiguration verwendet. Die Konfiguration stammt aus dem GitHub-Repository ossec-sysmon[6] von Hestat.

Regeln

Regeln in Wazuh werden im XML-Format erstellt. Jede eingehende Logdatei von den Agents wird mit den Regeln verglichen. Wenn eine Regeln zutrifft, wird ein Alert in Wazuh generiert. Die Regel definiert auch, welches Level der Alert haben wird. Falls keine Regel zutrifft, wird das Log verworfen.

Wazuh wird mit einem grundlegenden Regelwerk ausgeliefert, welches viele Logdateien von den Agents sammelt, aber nur wenige Anomalien entdeckt. Daher müssen weitere Regeln in Wazuh erstellt werden, um die Erkennungsrate zu verbessern. Um eine möglichst breite Abdeckung zu erzielen und möglichst viele Anomalien zu entdecken, müssen viele genau definierte Regeln geschrieben werden. Dies ist zeitintensiv und würde den Umfang dieser Bachelorarbeit ausfüllen. Daher wurden bereits vorhandene Regeln erweitert und angepasst.

[1] Abschnitt 5.2
[2] Abschnitt 6.2
[3] Unterunterabschnitt 3.4.1
[4] Abschnitt 6.3
[5] Abschnitt 5.3
[6] https://github.com/Hestat/ossec-sysmon

Methodik	Attackenvektor
Ausnutzen von Schwachstellen im OS	Ausführung von Mimikatz
Authentiserung in Active Directory	Pass-the-Hash Attacke
Antivirus Manipulation	Windows Defender Deaktivierung
Malicious Software	Kommandozeilenstart aus Microsoft Office Applikationen
Kopieren der Passwort Datenbank	Exzessive Verwendung von LAPS
Software Persistenz	Neu erstellte ‹Scheduled Tasks› in Windows

Tabelle 3.3.: Abdeckungsmatrix der getesteten Methoden

Die Basis dafür ist das GitHub Repository ossec-sysmon[7] von Hestat. Dieses beinhaltet benutzerdefinierte Regeln, welche auf den Sysmonevents basieren.

Diese Regeln wurden angepasst und optimiert, da sie teilweise nicht mit der aktuellen Version von Wazuh funktionierten. Zusätzlich wurden zwei Regeldateien hinzugefügt. Eine Datei für die Entdeckung von exzessiven LAPS-Anfragen und eine für die Erstellung von ‹Scheduled Tasks› unter Windows.

Installer

Der Wazuh-Installer ist ein Shell-Skript, welches alle benötigten Softwarepakete in der richtigen Reihenfolge installiert. Dazu gehören der komplette Elasticsearch-Logstash-Kibana (ELK)-Stack und das Wazuh-Plugin. Es werden Grundkonfigurationen vorgenommen, wie beispielsweise ein zufälliges Passwort für den Login, welches generiert wird. Es werden die zusätzlichen Regeln aus dem ossec-sysmon[8] Repository installiert und alle Konfigurationen für die Agents vorgenommen.

Benutzeranleitung

Das Benutzerhandbuch zu Wazuh[9] beinhaltet eine generelle Erklärung, was ein SIEM-System ist, wie die einzelnen Komponenten von Wazuh funktionieren und wie das GUI aufgebaut ist. Es wird erklärt, was Sysmon ist und welchen Einsatzzweck Sysmon in Windows und mit Wazuh hat. Zusätzlich werden noch Beispiele aufgezeigt, wie Attacken und ‹False Positives›[10] als Alerts in Wazuh aussehen könnten.

Dies soll KMUs eine grundlegende Übersicht geben, damit sie verstehen, warum der Einsatz eines SIEM-Systems, in diesem Falle Wazuh, bedeutsam ist. Mit den Beispielen sollen IT-Mitarbeitende geschult werden, damit sie eigenständig Attacken entdecken, ‹False Positives› herausfiltern, auf Attacken reagieren und diese dem externen IT-Dienstleister melden können.

3.4.2. Abdeckungsmatrix

Da die zusätzlichen Wazuh-Regeln aus dem Repository ossec-sysmon von Hestat stammen, wird auf die Abdeckungsmatrix[11] von diesem Repository referenziert.

Folgende Attacken und Methoden wurden überprüft und werden entdeckt von Wazuh:

[7] https://github.com/Hestat/ossec-sysmon
[8] https://github.com/KMU-Incident-Response/ossec-sysmon
[9] Kapitel 5
[10] Ein "False Positive" bei den Alerts ist ein Alert, welcher als Attacke aufgezeigt wird, aber eigentlich ein normales verhalten vom System ist. Dies kann passieren, wenn Wazuh Regeln zu generell sind.
[11] Zugriff: 04.06.2022: https://github.com/Hestat/ossec-sysmon/blob/master/mapping/OSSECSYSMON_Coverage.svg

3.5. Incident-Response-Plan-Vorlage

Der Incident-Response-Plan ist Teil der organisatorischen Vorbereitung auf den Incident-Response-Prozess. Für diesen wurden zwei Word-Dokumente vorbereitet: eine Incident-Response-Plan-Vorlage und eine Kontaktformular-Vorlage.

3.5.1. Incident-Response-Plan

Ein Incident-Response-Plan ist massgeblich für einen geordneten und definierten Ablauf im Falle eines Incidents. Die Vorlage definiert Rollen, Pflichten und Ansprechpartner in einem Cybersecurity-Incident. Ausserdem werden Kommunikations- und Eskalationswege definiert. Ein Beispiel einer Priorisierungsmatrix soll Unternehmen helfen, ihre eigenen Bedürfnisse in die Matrix einzuarbeiten und die Eskalationsstufen zu definieren.

3.5.2. Kontaktformular

Im Kontaktformular können Unternehmen ihre wichtigsten Kontaktpersonen in einem Dokument zusammenfassen. Dazu gehören interne Ansprechpersonen, externe Dienstleister, Internet-Service-Provider und Softwarehersteller. Dies soll im Falle eines Cybersecurity-Incidents die Prozesse beschleunigen, indem Unternehmen die betroffenen Parteien direkt erreichen können und nicht zuerst die Kontaktdaten suchen müssen.

Eine Beschreibung der Entitäten im Kontaktformular ist im Kapitel Kontaktformular[12] im Anhang zu finden.

3.6. Security-Best-Practices

In der Analyse wurde festgestellt, dass in vielen KMUs dieselben Herausforderungen vorhanden sind. Meist drehen sich diese um das Budget, das Know-how der Mitarbeitenden und die Höhe des initialen Investments. Daher wurde versucht, mit den Konzepten eine ergänzende Wirkung zu erzielen. Denn eine eindringliche Variante hat bei vielen KMUs keine Chance, umgesetzt zu werden. Es wurde angestrebt, mit Vorschlägen die IT-Sicherheit zu verbessern. Diese Vorschläge reichen von trivialen Konzepten zu konkreten, fortgeschrittenen Themen mit Implementationsanleitung.

Die Themen wurden mit Hilfe des Reports der ENISA über Security in KMUs[13] ermittelt und durch eigene Ideen ergänzt. Viele der Themen fokussieren sich ausserdem auf Microsoft-Umgebungen, da viele KMUs Windows verwenden. Es wurden folgende sieben Themen definiert, welche umgesetzt wurden.

Identity-and-Access-Management

Identity-and-Access-Management (IAM) wurde als Thema gewählt, da es ab einer gewissen Unternehmensgrösse Sinn ergibt, eine IAM-Lösung im Einsatz zu haben, da es das Benutzer- und Berechtigungsmanagement erleichtert.
Im Kapitel Identity-and-Access-Management werden die Vor- und Nachteile einer IAM-Lösung erklärt. Es wird auf zwei bekannte IAM, Active Directory und FreeIPA, eingegangen. Zusätzlich werden gängige Vorgehensweisen für eine Erhöhung der Sicherheit erklärt. Diese sind das ‹Least Privilege›-Prinzip, die Verwendung von persönlichen Accounts und von Rollen für Berechtigungen sowie die Festlegung eines definierten Prozesses für die Benutzerverwaltung.

Es werden keine konkreten Implementationsanleitungen angeboten.

Geräteverschlüsselung

Die Geräteverschlüsselung wurde als Thema gewählt, da die physische Sicherheit von Geräten genauso relevant ist wie die Verteidigung gegen Software-Attacken. Microsoft Windows bietet einfache Wege, die Festplatten

[12] Abschnitt 7.2
[13] [Ann21]

direkt in Windows zu verschlüsseln. Dies ist besonders wichtig für Notebooks, da diese ausserhalb eines Unternehmens gestohlen werden können.

Es werden zwei Möglichkeiten für die lokale Geräteverschlüsselung dargelegt – für die Home-Version und für die Pro-/Enterprise-Version von Windows 10. Dazu gibt es konkrete Implementationsanleitungen, wie die Geräteverschlüsselung auf allen Systemen im Unternehmen aktiviert werden kann.

Antivirus

Ein Antivirus (AV) gehört heutzutage auf alle Geräte. Als Antivirus für Windows wird der Microsoft Defender vorgeschlagen. Dieser ist kostenlos auf Windows-10-Geräten verfügbar und schliesst gut im Vergleich mit anderen Antivirusprogrammen[14] ab. Ausserdem wird noch aufgezeigt, wie Alerts vom Windows-Defender in Wazuh aussehen und welche zu beachten sind.

Local Administrator Password Solution

Local Administrator Password Solution (LAPS) ist eine Lösung von Microsoft. Mit LAPS werden die Passwörter der lokalen Administratoren, welche auf allen Windows Geräten vorhanden sind, zufällig und unterschiedlich voneinander gesetzt. Zusätzlich werden die Passwörter in einem gewissen Zeitraum automatisch neu gesetzt.

Dies verhindert, dass ein Angreifer auf weitere Systeme vordringen kann, wenn ein lokales Administratorpasswort kompromittiert ist. Die Passwörter sind in einem Attribut auf dem Computer Objekt im Active Directory hinterlegt. Zugriff auf dieses Attribut haben nur berechtigte Benutzer.
Diese Lösung wurde ausgewählt, da sie unkompliziert zu installieren ist und einen grossen Mehrwert bringt. Oftmals werden heutzutage einfachheitshalber noch die gleichen Administratoraccounts auf allen Computern mit dem gleichen Passwort eingerichtet.

Updates

Updates sind ein wesentliches Werkzeug für die Behebung von Softwareschwachstellen. Diese sollten immer möglichst zeitnah installiert werden.
Dieses Kapitel erklärt, wie man mit GPO automatisch Windows-Updates auf allen Computern installieren kann und die Benutzer dazu auffordert, dass sie den Computer nach einem Update neu starten. Ausserdem werden Beispiele dafür gegeben, wie ein Update-Konzept für Software aussehen kann, die sich nicht automatisch aktualisieren lässt.

Firewall

Im Kapitel Firewall werden gängige Best-Practices angeführt, wie eine Firewall eingerichtet und verwaltet werden kann. Dieses Kapitel ist rein konzeptionell und es gibt keine Implementationsanleitung. Zusätzlich wird aufgezeigt, dass mit Wazuh auch Logdateien von Firewalls gesammelt und verarbeitet werden können.

Backup

Im Kapitel Backup wird erklärt, wie ein Backup-Plan aussehen sollte und und dass ein ‹Emergency Plan› notwendig ist. Dies wird ebenfalls rein konzeptionell dargelegt.

[14] Zugriff: 31.05.2022 [Mic]

3.7. Incident-Detection-Training

Das Incident-Detection-Training kann in einer virtuellen Umgebung durchgeführt werden. Eine Cloudumgebung gibt die nötige Flexibiltät, um die Kosten für ein Incident-Detection-Training möglichst gering zu halten. Ausserdem ermöglicht sie ein einfaches und automatisches Deployment sowie das Entfernen der kompletten Infrastruktur.

3.7.1. Deployment

Die Umgebung wird mit Terraform[15] auf Azure[16] selbstständig erstellt und konfiguriert.

Das Deployment kann bequem im Hacking-Lab eingebunden und gestartet werden. Für das Hacking-Lab wurde die Instanz der OST verwendet. Diese ist nicht öffentlich verfügbar. Es ist auch möglich das Deployment manuell über die CLI zu starten. Die Codebasis des Incident-Detection-Trainings ist aufgrund einer Geheimhaltungsvereinbarung nicht öffentlich verfügbar.

3.7.2. Design

Das Lab wurde möglichst klein gehalten, um Kosten und Komplexität zu reduzieren. Es wird ein Ubuntu Server aufgesetzt, welcher die Wazuh-Installation beherbergt.

Der Server ist aus dem Internet via SSH und HTTPS zugänglich. SSH erlaubt den Shell-Zugriff auf dem Server, sowie das Starten des Attack-Simulators. Über HTTPS kann das Wazuh-Webinterface aufgerufen werden.

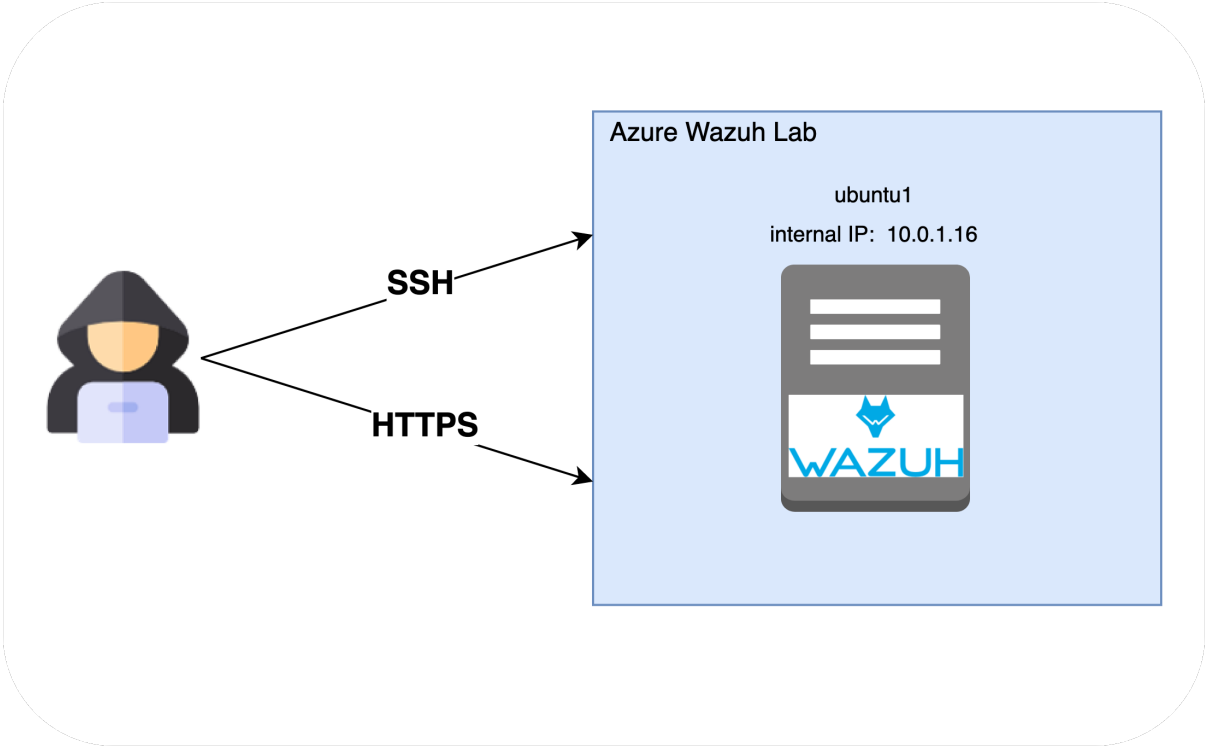


Abbildung 3.1.: Wazuh-Lab in Azure

[15] https://www.terraform.io/
[16] https://azure.microsoft.com/en-us/

3.7.3. Attack-Simulator

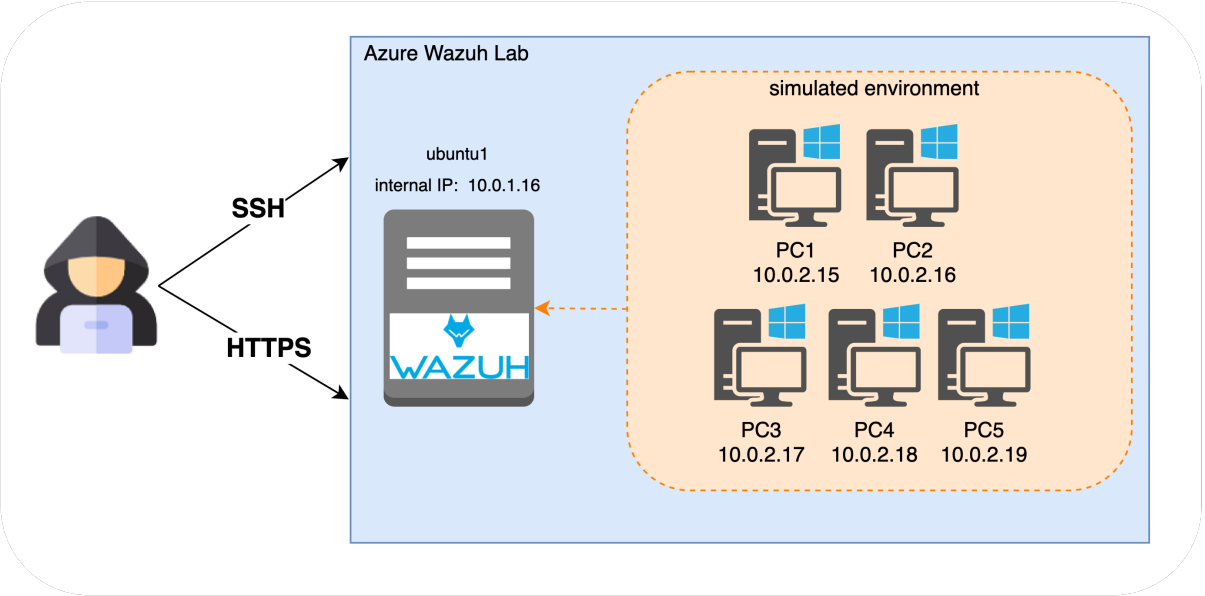


Abbildung 3.2.: simuliertes Wazuh Lab

Der Attack-Simulator läuft auf dem Ubuntu-Server und simuliert die Logdateien einer Microsoft-Windows-Umgebung. Es werden Logdateien direkt in die ‹Alerts›-Datei von Wazuh kopiert, welche dann von Wazuh im Web-GUI angezeigt werden. Die Beispiellogdateien stammen aus einer realen Microsoft-Windows-Umgebung, um eine echte Simulation darzustellen.

Architektur

Die Hauptaufgabe des Simulators ist es im SIEM Alerts zu generieren. Diese Alerts sollen den normal Betrieb des SIEMs simulieren. Das wird sichergestellt mit selbst erstellten Logeinträgen, in denen auch Attacken enthalten sind.

Dabei werden JSON-Dateien in die ‹Alerts›-Datei von Wazuh kopiert. Die ‹Alerts›-Datei ist eine JSON-Datei, welche standardmässig im Wazuh-Installationsordner existiert. Ausserdem müssen vor dem Kopieren noch die Zeitstempel in den zu kopierenden JSON-Dateien angepasst werden, damit diese der aktuellen Zeit entsprechen. Sonst werden diese im Wazuh-Web-GUI immer zur gleichen Zeit angezeigt, was nicht einer realen Simulation entspricht.

Für die Umsetzung des Simulators wurde auf Bash-Skripte gesetzt. Diese sind auf Ubuntu standardmässig verfügbar und erfüllen alle Anforderungen des Simulators. Bash-Skripte beinhalten die Kommandos für die Bash in Linux, welche ausgeführt werden sollen. Der Simulator ist auf dem Ubuntu-Server unter ‹/opt/simulator› abgespeichert.

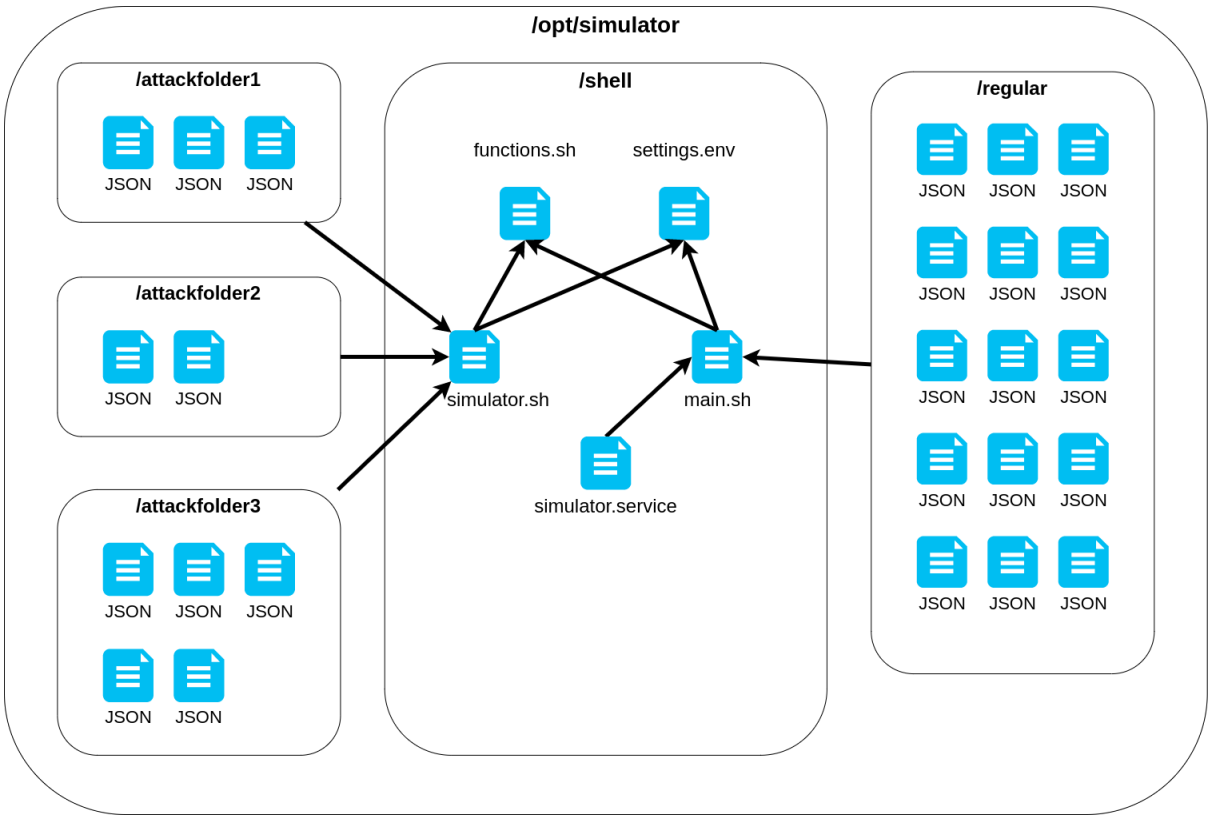


Abbildung 3.3.: Attack-Simulator

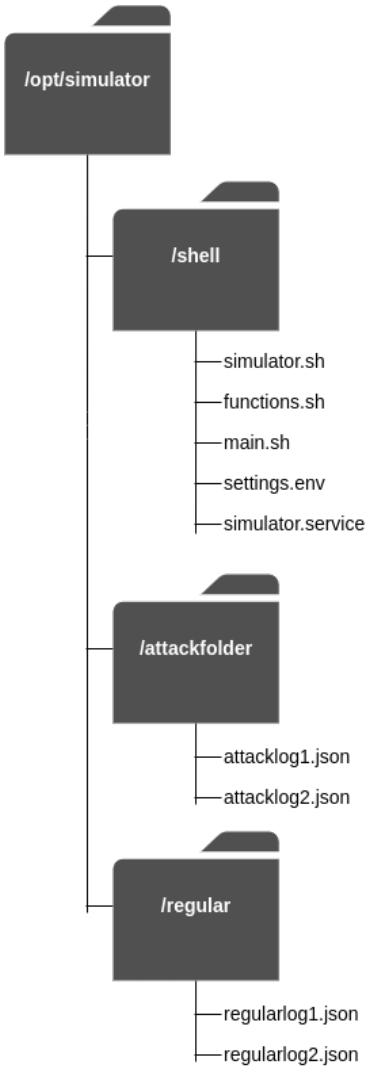


Abbildung 3.4.: Attack Simulator Ordnerstruktur

simulator.sh

Die Datei simulator.sh› ist der Einstiegspunkt für den Simulator. Sie importiert die ‹settings.en›-Datei und die ‹functions.sh›-Datei. Simulator.sh bietet ein Menu, in welchem man auswählen kann ob der Simulator gestartet werden soll und welche Attacken simuliert werden sollen. Bei einer Attacke werden alle JSON-Dateien aus einem /attackfolder kopiert.

simulator.service

Der ‹simulator.service› simuliert die eigentliche Umgebung. Es ist ein Service in Linux, welcher beim Deployment in den Service Ordner kopiert wird. Wenn der Service gestartet wird, führt dieser die ‹main.sh›-Datei aus.

functions.sh

Die Datei ‹functions.sh› beinhaltet die eigentlichen Funktionen, welche eine oder mehrere Dateien in die ‹Alerts›-Datei von Wazuh kopiert. Dabei werden auch gleich die Zeitstempel angepasst.

settings.env

Im ‹settings.env› sind Schlüssel-Wert-Paare abgebildet, welche von den Shell-Dateien verwendet werden können. Hier werden die Ordnerpfade definiert. Alle /attackfolder Ordner und der /regular Ordner werden hinterlegt, damit diese verwendet werden können.

main.sh

Die ‹main.sh› kopiert zu zufälligen Zeiten (etwa alle 10 bis 60 Sekunden) eine Logdatei aus dem /regular Ordner in die ‹Alerts›-Datei von Wazuh.

/attackfolder

Die /attackfolder Ordner beinhalten alle JSON-Dateien einer Attacke.

/regular

Der /regular Ordner beinhaltet Standard-JSON-Dateien wie Windows-Logins. Diese werden zufällig kopiert, damit es so aussieht, als ob echte Computer an Wazuh angebunden sind.

3.8. Validierung

Um sicherzustellen, dass das vollendete Produkt einen Mehrwert für KMUs generiert, wurde eine Validierung durchgeführt. Dabei wurde geprüft, ob die KMUs die Anleitungen verstehen und die Umsetzung für diese möglich ist.

Ein weiteres Ziel der Validierung war es das Produkt zu verbessern. Im Feedback wurden Verbesserungmöglichkeiten erfragt, diese anschliessend im Produkt identifiziert und entsprechend eingearbeitet.

Dies wurde in zwei Validierungsschritten bestätigt: einem mit Studierenden und einem mit KMUs.

3.8.1. Validierung mit Studierenden

Mithilfe des Incident-Detection-Trainings wird eine simulierte Umgebung von Wazuh als Cloud-Deplyoment aufgesetzt. Die Studierenden lesen die Benutzeranleitung zu Wazuh und wie man darin Cybersecurity-Incidents erkennt. Danach verbinden sie auf die Web-GUI von Wazuh des Cloud-Deployments und schauen die simulierten Alerts an. Es wird ein Feedback-Formular zur Verfügung gestellt, in welchem die Studenten erkannte Attacken und ‹False Positives› angeben können. Zusätzlich können sie bewerten, ob die Anleitungen verständlich waren und an welchen Stellen sie noch Mühe hatten.

3.8.2. Validierung mit KMUs

Auch unter Einbeziehung von KMUs werden die Anleitungen und Konzepte validiert. Die KMUs sollen diese, soweit möglich, durchlesen und umsetzen. Mithilfe eines Feedback-Formulars soll in Erfahrung gebracht werden, ob die Konzepte verständlich waren und wo Probleme auftraten. Ausserdem soll evaluiert werden, ob die Konzepte für die KMUs einen Mehrwert generiert haben.

KAPITEL 4

Resultate

Die Resultate bestehen aus den erarbeiteten Produkten, welche auf GitHub und im Anhang verfügbar sind. Ein beachtlicher Teil des Resultates ist die Nutzungsstudie, welche die Qualität der Produkte belegt.
Die Nutzungsstudie verwendet dabei die erarbeiteten Produkte und das Incident-Detection-Training, um die Qualität sicherzustellen.

4.1. Nutzungsstudie

Um den Anwendungsbereich der Produkte zu prüfen, wurde eine Validierung mit zwei Testgruppen durchgeführt.

Die Testgruppe 1, bestehend aus Informatikstudenten der Ostschweizer Fachhochschule (OST), wurde mit dem Incident-Detection-Training durch einen Teil der Wazuh Benutzeranleitung[1] geführt. Es wurden die Kapitel *Einleitung, Wazuh GUI und Benutzeranleitung* vorgegeben. Anschliessend wurde die Testgruppe mitels eines Formulares befragt, um einen Überblick darüber zu bekommen, wie das Produkt und das Incident-Detection-Training erlebt worden sind.

Die Testgruppe 2, bestehend aus zwei KMUs, bekam den Einstiegspunkt[2] des Endproduktes und hatte den Auftrag, dieses ohne weitere Instruktionen anzuschauen sowie die Installationen durchzuführen.

Die Vertreter der KMUs sind anschliessend mithilfe eines Formulars dazu befragt worden, wie das Erlebnis war, durch das Produkt geführt zu werden. Die Teilnehmer mussten auch bewerten, ob und wie das Produkt einen Mehrwert für ihr KMU generiert hat.

4.1.1. Auswertung

Die Rückmeldungen waren vorwiegend positiver Natur.

Vereinzelt gab es Kritik an spezifischen Aspekten. Diese Kritik wurde aufgegriffen, bewertet und eingearbeitet. Die meisten Kritikpunkte waren stylistischer Herkunft, also das beispielsweise die Bilder zu klein sind oder Rechtschreibfehler. Wo nötig, wurde das Dokument entsprechend umgestellt. Die KMUs gaben an, dass die Dokumente und der Installer einen grossen Mehrwert generiert haben.

Die volle Auswertung ist im Projektmanagementteil[3] einzusehen.

[1] Kapitel 5
[2] https://github.com/KMU-Incident-Response
[3] in der internen Dokumentation

KAPITEL 5

Schlussfolgerung

Das Ziel dieser Bachelorarbeit war es den KMUs unterstützende Dokumente zum Thema Incident-Response zu bieten, damit sich diese auf die Detektion und Reaktion eines Cybersecurity-Incidents vorbereiten können. Dies wurde durch Anleitungen, Vorlagen und ein Incident-Detection-Training ermöglicht. Die befragten KMUs bestätigten, dass dieses Ziel erreicht wurde und sie von einigen Punkten des Produktes profitieren konnten.

Das Incident-Detection-Training hat die Effektivität der ‹Wazuh Benutzeranleitung› verifiziert. Die Teilnehmenden haben mit wenigen Kapiteln der ‹Wazuh Benutzeranleitung› die Fähigkeit erlangt, Angriffe zu erkennen, und wussten, wie die nächsten Schritte eingeleitet werden.

Das Produkt ist zudem intuitiv, denn die Zielgruppe konnte sich ohne Instruktionen zurechtfinden und erlangte die Fähigkeit, einen Mehrwert im Bereich Cybersecurity für ihr Unternehmen zu generieren. Dadurch wird gewährleitstet, dass KMUs welche sich einarbeiten möchten, dies ohne weitere Hilfe vom Projektteam können.

Gegen Ende dieser Bachelorarbeit wurde dem Projektteam mitgeteilt, dass bereits weitere Firmen die Ergebnisse dieser Bachelorarbeit evaluieren. Mitstudierende des Projektteams haben den Einstiegspunkt an aktuelle Arbeitsgeber oder an KMUs von Bekannten weitergeleitet. Die Mitteilung von Mitstudierende, welche das Ergebnis dieser Bachelorarbeit gut befinden und an KMUs weitergeleitet haben, ist eine gute Bestätigung für das erreichen des Ziels.

5.1. Erweiterbarkeit

Das Produkt versucht, KMUs eine Hilfestellung für das Thema Cybersecurity zu bieten. Die Guides sind nicht abschliessend, denn der Bereich der Cybersecurity ist umfangreich. Es wäre denkbar, die Guides zu erweitern und weitere Unterstützungsangebote zu erstellen.

Es ist wesentlich, in diesem dynamischen Feld auf dem neuesten Stand zu bleiben. So könnte es sein, dass die Guides schon in naher Zukunft überholt sind und somit Anpassungsbedarf herrscht. Auch die Security-Best-Practices sind eine Momentaufnahme und es ist möglich, dass sie von anderen Standards und Vorgehensweisen abgelöst werden.

Eine andere denkbare Erweiterung wäre das Ergänzen und das Verfeinern des Regelwerkes in Wazuh. Denn neue Gefahren tauchen täglich auf und können vom aktuellen Regelwerk potenziell verpasst werden.

Teil II.

Anhang

KAPITEL 1

Verzeichnisse

Abbildungsverzeichnis

Tabellenverzeichnis

Literatur

[Ann21] Georgia Bafoutsou Anna Sarri Viktor Paggio. *Cybersecurity for SMES Challenges and Recommendations*. Techn. Ber. DOI: 10.2824/770352. Attiki, Greece: ENISA, Juni 2021.

[Mic] Microsoft. *Gartner names Microsoft a Leader in the 2021 Endpoint Protection Platforms Magic Quadrant*. URL: https://www.microsoft.com/security/blog/2021/05/11/gartner-names-microsoft-a-leader-in-the-2021-endpoint-protection-platforms-magic-quadrant/.

Glossar

Antivirus Ein Antivirus (AV) ist eine Software, die Schadsoftware wie zum Beispiel Viren, Würmer oder Trojanische Pferde aufspüren, blockieren und beseitigen soll. 7, 15, 17, 19, 33

Elasticsearch-Logstash-Kibana Elasticsearch, Logstash, Kibana sind drei Open-Source Projekte. Elasticsearch ist eine Such- und Analysesoftware für Logdateien. Logstash ist eine Software für das Sammeln von Logdateien von mehreren Quellen und übergibt diese an einen "Stash", zum Beispiel Elasticsearch. Kibana ist eine Visualisierungssoftware, welche Grafiken und Diagramme von einem "Stash" machen kann . 17, 33

Extensible Markup Language Die Extensible Markup Language ist ein Dateiformat zum Übertragen, Rekonstruieren und Speichern beliebiger Daten. Diese ist für Menschen sowie auch für Maschinen lesbar . 33

GitHub GitHub ist ein Anbieter von Internet-Hosting für Softwareentwicklung und Versionskontrolle mit Git. Es bietet die verteilte Versionskontrolle und die Quellcode-Verwaltungsfunktionen von Git sowie zusätzliche eigene Funktionen. 7, 14, 16, 17, 25, 30, 33, 37, 39, 42, 48

Graphical user interface Ein Graphical user interface, auch Grafische Benutzeroberfläche genannt, ist eine Schnittstelle für Benutzer, um mit einem elektronischen Gerät grafisch zu interagieren . 33

Group Policy Objects Group Policy Objects sind Richtlinien in Active Directory. Mit diesen kann in selbst definierten Bereichen der IT-Infrastruktur die Richtlinien durchgesetzt werden. Dazu gehören zum Beispiel Windows Einstellungen, welche auf allen Notebooks gleich gesetzt werden sollen. Ausserdem ist es auch möglich, Programme auf Clients zu installieren. 16, 33

Hacking-Lab Das Hacking-Lab ist ein Produkt der Compass-Security AG. Es ist eine Webapplikation, auf welcher Challenges in Verbindung mit Cybersecurity gelöst werden können . 20, 33

Identity-and-Access-Management Identitäts- und Zugriffsmanagement (IAM) können Administratoren autorisieren, wer auf bestimmte Ressourcen zugreifen darf. So ist es möglich die Kontrolle und Transparenz zentral zu verwalten. Für Unternehmen mit komplexen Organisationsstrukturen, Hunderten von Teams und vielen Projekten bietet IAM eine einheitliche Sicht auf die Sicherheitsrichtlinien in Ihrem gesamten Unternehmen mit integrierter Prüfung zur Vereinfachung der Compliance-Prozesse. 7, 15, 18, 33

JavaScript Object Notation Die JavaScript Object Notation ist ein Dateiformat, das menschenlesbaren Text verwendet, um Datenobjekte zu speichern und zu übertragen. Die Daten bestehen aus Attribut-Wert-Paaren und Arrays . 33

Local Administrator Password Solution Die Local Administrator Password Solution (LAPS) ermöglicht die Verwaltung der Passwörter lokaler Accounts von Computern, die der Domäne angeschlossen sind. Die Passwörter werden im Active Directory (AD) gespeichert. 7, 15, 19, 33

Operating System Ein Operatingsystem (OS), auch Betriebssystem genannt, ist eine Systemsoftware, die Computerhardware und Softwareressourcen verwaltet und allgemeine Dienste für Computerprogramme bereitstellt. 33

Security-Information-and-Event-Management Security-Information-and-Event-Management (SIEM) ist ein Bereich der Informatik, welcher sich mit dem sammeln und auswerten von Logdateien beschäftigt. Oftmals wird dies mit SIEM Softwaresystemen gemacht. 6, 11, 15–17, 33

Abkürzungsverzeichnis

AV Antivirus. 7, 15, 17, 19

ELK Elasticsearch-Logstash-Kibana. 17

ENISA European Union Agency for Cybersecurity. 10, 12

gh GitHub. 7, 14, 16, 17, 25, 30, 37, 39, 42, 48

GPO Group Policy Objects. 16, 19

GUI Graphical user interface. 17, 21, 22, 24

HL Hacking-Lab. 20

IAM Identity-and-Access-Management. 7, 15, 18

JSON JavaScript Object Notation. 22, 23, 34, 35

LAPS Local Administrator Password Solution. 7, 15, 17, 19

OS Operating System. 17

OST Ostschweizer Fachhochschule. 20, 25

SIEM Security-Information-and-Event-Management. 6, 11, 14–17, 22

XML Extensible Markup Language. 16

KAPITEL 3

Attack Simulator Benutzeranleitung

3.1. Aufstarten

Sobald das Deployment fertig ist, kann mit SSH auf den Server zugegriffen werden. Dort kann mit folgendem Befehl der Simulator gestartet werden:

```
cd /opt/simulator/shell/ && sudo bash simulator.sh

# Output should be an interactive tool, use according to description above
1) Start Simulator  5) Brute Force Attack SSH
2) Stop Simulator  6) Password Spray Attack SSH
3) Run Mimikatz Attack  7) Quit
4) Deactivate Windows Defender
Please enter your choice:
```

3.2. Skalierbarkeit

Der Attack Simulator lässt sich mit neuen Attacken und standard Logdateien erweitern.

Für neue Attacken erstellt man einen neuen "/attackfolder". In diesem Ordner können die JSON Dateien ablegen. Diese kann man aus der "alerts.json"[1] Datei einer Wazuh Live Umgebung kopieren. In den JSON müssen folgende Daten durch Variablen ersetzt werden. Diese werden während der Simulation durch aktuelle Daten ersetzt:

Timestamp

```
    "timestamp":"2022-06-02T10:38:58.000+0000"
    "timestamp":"DATETIME"
```

AlertID

```
    "id":"12432.4302"
    "id":"ALERTID"
```

Optional: UtcTime

Kann mehrmals und in verschiedenen Formaten vorkommen.

```
    "UtcTime": "2022-06-02T10:43:08.000"
    "UtcTime": "UTCTIME"
```

[1] Die alerts.json Datei befindet sich in einer Wazuh Installation unter "/var/ossec/logs/alerts/alerts.json"

Optional: SystemTime
Kann mehrmals und in verschiedenen Formaten vorkommen.

```
1     "systemTime":"2022-06-02T10:43:56.0000000Z"
2     "systemTime":"SYSTEMTIME"
```

Dabei muss beachtet werden, dass die JSON Dateien einzeilig sind. Die Dateien werden vom Simulator in alphabetischer Reihenfolge anhand des Dateinamen kopiert. Der Pfad des neuen "/attackfolder" muss in der settings.env Datei hinterlegt werden. Zum Schluss muss in der simulator.sh die neue Attacke noch als Menupunkt hinzugefügt werden.

Neue Simulationsdatei können als JSON Datei in den "/regular Ordner" kopiert und gleich angepasst werden.

3.3. Fehlerbehandlung

Das "Errorhandling" beim Start und Stop der Applikation wurde auf systemd ausgelagert, da sich dort die einzige Fehlerquelle der Applikation befindet. Das kopieren von Attacken kann fehlschlagen. In einem solchen Fall wird ein Log auf der Konsole angezeigt. Tritt ein Fehler beim Starten des Daemons auf wird der Fehler von systemd direkt im journal geloggt. Mit folgendem Kommando kann das Journal nach dem Simulator abgefragt werden:

```
1     jorunalctl -u simulator.service
```

Teil III.

Erarbeitete Resultate

KAPITEL 1

GitHub Organisation Readme

KMU Incident Response

empfohlene Zeit 16 Stunden

Willkommen auf dem GitHub Repository von KMU-Incident-Response. Alle arbeiten dieser GitHub Organisation sind das Produkt einer Bachelorarbeit an der OST von Marco Martinez und Severin Grimm. Ziel dieser Repositories ist es, KMUs auf den Incident Response Prozess vorzubereiten und Security Best-Practices zu vermitteln. Dabei wird wert darauf gelegt, Kosten für Software möglichst tief zu halten.

Die Vorbereitung auf das Incident Response wird mit der Erstellung eines Incident Response Plan und dem Einrichten eines SIEM System erreicht. Die Security Best-Practices behandeln verbreitete Themen, welche viele KMUs betreffen.

Einstiegspunkt

Einstiegspunkt für KMUs ist das Repository KMU-Security-Best-Practices.

Übersicht der Repositories

- KMU-Security-Best-Practices: Dieses Repository beinhaltet alle Dokumente für die Installation des SIEM Systems Wazuh, die Vorlagen für ein Incident Response Plan und die Security Best-Practices.
- KMU-Basis-Logging: Dieses Repository beinhaltet alle Installationsdateien für das SIEM System.
- ossec-sysmon: Dieses Repository beinhaltet alle Regeln und Konfigurationen für das SIEM System.
- .github: Dieses Repository beinhaltet das Readme, dass du gerade liest.

KAPITEL 2

GitHub KMU-Security-Best-Practices Readme

Incident Response für KMU

Die Incident Response ist ein Bereich in der Informatik, der viel Fachwissen benötigt. Fachwissen welches oftmals in kleineren Unternehmen nur beschränkt zur Verfügung steht. Daher ist es schwierig, ein KMU in der Incident Response zu trainieren. KMUs können sich aber vorbereiten, um den gesamten Incident Response Prozess zu verbessern und dadurch Incidents schneller erkennen und darauf reagieren.

Dieses Repository hat sich dies zum Ziel gesetzt. Mithilfe von Vorlagen und Anleitungen sollen sich KMUs besser schützen können. Es wird empfohlen die Dokumente in folgender Reihenfolge zu lesen:

1. Usageguide für Wazuh
2. Installationsguide für Wazuh
3. Incident Response Plan Vorlage
4. Security Best-Practices für KMUs

Mikro & kleine KMUs (unter 50 Angestellte) können Schritt 1. und 2. überspringen und direkt bei der Incident Response Plan Vorlage beginnen.

1. Usageguide für Wazuh

Wazuh ist ein Open-Source und kostenlos verfügbares SIEM System. Dieser Guide erklärt was Wazuh ist und enthält eine Benutzeranleitung zur Benutzung und Betreuung von Wazuh.

Version aus dem aktuellen Release

2. Installationsguide für Wazuh

Beinhaltet den Installationsguide für die Installation von einem Wazuh Server, benutzerdefinierte Regeln ausgelegt auf KMU und zusätzlich benötigte Software.

Version aus dem aktuellen Release

3. Incident Response Plan Vorlage

Ein Incident Response Plan ist wichtig für einen geordneten und definierten Ablauf im Falle eines Incidents. Dazu wurden zwei Vorlagen vorbereitet, welche KMUs auf ihre Bedürfnisse anpassen können. Template zur Definition von Pflichten und Ansprechpartnern in einem Incident Response Fall.

Incident Response Plan - Version aus dem aktuellen Release: Definiert den Ablauf, die Pflichten und die Reaktion bei einem Incident.

Kontaktformular - Version aus dem aktuellen Release: Definiert alle Ansprechspartner, inklusive Kontaktdaten.

4. Best Practices

Dieser Guide beinhaltet eine Sammlung von Security Best-Practices für KMUs.

Version aus dem aktuellen Release

KAPITEL 3

GitHub KMU-Basis-Logging Readme

KMU Basis Logging

Für eine Übersicht über das gesamte KMU-Incident-Response Projekt, starte bitte bei KMU-Incident-Response.

Inhalt

Dieses Repository stellt foglende Komponenten zur Verfügung:

Unterverzeichnis	Inhalt
`universal_installer/`	Installer für Wazuh Server und Custom Rules
`wazuh_server/`	Basisinstallation ohne Rules
`custom_rules/`	Logging Rules für Wazuh ausgelegt auf KMUs

Quick Start

Es wird empfohlen die vollständige Installation vorzunehmen. Die vollständige Installation wird hier erklärt.

Basic Installation

Falls nur ein Wazuh Server gewünscht ist, kann dieser ohne jegliche zusätzlichen Rules hier installiert werden.

Universal Installer

Der universal Installer hilft bei der Installation vom Wazuh Server, sowie auch mit dem installieren der empfohlenen Rules für KMUs. Alle Kompenenten können einzeln installiert werden. Bedingung für die Rules ist, dass Wazuh schon auf dem Server vorhanden ist.

Voraussetzungen

Die Installation ausgelegt auf KMUs und bietet sinnvolle Standardeinstellungen.

Achtung: Zur Zeit werden nur debian basierte Systeme unterstützt. Es wird Ubuntu 20.04 LTS empfohlen.

Installation

Die Installation wird über den universal Installer verrichten und kann wie folgt vorgenommen werden:

1. Login als Root auf dem zukünftigen Wazuh Server
2. Installieren von Wazuh **mit** vorbereiteten Regeln

```
curl -s https://raw.githubusercontent.com/KMU-Incident-Response/KMU-Basis-Logging/main/universal_installer/installer.sh | bash -s -- -a
```

Am Ende des Installers werden in der Shell alle gesetzten Passwörter angezigt. **Diese sollten sicher aufbewahrt werden!**

3. Login auf dem Web UI mit dem Elastic User und dem Passwort in der Shell ersichtlich.

Firewall

Wenn eine Firewall verwendet wird müssen folgende Ports freigeschaltet werden.

```
443/tcp         -  Kibana web interface
514/UDP/tcp     -  Syslog
1514/UDP/tcp    -  To get events from the agent.
1515/tcp        -  Port Used for agent Registration.
1516/tcp        -  Wazuh Cluster communications.
9200/tcp        -  Elasticsearch API
55000/tcp       -  Wazuh API port for incoming requests.
```

Mit folgendem Command kann dies auf ufw erreicht werden. (Default auf Ubuntu)

```
ufw allow to any proto udp port 514,1514
ufw allow to any proto tcp port 443,514,1514,1515,1516,9200,55000
```

Mit folgendem Command kann dies auf firewalld erreicht werden.

```
firewall-cmd --permanent --add-port={443,514,1514,1515,1516,9200,55000}/tcp
firewall-cmd --permanent --add-port={514,1514}/udp
firewall-cmd --reload
```

Weiteres vorgehen

Wazuh braucht noch weitere Software, um voll funktionsfähig zu sein. Anleitung für die Installation dieser Software findest du im Installationsguide

---

Allgemeine Bedienung Universal Installer

Der Wazuhinstaller kann automatisch mit `curl` ausgeführt werden oder manuell heruntergeladen werden und als CLI Tool verwendet werden.

Parameter

Der Installer bietet folgende Parameteroptionen. Alle Parameter sind exklusiv und können nicht kombiniert werden.

```
root@ubuntu:~# ./installer.sh -h
script usage:
 -a  Install Wazuh server and rules
 -n  no rules (Install server without rules)
 -o  only rules (Install only custom rules, no server)
 -h  print usage
```

Es ist möglich zuerst den Parameter `-n` und nachher den Parameter `-o` zu verwenden. Es ist nicht empfohlen die Parameter `-a, -n` mehrmals auf der selben Maschine auszuführen.

Automatisch

Im Code unten muss der Parameter an der Stelle `<parameter>` eingefügt werden.

```
curl -s https://raw.githubusercontent.com/KMU-Incident-Response/KMU-Basis-
Logging/main/universal_installer/installer.sh | bash -s -- <parameter>
```

Manuell

Den Installer auf GitHub herunterladen und in ein `installer.sh` schreiben. Im Code unten muss der Parameter an der Stelle `<parameter>` eingefügt werden.

```
bash installer.sh <parameter>
```

Wazuh Server Installer

Hier befinden sich alle Files benötigt für eine Basisinstallation von Wazuh.

Installation

Die komplette Installation (empfohlen) wird über den universal Installer gemacht.

manuelle Server Installation ohne Rules

1. Login als Root auf dem zukünftigen Wazuh Server
2. Installieren von Wazuh **ohne** vorbereitete Regeln

```
curl -s https://raw.githubusercontent.com/KMU-Incident-Response/KMU-Basis-Logging/main/universal_installer/installer.sh | bash -s -- -n
```

3. Login auf dem Web UI mit dem Elastic User und dem Passwort in der Shell ersichtlich

KAPITEL 4

GitHub ossec-sysmon Readme

ossec-sysmon

A Ruleset to enhance detection capabilities of Ossec using Sysmon

Special thanks to @Hestat for the primary ossec-sysmon repository, which made this possible.

Einstiegspunkt

Für eine Übersicht über das gesamte KMU-Incident-Response Projekt, starte bitte bei KMU-Incident-Response.

Manuelle Installation von Rules

Die Regeln können über den universal Installer installiert werden.

1. Login als Root auf dem zukünftigen Wazuh Server
2. Installieren von vorbereiteten Regeln

```
curl -s https://raw.githubusercontent.com/KMU-Incident-Response/KMU-Basis-Logging/main/universal_installer/installer.sh | bash -s -- -o
```

3. Login auf dem Web UI mit dem Elastic User und dem Passwort in der Shell ersichtlich

INSTITUTE FOR NETWORKED SOLUTIONS

OST Eastern Switzerland University of Applied Sciences

Wazuh Benutzeranleitung

Ein Guide für KMUs

Studiengang Informatik
Ostschweizer Fachhochschule
Campus Rapperswil-Jona

Autoren:	Severin Grimm Marco Martinez
Version:	31. Mai 2022

Inhaltsverzeichnis

KAPITEL 1

Einleitung

1.1 Umfang

Dieses Dokument ist für Informatikverantwortliche- und Mitarbeitende welche Wazuh als SIEM im Unternehmen einsetzten und verwenden möchten.

Es erläutert den Incident Response Prozess[1] definiert vom SANS Institue. Ausserdem wid grundlegend die Struktur von Wazuh und dessen Web GUI aufgezeigt. Es wird auch darauf eingegangen wie das GUI effizent verwendet wird. Anhand von Beispielen werden die aufgegriffenen Punkte visualisiert.

Zusätzlich wird Sysmon erläutert und wieso Sysmon ein wichtiger Teil für die Verwendung von Wazuh ist.

Teile dieses Dokumentes sind dazu gedacht um im Zweifelsfall nachzuschlagen. Der Wazuh Übersicht's Teil gibt etwas Kontext, welcher nicht benötigt wird, falls der Wazuh Installer[2] verwendet wird. Es wird auf die Struktur und die Teile von Wazuh eingegangen um aufzuzeigen, wie Wazuh funktioniert.

1.2 SIEM System

Security Information and Event Management (SIEM) ist ein Bereich der Cybersecurity, welcher sich mit dem sammeln und auswerten von Logdateien beschäftigt. Oftmals wird dies mit SIEM Softwaresystemen gemacht.

Diese Systeme sammeln die Logdateien von Windows Systemen, Netzwerkgeräten und weiteren Geräten. Die Logdateien werden dann an das SIEM System weitergeleitet. Dort werden mittels definierten Regeln anomalien entdeckt und Logs korreliert.

1.3 Sysmon & Wazuh

Das Repository enthält neben dieser Anleitung einen Installer für Wazuh mit vordefinierte Regeln/Gruppen. Zusätzlich gibt es Installationsanleitungen, wie man die Agents installiert und wie man Sysmon installiert.

Wazuh und Sysmon ergänzen sich sehr gut. Die Regeln, welche von diesem Repository installiert werden, **brauchen** Sysmon um überhaupt ausgelöst zu werden. Ohne Sysmon sind die Regeln nutzlos. Daher ist es wichtig, dass alle verwendeten Produkte installiert werden.

[1] Zugriff: 14.05.2022 [Kra12]
[2] Link: https://github.com/KMU-Incident-Response/KMU-Basis-Logging/blob/main/universal_installer/README.md#Installation

1.4 Incident Response Prozess

Der Incident Response Prozess des SANS Institute (SANS) definiert die Vorbereitung und den Ablauf eines Incidents, sowie die Wiederherstellung nach einem Incident. Dieser wird in sechs Schritte aufgeteilt.

1.4.1 Prepare

In der Phase "Prepare" wird ein Unternehmen auf einen Incident vorbereitet. Dazu gehört die technische, wie auch die organisatorische Vorbereitung.

In der technischen Vorbereitung werden Unternehmen mit Sicherheitsmassnahmen, Software und Hardware geschützt. Ausserdem wird sichergestellt, dass das Incident Response Team die nötigen Berechtigungen hat, um einen Incident behandeln zu können.

In der organisatiorischen Vorbereitung werden Richtlinien definiert, was in einem Unternehmen erlaubt ist im Umgang mit der IT Infrastruktur und wo Einschränkungen getroffen werden. Es wird ein Incident Response Plan erstellt, welcher den Ablauf im Falle eines Incidents regelt. Dabei wird auch das Vorgehen in der Kommunikation definiert und und Notfallkontakte definiert.

In dieser GitHub Organisation[3] wird der "Prepare" Teil durch das Incident Response Plan Template, die Installation von Wazuh und den Security Best Practices abgedeckt.

1.4.2 Identify

In der Phase "Identify" wird geregelt, wie Incidents erkannt werden. Nachfolgend kann der vorhergehend definierte Plan gestartet werden. Dies kann über Mitarbeitende passieren, die einen Incident dem IT Support melden, über ein automatisches Intrusion Detection System oder über Alerts von einem SIEM. Falls ein Incident festgestellt wird, sollte der externe IT Dienstleister umgehend informiert werden.

In dieser GitHub Organisation[4] wird der "Identify" Teil durch die Erklärungen und Beispiele von Wazuh abgedeckt.

1.4.3 Contain

Die "Containment" Phase beinhaltet die Eindämmung eines Incidents, um weitere Folgeschäden zu vermeiden. Diese Phase ist in drei Schritte aufgeteilt. Das "short-term Containment", das "System Backup" und das "long-term Containment".

Im "short-term Containment" ist der Fokus, den Schaden möglichst schnell einzudämmen. Dies kann unter anderem durch trennen der betroffenen System vom Netzwerk sein, betroffene Systeme herunterfahren und/oder Zugriffsrechte von Benutzeraccounts einzuschränken. Dieser Teil kann oftmals direkt vom IT Support ausgeführt werden, bevor ein externer IT Dienstleister bereit ist einzugreifen.

Im "System Backup" Teil werden forensische Abbildungen der betroffenen Systeme erstellt. Mit diesen kann in der "Lessons learned" Phase nachvollzogen werden, wie Angreifer in die Systeme eingedrungen sind und wo allfällige Schwachstellen sind. Für forensische Abbildungen werden spezifische Tools benötigt, welche ein KMU nicht besitzt. Daher sollte dieser Schritt vom externen IT Dienstleister durchgeführt werden.
Im "long-term Containment" werden die betroffenen Systeme soweit gesichert, dass diese wieder vorübergehend Produktuionsfähig sind, bevor in der nächsten Phase "Eradicate" saubere Systeme aufgesetzt werden.

1.4.4 Eradicate

Die "Eradicate" Phase behandelt die eigentliche Entfernung aller kompromittierten Systeme und Malware im Netzwerk. Bevor die Systeme wiederhergestellt werden, muss sichergestellt werden, dass alle Eintrittspunkte

[3] Link: https://github.com/KMU-Incident-Response
[4] Link: https://github.com/KMU-Incident-Response

der Angreifer blockiert wurden und keine Malware sich im Netzwerk mehr befindet. Sonst werden neue Systeme direkt wieder kompromittiert.

1.4.5 Recover

In der "Recover" Phase werden die betroffenen Systeme wiederhergestellt. Es ist wichtig, die neuen Systeme genau zu überwachen um sicherzugehen, dass diese nicht direkt wieder kompromittiert werden.

1.4.6 Lessons learned

In der "Lessons learned" Phase werden alle Dokumentationen fertiggestellt, alle Erkentnisse aus dem Incident zusammengefasst und ein Report erstellt. Dies soll für weitere Incidents helfen, schneller reagieren zu können oder als Fallbeispiel für neue Mitarbeitende zu Verfügung stehen.

KAPITEL 2

Wazuh Übersicht

2.1 Umfang

Dieses Kapitel geht auf die technischen Gegebenheiten und den kompletten Ablauf im Hintergrund von Wazuh ein. Dies ist vorallem für Interessierte gedacht und muss nicht zwingend gelesen werden, um dem weiteren Verlauf des Dokumentes folgen zu können.

Wazuh ist aus dem Open-Source Projekt ossec[1] entstanden. Wie ossec ist Wazuh komplett Open-Source und kostenlos verfügbar.

2.2 Aufbau

Wazuh basiert auf dem Elasticsearch Logstash Kibana (ELK) Stack. Wazuh beinhaltet den Manager, auf welchen sich die Wazuh Agents verbinden. Der Manager ist ein Plugin, welches in den ELK Stack integriert werden kann und mithilfe von Agents auf den Computern Logdateien sammelt.

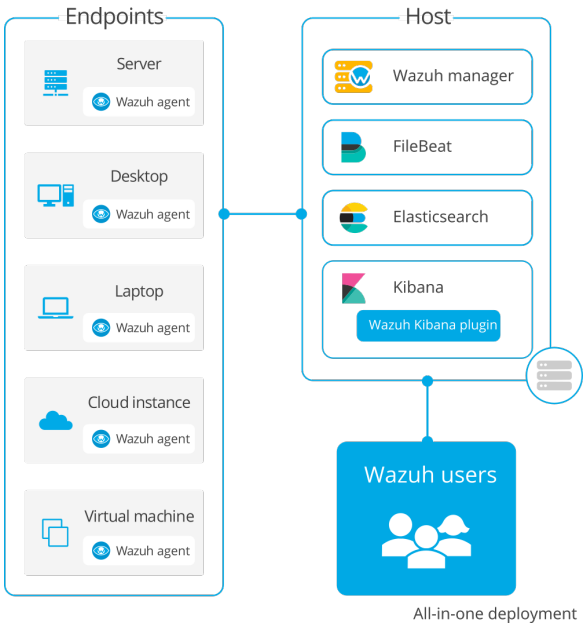


Abbildung 2.1: Übersicht Wazuh[2]

[1] Link: https://github.com/ossec
[2] Zugriff: 24.04.2022 [Waz]

2.3 Prozessablauf

Die Agents senden die Logeinträge an den Wazuh Manager. Danach werden die Logeinträge mit einem Decoder strukturiert und die Regeln werden auf die Logeinträge angewendet. Wenn eine Regel zutrifft, wird ein Alert generiert und angezeigt. Wenn keine Regel zutrifft, wird der Logeintrag verworfen. In der ossec.conf kann eingestellt werden, dass auch die Logeinträge abgespeichert werden, die auf keine Regel zutreffen. Dabei sammeln sich grosse Datenmengen an und dies ist hauptsächlich für Debugging empfohlen.

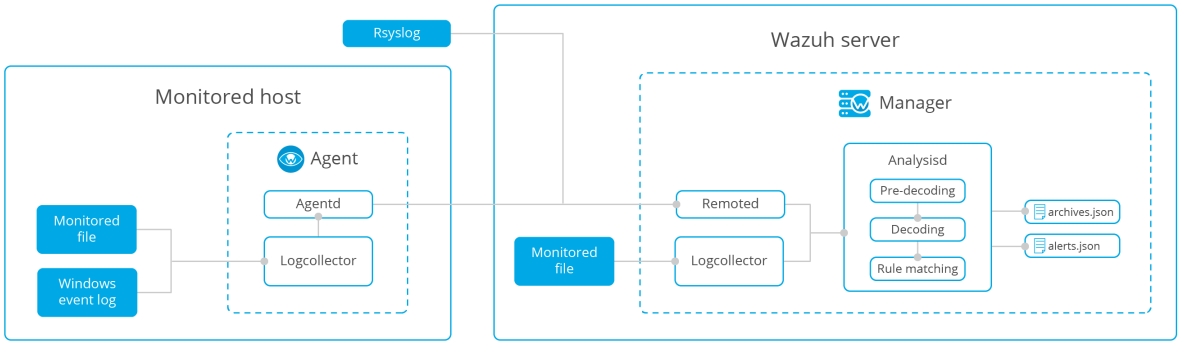


Abbildung 2.2: Wazuh Ablauf[3]

2.4 Wazuh Manager

Der Wazuh Manager wird auf einem Linux Server installiert und beinhaltet den kompletten ELK Stack, mit Wazuh Plugin. Er ist verantwortlich für die Verarbeitung der eingehenden Logeinträge. Dazu werden Groups, Decoder und Rules verwendet.

2.4.1 Groups

Die Gruppen werden verwendet, um ähnliche Geräte zu gruppieren. Für jede Gruppe kann man eine agent.conf einrichten, in welcher eingetragen wird welche Logdateien von diesen Systemen verarbeitet werden sollen.

agent.conf

In der agent.conf kann definiert werden, welche Logdateien an den Wazuh Manager weitergeleitet werden. Eine Lokation wird mit <localfile> angegeben:

```
<agent_config os="Windows">
    <localfile>
        <location>Microsoft-Windows-Sysmon/Operational</location>
        <log_format>eventchannel</log_format>
    </localfile>
</agent_config>
```

Weitere Informationen wie neue Orte mit Logdateien eingebunden werden können, findet man in der Wazuh Dokumentation[4]

2.4.2 Decoders

Da Logs in allen möglichen Formen daherkommen, braucht es je nach Herkunft verschiedene Decoder. Die Decoder bringen die eingehenden Logs in eine einheitliche Struktur, um die Regeln darauf anwenden zu können. Es werden Decoder für einige bekannten Logformate angeboten, wie zum Beispiel für den Windows Event Manager oder Cisco IOS Logs.

[3] Zugriff: 24.04.2022 [Waz]
[4] Link: https://documentation.wazuh.com/current/user-manual/reference/centralized-configuration.html?highlight=agent%20conf

2.4.3 Rules

Alert Level

Es gibt Alert Levels von 0 bis 16. Diese bedeuten nicht wie schwerwiegend ein Ereignis ist, sondern jedes Level hat eine spezielle Bedeutung. Die wichtigsten Level sind folgende:

- **Level 3** sind Alerts, welche authorisiert sind und tendenziell nicht gefährlich.
- **Level 12** sind Alerts, welche eine Anomalie darstellen und potenziell gefährlich sind.

Alle Alert Level findet man in der Wazuh Dokumentation[5].

2.4.4 Konfiguration

In der ossec.conf Datei sind alle Konfigurationen vom Wazuh-Manager abgespeichert. Die Konfigurationsdatei kann im GUI bearbeitet werden. Alternativ liegt die Datei unter:

```
/var/ossec/etc/ossec.conf
```

2.5 Wazuh Agent

Der Wazuh Agent wird auf dem Client installiert. Es werden die meisten Betriebssysteme unterstützt. Darunter viele Linux Systeme, Windows und MacOS.

Der Wazuh Agent leitet alle Logdateien, die in der agent.conf definiert sind, weiter an den Wazuh Manager. Zusätzlich überwacht der Wazuh Agent auch alle Systemdatei- und Registryänderungen und leitet diese an den Wazuh Manager weiter.

[5] Link: https://documentation.wazuh.com/current/user-manual/ruleset/rules-classification.html

KAPITEL 3

Sysmon

3.1 Übersicht

System Monitor (Sysmon) ist ein Windows-Systemdienst und -Gerätetreiber, der, sobald er auf einem System installiert ist, bei jedem Neustart des Systems aktiv bleibt, um die Systemaktivitäten zu überwachen und im Windows-Ereignisprotokoll zu protokollieren. Er liefert detaillierte Informationen über die Erstellung von Prozessen, Netzwerkverbindungen und Änderungen der Dateierstellungszeit. Durch das Sammeln der von ihm erzeugten Ereignisse mithilfe der Windows-Ereignissammlung oder SIEM-Agenten und die anschließende Analyse dieser Ereignisse können Sie bösartige oder anomale Aktivitäten identifizieren und verstehen, wie Eindringlinge und Malware in Ihrem Netzwerk operieren.

Beachten Sie, dass Sysmon keine Analyse der von ihm erzeugten Ereignisse bereitstellt und auch nicht versucht, sich vor Angreifern zu schützen oder zu verstecken.[1]

3.2 Konfiguration

Sysmon alleine macht nichts. Erst mit einer Konfiguration, in welcher definiert wird was alles in den Eventlog geschrieben wird, kann Sysmon verwendet werden. Diese Konfiguration ist im XML Format.

Wichtig ist zu wissen, dass Sysmon eventuell auch businesskritische oder vertrauliche Daten von Prozessen loggt und diese dann über den Wazuh Agent an den Manager gesendet werden. Dies kann datenschutztechnische Probleme geben oder vertrauliche Daten können von unbefugten Mitarbeitenden im Wazuh GUI gesehen werden. Daher sollte die Konfiguration immer zuerst den Anforderungen entsprechend angepasst und überprüft werden. Proprietäre Software kann auch vom Sysmon Logging ausgeschlossen werden.

[1] Übersetzt mit www.DeepL.com/Translator: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

KAPITEL 4

Wazuh GUI

4.1 Startseite

Die Wazuh Startseite kann mit dem Webbrowser aufgerufen werden.

Auf der Startseite sieht man alle aktiven und inaktiven Computer, die mit dem Wazuh Manager verbunden sind. Von hier aus hat man Schnellzugriff auf alle "Module", die Wazuh anbietet.

Alle Module und Einstellungen findet man auch im Menü, welches sich durch klicken vom Wazuh Logo öffnen lässt.

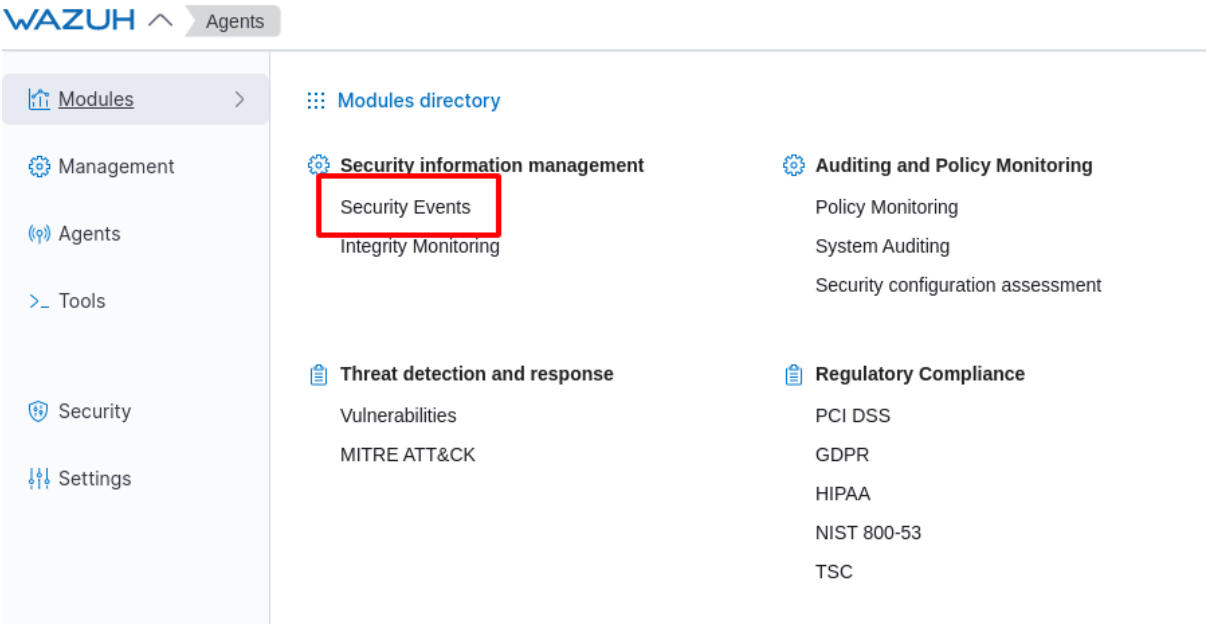


Abbildung 4.1: Wazuh Menü

4.2 Security Events

Die Security Events findet man unter **Wazuh** → **Modules** → **Security Events**. Im Modul Security Events werden alle Alerts angezeigt, welche durch die definierten Regeln ausgelöst werden.

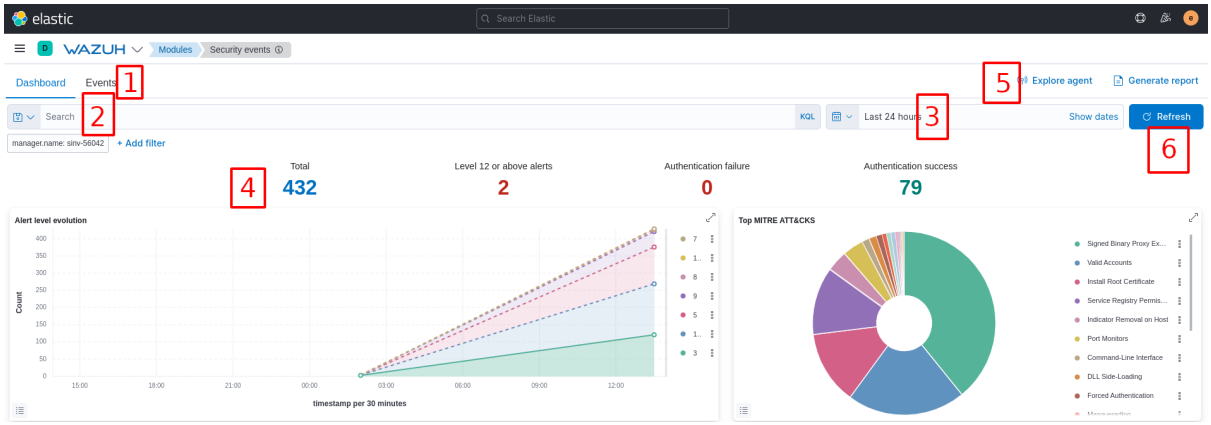


Abbildung 4.2: Security Events

1. Navigation zwischen dem Dashboard und den Events. Das Dashboard zeigt die Alerts und zusammenfassende Diagramme an. Unter Events sieht man nur die Alerts, dafür aber zusätzlich bessere Filter.
2. In diesem Eingabefeld kann man die Alerts durchsuchen. Mithilfe von Filtern kann man gewünschte Alerts ausblenden oder nur gewählte Anzeigen lassen.
3. Hier kann man die Zeitspanne angeben, wie lange zurück man die Alerts ansehen möchte.
4. Diese Übersicht zeigt an, wie viele Alerts in der eingestellten Zeitspanne generiert wurden und wieviele davon über Level 12 (Kritisch) sind, wieviele davon erfolgreiche Logins und wieviele fehlgeschlagene Logins. Ausserdem zeigt es noch zusammenfassende Diagramme an.
5. Bei "Explore Agent" kann man einen Agent auswählen um nur dessen Alerts anzuzeigen.
6. Mit "Refresh" kann man die neusten Alerts laden.

Auf der Seite unten findet man auch die Alerts. In der Liste werden die Alerts angeziegt. Diese können nach Titel sortiert werden.

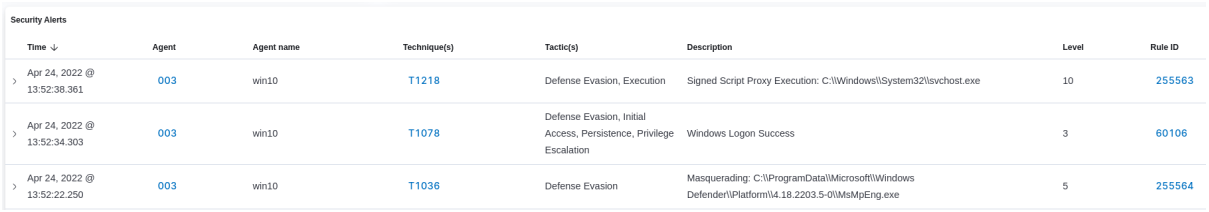


Abbildung 4.3: Security Events

- **Time** zeigt die Zeit, wann der Alert eingegenen ist.
- **Agent** zeigt von welchem Agent der Alert eingegenen ist.
- **Agent name** zeigt den Hostname des Agent.
- **Technique & Tatic** zeigt die Mitre Attack Framework[1] Technik an, welcher dieser Alert sein könnte.

[1] Link: https://attack.mitre.org/techniques/enterprise/

- **Description** zeigt eine Beschreibung, um was es sich bei diesem Alert handelt.
- **Level** zeigt das Level des Alerts an.
- **Rule ID** zeigt an, welche Regel diesen Alert generiert hat.

4.3 Integrity Monitoring

Das Integrity Monitoring findet man unter **Wazuh** → **Modules** → **Integrity Monitoring**. Im Inventory Monitoring werden alle veränderten Systemdateien und Registry Einträge geloggt. Damit kann man bei einem Sicherheitsvorfall eventuell nachvollziehen, wie vorgegangen wurde.

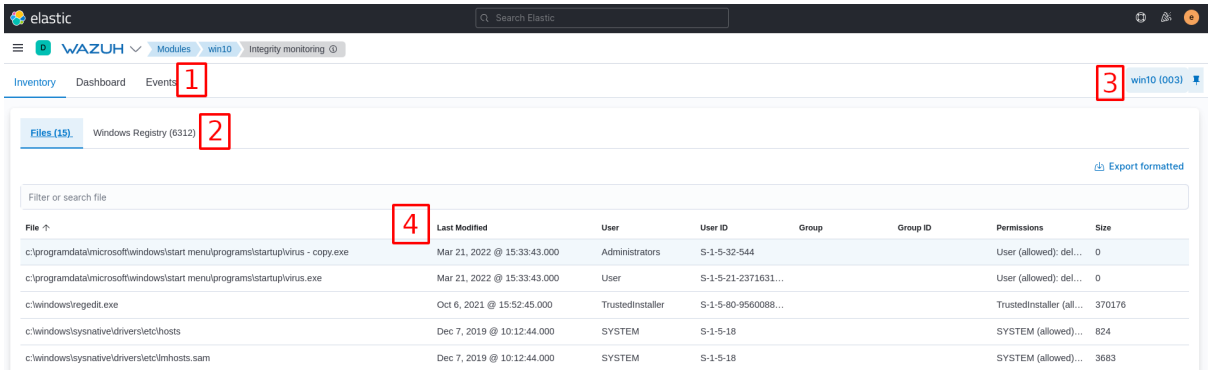


Abbildung 4.4: Inventory Monitoring

1. Navigation zwischen dem Inventory, dem Dashboard und den Events. **Inventory** zeigt die veränderten Systemdateien und Registry Einträge an. Im **Dashboard** findet man zusammenfassende Diagramme und unter **Events** werden auch alle Änderungen angezeigt, aber zusätzlichen mit einer unterstützenden Suche.
2. Navigation zwischen den geänderten Systemdateien und Registry Einträgen.
3. Agent auswählen, welcher man anschauen möchte.
4. Liste von bearbeiteten Systemdateien oder Registry Einträgen.

4.4 Rules

Die Regeln findet man unter **Wazuh** → **Management** → **Rules**. Hier können alle Regeln angeschaut und eigene Regeln hinzugefügt werden.

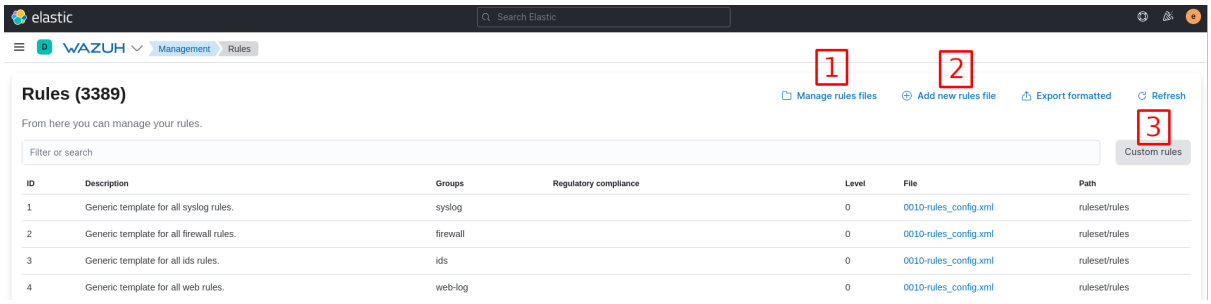


Abbildung 4.5: Rules

1. "Manage rules files" kann alle Dateien, welche die Regeln beinhalten, anschauen.

2. "Add new rules file" kann eine neue Datei hinzufügen, um neue Regeln zu definieren.
3. "Custom rules" kann die eigenen Regeln oder Regeldateien anzeigen lassen. Alle Regeln von Wazuh werden ausgeblendet.

4.5 Decoders

Das Decoder findet man unter **Wazuh** → **Management** → **Decoders**. Diese Seite ist gleich aufgebaut wie die Rules Seite.

4.6 Groups

Die Gruppen findet man unter **Wazuh** → **Management** → **Groups**. Auf dieser Seite findet man alle definierten Gruppen, kann neue Gruppen hinzufügen und entfernen.

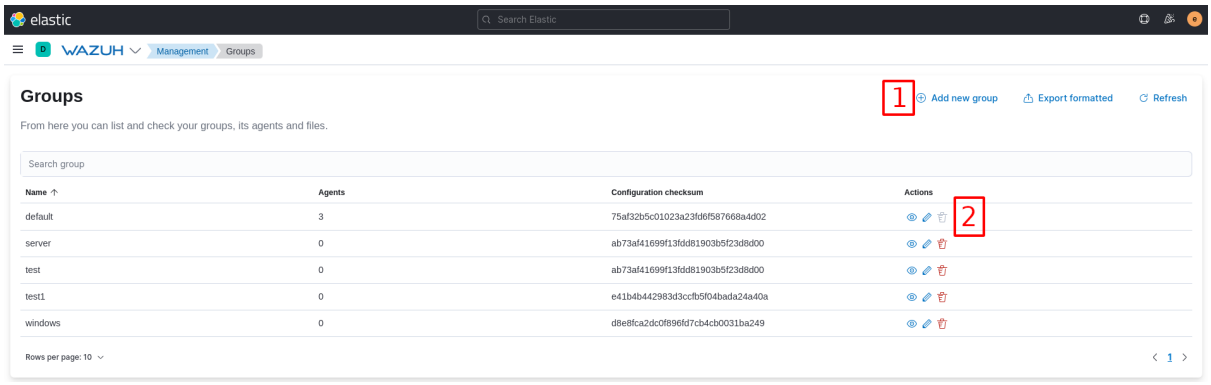


Abbildung 4.6: Groups

1. "Add new group" kann eine neue Gruppe hinzufügen.
2. Hier kann man die einzelnen Gruppen verwalten. Mit dem Aug-Symbol kann man alle Agents anschauen, die dieser Gruppe zugewiesen sind. Mit dem Stift-Symbol kann man die agent.conf bearbeiten und mit dem Papierkorb-Symbol kann man die Gruppe löschen.

4.7 Konfiguration des Managers

Die Konfiguration findet man unter **Wazuh** → **Management** → **Configuration**. Hier gibt es eine Übersicht von allen Wazuh Manager Einstellungen und diese können bearbeitet werden.

4.8 Wazuh Agents

Die Konfiguration findet man unter **Wazuh** → **Agents**. Hier sieht man alle registrierten Agents und kann neue Agents hinzufügen.

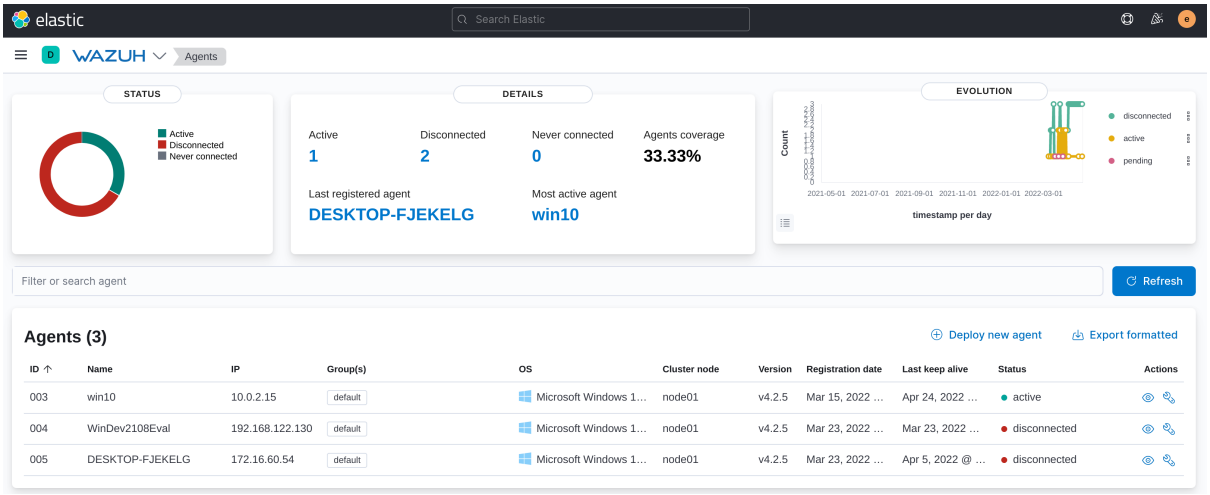


Abbildung 4.7: Agents

KAPITEL 5

Benutzeranleitung

5.1 Einleitung

Wazuh kann zwar Alerts für jegliche Logdateien generieren und anzeigen lassen, die Erkennung eines Incident muss jedoch weiterhin von einer Fachperson gemacht werden. Dies ist leichter gesagt als getan. Bei jedem SIEM System gibt es auch sogenannte "False Positives", Alerts die angezeigt werden aber eigentlich keine Incidents sind. "False Negatives" sind Incidents die keine Alerts generieren. Die "False Negatives" entdecken ist schwierig und kann nur durch eine Ergänzung der Wazuh Rules erreicht werden. Bei den "False Positives" kann man durch Untersuchung der betroffenen Entitäten feststellen, ob es sich wirklich um einen Incident handelt.

In diesem Kapitel wird angeschaut, wie man im Wazuh Web GUI mit Queries die Alerts filtern kann, es werden Beispiele von realen Attacken aufgezeigt und wie man "False Positives" erkennen kann.

Die Security Events findet man im Wazuh Web GUI unter **Wazuh** → **Modules** → **Security Events**.

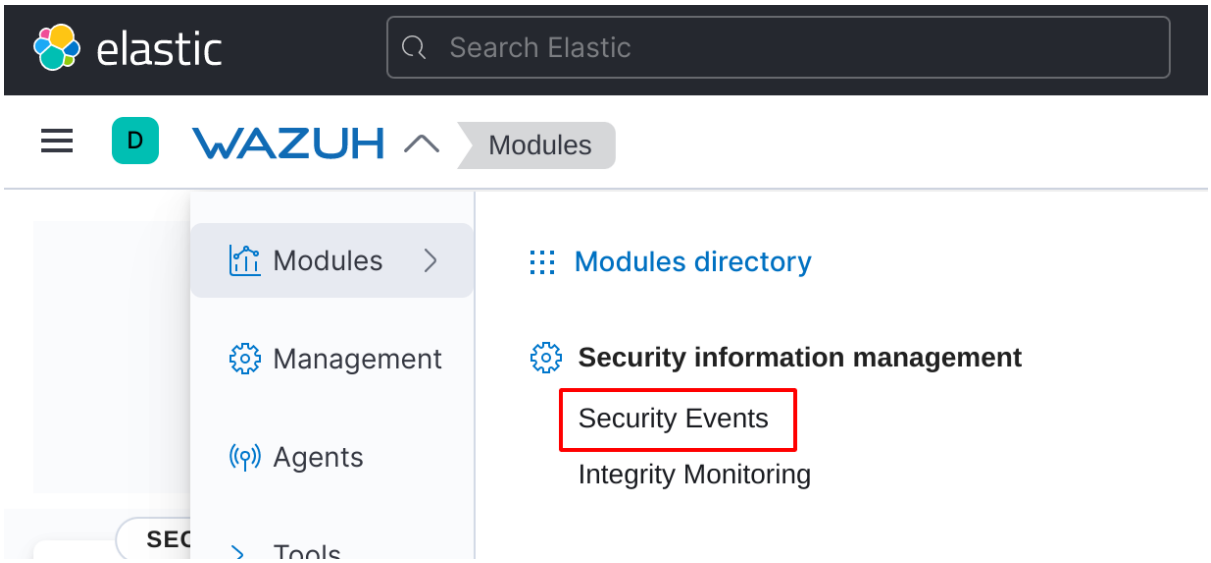


Abbildung 5.1: Wazuh Security Events

Im Register Events findet man dann eine gute Übersicht

5.2 Filter

Das Filtern der Alerts wird in Wazuh mittels der Kibana query language (KQL) gemacht. Der Wazuh Manager unterstützt das schreiben dieser Queries mit einem kleinen Interface, wo man die Filter zusammenklicken kann.

Dieses Interface befindet sich bei den Security Events im Reiter "Dashboard" und "Events". Events gibt eine bessere Übersicht über alle möglichen Filter und eine bessere Auflistung aller Informationen eines Alerts.

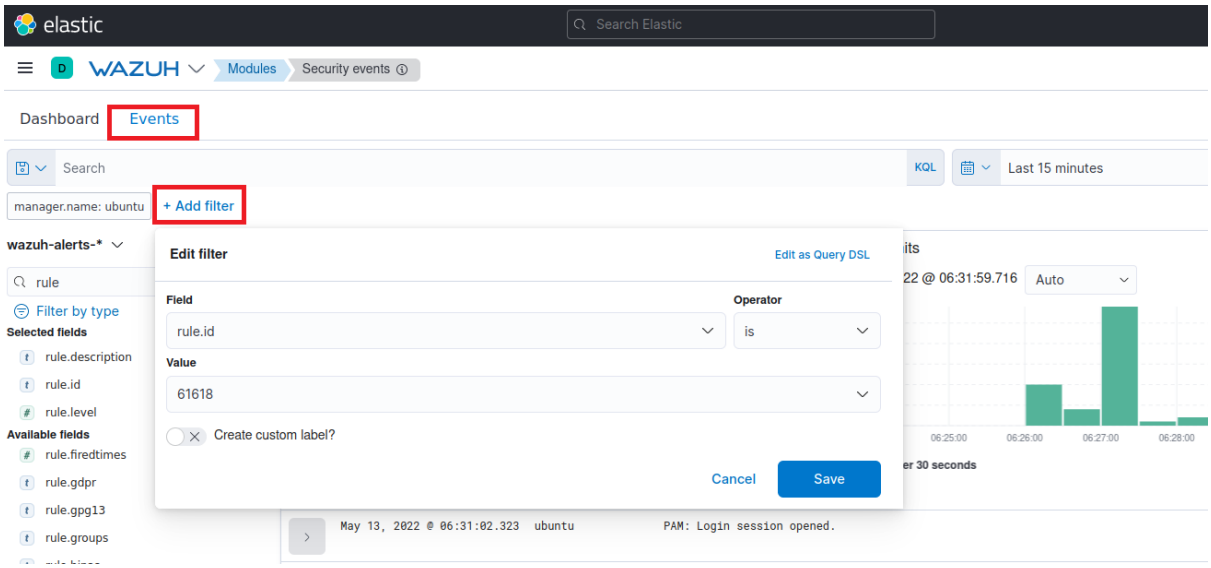


Abbildung 5.2: KQL Filter in Wazuh

In diesem Interface kann das Feld ausgewählt werden, dazu die Art des Vergleichs und der Wert. Im Bild oben werden zum Beispiel nur noch Rules angezeigt, welche die ID 61618 haben. Auf diese Weise kann man auch unnötige Rule IDs ausblenden, oder nur bestimmte Rule IDs eines bestimmten PCs anzeigen.

Filter sind Modular aufgebaut. Alle aktiven Filter sieht man unter der Suchleiste nebeneinander aufgelistet.

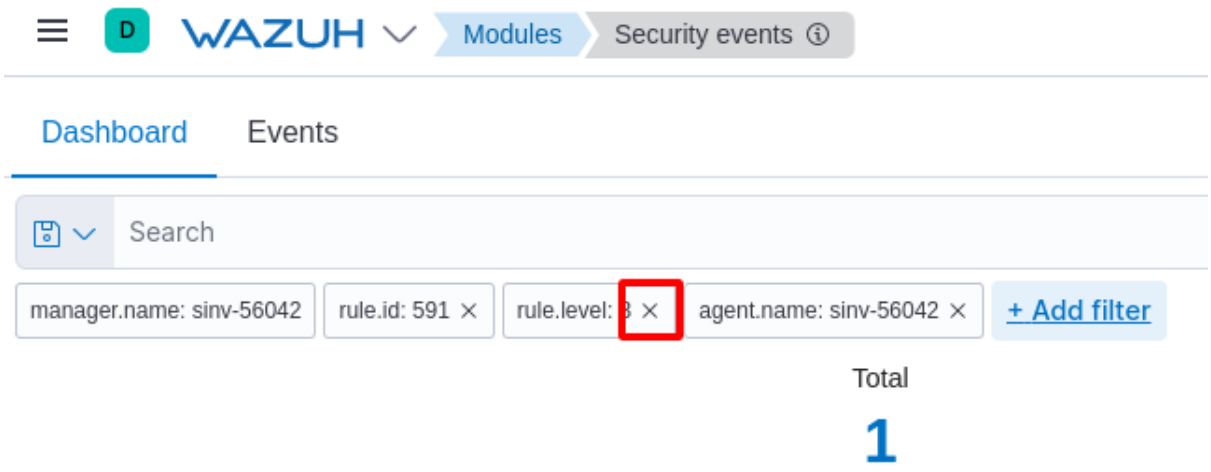


Abbildung 5.3: Aktive Filter in Wazuh

Diese kann man mit dem kleinen × rechts im Feld wieder löschen.

Der angezeigte Zeitintervall kann man rechts von der Suchleiste einstellen. Dies ist grundsätzlich auch ein Filter für das Feld "Time". Dieses Feld sollte immer wieder überprüft werden um sicherzugehen, dass zum Beispiel nicht nur die letzten 15 minuten angezeigt werden.

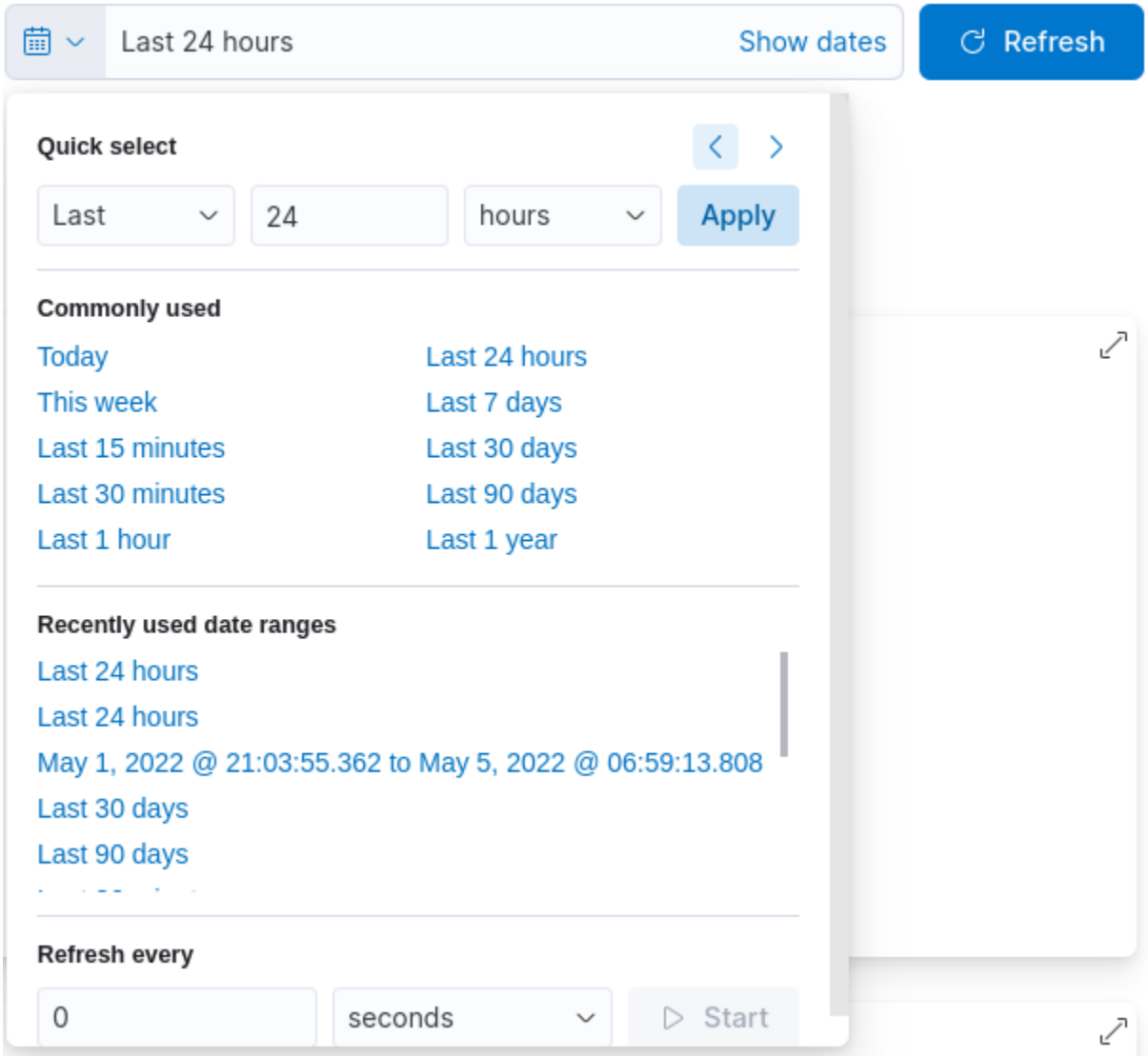


Abbildung 5.4: Zeitfilter in Wazuh

5.3 Alerts überprüfen

Die Alerts müssen in einem definierten Rhythmus angeschaut werden, sonst bleiben Attacken weiterhin unentdeckt. Eine Empfehlung ist es, jeden Morgen kurz die Level 12 Alerts anzuschauen und den auffälligen Alerts nachzugehen. Dabei ist Wichtig zu beachten, dass man den Zeitfilter korrekt setzt. Wenn zum Beispiel alle 2 Tage die Alerts überprüft werden, sollte auch der Zeitfilter um die 48 Stunden sein.

Es gibt auch die Möglichkeit, E-Mails für level 12 Alerts zu erhalten. Die Einrichtung dazu wird in diesem Repository und deren Guides nicht erklärt. Weitere Infos zu Einrichtung sind in der Dokumentation von Wazuh[1] erhältlich.

[1]Link: https://documentation.wazuh.com/current/user-manual/manager/manual-email-report/index.html?highlight=email

5.4 Attacken Beispiele

In diesem Kapitel werden zwei Beispiele von Attacken aufgezeigt. Dies sind nicht alle möglichen Attacken und die Liste ist daher nicht vollständig. Es sollen nur zwei Beispiele sein, damit Anwendern einen Anhaltspunkt haben wie mögliche Attacken aussehen könnten.

Attacken mit und ohne Kompromittierung generieren oftmals einen Level 12 Alert. Daher lohnt es sich, täglich die Level 12 Alerts in Wazuh anzuschauen. Um nach diesen zu Filtern gibt es unter Security Events im Reiter "Dashboard" einen Shortcut:

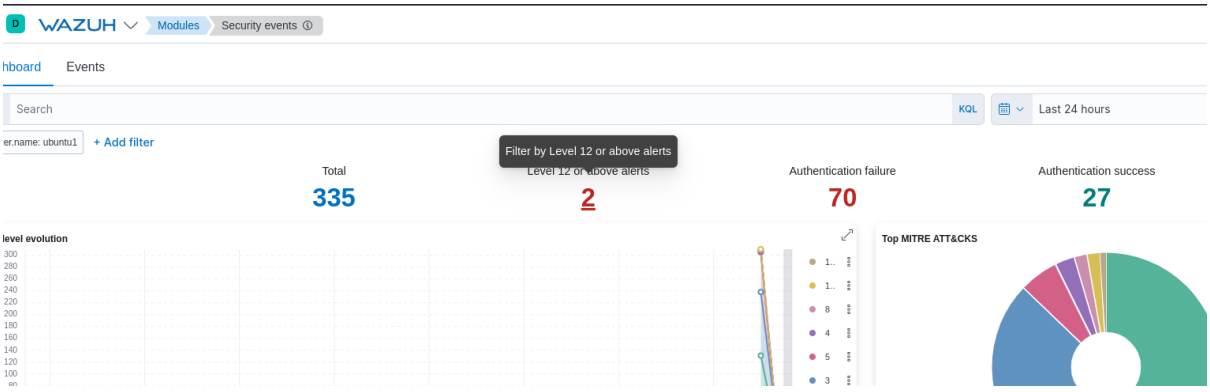


Abbildung 5.5: Level 12 Alerts Filter

5.4.1 Mimikatz

Mimikatz ist eine Software mit welcher es möglich ist, die gespeicherten Passwort Hashes von Benutzern auf Windows auszulesen. Mit diesem Hash kann dann zum Beispiel eine Pass-The-Hash[2] Attacke ausgeführt werden.

Mimikatz Attacken sind besonders gefährlich wenn Sie unentdeckt bleiben und sich auf dem kompromittierten System zuvor ein Domänen Administrator angemeldet hat.

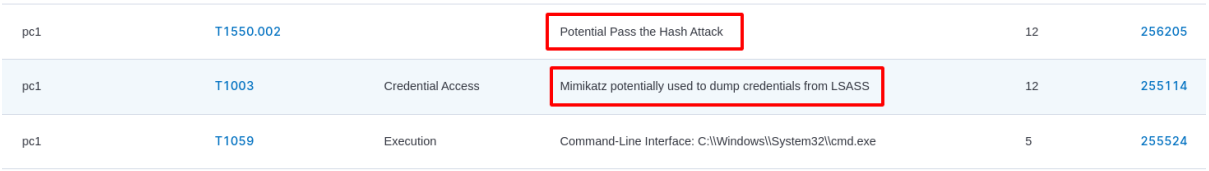


Abbildung 5.6: Mimikatz Attacke in Wazuh

Massnahmen

Bei einer Mimikatz Attacke sollten die Domänenadministratoren soweit möglich deaktiviert und die Passwörter dieser zurückgesetzt werden.

Prävention

Ein effektiver Weg sich gegen eine Mimikatz Attacke zu schützten, ist LAPS auf den Computern zu installieren. Ausserdem sollten möglichst wenige Domänenaccounts Administrator auf mehreren Computer sein. Genauere Anleitungen dazu befinden sich im Dokument "Security Best Practices" in diesem GitHub Repository.

[2]Link: https://en.wikipedia.org/wiki/Pass_the_hash

5.4.2 Brute Force

Attacken können auch Alerts mit anderen Leveln auslösen. Eine SSH Brute Force Attacke löst zum Beispiel einen "sshd: authentication failed." Alert mit Level 5 aus. Wenn zu viele von diesen Alerts in kurzer Zeit ausgelöst werden, gibt es einen "sshd: Multiple authentication failures." Alert mit Level 10.

Dadurch stand das betroffene System wahrscheinlich unter Angriff, aber noch ohne Erfolg. Wenn ein Angreifer erfolgreich ist, wird eine "Multiple authentication failures followed by a success." Alert mit Level 12 ausgelöst.

ubuntu1	T1078 T1110	Defense Evasion, Initial Access, Persistence, Privilege Escalation, Credential Access	Multiple authentication failures followed by a success.	12	40112
ubuntu1	T1110	Credential Access	sshd: authentication failed.	5	5716
pc1			Sysmon - Event 22: DNSEvent (DNS query) by C:\\Windows\\SystemApps\\Microsoft.Windows.Search_cw5n1h2txyewy\\SearchApp.exe	3	254006
ubuntu1	T1110	Credential Access	sshd: authentication failed.	5	5716
ubuntu1	T1110	Credential Access	sshd: Multiple authentication failures.	10	5720
ubuntu1	T1110	Credential Access	sshd: authentication failed.	5	5716
ubuntu1	T1110	Credential Access	sshd: authentication failed.	5	5716
ubuntu1	T1110	Credential Access	sshd: authentication failed.	5	5716

Abbildung 5.7: Brute Force Attacke in Wazuh

Massnahmen

Bei einer Brute Force Attacke sollten alle Daten gesammelt werden.

- Welches Gerät wurde von welcher IP angegriffen?
- Ist die Brute Force Attacke per SSH, RDP, physisch beim Windows Login oder über andere Wege?
- Befindet sich der Angreifer im lokalen Netzwerk oder extern?

Dadurch kann man definieren, wie die Brute Force Attacken geblockt werden können.

Prävention

Die beste Prävention gegen Brute Force Attacken ist eine gute Passwortrichtlinie und somit starke Passwörter von Benutzern. Genauere Anleitungen dazu befinden sich im Dokument "Security Best Practices" in diesem GitHub Repository.

5.5 False Positives

False Positives können am besten durch genauere Untersuchen der Alerts festgestellt werden. Eventuell hat ein Benutzer sein Passwort vergessen und erst beim 10. Versuch richtig eingegeben. Daher sollte man mit den Benutzern der Systeme Kontakt aufnehmen, falls die Möglichkeit besteht, dass es ein legitimer Fehler eines Benutzers war.

5.5.1 Dateihashes vergleichen

Angreifer benutzen gerne bekannte Namen von Betriebssystem Dateien, um ihre Schadsoftware zu verdecken. Der Name kann zwar gefälscht werden oder die Datei modifiziert, jedoch ändert sich der Hash der Datei damit. Durch überprüfen des Hashs kann festgestellt werden, ob es sich um die legitime Datei handelt.

Wazuh logt bei Alerts von ausgeführten Prozessen auch den Hash mit. In diesem Beispiel wurde der Prozess svchost.exe ausgeführt:

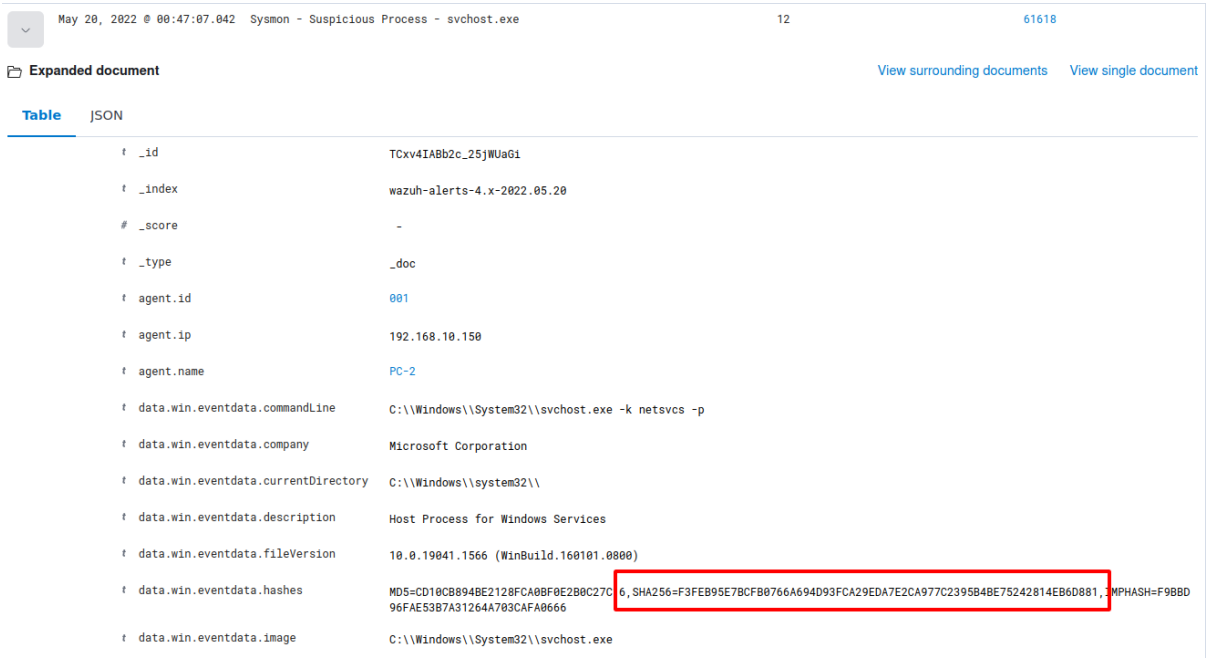


Abbildung 5.8: Hash vergleichen

Windows hat ein eingebautes Tool, um den Hash von Dateien zu berechnen. Dieses heisst "certutil". Damit kann der Hash von einer nicht komprimittierten svchost.exe Datei berechnet und verglichen werden. Dabei muss beachtet werden, dass es sich auch um die gleiche Version der .exe Datei handelt.

```
certutil -hashfile "C:\Windows\System32\svchost.exe" SHA256
#Hash: F3FEB95E7BCFB0766A694D93FCA29EDA7E2CA977C2395B4BE75242814EB6D881
```

Alternativ gibt es auch Online Tools wie VirusTotal[3], bei welchen die Datei, ein URL oder der Hash abgefragt werden können. **Achtung**, beim hochladen einer Datei wird diese veröffentlicht. Es ist besser den Hash einer Datei zu überprüfen oder nur nicht vertrauliche Dateien hochzuladen.

5.6 Massnahmen

Beim Verdacht eines Incidents sollten als erstes möglichst schnell die betroffenen Systeme eingedämmt werden. Hilfreich dafür ist das trennen der Geräte vom Netzwerk, sperren von betroffenen Benutzeraccounts und das herunterfahren von Systemen. Das kann eine Ausbreitung verhinderen und der Kontakt zum Angreifer könnte unterbrochen werden.

Danach sollte Anhand des Incident Response Plan gearbeitet und der externe IT Dienstleiter kontaktiert werden. Es ist besser, den externen IT Dienstleister einmal mehr als nötig zu informieren, um Folgeschäden von Angriffen zu vermeiden.

[3]Link: https://www.virustotal.com/gui/home/upload

KAPITEL 6

Verzeichnisse

Abbildungsverzeichnis

Tabellenverzeichnis

Literatur

[Kra12] Patrick Kral. *Incident Handler's Handbook*. Techn. Ber. United States: SANS, Feb. 2012.

[Waz] Wazuh-Team. *Wazuh Dokumentation*.

KAPITEL 7

Anhang

Glossar

Elasticsearch Logstash Kibana Elasticsearch, Logstash, Kibana sind drei Open-Source Projekte. Elasticsearch ist eine Such- und Analysesoftware für Logdateien. Logstash ist eine Software für das Sammeln von Logdateien von mehreren Quellen und übergibt diese an einen "Stash", zum Beispiel Elasticsearch. Kibana ist eine Visualisierungssoftware, welche Grafiken und Diagramme von einem "Stash" machen kann . 7, 28

Graphical user interface Ein Graphical user interface, auch Grafische Benutzeroberfläche genannt, ist eine Schnittstelle für Benutzer, um mit einem elektronischen Gerät grafisch zu interagieren . 28

Kibana query language Die Kibana query language (KQL) ist eine einfache Abfragesprache, mit welcher man in Text oder Feldbasierter Suche die Elasticsearch Daten durchsuchen kann . 17, 28

Local Administrator Password Solution Die Local Administrator Password Solution (LAPS) ermöglicht die Verwaltung der Passwörter lokaler Accounts von Computern, die der Domäne angeschlossen sind. Die Passwörter werden im Active Directory (AD) gespeichert. 28

SANS Institute Das SANS (SysAdmin, Audit, Network, and Security) Insitute ist ein private Unternehmen, welches sich auf die Ausbildung und Zertifizierung im Bereich der Cyber Security spezialisiert hat . 5, 28

Security Information and Event Management Security Information and Event Management (SIEM) ist ein Bereich der Informatik, welcher sich mit dem sammeln und auswerten von Logdateien beschäftigt. Oftmals wird dies mit SIEM Softwaresystemen gemacht. 4, 28

Abkürzungsverzeichnis

ELK Elasticsearch Logstash Kibana. 7, 8

GUI Graphical user interface. 2, 4, 9, 11–16

KQL Kibana query language. 17, 23

LAPS Local Administrator Password Solution. 19

SANS SANS Institute. 5

SIEM Security Information and Event Management. 2, 4, 5, 16

INSTITUTE FOR NETWORKED SOLUTIONS

OST Eastern Switzerland University of Applied Sciences

Wazuh Installationsanleitung

Eine einfache Installation für KMUs

Studiengang Informatik
Ostschweizer Fachhochschule
Campus Rapperswil-Jona

Autoren:	Severin Grimm Marco Martinez
Version:	31. Mai 2022

Inhaltsverzeichnis

KAPITEL 1

Einleitung

1.1 Umfang

Dieses Dokument ist für Informatikverantwortliche- und Mitarbeitende welche Wazuh im Unternehmen installieren und verwenden möchten.

Es erläutert die skriptbasierte Installation des Wazuh Managers auf einem Ubuntu Server inklusive einiger zusätzlichen Punkte. Ausserdem wird eine Möglichkeit zur automatischen Installation des Wazuh Agent und Sysmon auf allen Computern im Unternehmen aufgezeigt.

KAPITEL 2

Wazuh Server Installation

2.1 Voraussetzungen

Die Installationsanleitung für KMUs unterstützt debian-basierte Systeme. Es wird Ubuntu 20.04 LTS[1] empfohlen. Es muss auch beachtet werden, dass der Server genug Ressourcen zur Verfügung hat. Der Server braucht mindestens 2 CPU Cores, 4GB RAM und 100 GB Speicher. Der Speicher hängt von der Anzahl Clients ab. Weitere Informationen dazu gibt es in der Wazuh Dokumentation[2].

2.2 Installation

Die Installationsanleitung kann direkt im README.md[3] auf GitHub eingesehen werden.

2.2.1 Firewall

Es ist empfohlen eine hostbased Firewall zu verwenden. Auf Ubuntu wird standardmässig UFW[4] verwendet. Es ist auch möglich Firewalld[5] einzusetzen, welches auf den meisten anderen Linuxsystemen als default verwendet wird.

Ports

```
443/tcp         -  Kibana web interface
514/UDP/tcp     -  Syslog
1514/UDP/tcp    -  To get events from the agent.
1515/tcp        -  Port Used for agent Registration.
1516/tcp        -  Wazuh Cluster communications.
9200/tcp        -  Elasticsearch API
55000/tcp       -  Wazuh API port for incoming requests.
```

Weitere Informationen können dem Architekturkonzept[6] von Wazuh entnommen werden.

[1] Link: https://releases.ubuntu.com/20.04.4/ubuntu-20.04.4-live-server-amd64.iso
[2] Link: https://documentation.wazuh.com/current/installation-guide/requirements.html#all-in-one-deployment
[3] Link: https://github.com/KMU-Incident-Response/KMU-Basis-Logging/blob/main/universal_installer/README.md#installation
[4] Link: https://help.ubuntu.com/community/UFW
[5] Link: https://firewalld.org/
[6] Link: https://documentation.wazuh.com/current/getting-started/architecture.html#required-ports

2.2.2 SELinux

Es ist empfohlen SELinux auf der "permissive" oder "disabled" Stufe zu halten. Im Scope von dieser Anleitung wird keine SELinux "enforcing" Variante angeboten.

2.3 Upgrade

Das Upgrade des Wazuhserver kann über den Packagemanager gemacht werden. Es ist zu beachten, dass nur die unterstützen Versionen von Wazuh, Elasticsearch und Kibana installiert werden sollen. Informationen zu unterstützten Versionen können der Webseite[7] von Wazuh entnommen werden. Ein Upgrade könnte nachher wie folgt aussehen:

```
apt-get install elasticsearch=7.14.2
```

2.4 Wazuh Rules

Bei der Installation vom Wazuh Server für KMUs wird automatisch auch eine Palette von Regeln bereitgestellt. Es ist möglich die Regeln ohne die Serverinstallation zu importieren. Dazu wird ein bereits installierter Wazuhserver benötigt. Mehr Informationen kann man im GitHub README[8] finden.

2.5 SSL Zertifikat

Die Wazuhinstallation wird mit einem Self-Signed Zertifikat ausgeliefert. Es ist empfohlen das Standard Zertifikat durch ein eigenes zu ersetzen.

Das Zertifikat muss später im Kibana hinterlegt werden und der Service neugestartet.

```
    sudo mv my-cert.crt /etc/kibana/certs/kibana.crt
    sudo mv my-cert.key /etc/kibana/certs/kibana.key
    sudo chmod 440 /etc/kibana/certs/kibana.{key,crt}
    sudo chown kibana:kibana /etc/kibana/certs/kibana.{key,crt}
    sudo systemctl restart kibana.service
```

[7] Link: https://documentation.wazuh.com/current/upgrade-guide/compatibility-matrix/index.html
[8] Link: https://github.com/KMU-Incident-Response/ossec-sysmon/tree/master#manuelle-installation-von-rules

KAPITEL 3

Wazuh Agent Installation

3.1 Installation via GPO

Der Wazuh Agent kann per Group Policy auf allen Windows Geräten installiert werden. Dazu muss als erstes die Installationsdatei für den Agent auf der Webseite von Wazuh[1] heruntergeladen werden.

Die Installationsdatei braucht eine Konfigurationsdatei welche die Netzwerkadresse des Wazuh Managers enthält. Eine solche Konfigurationsdatei kann mithilfe dem Windows Tool "Orca" erstellt werden, welches Teil der Windows SDK ist. Das Windows SDK kann man auf der Webseite von Microsoft[2] herunterladen.

Bei der Installation der Windows SDK kann eine grosse Anzahl Features ausgewählt werden. Für Orca wird jedoch nur das Feature "MSI Tools" benötigt, alle andere Features können abgewählt werden.

[1] Link: https://documentation.wazuh.com/current/installation-guide/packages-list.html
[2] Link: https://developer.microsoft.com/de-de/windows/downloads/windows-sdk/

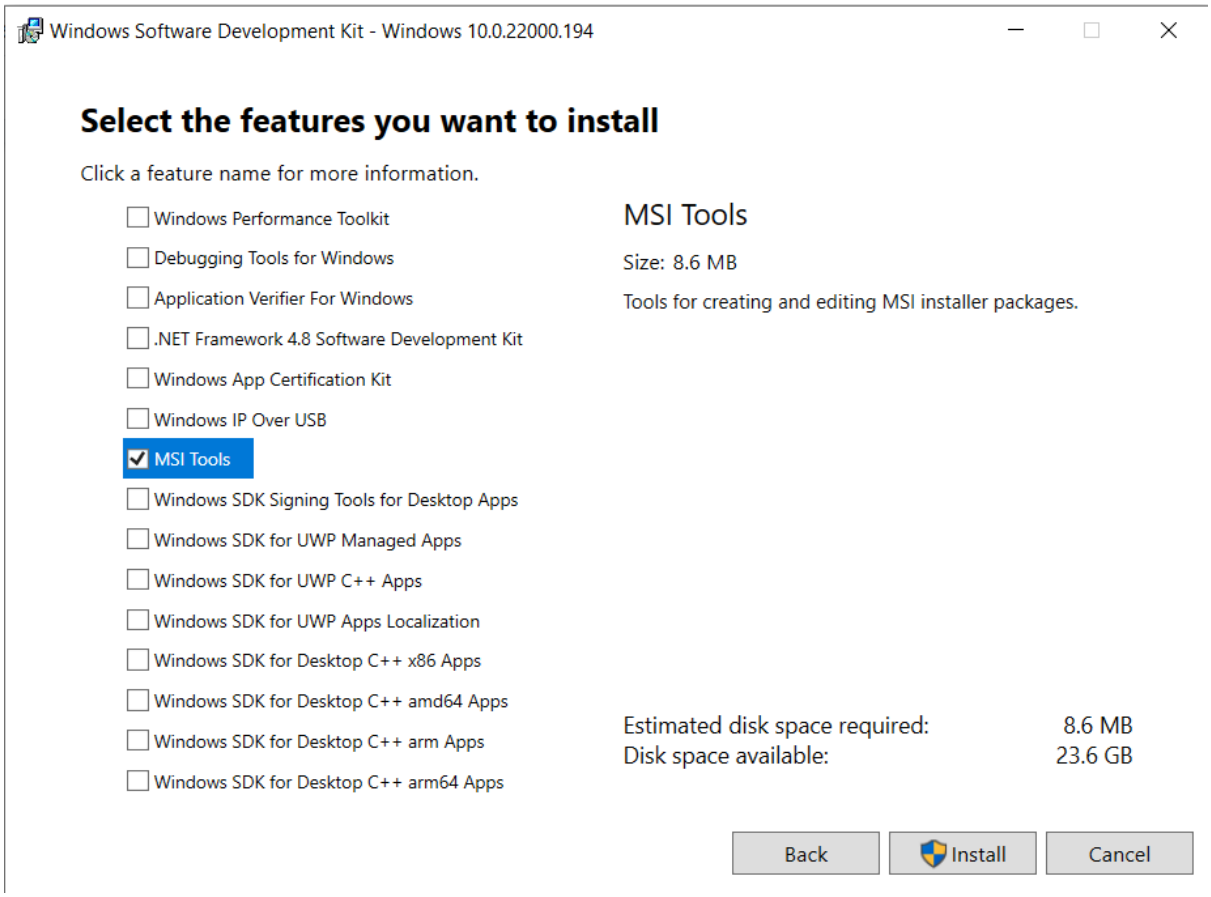


Abbildung 3.1: MSI Tools der Windows SDK

Orca befindet sich nun unter

```
C:\Program Files (x86)\Windows Kits\10\bin\<Version>\x86\Orca-x86_de-de.msi
```

und kann mit dieser .msi Installationsdatei installiert werden. Sobald Orca installiert ist wird im Kontextmenu bei .msi Dateien einen neuen Punkt mit "Edit with Orca" ersichtlich.

Mit einem Rechtsklick auf die Wazuh Agent .msi Datei kann via "Edit with Orca" eine Konfigurationsdatei erstellt werden.

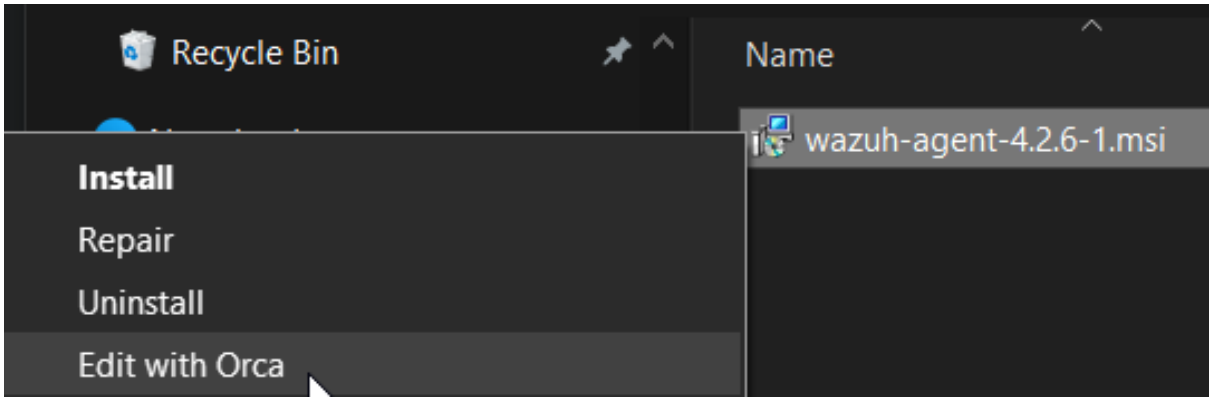


Abbildung 3.2: Mit Orca bearbeiten

In Orca muss man in der Menüleiste unter **Transform** → **New Transform** einen neuen Änderungsnachweis erstellen.

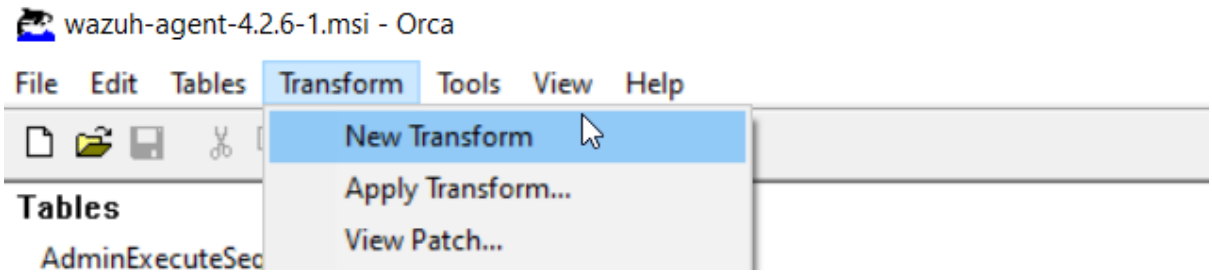


Abbildung 3.3: Neuer Änderungsnachweis in Orca

Auf der linken Seite unter "Tables" auf die Tabelle "Property" gehen. Dort werden neue "Key - Value" Paare hinzugefügt. Es braucht folgende Paare:

- **WAZUH_MANAGER**: <Hostname Wazuh Manager>
- **WAZUH_REGISTRATION_SERVER**: <Hostname Wazuh Manager>
- **WAZUH_AGENT_GROUP**: Windows
- **WAZUH_REGISTRATION_PASSWORD**: <Password gesetzt bei Installation>

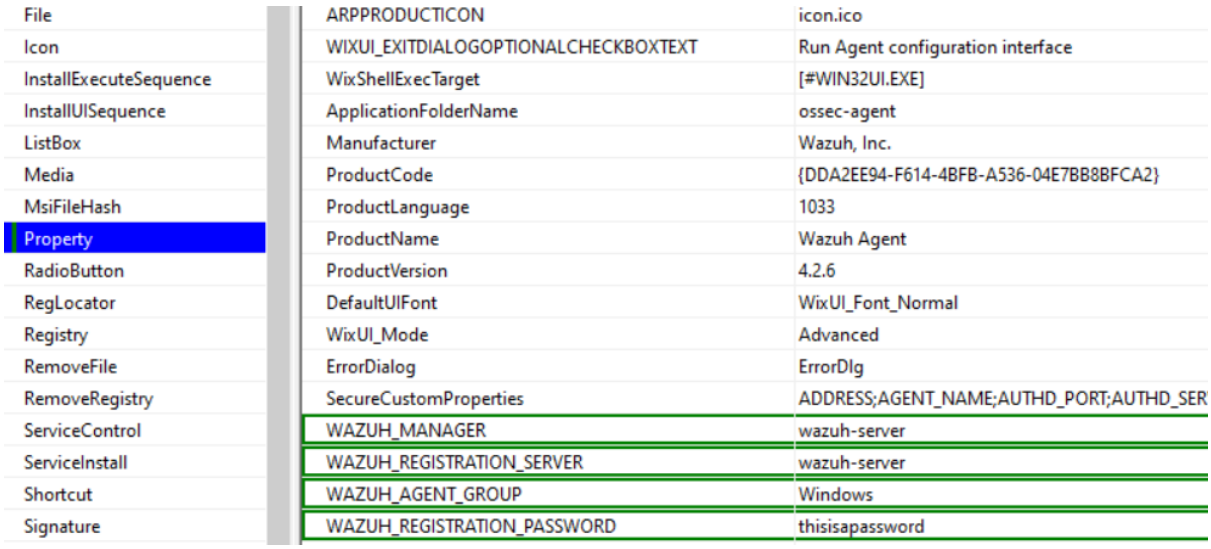


Abbildung 3.4: Wazuh Installationsparameter

In der Menüleiste unter **Transform** → **Generate Transform** die Konfigurationsdatei exportieren und unter einem beliebigen Namen, zum Beispiel "custom-wazuh-settings.mst", abgespeichern.

Die .msi und .mst Dateien müssen nun in einem freigegebenen Netzlaufwerk abgespeichert werden, auf welches alle Windows Geräte Zugriff haben. Zum Beispiel auf dem Domain Controller unter:

```
C:\Windows\SYSVOL\sysvol\<Domain>
```

Nun muss eine neue Group Policy erstellt werden, mit welcher der Wazuh Agent auf den Windows Geräten installiert wird. Dazu öffnet man das Group Policy Management auf dem Domain Controller und erstellt eine neue Group Policy, welche mit der OU verknüpft ist, die alle Windows Geräte enthält.

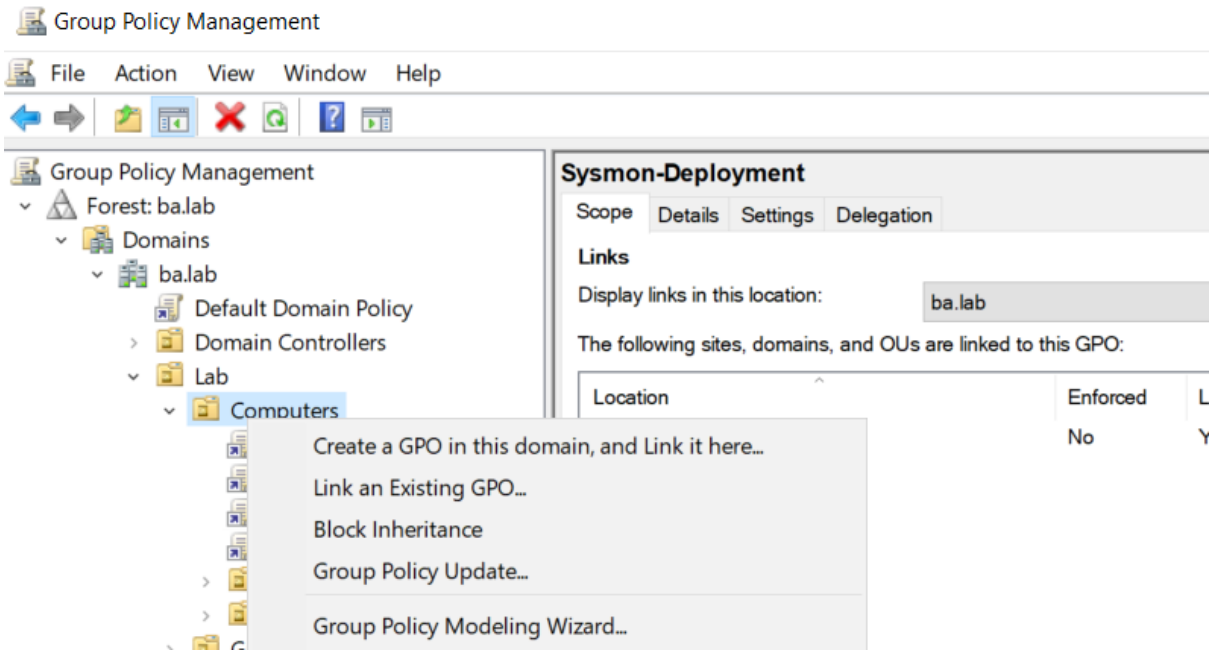


Abbildung 3.5: Neue Group Policy für Agent Deployment

In der neuen Group Policy muss unter **Computer Configuration** → **Policies** → **Software Settings** → **Software installation** mit **Rechtsklick** → **New** → **Package...** eine Datei ausgewählt werden, welche installiert werden soll.

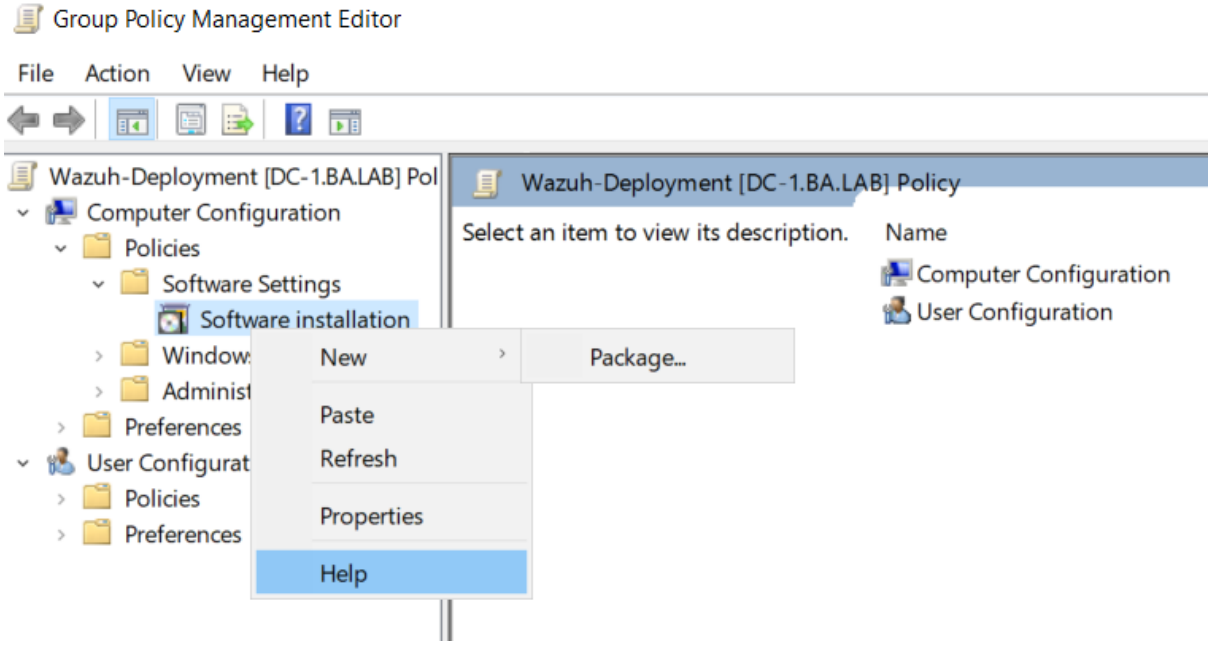


Abbildung 3.6: Neue Group Policy für Agent Deployment

Im neuen Fesnter wählt man die .msi Datei, welche im freigegebenen Netzlaufwerk abgelegt wurde. Beim Installationstyp wählt man anschliessen "Advanced" und klickt weiter. Ein neues Fenster öffnet sich, in welchem man Anpassungen für die Installation angeben kann. Unter **Modifications** → wählt man nun die .mst Datei aus, welche vorher erstellt wurde.

Nun kann man mit OK Bestätigen. Die Group Policy ist bereit und kann geschlossen werden. Der Wazuh Agent wird beim Einloggen auf den Geräten installiert und verbindet sich automatisch mit dem Server.

3.2 Manuelle Installation

Der Wazuh Agent kann über die Commandline von mehreren Betriebssystemen installiert werden. Für Windows zum Beispiel mit Powershell. Die Commands der einzelen Betriebssystem findet man im Wazuh Manager. Dazu öffnet man den Wazuh Manager und geht auf **Wazuh** → **Agent**. Auf der rechten Seite der Tabelle mit allen Agents klickt man auf "Deploy new Agent".

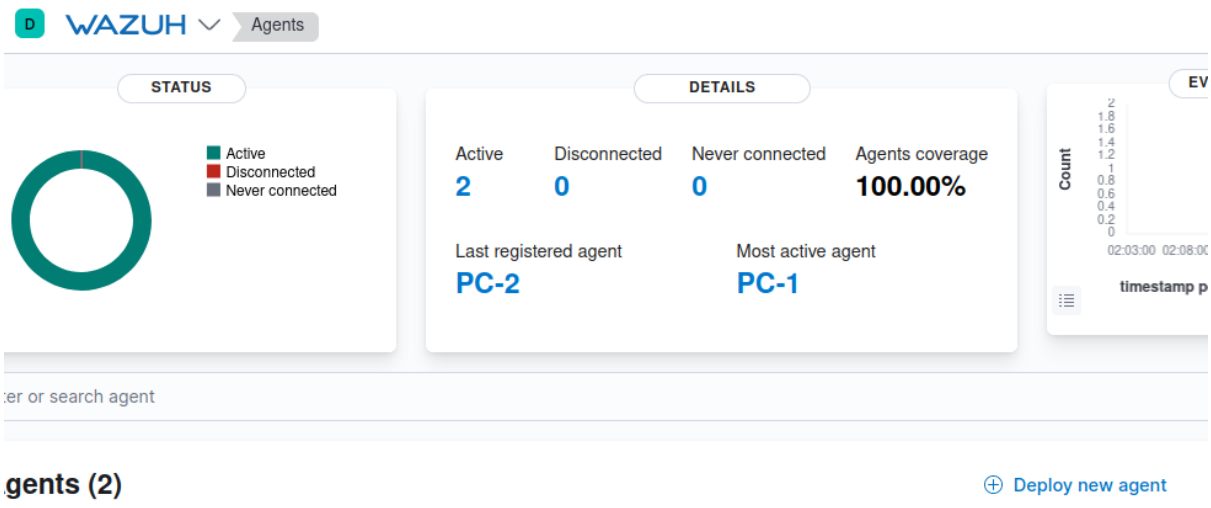


Abbildung 3.7: Agent deployment

Auf der nächsten Seite gibt man alle nötigen Daten an und kann unten den Powershell Command kopieren.

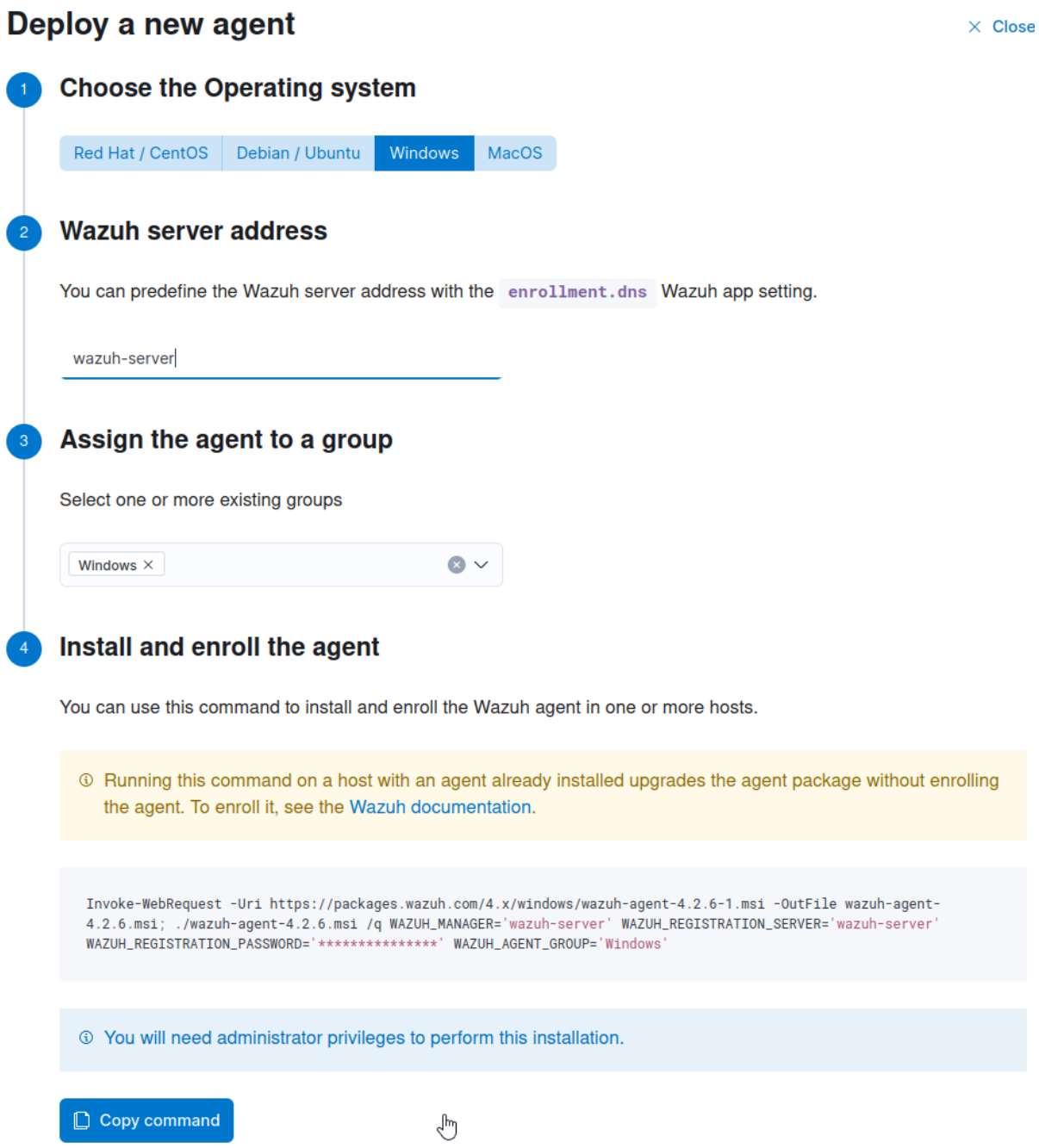


Abbildung 3.8: Wazuh Agent manuell installieren

Auf dem Windows Gerät Powershell als Administrator starten und das zuvor kopierte Command eingeben:

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/Der Wazuh/wazuh-agent-mit einem.2.6-1.msi
    -OutFile wazuh-agent-4.2.6.msi; ./wazuh-agent-4.2.6.msi /q WAZUH_MANAGER='wazuh-server'
    WAZUH_REGISTRATION_SERVER='wazuh-server' WAZUH_REGISTRATION_PASSWORD=<Password>
    WAZUH_AGENT_GROUP='Windows'
```

Auf der Deployment Seite vom Wazuh Manager können auch Red Hat, Debian und MacOS ausgewählt werden. Dann werden die Commands für diese Geräte angezeigt.

KAPITEL 4

Sysmon Installation

4.1 Installation via GPO

Sysmon kann auf der Webseite von Microsoft[1] heruntergeladen werden. Es gibt eine 32- und 64-Bit Version von Sysmon.
Zusätzlich braucht es noch eine Konfigurationsdatei welche definiert, was Sysmon in den Event Log schreibt. Die Konfiugrationsdatei kann man im KMU-Incident-Response Repository[2] herunterladen.

Die .exe und .xml Dateien müssen in einem freigegebenen Netzlaufwerk abgespeichert werden, auf welches alle Windows Geräte Zugriff haben. Zum Beispiel auf dem Domain Controller unter:

```
C:\Windows\SYSVOL\sysvol\<Domain>
```

Nun muss eine neue Group Policy erstellt werden, mit welcher Sysmon auf den Windows Geräten installiert wird. Dazu öffnet man das Group Policy Management auf dem Domain Controller und erstellt eine neue Group Policy, welche mit der OU verknüpft ist, die alle Windows Geräte enthält.

[1] Link: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
[2] Link: https://github.com/KMU-Incident-Response/KMU-Basis-Logging

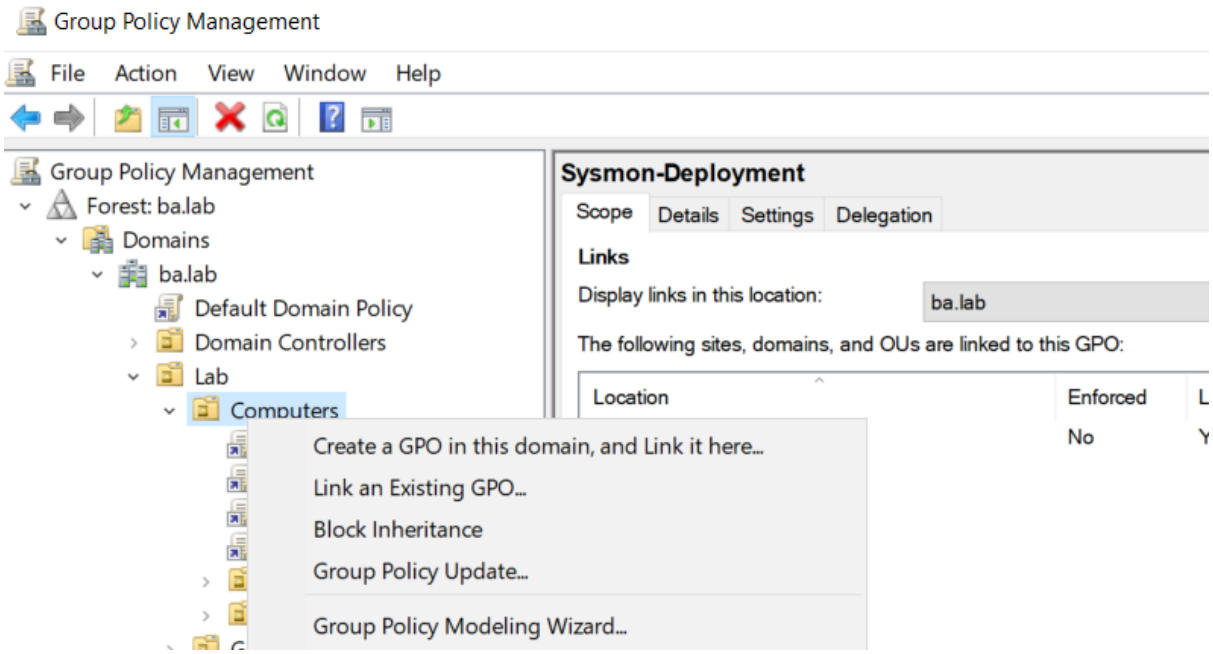


Abbildung 4.1: Neue Group Policy für Sysmon Deployment

Die Group Policy muss mit **Rechtsklick** → **Edit** bearbeitet werden. Unter **Computer Configuration** → **Preferences** → **Windows Settings** → **Folder** kann mit **Rechtsklick** → **New** → **Folder** ein neuer Ordner auf den Windows Geräten angelegt werden. Dieser wird benötigt, um die Dateien vom freigegebenen Netzlaufwerk in diesen Ordner zu kopieren. Es müssen folgende Einstellungen vorgenommen werden:

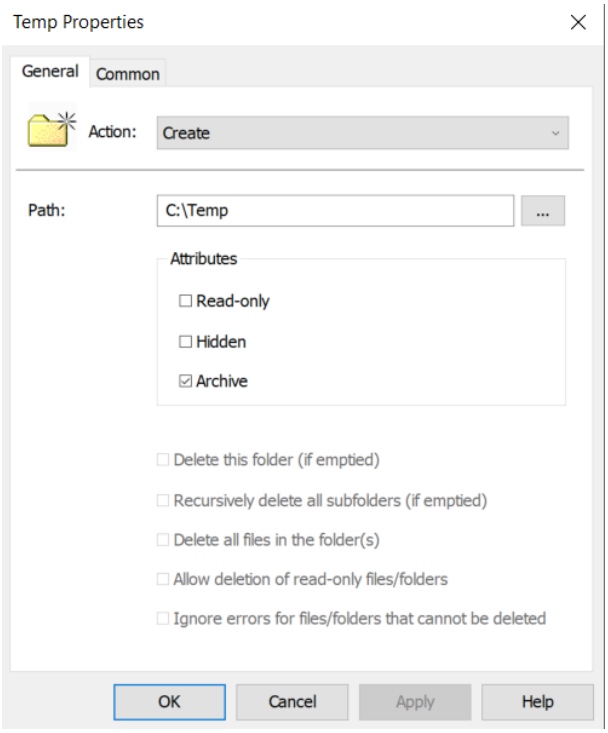


Abbildung 4.2: Neuer Ordner mit GP erstellen 1

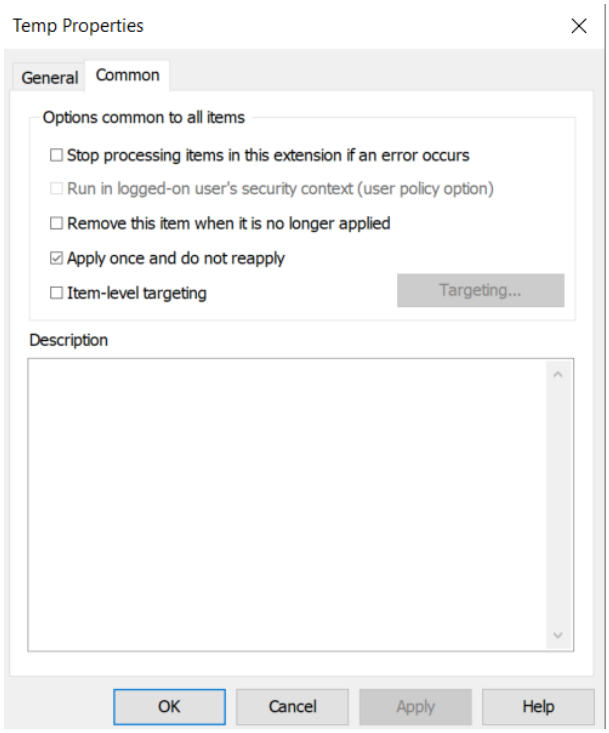


Abbildung 4.3: Neuer Ordner mit GP erstellen 2

Danach kann man mit "OK" bestätigen.

Als nächstes wird das kopieren der Dateien eingerichtet. Dazu macht man im Menu links auf Files **Rechtsklick**

→ **New** → **Files** und erstellt eine neue Policy. Dies muss einmal für die .exe und zusätzlich für die .xml Datei gemacht werden. Als **Action** wählt man "Create". Als **Source File** wählt man die Dateien auf dem freigegebenen Netzlaufwerk. Als **Destination File** wählt man den zuvor erstellten Ordner. Unter dem Reiter **Common** muss wieder ein Hacken bei "Apply once and do not reapply" gesetzt werden:

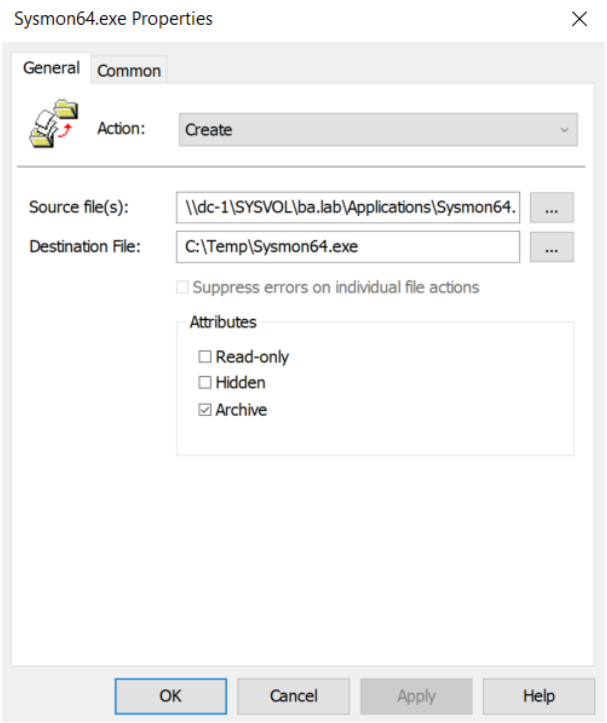


Abbildung 4.4: Sysmon.exe kopieren

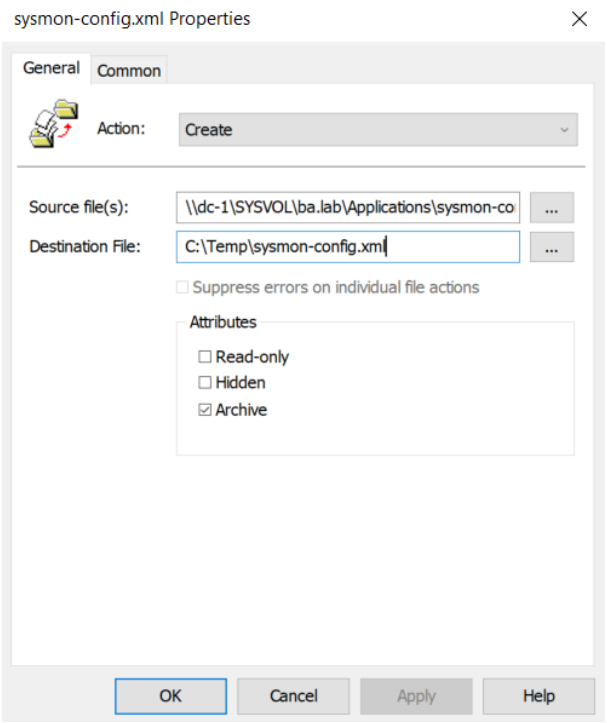


Abbildung 4.5: sysmon-config.xml kopieren

Zuletzt muss noch ein neuer Immediate Task unter **Computer Configuration** → **Preferences** → **Control Panel Settings** → **Scheduled Tasks** mit **Rechtsklick** → **New** → **Immediate Task (At least Windows 7)** erstellt werden.

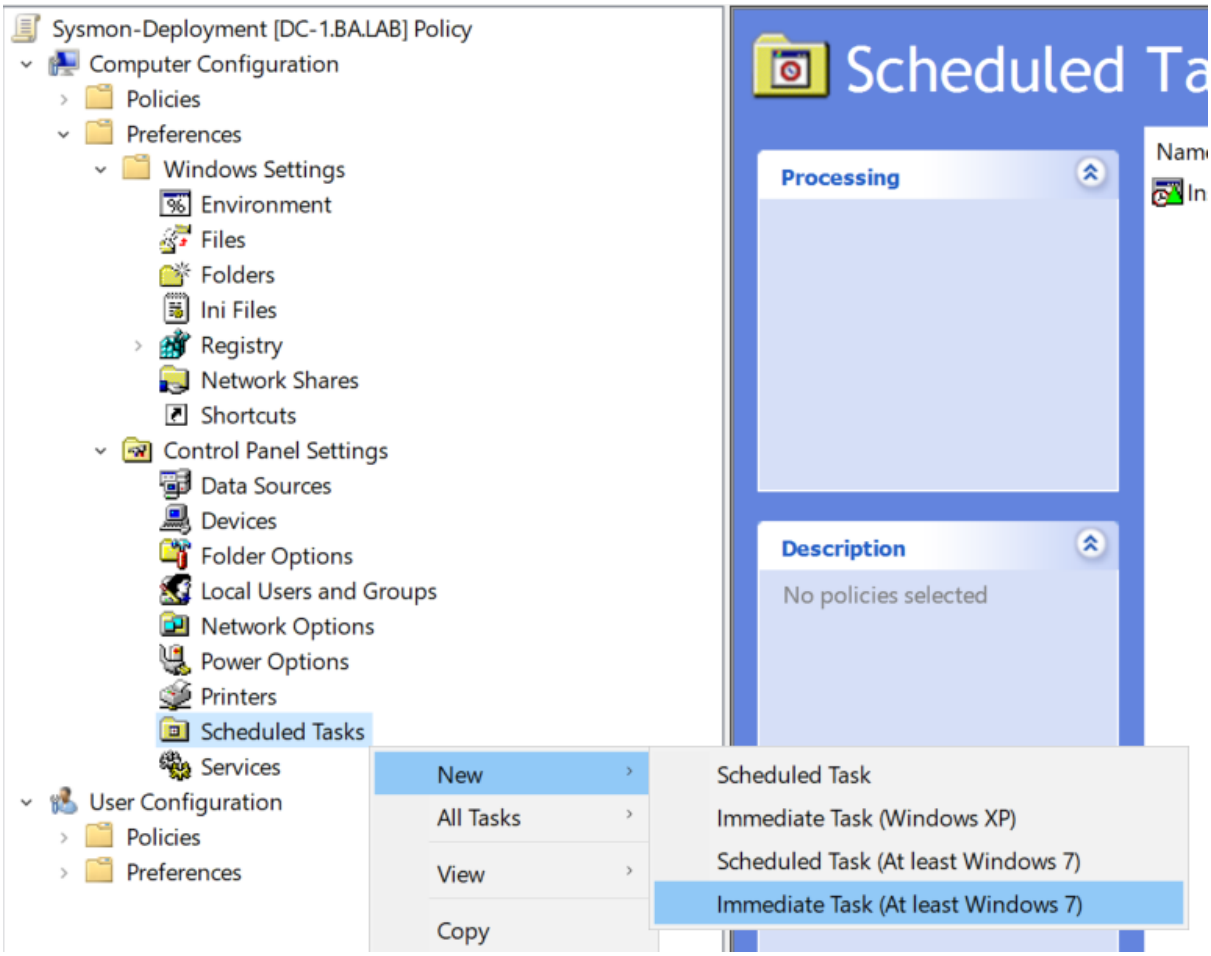


Abbildung 4.6: Neuen Immediate Task erstellen

Unter dem Reiter **Common** muss wieder ein Hacken bei "Apply once and do not reapply" gesetzt werden. In den Reitern **General** und **Action** werden folgende Einstellungen getroffen:

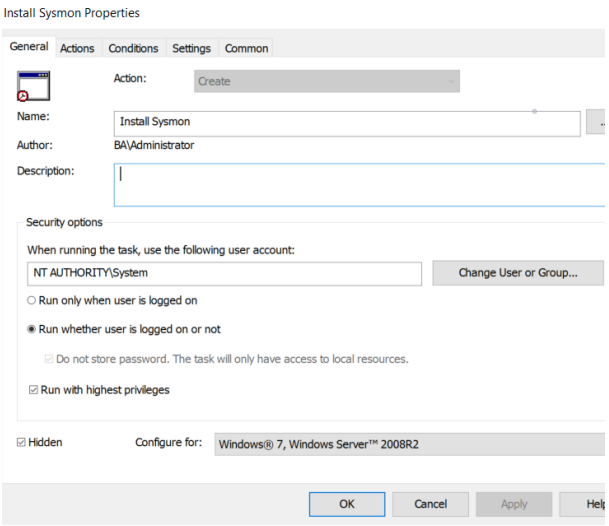


Abbildung 4.7: Einstellungen Immediate Task 1

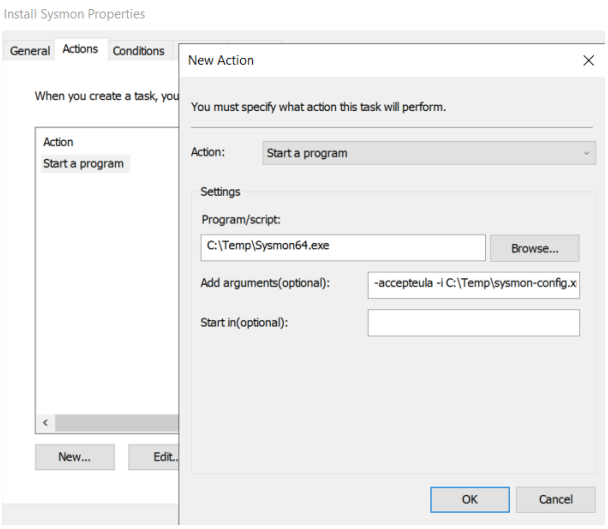


Abbildung 4.8: Einstellungen Immediate Task 2

Add Arguments:

```
-accepteula -i C:\Temp\sysmon-config.xml
```

Die Group Policy ist bereit und kann geschlossen werden. Sysmon wird beim Einloggen auf den Windows Geräten installiert.

4.2 Manuelle Installation

Um Sysmon manuell auf einem Windows Gerät zu installieren, muss man, wie im vorherigen Kapitel beschrieben, die Dateien herunterladen. Die Konfigurationsdatei kann in das gleiche Verzeichnis wie die .exe kopiert werden. Danach öffnet man die Kommandozeile als Administrator und wechselt in das Verzeichnis der heruntergeladenen und entpackten Dateien. Dort gibt man folgendes Kommando ein:

```
    sysmon64.exe -accepteula -i sysmon-config.xml
```

Sysmon wird nun auf dem Windows Gerät installiert.

KAPITEL 5

Verzeichnisse

Abbildungsverzeichnis

Tabellenverzeichnis

KAPITEL 6

Anhang

Glossar

Group Policy Object Ein Group Policy Object (GPO) ist eine Sammlung von Richtlinieneinstellungen. Ein GPO hat einen eindeutigen Namen, z. B. eine GUID. Gruppenrichtlinieneinstellungen sind in einem GPO enthalten. 22

Organizational Unit Mit Organizational Units (OUs) in einer von Active Directory (AD) verwalteten Domäne können Objekte wie Benutzeraccounts, Serviceaccounts oder Computer logisch gruppieren. 22

Abkürzungsverzeichnis

GPO Group Policy Object. 2, 6, 12

OU Organizational Unit. 8, 12

KAPITEL 7

Incident Response Plan Vorlage

APRIL 14, 2022

Firmen-Logo

INCIDENT RESPONSE PLAN

1. Änderungsnachweis

Version	Änderung	Name	Datum
V0.1	Erstellung des Dokumentes	Editor	14.04.2022

2. Inhaltsverzeichnis

3. Organisation

Dieses Dokument ist eine Vorlage und nicht für die 1:1 Übernahme gedacht. Abhängig von der Firmenstruktur, sollten Teile dieses Dokumentes angepasst werden.

3.1. Erklärung der Geschäftsleitung

Ein definiertes Sicherheitsereignis-Konzept im Unternehmen ist eine Voraussetzung für die Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit der IT-Infrastruktur. Durch eine schnelle Reaktion können Schäden minimiert und mittels Dokumentation die Wahrscheinlichkeit einer Wiederholung eines Vorfalls protokolliert werden.

Dieser Leitfaden beschreibt, wie Ereignisse unterschiedlicher Art priorisiert, kategorisiert, behandelt und kommuniziert werden. Als Grundlage zur Ergreifung der richtigen Massnahmen.

3.2. Umfang

Dieses Dokument beinhaltet den Umgang und die Vorgehensweise mit Sicherheitsereignissen- und Vorfällen im Zusammenhang mit der IT-Infrastruktur. Sicherheitsereignisse werden anhand einer vorgegebenen Priorisierung kategorisiert.

3.3. Definitionen

Sicherheitsereignis

Ein Sicherheitsereignis ist eine Anomalie in einem IT-System, welche durch Mitarbeitende oder ein Sicherheitssystem entdeckt wird.

Beispiele für Sicherheitsereignisse sind:

- Logins von fragwürdigen Orten
- Ein Laptop ging verloren / wurde gestohlen
- Verdächtiger Netzwerkverkehr

Sicherheitsvorfall

Ein Sicherheitsvorfall ist ein Sicherheitsereignis, bei welchem ein begründeter Verdacht besteht, dass Unternehmensressourcen kompromittiert wurden. Jeder Sicherheitsvorfall ist ein Sicherheitsereignis. Nicht jedes Sicherheitsereignis ist ein Sicherheitsvorfall.

Beispiele für Sicherheitsereignisse sind:

- Ein Benutzer hat sein Passwort auf einer Phishing-Webseite eingegeben
- Ransomware wurde ausgeführt

3.4. Rollen und Zuständigkeiten

Je nach Unternehmensgrösse kann oder muss eine Person mehrere Rollen und Zuständigkeiten übernehmen.

IT-Support

Der IT-Support ist die erste Anlaufstelle für Mitarbeitende, überwacht die Systeme und ist für Supportangelegenheiten bei Sicherheitsereignissen- und Vorfällen zuständig. Ab einem Sicherheitsereignis ist der IT-Support für die Registrierung und Protokollierung zuständig.

Ab einem Sicherheitsvorfall eskaliert der IT-Support den Vorfall an den Vorfallmanager.

Befugnisse

- Benutzer bei falschem Umgang mit IT-Ressourcen benachrichtigen
- Die Vorgesetzten eines Mitarbeitenden bei Verstössen gegen die IT-Richtlinien informieren.
- Bei Verdacht auf Kompromittierung von Benutzeraccounts den Zugang und Berechtigungen von Mitarbeitenden sperren
- Jegliche Systeme und Clients mit Malware sofort herunterzufahren.
- Eskalation von Sicherheitsvorfällen an den Vorfallmanager

Vorfallmanager

Eine oder mehrere Personen, die während des Zeitraumes eines Sicherheitsvorfalls für den Incident-Response Prozess verantwortlich sind und die Koordination übernehmen.

Befugnisse

- Einleiten von Managementmassnahmen bei schwerwiegenden Sicherheitsvorfällen.
- Involvieren aller betroffenen Parteien.
- Fortlaufendes informieren der Geschäftsleitung bei einem Sicherheitsvorfall
- Involvieren von externen Spezialisten, welche gegebenenfalls Kosten generieren

Sicherheitsverantwortlicher

Eine Person, die die Gesamtverantwortung für die Informationssicherheit der IT-Infrastruktur trägt. Der Sicherheitsverantwortliche ist der Ansprechpartner für alle Sicherheitsmassnahmen, welche in der IT-Infrastruktur eingesetzt werden.

Befugnisse

- Systematische Sicherheitschecks durchführen.
- Die Zusammenarbeit mit den Behörden sicherstellen.
- Definieren von IT-Richtlinien und deren Durchsetzung.
- Berichte an die Geschäftsleitung.

Kommunikationsverantwortlicher

Eine oder mehrere Personen, die während des Zeitraumes eines Sicherheitsvorfalls für die Kommunikation zuständig sind. Dies beinhaltet die interne Kommunikation zu Mitarbeitenden, die Kommunikation zu betroffenen Kunden und, wenn nötig, die Kommunikation extern mit Medien, Behörden.

Incident Response Team

Ein definiertes Team von internen und/oder externen IT-Spezialisten, die im Falle eines Sicherheitsvorfalls die Incident Response übernehmen. Das Incident Response Team ist zuständig für die Bestimmung der Auswirkungen, des Umfangs und der Art des Vorfalls. Zusätzlich reagiert das Incident Response Team auf den Vorfall und führt die Bereinigung durch.

3.5. Kontaktdaten

Ausgehend vom Speicherort der Datei und der Benennung.

Die Kontaktdaten befinden sich in der Datei “Incident Response Kontaktformular.docx”.

4. Response Plan

4.1. Mission

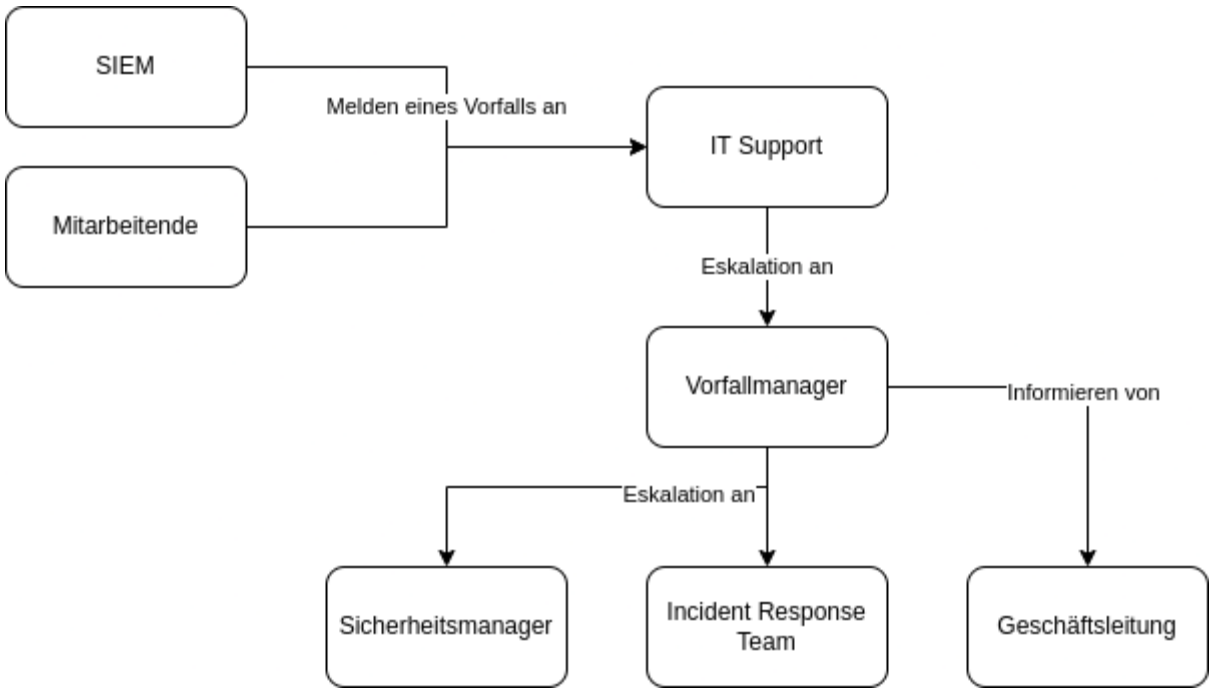
Bei einem Sicherheitsvorfall gilt es schnell zu reagieren, um Schäden möglichst minimal zu halten. Dies soll mit einem definierten Ablauf erreicht werden. Dadurch wissen alle Mitarbeitenden, wie Sie bei einem Vorfall reagieren müssen und wen es zu kontaktieren gilt.

4.2. Strategien und Ziele

Durch die Priorisierung kann schneller entschieden werden, wann ein Vorfall eskaliert werden muss. Dies minimiert die Zeit bei Entscheidungen und gewährleistet ein einheitliches Vorgehen.

Ziel ist es, dass bei Sicherheitsvorfällen möglichst schnell reagiert wird und die richtigen Personen informiert, beziehungsweise involviert werden.

4.3. Kommunikationsablauf



4.4. Priorisierung von Vorfällen

Die Priorisierungsmatrix muss ausgehend von den eingesetzten Systemen im Unternehmen angepasst werden.

Die Priorisierung wird anhand nachfolgender Tabelle gemacht. Falls mehrere Prioritätsstufen auf ein Ereignis zutreffen, gilt es die höchste Priorität zu wählen.

Priorisierungsmatrix

	Auswirkung			
Betroffene Entität	**Kritisch**	**Hoch**	**Mittel**	**Klein**
Unternehmenskritische Systeme: - **AD** - **Datenbanken** - **VIP-User Accounts**	1	1	2	3
Reguläre Systeme: - **DHCP-Server** - **Applikationsserver**	1	2	3	4
Computer	2	3	3	4
Benutzeraccounts	2	3	4	4

Legende

Priorität:	**Auswirkung:**
1. Sehr hoch 2. Hoch 3. Mittel 4. Niedrig	• **Kritisch:** Kompromittierung und Ausfall • **Hoch:** Kompromittierung • **Mittel:** Hohe Wahrscheinlichkeit einer Kompromittierung • **Klein:** Keine Kompromittierung

4.5. Reaktion auf Vorfälle

Kommunikation

Beim Umgang mit einem Sicherheitsvorfall muss mit einer gewissen Diskretion kommuniziert werden. Wenn möglich sollte die Anzahl informierter Personen auf einem Minimum beschränkt werden, bis sich der Sicherheitsvorfall geklärt hat. Personen im definierten Ablauf müssen immer involviert werden.

Eskalation

Ab **Priorität 3** eskaliert der IT-Support den Vorfall an den Vorfallmanager. Dieser trifft weitere Entscheidungen über den Verlauf des Vorfalls und involviert nötige Parteien. Er entscheidet in Absprache mit dem IT-Support, ob der Vorfall weiter eskaliert werden muss oder nicht.

Ab **Priorität 2** informiert der Vorfallmanager die Geschäftsleitung über den Vorfall. Zusätzlich muss das Incident Response Team involviert werden.

Deeskalation

Die Deeskalation wird vom Vorfallmanager übernommen. Dieser entscheidet in Absprache mit dem Incident Response Team, ab wann ein Sicherheitsvorfall bewältigt ist und sich das Unternehmen wieder im Normalzustand befindet.

Dokumentation

Alle Schritte während der Bewältigung eines Incidents werden dokumentiert und abgelegt.

Dies beinhaltet:

- Betroffene Systeme
- Betroffene Benutzer
- Gefundene Anomalien
- Eintrittsort
- Verbreitungsweg

Nacharbeiten

Nach der Bewältigung eines Vorfalls werden, wenn möglich, neue Sicherheitsmassnahmen definiert, um die Wahrscheinlichkeit eines erneuten Eintretens eines solchen Sicherheitsvorfalls zu minimieren.

5. Genehmigung durch die Geschäftsleitung

Hiermit bestätigt die Geschäftsleitung, dass folgendes Dokument per XX.XX.XXXX in Kraft tritt.

Datum, Ort	Name, Vorname
_____	_____

Wegleitung Kontaktformular

Diese Seite ist nur für Erklärungen und kann gelöscht werden.

Im Kontaktformular werden alle benötigten Kommunikationswege zu Kontaktpersonen aufgelistet. Dies wird gemacht, damit bei einem Sicherheitsvorfall nicht zuerst noch die Kontaktdaten zusammengesammelt werden müssen und dadurch Zeit gespart werden kann.

Definition der unten genannten Kontakte:

- ***IT-Support***, ***Vorfallmanager***, ***Sicherheitsverantwortlicher*** *und* ***Incident Response Team*** *sind im Dokument "Incident Response Plan" definiert.*
- ***Geschäftsleitung*** *ist die Geschäftsleitung des Unternehmens*
- *Das* ***NCSC*** *ist das Nationale Zentrum für Cybersicherheit. Dieses kann bei Sicherheitsvorfällen informiert werden und gibt Hilfestellungen nach Melden eines Vorfalls. Ausserdem hilft es dem NCSC, trends zu erkennen und gegebenenfalls proaktive Massnahmen zu treffen.*
- *Der* ***ISP*** *ist der Internet Service Provider. Also zum Beispiel die Swisscom oder Sunrise.*
- *Als* ***Cloudanbieter*** *gelten alle extern gehosteten Services. Zum Beispiel Email Hosting bei Microsoft oder ein Webserver bei einem Webhoster.*
- *Bei den* ***Software*** *Kontaktpersonen werden Kontaktpersonen der eingesetzten properitären Softwaren aufgeschrieben. Dies hilft einerseit für die Inventur und falls Schwachstellen dieser Softwaren ausgenutzt werden.*

Incident Response Kontaktformular

IT-Support - Erster Ansprechpartner _____
_____
Notizen: _____
_____
_____

Vorfallmanager
Name: _____
E-Mail: _____
Telefonnummer: _____
Notizen: _____
_____
_____
_____

Sicherheitsverantwortlicher
Name: _____
E-Mail: _____
Telefonnummer: _____
Notizen: _____
_____
_____
_____

Ansprechpartner Geschäftsleitung
Name: _____
E-Mail: _____
Telefonnummer: _____
Notizen: _____
_____
_____
_____

Stv. Ansprechpartner Geschäftsleitung
Name: _____
E-Mail: _____
Telefonnummer: _____
Notizen: _____
_____
_____
_____

Kontakt Incident Response Team
Firma: _____
Name: _____
E-Mail: _____
Telefonnummer: _____
Notizen: _____
_____
_____
_____

Stv. Kontakt Incident Response Team
Firma: _____
Name: _____
E-Mail: _____
Telefonnummer: _____
Notizen: _____
_____
_____
_____

National Cyber Security Centre NCSC:
Name: Nationales Zentrum für Cybersicherheit
E-Mail: info@ncsc.admin.ch _____
Telefonnummer: _____
Notizen: _____
Incident melden: https://www.report.ncsc.admin.ch/de/ _____
_____
_____

Incident Response Kontaktformular

Primärer ISP Kontaktperson_____
Bezeichnung: _____
Name: _____
E-Mail: _____
Telefonnummer: _____
Notizen: _____
_____
_____
_____

Sekundärer ISP Kontaktperson_____
Bezeichnung: _____
Name: _____
E-Mail: _____
Telefonnummer: _____
Notizen: _____
_____
_____
_____

Cloudanbieter Kontaktperson_____
Bezeichnung: _____
Name: _____
E-Mail: _____
Telefonnummer: _____
Notizen: _____
_____
_____
_____

Cloudanbieter Kontaktperson_____
Bezeichnung: _____
Name: _____
E-Mail: _____
Telefonnummer: _____
Notizen: _____
_____
_____
_____

Software Kontaktperson_____
Bezeichnung: _____
Name: _____
E-Mail: _____
Telefonnummer: _____
Notizen: _____
_____
_____
_____

Software Kontaktperson_____
Bezeichnung: _____
Name: _____
E-Mail: _____
Telefonnummer: _____
Notizen: _____
_____
_____
_____

Software Kontaktperson_____
Bezeichnung: _____
Name: _____
E-Mail: _____
Telefonnummer: _____
Notizen: _____
_____
_____
_____

Software Kontaktperson_____
Bezeichnung: _____
Name: _____
E-Mail: _____
Telefonnummer: _____
Notizen: _____
_____
_____
_____

INSTITUTE FOR NETWORKED SOLUTIONS

OST Eastern Switzerland University of Applied Sciences

Security Best Practices

Ein Guide für KMUs

Studiengang Informatik
Ostschweizer Fachhochschule
Campus Rapperswil-Jona

Autoren:	Severin Grimm Marco Martinez
Version:	31. Mai 2022

Inhaltsverzeichnis

KAPITEL 1

Einleitung

1.1 Umfang

Dieses Dokument enthält eine Sammlung von Konzepten und Best Practices ausgelegt auf KMUs.

Das Dokument reicht von sehr abstrakten Konzepten bis zu konkreten Best Practices. Der Guide ist so generell und herstellerunabhängig als möglich gehalten. Bei defacto Standards in der KMU IT-Landschaft, gibt es kleine Anleitungen zur Bedienung oder Konfiguration des Produktes. Der Guide fokussiert sich auf Open-Source Software soweit möglich und realistisch.

Dieser Guide sollte für KMUs der entsprechenden Grösse in der Matrix relevant sein.

Guide	mikro KMU	kleines KMU	mittleres KMU
Geräteverschlüsslung	X	X	X
Antivirus	X	X	X
Backup	X	X	X
Updates & Patching	O	X	X
Firewall	O	X	X
Identity and Access Management (IAM)		X	X
Local Administrator Password Solution (LAPS)		O	X

X = starke Empfehlung, O = Empfehlung

Tabelle 1.1: Guiderelevanz entsprechend KMU Grösse

Abbildung 1.1: Einteilung KMU Grössen

1.2 Ausgewählte Themen

Die ausgewählten Themen sind alles wichtige Bestandteile, die von Firmen umgesetzt werden um die Sicherheit in der IT-Infrastruktur zu erhöhen. Die Themen wurden aus folgenden Gründen gewählt:

- **Geräteverschlüsselung**: Physische Sicherheit bei Diebstahl oder Verlust.
- **Antivirus**: Sicherheit bei Viren und Malware.
- **Backup**: Recovery bei Verlust oder Ransomware.
- **Updates & Patching**: Fortlaufende Sicherheit bei neuen Attacken.
- **Firewall**: Sicherheit zwischen Netzwerken und im Internet.
- **IAM**: Zugriffskontrolle und Verwaltung. Sicherheit vor Datendiebstahl.
- **LAPS**: Sicherheit vor der Ausbreitung von Malware bei kompromittiert Geräten.

KAPITEL 2

Identity and Access Management (IAM)

2.1 Umfang

In diesem Kaptiel werden die On-Premise Identity and Access Management (IAM) Lösungen erläutert. Die Federation IAM haben einen sehr spezifischen Use-Cases und sind hauptsächlich bei Cloud-First Archtitekturen zu finden. Daher sind diese in diesem Dokument ausserhalb des Umfangs und werden nicht weiter behandelt.

2.2 IAM Varianten

Ein Identity and Access Management (IAM) ist ein zentrales System welches die Entitäten, wie Benutzeraccounts und Computer, erfassen kann. Zudem können Berechtigungen auf Entitäten in einer Domäne verwaltet werden.

Braucht es ein IAM?
Es ist grundsätzlich möglich ohne ein IAM System zu arbeiten, wobei der Aufwand für das Management der Userverwaltung auf allen Maschinen schnell den Rahmen des Budgets sprengt. Der allgemeine Konsenus ist, dass ab 15 aktiven Bentuzern ein IAM verwendet werden soll. Eine IAM Lösung bringt viele Vorteile, gleichzeitig birgt es auch Risiken.

Vorteile:

- zentrales Accountmanagement
- zentrales Accessmanagement
- schnelle Skalierung Server/Client Umgebung
- single Source of Truth[a]
- Policysystem zur Konfiguration von Client
- meist gebündelt mit nützlichen Features[b]
- Single Sign-On

Tabelle 2.1: Vorteile IAM

Nachteile:

- hoher initial Aufwand
- höchste Priorität eines Angreifers
- anfällig auf Misskonfigurationen
- abhängigkeit eines stabilen Systems

Tabelle 2.2: Nachteile IAM

[a] https://de.wikipedia.org/wiki/Single_Point_of_Truth
[b] DHCP, DNS, NTP, CA etc. (Produktabhängig)

Wie bei vielem ist es wichtig das richtige Produkt für seine Umgebung zu finden. Als nächstes werden zwei, im Markt beliebte Produkte vorgestellt.

2.2.1 Active Directory

Active Directory ist ein Produkt von Microsoft und kann exklusiv auf einem Microsoft Windows Server installiert werden. Active Directory ist einfach zu installieren, wobei die Konfiguration Herausforderungen mit sich bringen kann.

Active Directory ist mit mehr als 80% Marktanteil der Marktführer. Das Produkt bietet alle grundlegenden Funktionen wie User-, Geräte- und Berechtigungsverwaltung. Ausserdem lässt sich Active Directory integrieren mit anderen Windows Server Funktionen wie DHCP, DNS, NTP und weiteren externen Funktionen von anderen Anbietern. Vorallem in Windowsnetzwerken ist die Integration sehr gut und intuitiv.

Active Directory bietet in fast allen Fällen was ein KMU braucht und viel mehr. Deshalb ist die Wahl von Active Directory für KMUs meist die richtige Wahl. Es gibt nur wenige sehr spezifische Fälle in denen ein anderes Produkt besseren Nutzen erbringt.

2.2.2 FreeIPA

FreeIPA ist eine Open-Source Implementation eines IAMs, entwickelt durch die Community und Upstream von Red Hat Identity Management. Exklusiv verfügbar auf RPM-basierten Linux Systemen.

FreeIPA bietet von den Features einen ähnlichen Umfang wie Active Directory, aber mit dem grossen Unterschied, dass die Hauptzielgruppe Linux Server und Clients sind. Es werden auch User-, Geräte- und Berechtigungsverwaltung, DHCP, DNS, NTP und viele weitere einfache, bis zu komplexen Funktionen angeboten.

FreeIPA ist eine gute Wahl in exklusiven Linuxnetzwerken. Für KMUs ist in den meisten Fällen FreeIPA die falsche Wahl und Active Directory sollte vorgezogen werden.

2.3 Betreiben eines IAMs

Das Betreiben eines IAMs kann Herausforderungen bieten. Es gibt viele Dinge zu beachten. Das wichtigste ist es ein Verständnis zu erlangen wie kritisch das IAM System ist. Ein Ausfall des IAM Systems kann das ganze Netzwerk beeinträchtigen und bewirken, dass das Arbeiten für die ganze Firma schwerer, bis unmöglich wird. Eine Misskonfiguration kann die Türe für einen Cybersecurityvorfall öffnen. Das IAM ist oftmals das primäre Angriffsziel eines Angreifers, da ab diesem alle Systeme und deren Zugriff verwaltet wird.

Um die Angriffsfläche und somit das Risiko zu minimieren sollten die unten beschriebenen Konzepte beachtet und wenn möglich strikt implementiert werden.

2.3.1 Least Privilege

Das "least privilege principle" ist ein grundlegender Security Best Practice, denn man überall wieder findet.

Das Prinzip besagt jeder Benutzer soll genau soviel Rechte haben, wie er für seine tägliche Arbeit benötigt. Alles weitere soll blockiert werden. Somit kann die Angriffsfläche bei Vorfällen massiv verringert werden.

Für privilegierte Benutzer wie z.B. ein Systemadministrator sollen zusätzliche, spezielle Accounts bereitgestellt werden. Denn die meiste Arbeit kann mit einem nicht privilegierten Nutzer verrichtet werden.

Zusätzlich soll auch beachtet werden, dass es keine "Masteraccounts" gibt, welche alle Rechte besitzen. Den diese sind für Angreifer besonders interessant und für das Unternehmen gefährlich.

2.3.2 Persönliche Accounts

Es muss versucht werden die Anzahl unpersönliche Accounts auf ein Minimum beschränkt zu halten. Bei einem Incident sind die Logs ausschlaggebend.

Arbeiten alle Benutzer mit dem Account "Finanzen" ist es schwer Rückschlüsse zu ziehen, wo kritische Aktionen oder ilegitime Zugriffe passiert sind. In einem Vorfall wäre es klar, dass der Verstoss mit dem Account "Finanzen" passiert ist, aber welcher der 10 Personen die den Account benutzen den Verstoss begangen hat ist schwer, bis unmöglich Rückzuschliessen.

2.3.3 Rollen als Berechtigungen

Unternehmungen sind ermutigt Jobprofile zu erstellen, um geeignetes Personal zu finden. Es ist ähnlich in der Verteilung von Benutzerrechten. Eine Person ist angestellt um eine bestimmte Arbeit zu verrichten. Diese Zuteilung wird nun auf eine Rolle abgebildet. Die Rolle mit den Rechten erhalten alle Angestellten mit dem gleichen Auftrag. Oftmals werden Rollen in einem IAM "Gruppen" genannt, welcher man Benutzer und andere Gruppen hinzufügen kann.

Das Verteilen von Rollen erleichtert den Überblick der einzelnen Berechtigungen in der Unternehmung. Bei individual Berechtigungen verliert man schnell den Überblick. Mit administrativen Wechseln wie interne Umorientierungen kann es dazu führen, dass Nutzer zu viele Berechtigungen für Ihren Job haben und somit das "least privilege principle" verletzen. Mit Rollen kann bei internen Wechseln lediglich die alte Rolle entfernt und die neue Rolle hinzugefügt werden.

2.3.4 Automatische Benutzerverwaltung

Es ist empfohlen die Benutzerverwaltung zu automatisieren oder einen klaren Prozess festzulegen. Dies betrifft vorallem die Benutzer, welche das Unternehmen verlassen. Die Accounts sollten beim Austritt deaktiviert und nach einer definierten Zeit gelöscht werden.

2.3.5 Zuständigkeitsbereich eines IAM

Es kann eine Herausforderung entstehen, wenn man alle seine Geräte an das IAM anbinden will.

Im Idealfall sind alle Geräte an das IAM angebunden. Es gibt aber auch Instanzen, in welchen diese Lösung nicht wirtschaftlich vertretbar ist. Das geht in Ordnung. Bei solchen Geräten sollte sich überlegt werden, wie sie adäquat geschützt werden können.

2.3.6 IAM Schlusswort

Ein IAM kann Agilität, Komfort und Sicherheit bringen. Mit den Vorteilen bringt ein IAM auch Risiken, wie Sicherheitsbedenken und Abhängigkeit für den produktiven Betrieb. Daher sollte ein IAM bestmöglich geschützt werden. Editorberechtigung im IAM sollten nur Personen zustehen, welche diese auch wirklich brauchen (least privilege).
In den meisten Fällen ist ein IAM die beste Lösung. Der grösste Teil der Vorfälle kann mit den zuvor genannten Konzepten mitigiert oder sogar ganz vermieden werden.

2.4 Active Directory Best Practices

2.4.1 Passwortrichtlinien

Es gibt verschiedene Möglichkeiten, wie Angreifer an Passwörter kommen können. Darunter gehören zum Beispiel:

- Bruteforce Attacken: Auf einem Account verschiedene Passwörter testen.
- Spraying Attacken: Ein Passwort mit verschiedenen Accounts testen.
- Dictionary Attacks: Bruteforce-Attacke mit einer Liste von bekannten Passwörtern.
- Social-Engineering: Angreifer versuchen das Passwort direkt vom Benutzer zu bekommen.

Best Practice für die Passwortvorgaben für User und Administratoren sind folgend[1]:

- Lange Passwörter sind besser als komplexe Passwörter.
- Lange Passwörter müssen **nicht** in einem gewissen Interval gewechselt werden.
- Passwort Hinweise beim Login sollten deaktiviert werden. (Standard in AD)
- Anzahl möglicher Anmeldeversuche sollte eingeschränkt werden.

NIST empfiehlt für die mindestlänge eines Passwortes 8 Zeichen. Dieser Guide empfiehlt jedoch mindestens 12 Zeichen. Hier ein Vergleich von einem 8-Stelligen und einem 12-Stelligen Passwort, welches Gross- und Kleinschreibung und Zahlen enthält[2]:

Substrings	Type	Entropy	Computation time
***	Word (English)	17 Bit	
***	Other characters	24 Bit	
Aufwandschätzung		40 Bit	14 seconds

Abbildung 2.1: Passwort mit 8 Stellen

Substrings	Type	Entropy	Computation time
***	Word (English)	17 Bit	
***	Word (English)	17 Bit	
***	Other characters	30 Bit	
Aufwandschätzung		63 Bit	3 years

Abbildung 2.2: Passwort mit 12 Stellen

Group Policy für Passwortrichtlinien

Die Passwortrichtlinien können per Group Policy gesetzt werden. Im Group Policy Management existiert unter **Forest: <Domänen-Namen>** → **Domains** → **<Domänen-Namen>** die "Default Domain Policy". In dieser setzt man unter **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Account Policies** folgende Richtlinien:

Password Policy:

Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	0
Minimum password age	1 days
Minimum password length	12 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Relax minimum password length limits	Not Defined
Store passwords using reversible encryption	Disabled

Abbildung 2.3: Passwortrichtlinien

Account Lockout Policy:

Policy	Policy Setting
Account lockout duration	30 minutes
Account lockout threshold	10 invalid logon attempts
Reset account lockout counter after	30 minutes

Abbildung 2.4: Account Lockout Richtlinien

Die Group Policy kann nun so geschlossen werden. In den AD Objekten der Benutzer ist nun unter "Account" ein Hacken bei "Password never expires". Falls die Passwordrichtline vorher bei weniger als 12 Zeichen war,

[1] Zugriff: 16.04.2022 [Gra22]
[2] Berechnet mit: https://www.passwortcheck.ch/

müssen nun die Benutzer noch aufgefordert werden, ihr Passwort zu ändern. Dies kann mit Powershell gemacht werden:

```
Get-ADUser -SearchBase "<OU der Benutzer>" -Filter * | Set-ADUser -ChangePasswordAtLogon $True

#Beispiel:
Get-ADUser -SearchBase "OU=Employees,OU=Users,OU=Lab,DC=ba,DC=lab" -Filter * | Set-ADUser
    -ChangePasswordAtLogon $True
```

Dies sollte mit dem Management abgeklärt werden und die Benutzer sollten frühzeitig informiert werden. Man kann auch zuerst die Mindestlänge in der Group Policy setzen und erst nach einem Zyklus, wenn alle Mitarbeitenden ihr Passwort auf die neue Länge gesetzt haben, die Option "Maximum password age" auf 0 setzen.

Bei der Passwortrichtlinie für Administratoren wird empfohlen, dass diese ihr Passwort weiterhin mindestens alle 180 Tage wechseln müssen. Dazu kann eine neue Group Policy auf Höhe der OU mit den Administratoren erstellt werden:

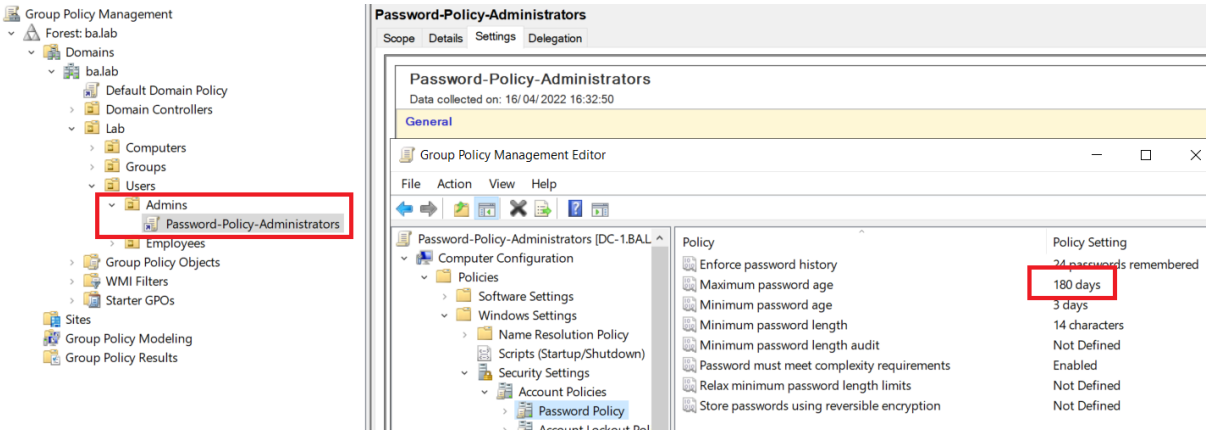


Abbildung 2.5: Passwortrichtlinien Administratoren

Die Account Lockout Policy bleibt gleich.

2.4.2 Active Directory Auditing

Active Directory bietet die Möglichkeit, Änderungen an Gruppen und Benutzern im Event Log festzuhalten. Dies ist nützlich um nachvollziehen zu können, wann welche Änderungen gemacht wurden und zusammen mit Wazuh erkennen zu können, ob Änderungen gemacht wurden die nicht von Administratoren kamen.

Diese Logs müssen mit einer Group Policy aktiviert werden. Im Group Policy Management existiert unter **Forest: <Domänen-Namen>** → **Domains** → **<Domänen-Namen>** → **Domain Controllers** die "Default Domain Controllers Policy". In dieser setzt man unter **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Local Policies** → **Audit Policy** in der Richtlinie "Audit account Management" folgende Einstellungen:

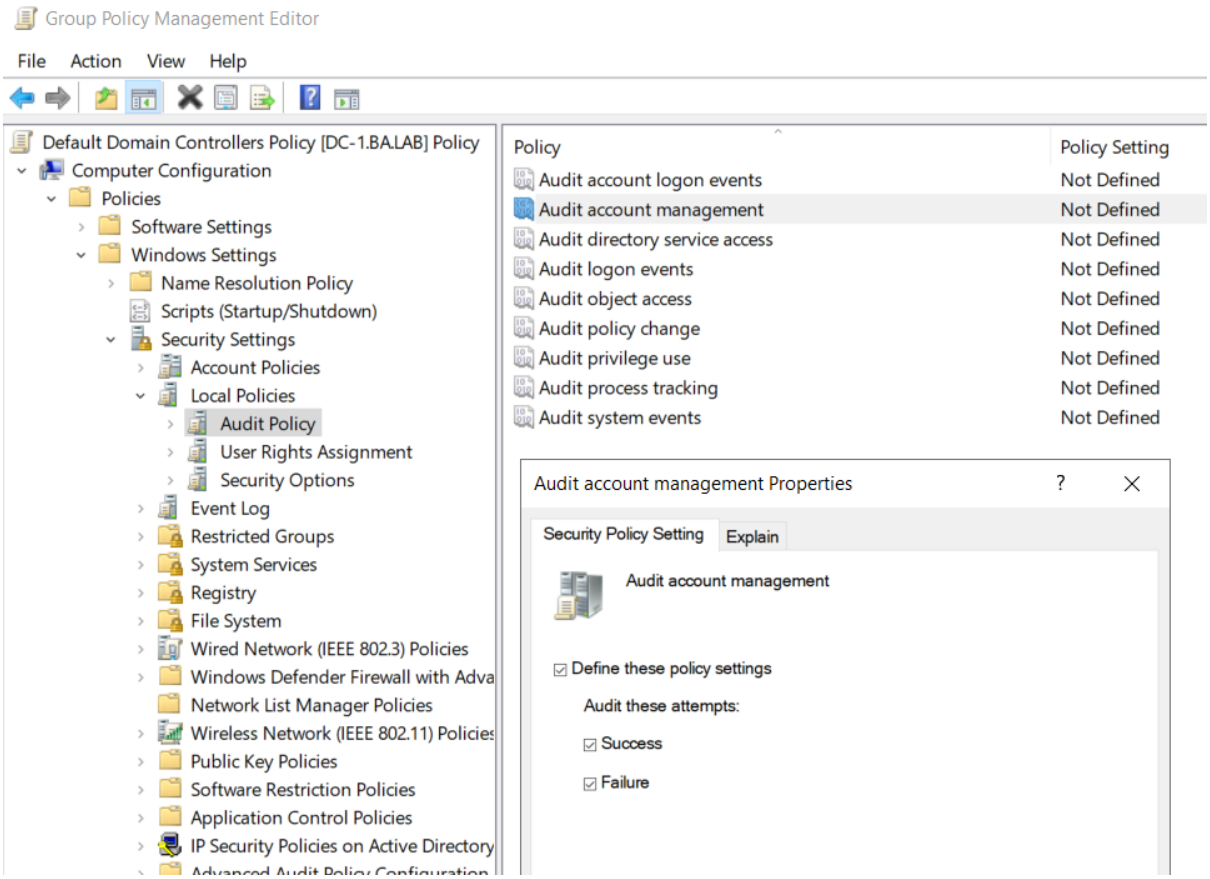


Abbildung 2.6: Active Directory Audit Policy

2.5 Intergration in Wazuh

2.5.1 Account Lockout

Wenn ein Benutzer sein Passwort zu oft falsch eingibt (wenn aktiviert in der Group Policy), generiert Wazuh ein Alert. Dieser sieht folgendermassen aus:

Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Apr 16, 2022 @ 16:42:38.597	003	DC-1	T1110 T1531	Credential Access, Impact	User account locked out (multiple login errors)	9	60115

Abbildung 2.7: Account Lockout Alert Beispiel

2.5.2 Änderungen in AD

Wazuh loggt standardmässig alle Änderungen in Active Directory. Dies beihnaltet Änderungen an Accounts und Gruppen:

```
Security Enabled (Local|Global|Universal) Group (Created|Changed|Deleted)
Security Enabled (Local|Global|Universal) Group Member (Added|Removed)
```

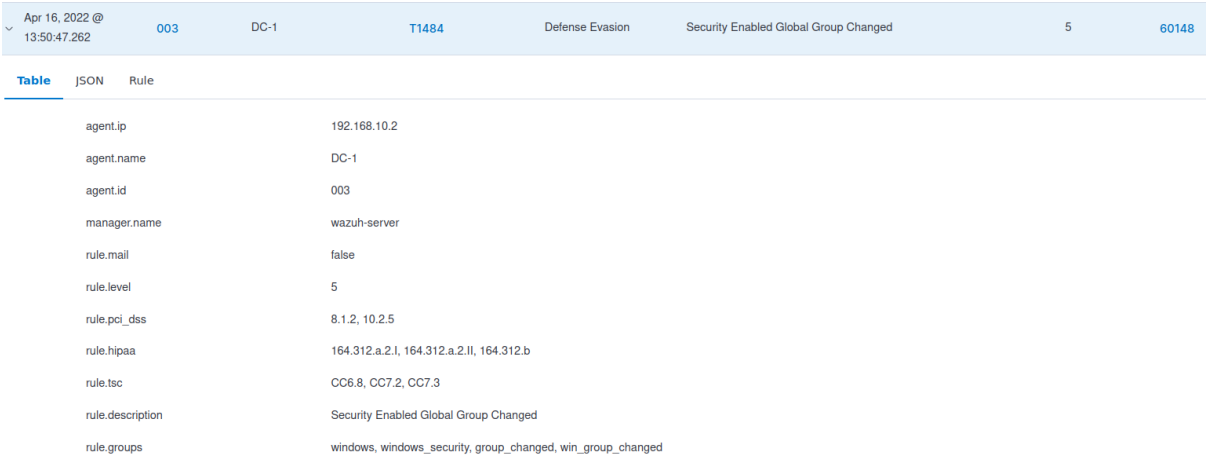


Abbildung 2.8: Security Group Alert Beispiel

Zusätzlich gibt es noch Alert mit Level 12, falls eine Standardgruppe mit erhöhten Berechtigungen geändert wird. Dazu gehören folgende Gruppen:

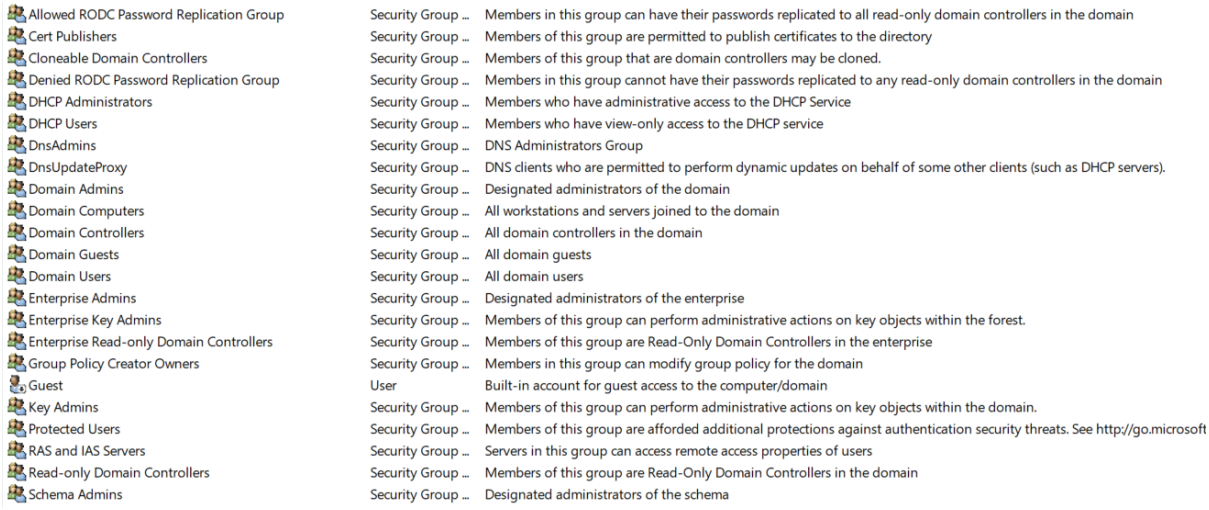


Abbildung 2.9: Gruppen mit erhöhten Berechtigungen

Die Alerts sehen wie folgt aus:

Abbildung 2.10: Security Group Level 12 Alert Beispiel

KAPITEL 3

Geräteverschlüsselung

3.1 Einleitung

Die Verschlüsselung der Daten auf Geräten ist Teil der physischen Sicherheit. Damit kann sichergestellt werden, dass keine Daten gestohlen werden können, wenn das Geräte verloren geht oder gestohlen wird. Diese Sicherheit ist besonders wichtig, wenn Notebooks in der Firma eingesetzt werden.

3.2 Verschlüsselung unter Windows

In Windows gibt es zwei im OS integrierte Möglichkeiten, die Daten auf dem Gerät zu verschlüsseln. In Windows Home gibt es die sogenannte "Geräteverschlüsselung" in den Systemeinstellungen. Ab Windows Pro kann man Geräte mit "BitLocker" verschlüsseln.

3.2.1 Windows Home Version

In der Windows 10 Home Version gibt es die "Geräteverschlüsselung". Da Windows 10 Home nicht für Unternehmen gedacht ist, gibt es auch keine Möglichkeit, die Geräteverschlüsselung zentral zu verwalten. Sie muss auf jedem Gerät einzeln aktiviert werden.
Die "Geräteverschlüsselung" findet man unter **Settings** → **Update & Security** → **Device encryption**

3.2.2 Windows Pro/Enterprise Version

Mit BitLocker kann man die Festplatten auf den Geräten schnell und einfach verschlüsseln. Der Recovery Key wird im Computer Objekt in Active Directory hinterlegt.

Voraussetzungen

Um BitLocker unter Windows zu verwenden, wird ein Trusted Platform Module (TPM) Chip benötigt. Falls das Gerät einen TPM Chip hat, ist dieser im Gerätemanager unter "Security Devices" ersichtlich:

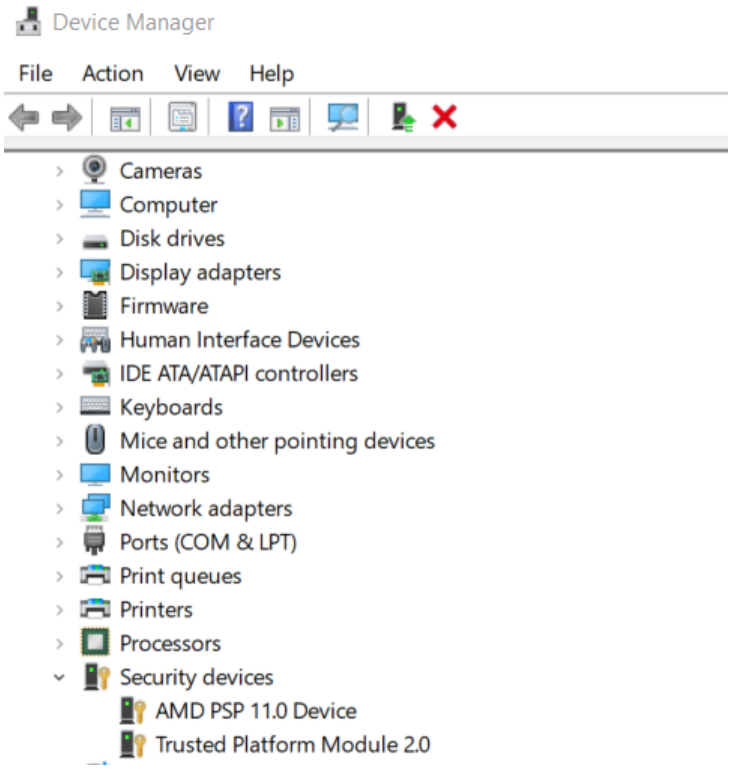


Abbildung 3.1: TPM Chip im Gerätemanager

Es gibt auch die Möglichkeit BitLocker ohne TPM Chip zu verwenden. Dann muss jedoch bei jedem aufstarten ein Passwort eingegeben werden.

BitLocker Feature

Damit der Recovery Key in Active Directory hinterlegt wird, muss zuerst das BitLocker Feature auf dem Domain Controller aktiviert werden. Dazu öffnet man den Server Manager, navigiert zu **Manage** → **Add Roles and Features**. Unter "Features" wählt man "Bitlocker Drive Encryption" und installiert dieses Feature:

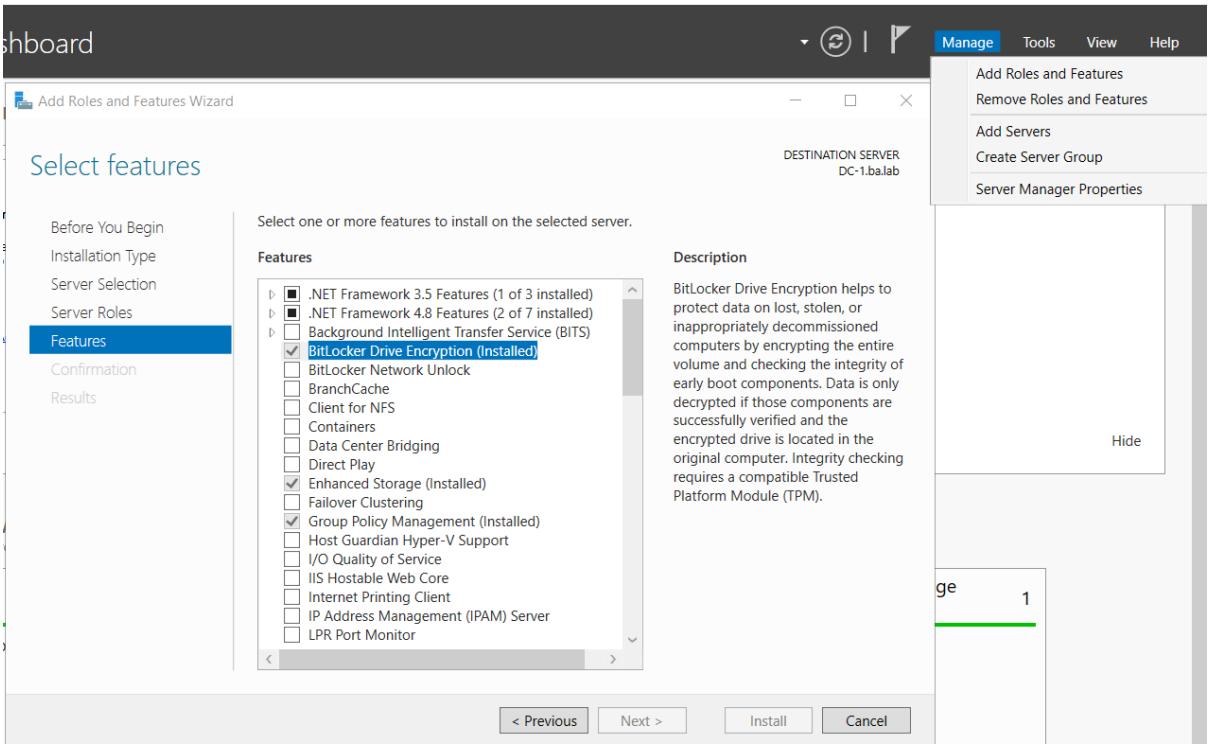


Abbildung 3.2: BitLocker Feature

Wichtig: Nach dem installiern muss der Server neugestartet werden.

Group Policy

Im Group Policy Management muss eine neue Group Policy erstellt werden, welche mit der OU verknüpft ist, die die zu verschlüsselnden Windows Geräte enthält. Mit **Rechtsklick** → **Edit** kann die neue Group Policy bearbeitet werden. Unter **Computer Configuration** → **Policies** → **Administrative Templates** → **Windows Components** → **BitLocker Drive Encryption** → **Operating System Drives** kann mit **Rechtsklick** → **New** → **Package...** wird die Policy "Choose how BitLocker-protected operating system drives can be recovered" wie folgt eingerichtet:

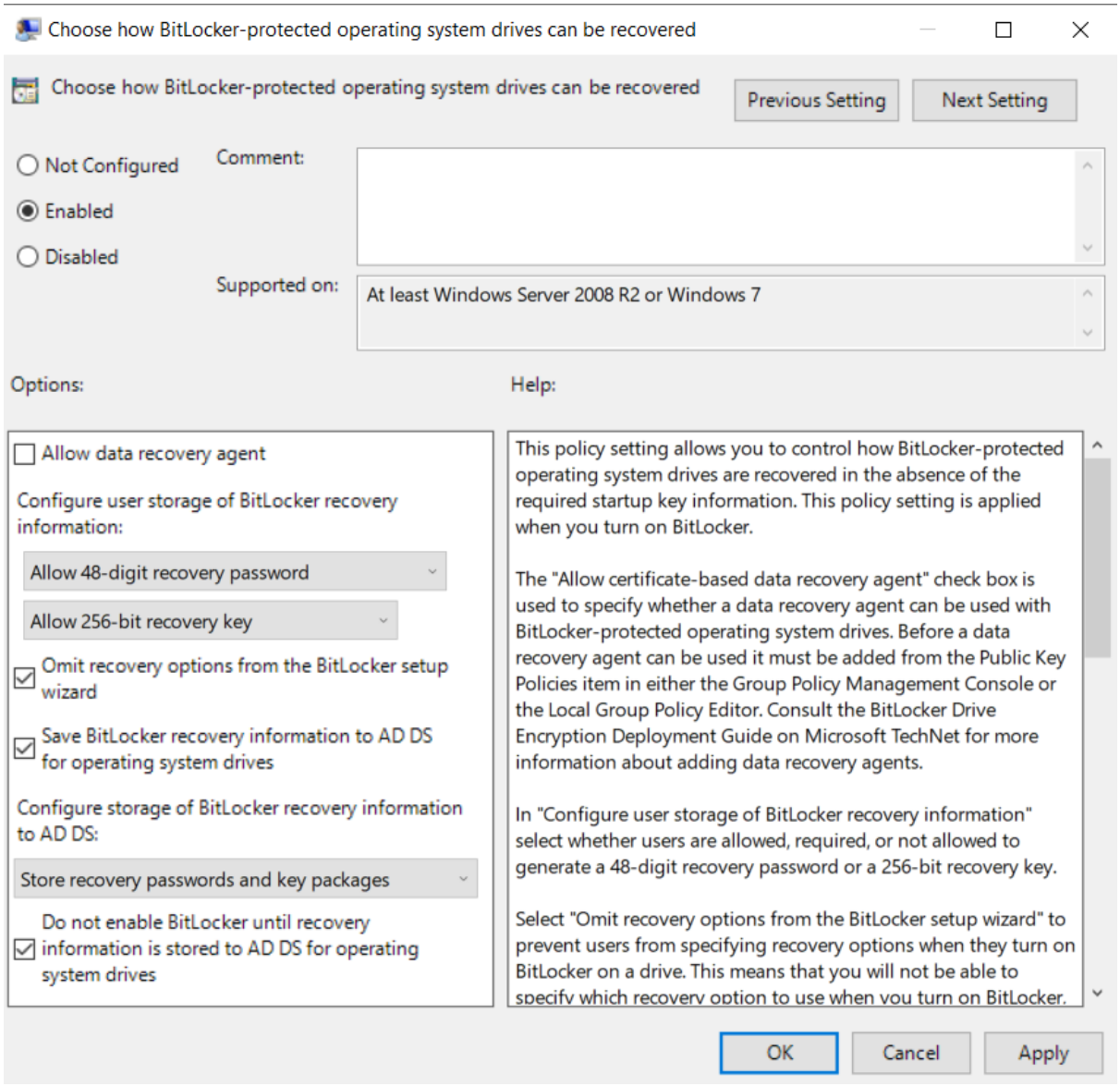


Abbildung 3.3: BitLocker Policy

Da Microsoft keinen zentralen Weg bietet, BitLocker auf den Geräten zu aktivieren, wird dies mit einem Script erledigt. Dazu speichert man folgenden Powershell Code als .ps1 Datei ab:

```
$BitLockerVolume = Get-BitLockerVolume -MountPoint 'c:'
if ($BitLockerVolume.VolumeStatus -eq 'FullyDecrypted') {
    Add-BitLockerKeyProtector -MountPoint 'c:' -RecoveryPasswordProtector
    Enable-Bitlocker -MountPoint 'c:' -TpmProtector
}
```

Das Script muss auf einem freigegebenen Netzlaufwerk abgespeichert werden, auf welches alle Geräte Lesezugriff haben. Zum Beispiel auf dem Domain Controller unter:

```
C:\Windows\SYSVOL\sysvol\<Domain>\scripts
```

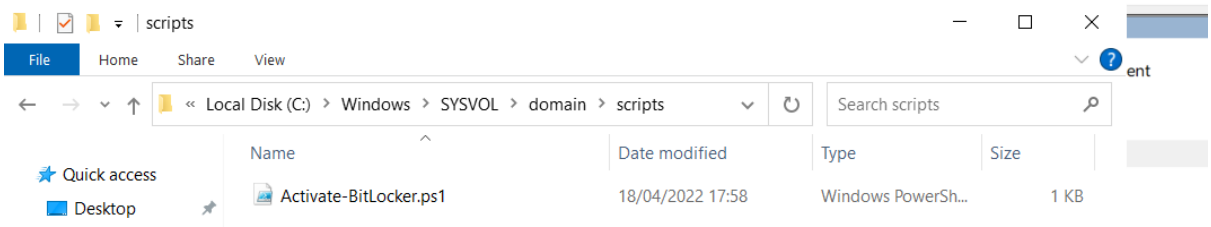


Abbildung 3.4: BitLocker Scripts

Da die Installation mit einem Script gemacht wird, muss zuerst noch erlaubt werden, dass in Powershell Skripte ausgeführt werden dürfen. Die Erlaubnis kann unter **Computer Configuration** → **Policies** → **Administrative Templates** → **Windows Components** → **Windows Powershell** mit der Policy "Turn on Script Execution" erteilt werden:

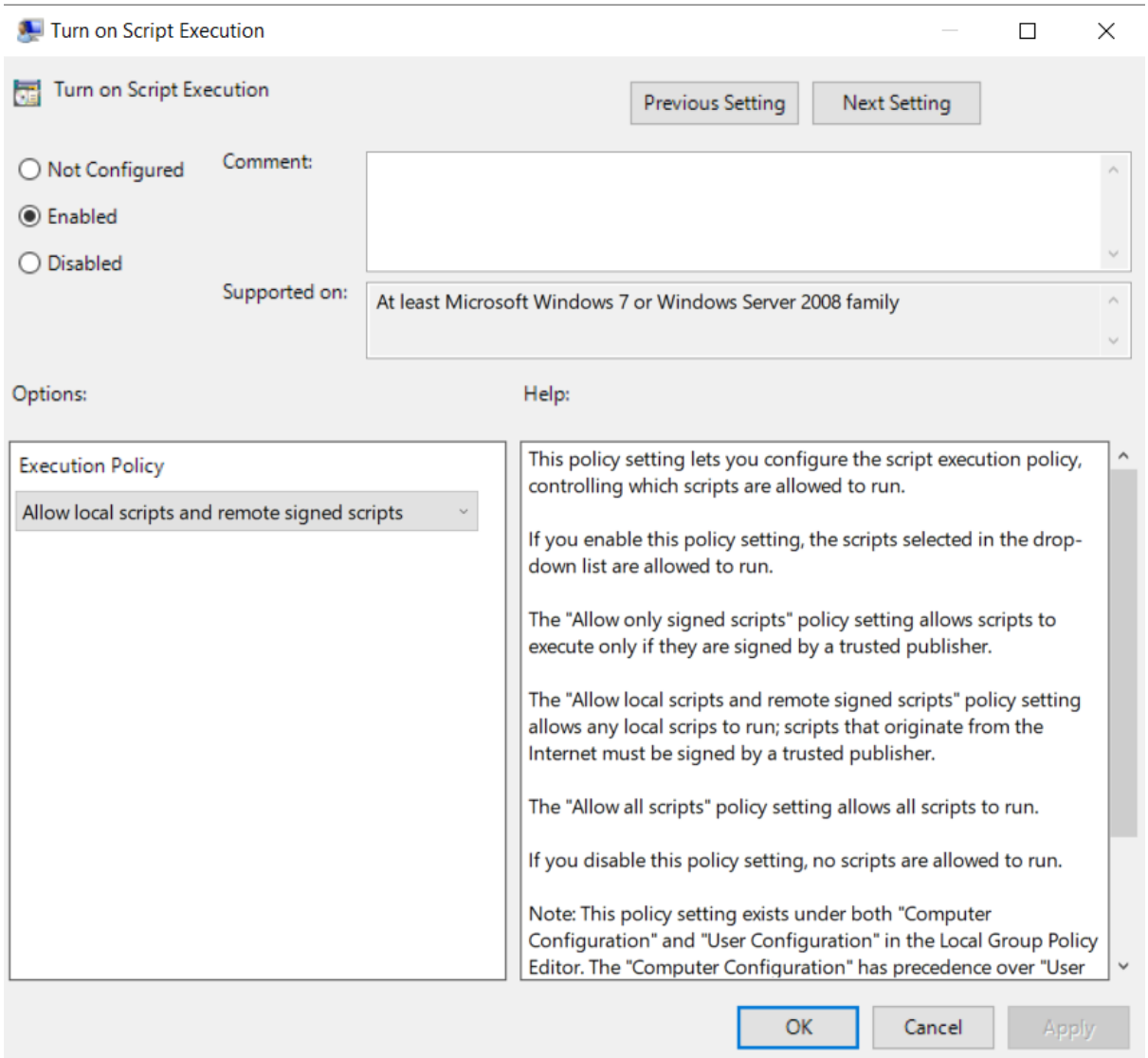


Abbildung 3.5: Powershell Scripts aktivieren

Als nächstes muss unter **Computer Configuration** → **Preferences** → **Control Panel Settings** → **Scheduled Task** ein neuer "Immediate Task (At least Windows 7)" erstellt werden:

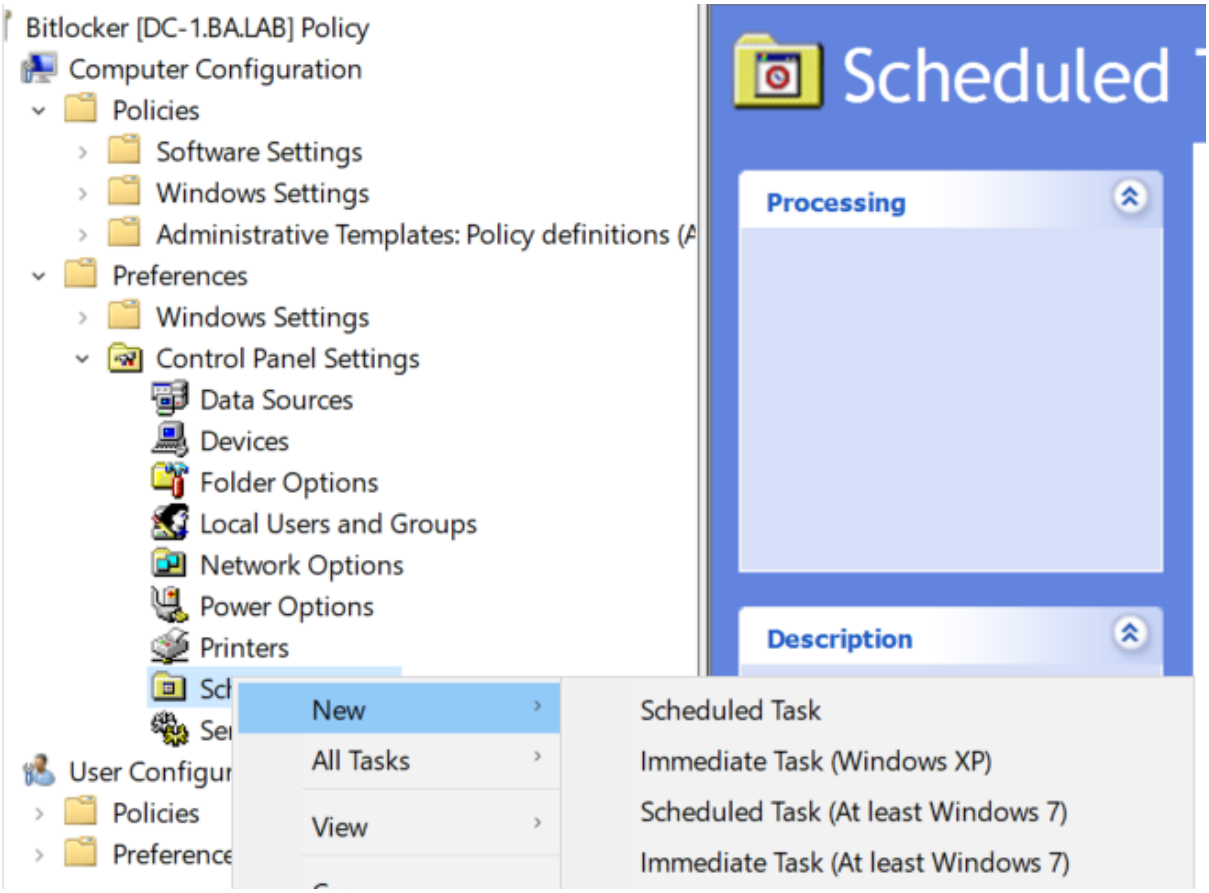


Abbildung 3.6: Neuer Scheduled Task für BitLocker

Beim Scheduled Task werden folgende Einstellungen getroffen:

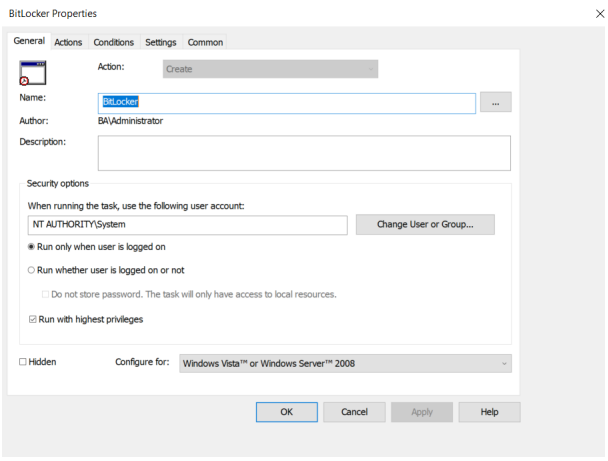


Abbildung 3.7: Scheduled Task Einstellungen 1

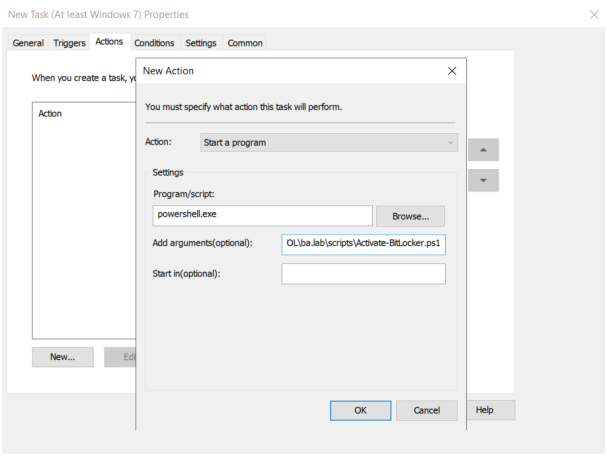


Abbildung 3.8: Scheduled Task Einstellungen 2

Bei "Add Arguments" in "New Action" wird der **freigegebene** Pfad vom .ps1 Script angegeben.
Zum Beispiel:

```
\\<Hostname DC>\SYSVOL\<Domäne>\scripts\Activate-BitLocker.ps1
```

Die Festplatte wird beim nächsten Neustart verschlüsselt. Es wird nur die Festplatte mit dem Betriebssystem verschlüsselt. Falls man weitere Festplatten verschlüsseln will, muss man den "MountPoint" Parameter im

Script anpassen.

BitLocker ohne TPM

BitLocker kann wie erwähnt auch ohne TPM Chip verwendet werden, dann muss jedoch ein Passwort gesetzt werden. Wenn BitLocker so verwendet werden möchte, muss man noch eine zusätzliche Policy für diese Geräte aktivieren. Die Policy befindet sich am gleichen Ort wie die vorherige Policy um BitLocker zu aktivieren und heisst "Require additional authentication at startup". Dort setzt man folgende Einstellungen:

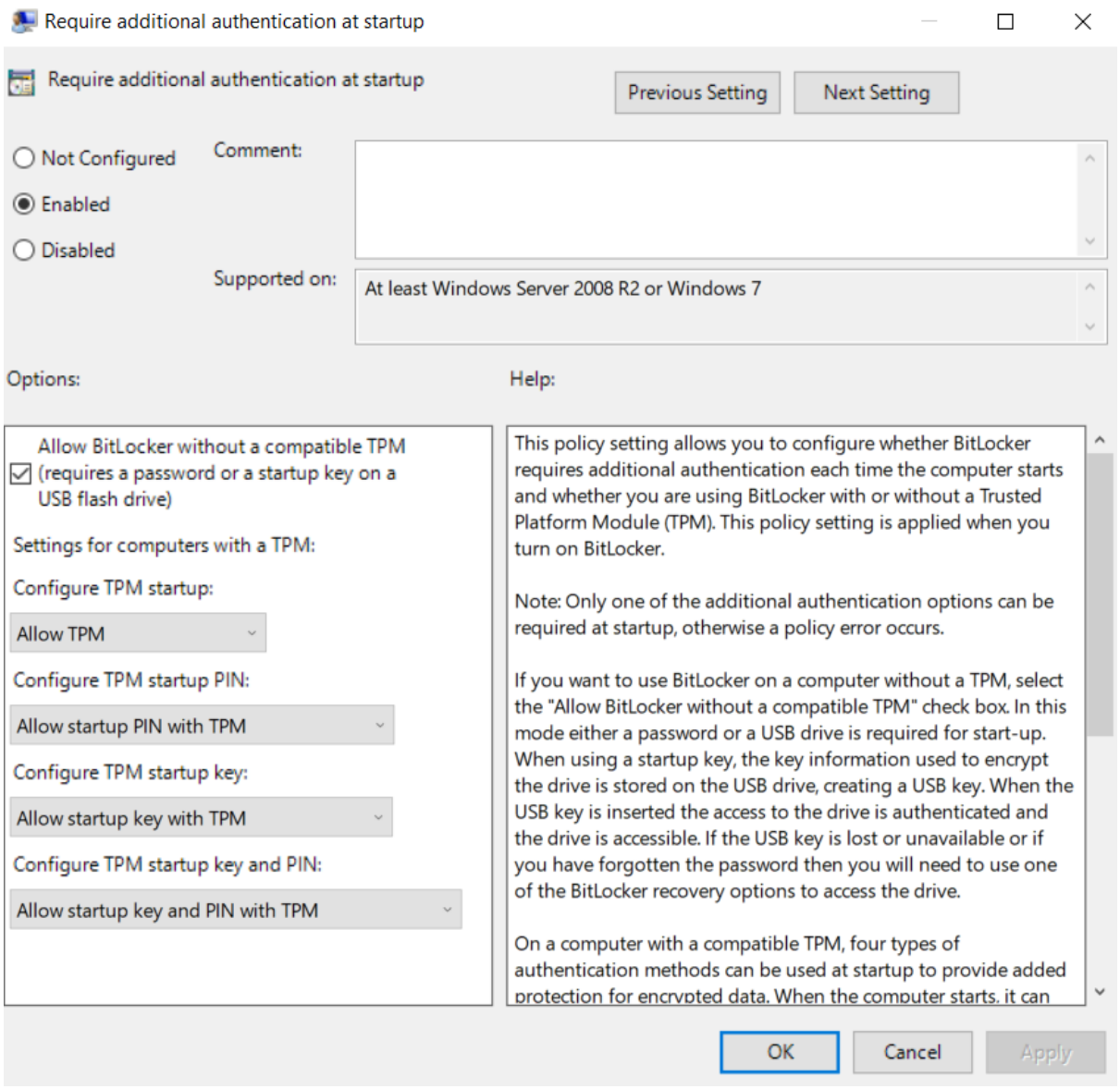


Abbildung 3.9: GPO für BitLocker ohne TPM

Zusätzlich kann nicht das Script verwendet werden, da vom Benutzer ein Passwort gesetzt werden muss. Daher ist es am einfachsten, BitLocker für diese Geräte manuell zu aktivieren. Dies geht auch mit Powershell ausgeführt als Administrator:

```
$Password = Read-Host -AsSecureString
Add-BitLockerKeyProtector -MountPoint 'c:' -RecoveryPasswordProtector
Enable-Bitlocker -MountPoint 'c:' -PasswordProtector -Password $Password
```

Die Festplatte wird beim nächsten Neustart verschlüsselt.

Recovery Key auslesen

Der Recovery Key ist auf den Computer Objekten in der Active Directory hinterlegt. Dazu öffnet man die Einstellungen eines Computer Objektes und öffnet den Tab "BitLocker Recovery":

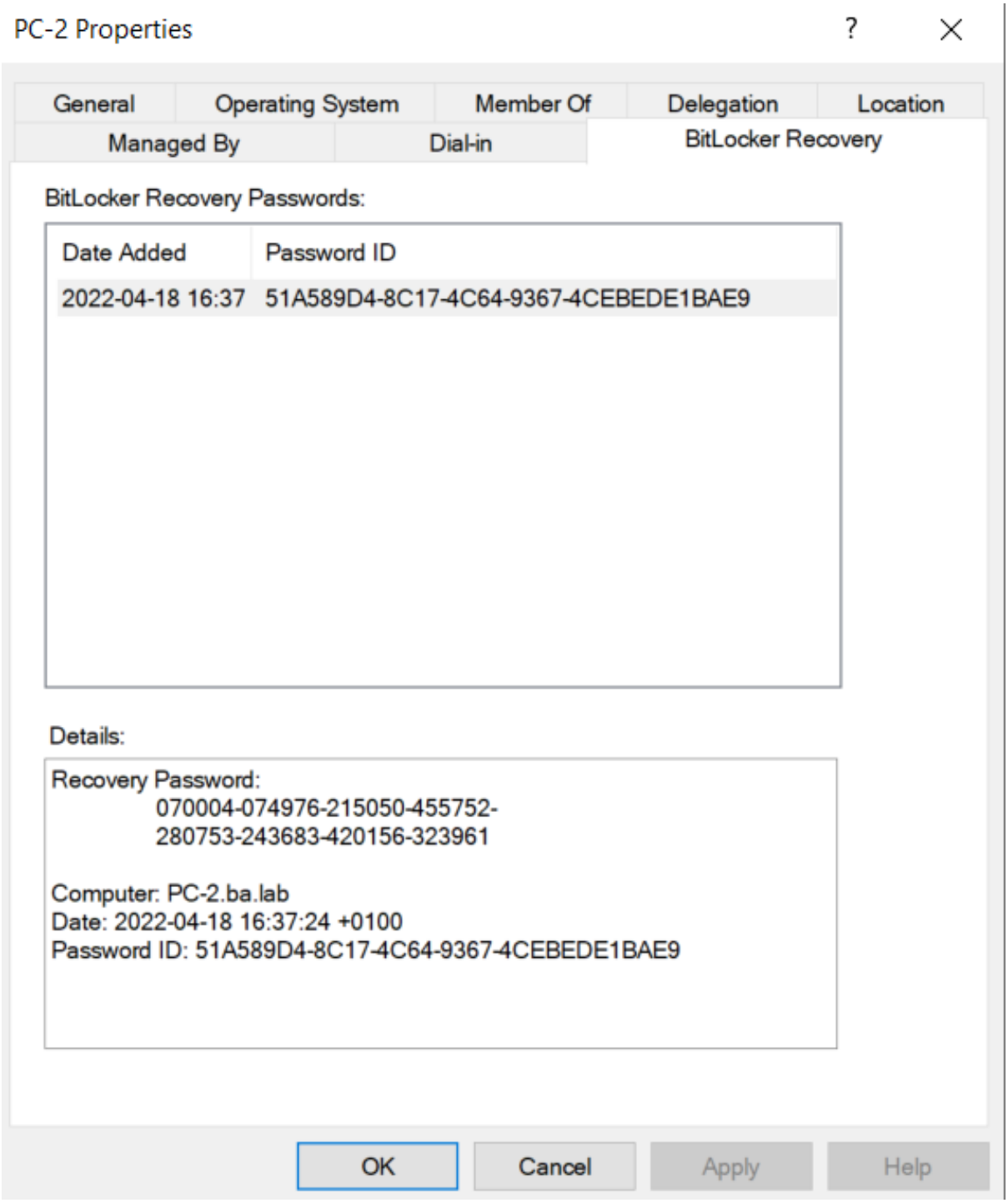


Abbildung 3.10: Recovery Key für BitLocker

Dort findet man unter "Recovery Password" das Passwort um den Computer im Notfall zu entschlüsseln.

KAPITEL 4

Antivirus

4.1 Allgemeines

Ein Antivirus (AV) ist der erste Verteidigungsmechanismus in einem Netzwerk. Angriffe, darunter Schadsoftware, kommen in den meisten Fällen über einen Endpoint (z.B. Notebook) in ein Firmennetzwerk.

Eine gegebene Struktur ist immer nur so stabil, wie sein schwächstes Glied. Dies gilt bei Häusern wie auch bei Computernetzwerken. Oftmals ist das schwächste Glied ein Client oder ein Server, da diese Geräte vielfach mit dem Internet kommunizieren. Dies macht genau diese Geräte besonders schützenswert.

Server und Clients werden mit einem Antivirus versucht zu schützen. Ein Antivirus hilft bekannte Schadsoftware zu detektieren und zu entfernen. Neue Schadsoftware wird versucht mit komplexen Algorithmen zu erkennen und deren Vorhaben zu blockieren. Schadsoftware kann sich sehr schnell vermehren und sich im ganzen Netzwerk ausbreiten. Das kann den Effekt haben, dass die ganze Unternehmung beeinträchtigt wird. Deshalb ist eines der wichtigesten Erkenntnisse, dass ein Antivirus auf **allen** Endpoints (Server und Client) benötigt wird.

4.2 Windows Defender

Antivirus (AV) Programme kommen in allen Arten und Formen. Es ist schwer den Überblick über die Landschaft der Antivirus Programme zu behalten.

Microsoft bietet für seine Produkte einen eigenen kostenfreien Antivirus an. Der Windows Defender ist nicht eine allround Lösung, wie andere AV Produkte, mit unzähligen Features. Er ist einer der besten kostenfreien Lösungen und ist für KMUs sehr geeignet, da dort meist keine massgeschneiderte Lösung gewünscht wird. Laut dem Gartner Magic Quadrant für Endpoint Protection[1] ist die Microsoft Lösung eine der Marktführer in diesem Bereich. Der Windows Defender erkennt die meisten Gefahren und löst die erkannten Probleme sehr kompetent.

[1] Link: https://www.microsoft.com/security/blog/2021/05/11/gartner-names-microsoft-a-leader-in-the-2021-endpoint-protection-platforms-magic-quadrant/

Hier eine Übersicht der Vor- und Nachteile:

Vorteile:
• kostenfrei
• Realtime Protection funktioniert zuverlässig
• in Windows integriert
• einfache Bedienung

Tabelle 4.1: Vorteile Windows Defender

Nachteile:
• beschränkte Konfigurationsmöglichkeiten
• Keine cloudbasiertes Dashboard/Management
• Machine Learning nicht vorhanden

Tabelle 4.2: Nachteile Windows Defender

4.2.1 Wazuh Integration

In Wazuh existieren Regeln, welche das Verhalten vom Windows Defender loggen. Dazu gehören auch alle durchgeführten Scans.

Die wichtigsten zwei Regeln sind folgende:

Real-time protection disabled

Wenn die Real-time Protection deaktiviert wird, kann möglicherweise bösartige Software ausgeführt werden. Daher wird in Wazuh ein Level 12 Alert erstellt:

Apr 23, 2022 @ 13:23:12.159	T1089	Defense Evasion	Windows Defender Real-time Protection was disabled.	12	255303

Abbildung 4.1: Real-time Protection wurde deaktiviert

Defender found a threat

Wenn schädliche Software auf einen Computer herunterdeladen wird, sollte Windows Defender diese erkennen. Somit wird folgender Alert generiert:

Apr 23, 2022 @ 13:36:01.614	Windows Defender: Antimalware platform detected potentially unwanted software ()	12	62123

Abbildung 4.2: Malware wurde entdeckt

Auf diesen Alert sollte normalerweise folgender Alert folgen:

Apr 23, 2022 @ 13:36:08.444	Windows Defender: Antimalware platform performed an action to protect you from potentially unwanted software ()	3	62124

Abbildung 4.3: Malware wurde entfernt

Dieser bestätigt, dass Windows Defender die schädliche Software entfernt hat.

KAPITEL 5

Local Administrator Password Solution (LAPS)

5.1 Einleitung

Die Local Administrator Password Solution (LAPS) ist eine Lösung von Microsoft. Mit LAPS werden die Passwörter der lokalen Administratoren, welche auf allen Windows Geräten vorhanden sind, zufällig und unterschiedlich voneinander gesetzt. Zusätzlich werden die Paswörter in einem gewissen Zeitraum automatisch neu gesetzt.

Dies verhindert, dass ein Angreiffer auf weitere Systeme vordringen kann, wenn ein lokales Administratorpasswort kompromittiert ist. Die Passwörter sind in einem Attribut auf dem Computer Objekt im Active Directory hinterlegt. Zugriff auf dieses Attribut haben nur berechtigte Benutzer.

5.1.1 Voraussetzungen

Um LAPS einsetzen zu können, wird eine Active Directory benötigt mit allen Windows Geräten als Computer Objekte.

5.2 Installation

Die Installation ist in drei Schritte unterteilt.

1. Als erstes wird LAPS via Group Policy auf allen Windows Geräten installiert.
2. Danach wird das Active Directory für LAPS vorbereitet. Das Active Directory braucht zwei zusätzliche Attribute auf den Computer Objekten um die Passwörter verwalten zu können.
   - **ms-Mcs-AdmPwd**: Speichert das Administrator Passwort in Klartext.
   - **ms-Mcs-AdmPwdExpirationTime**: Speichert den Zeitpunkt für den Passwortwechsel.
3. Zum Schluss wird LAPS per Group Policy aktiviert.

5.2.1 Installation via GPO

LAPS kann auf der Webseite von Microsoft[1] heruntergeladen werden. Die .msi Datei muss in einem freigegebenen Netzlaufwerk platziert werden, auf welches alle Windows Geräte Zugriff haben. Zum Beispiel auf dem Domain Controller unter:

[1] Link: https://www.microsoft.com/download/details.aspx?id=46899

```
C:\Windows\SYSVOL\sysvol\<Domain>
```

Dieses Verzeichnis ist Standardmässig auf Domain Controllern freigegeben.

Im Group Policy Management muss eine neue Group Policy erstellt werden, welche mit der OU verknüpft ist, die alle Windows Geräte enthält.

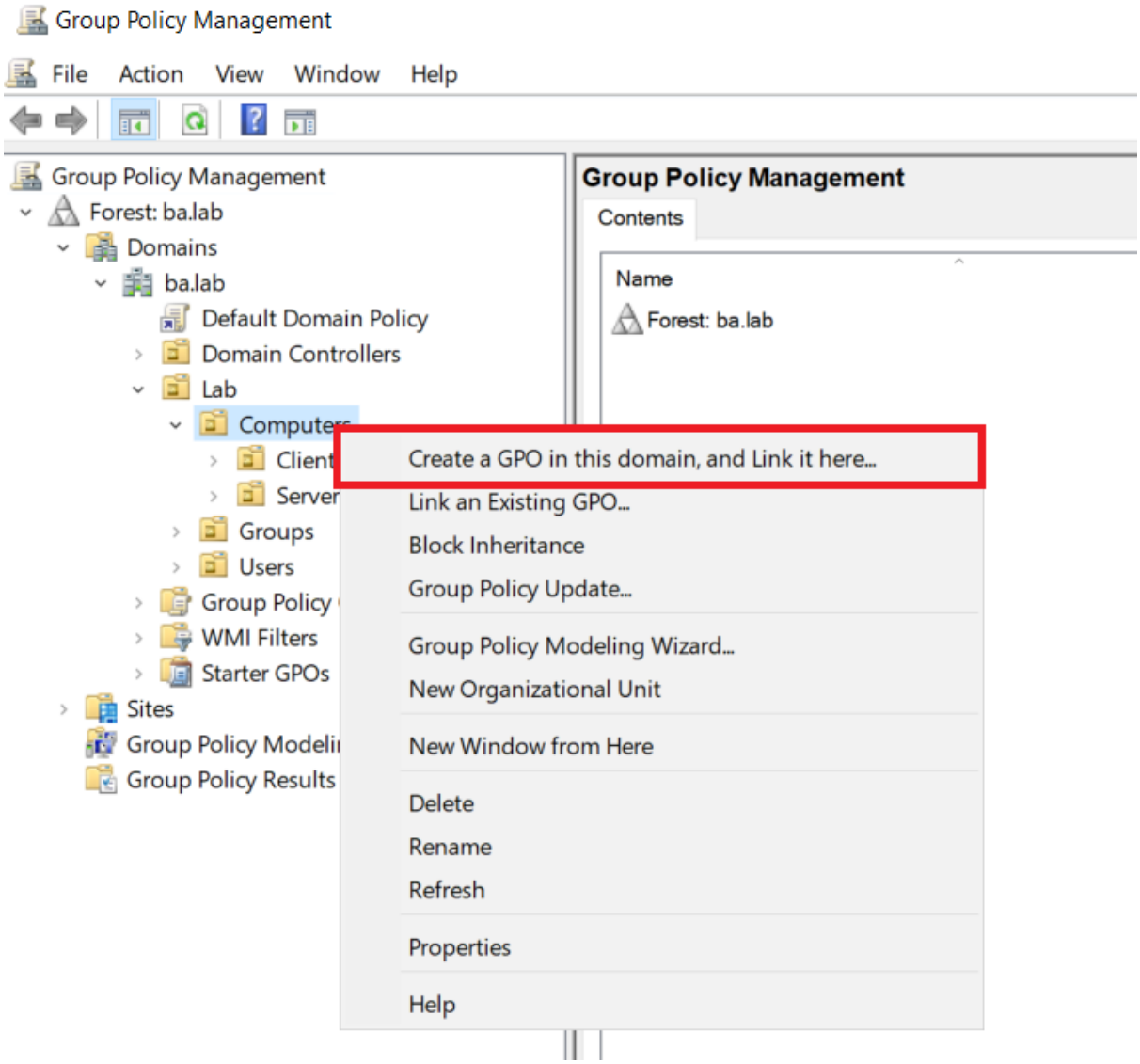


Abbildung 5.1: Neue GPO für LAPS Deployment

Mit **Rechtsklick** → **Edit** kann die neue Group Policy bearbeitet werden. Unter **Computer Configuration** → **Policies** → **Software Settings** → **Software installation** kann mit **Rechtsklick** → **New** → **Package...** eine Datei ausgewählt werden, welche installiert werden soll. Hier muss man die zuvor im freigegebenen Netzlaufwerk abgelegte Installationsdatei auswählen.

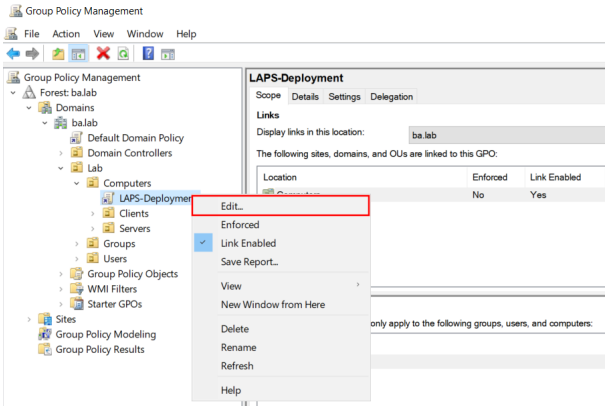


Abbildung 5.2: GPO für LAPS Deployment bearbeiten

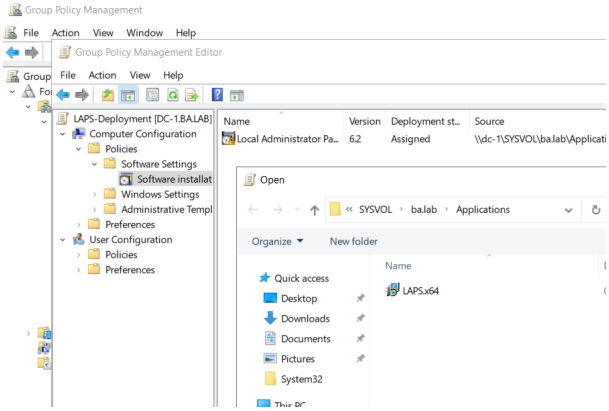


Abbildung 5.3: LAPS Installationsdatei auswählen

Die Group Policy kann nun geschlossen werden. LAPS wird beim Einloggen auf den jeweiligen Geräten installiert.

Domain Controller

Auf dem Domain Controller sollte man LAPS manuell installieren. Bei der manuellen Installation müssen die zusätzlichen Features installiert werden. Diese sind das GUI, das Powershell Modul und die GPO Richtlinien. Dazu die Installationsdatei ausführen und alle Features installieren.

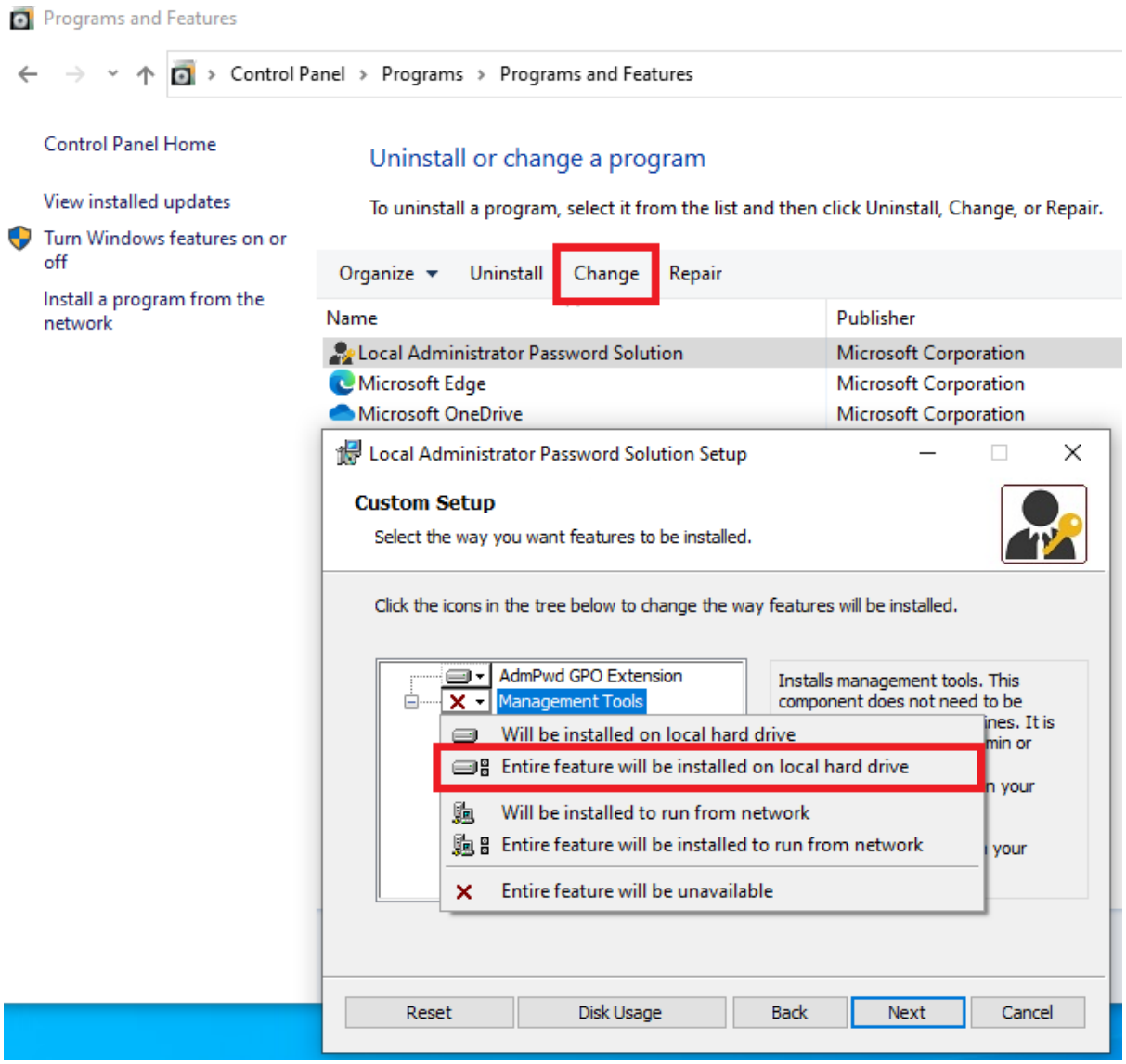


Abbildung 5.4: LAPS manuelle Installation

LAPS GUI für Admins

Über die GPO wird auf den Computern LAPS ohne GUI installiert. Mit dem GUI kann das Passwort von beliebigen Windows Geräten in der Domäne abgefragt werden.

Das GUI kann über die Systemeinstellungen installiert werden, wenn LAPS bereits installiert ist. Die Installationsdatei wird dafür nicht benötigt. In der Programmliste in den Systemeinstellungen auf LAPS klicken und im Balken auf **Change** klicken.

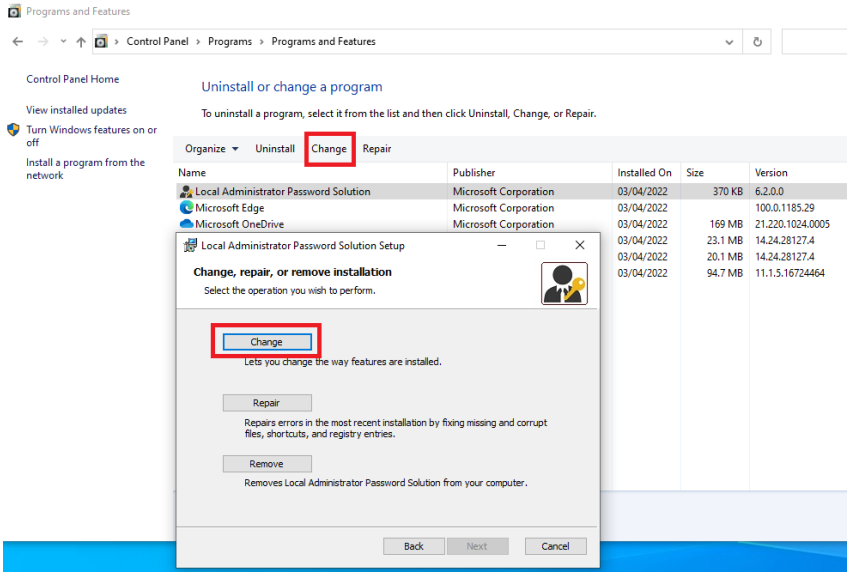


Abbildung 5.5: LAPS GUI Installieren 1

Das **Management Tools** Feature auswählen und dem Installationsprozess folgen.

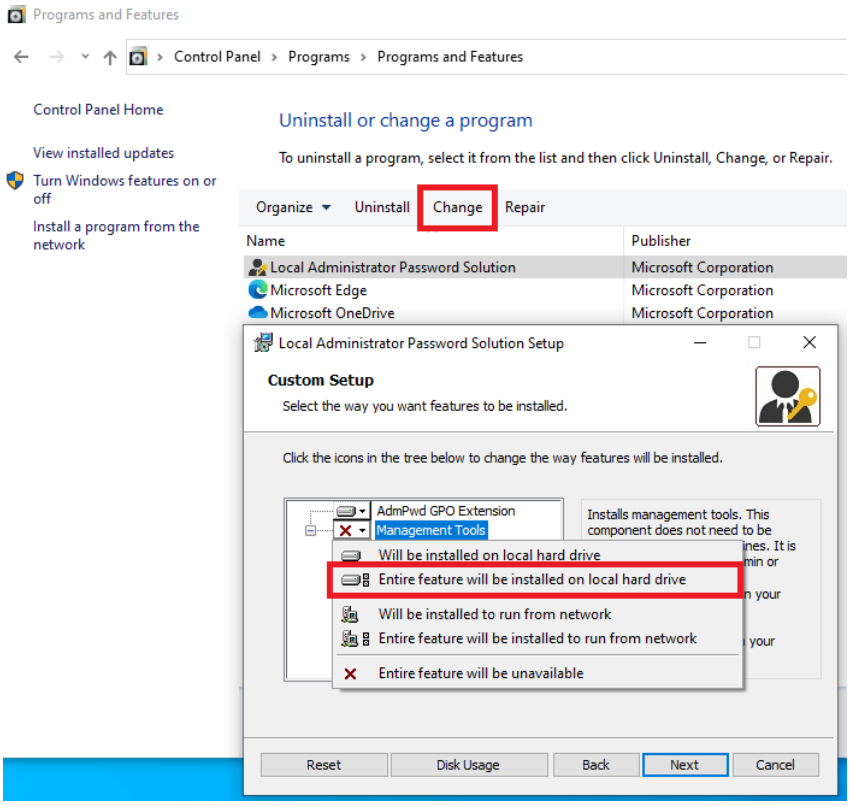


Abbildung 5.6: LAPS GUI Installieren 2

5.2.2 Active Directory vorbereiten

Die zusätzlichen Extension Attributes können per Powershell hinzugefügt werden. Der ausführende Domänenbenutzer muss ein "Schema Admin" in Active Directory sein.

Abbildung 5.7: Schema Admins Gruppe

Powershell mit dem Schema Admin Benutzer starten und folgendes Eingeben

```
Import-module AdmPwd.PS
Update-AdmPwdADSchema

#Resultat:
#Operation            DistinguishedName                                          Status
#---------            -----------------                                          ------
#AddSchemaAttribute   cn=ms-Mcs-AdmPwdExpirationTime,CN=Schema,CN=Configuration,DC=b Success
#AddSchemaAttribute   cn=ms-Mcs-AdmPwd,CN=Schema,CN=Configuration,DC=ba,DC=lab       Success
#ModifySchemaClass    cn=computer,CN=Schema,CN=Configuration,DC=ba,DC=lab           Success

Set-AdmPwdComputerSelfPermission -OrgUnit "<Name der OU>"
#Resultat:
#Name                 DistinguishedName                                          Status
#----                 -----------------                                          ------
#Clients              OU=Clients,OU=Computers,OU=Lab,DC=ba,DC=lab                Delegated
```

Nun muss noch eine Active Directory Gruppe erstellt werden. Dieser Gruppe kann man alle Benutzer hinzufügen, welche Zugriff auf die Passwörter bekommen sollen.

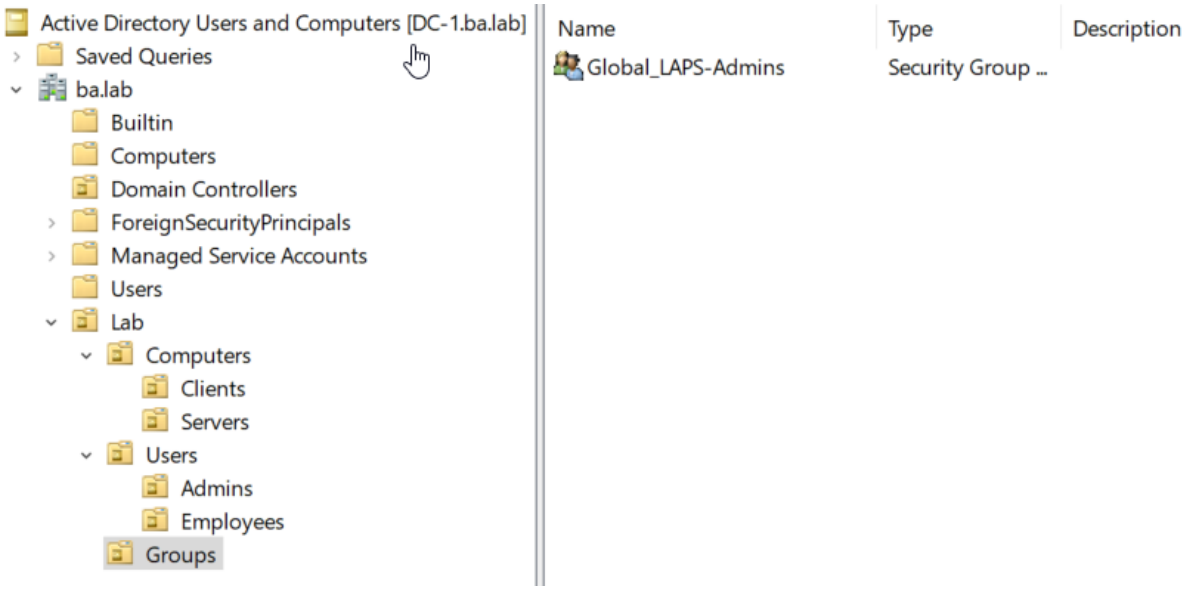


Abbildung 5.8: LAPS Active Directory Gruppe

Nach dem Erstellen der Gruppe, muss zusätzlich noch eine Berechtigung auf der OU für die Gruppe eingerichtet werden. Dazu muss ASEdit und die Eigenschaften der OU geöffnet werden. Im "Security" Tab

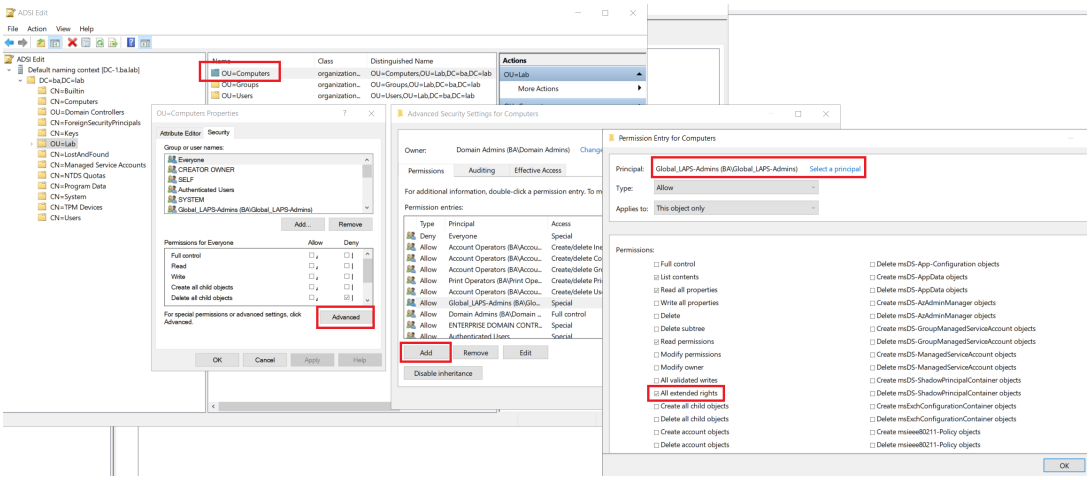


Abbildung 5.9: ASEdit

unter "Advanced" muss die neue Gruppe hinzugefügt werden mit der Berechtigung "All Extended Rights".

Nun muss für LAPS noch die Verknüpfung zwischen dieser Gruppe und der OU erstellt werden. Dies kann mit Powershell erledigt werden:

```
Set-AdmPwdReadPasswordPermission -OrgUnit "<Name der OU>" -AllowedPrincipals Global_LAPS-Admins
Set-AdmPwdResetPasswordPermission -OrgUnit "<Name der OU>" -AllowedPrincipals Global_LAPS-Admins
```

Die Read Berechtigung erlaubt das Lesen der Passwörter. Die Reset Berechtigung erlaubt das setzen eines Ablaufdatums eines Passwortes. Die Berechtigung kann nun noch mii Powershell überprüft werden:

```
Find-AdmPwdExtendedrights -identity "<Name der OU>"
```

5.2.3 LAPS aktivieren

Zum Schluss muss LAPS noch mit einer neuen Group Policy aktiviert werden.
Im Group Policy Management muss eine neue Group Policy erstellt werden, welche mit der gleichen OU verknüpft ist, wie die Group Policy für das Deployment.

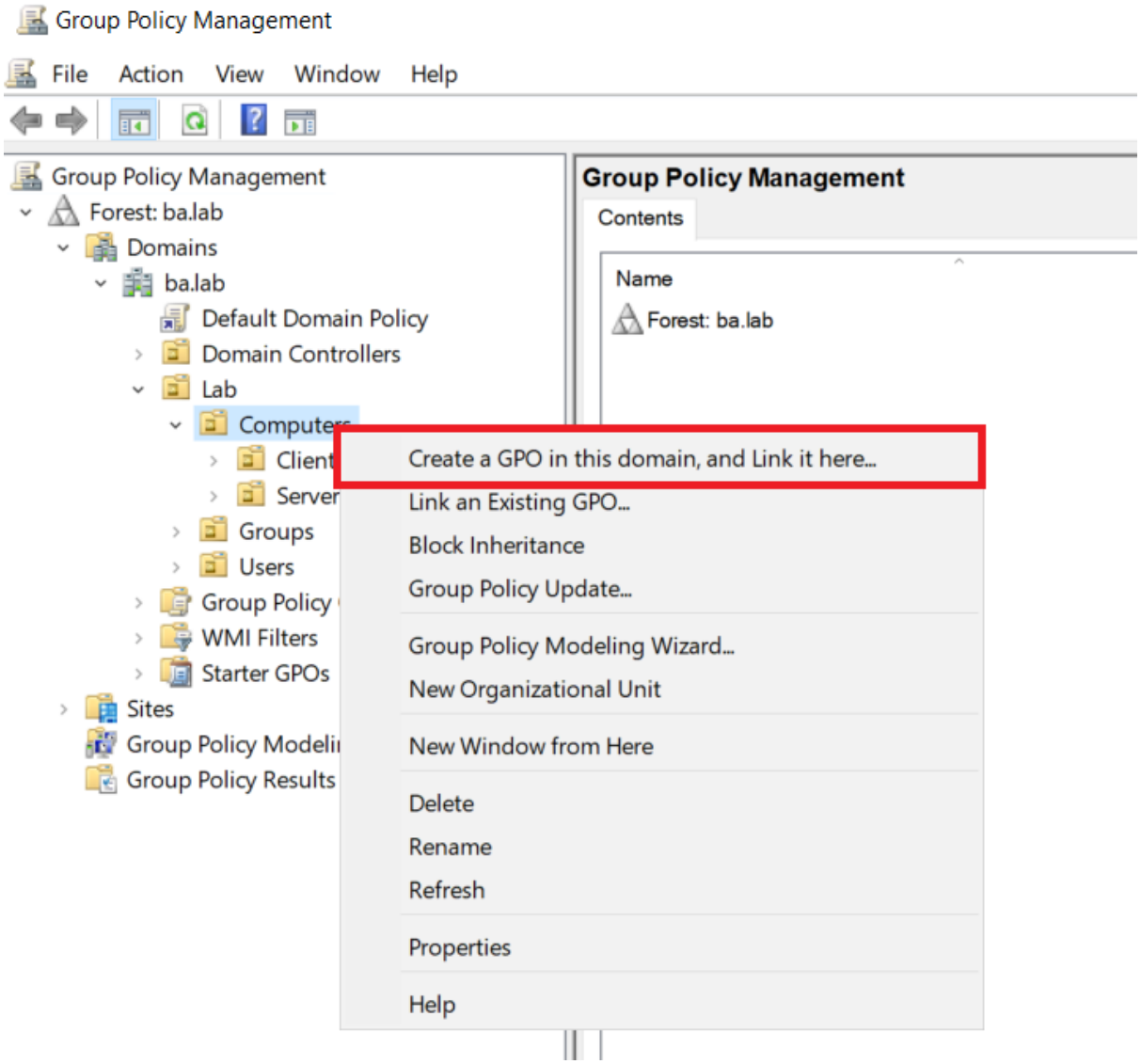


Abbildung 5.10: Neue Group Policy für LAPS Deployment

Mit **Rechtsklick** → **Edit** kann die neue Group Policy bearbeitet werden. Unter **Computer Configuration** → **Policies** → **Administrative Templates** → **Laps** findet man die Einstellungen von LAPS. Mit **Rechtsklick** → **Edit** auf "Enable local admin password management" kann man die Einstellung öffnen und links auf "Enabled" setzen. Mit OK bestätigen.

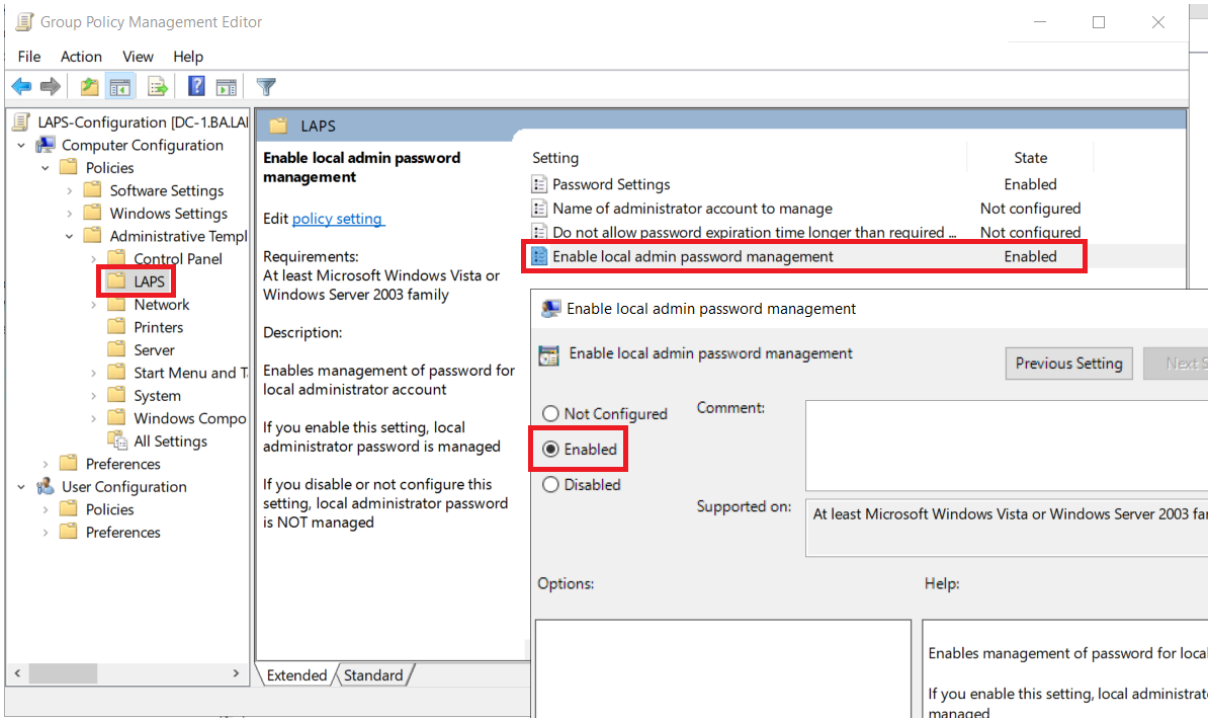


Abbildung 5.11: LAPS aktivieren

In der Einstellung "Password Settings" kann man die Passwort Länge und den Zyklus setzen, wie oft das Passwort gewechselt werden soll.

Zusätzlich muss noch der lokale Administrator aktiviert werden. Dieser ist standardmässig bei Computern welche der Active Directory beigetreten sind deaktiviert. Unter **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Local Policies** → **Security Options** findet man die Einstellungen "Accounts: Administrator Account Settings". Diese setzt man auf "Enabled". Die Group Policy kann nun geschlossen werden.

5.3 Verwendung

5.3.1 Mit dem GUI

Das Auslesen eines Passwortes über das GUI geht nur, wenn das GUI auch installiert wurde. Die Installation des GUI wird im Kapitel LAPS GUI für Admins erklärt.

Im Startmenü muss man nach **LAPS UI** suchen. Falls der in Windows angemeldete Benutzer Berechtigung besitzt, LAPS Passwörter auszulesen, kann LAPS direkt gestartet werden.
Falls nicht, muss man den Speicherort der Datei öffnen. Dann kann man mit **Shift** + **Rechtsklick** das Kontextmenü öffnen und die Datei mit "Run as different user" als anderen Benutzer ausführen. Ein Eingabefenster öffnet sich, wo man den berechtigten Benutzer und das Passwort des Benutzer eingeben kann. Berechtigt sind alle Benutzer in der zuvor erstellten Gruppe und Domänen Administratoren.

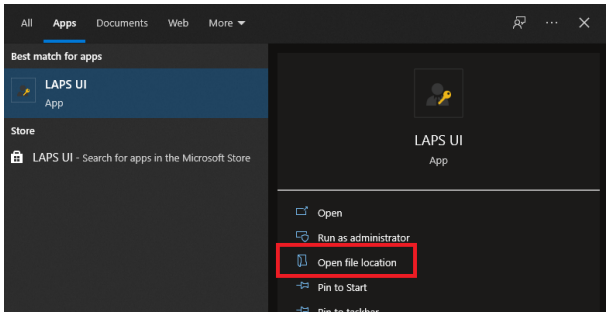


Abbildung 5.12: LAPS Speicherort öffnen

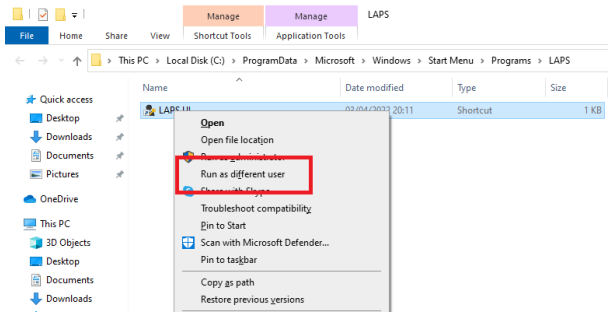


Abbildung 5.13: LAPS als anderer Benutzer starten

Im LAPS UI gibt man im Feld "Computer name" den Namen des Computers ein, von welchem man das lokale Passwort möchte. Das Passwort wird dann im Feld "Password" angezeigt.

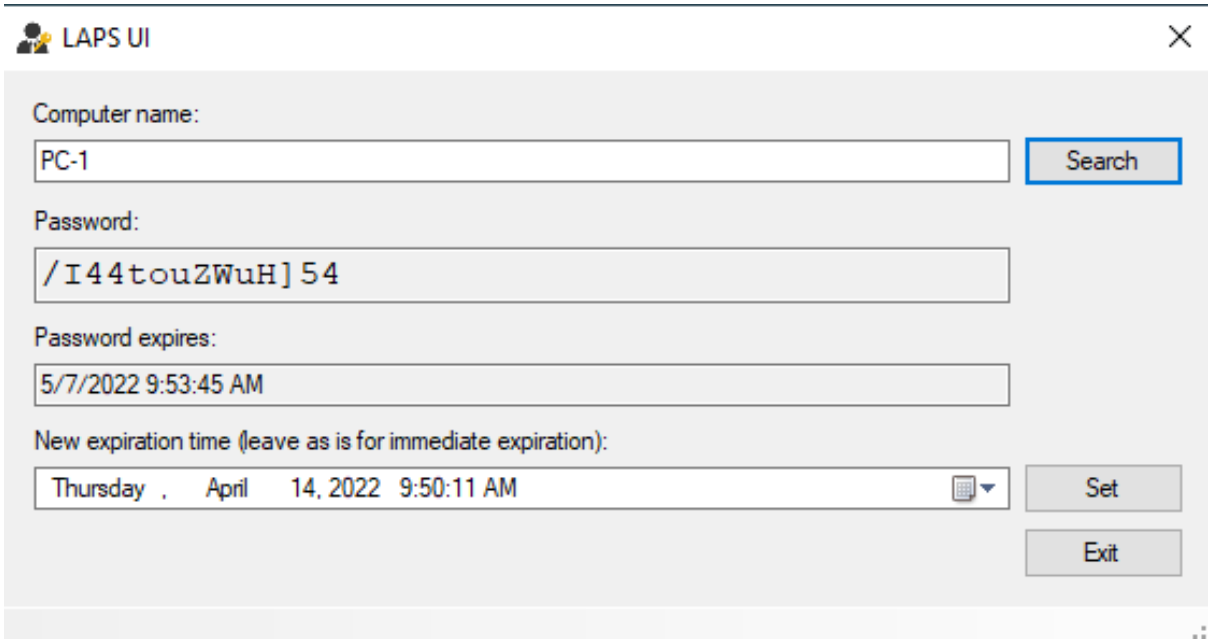


Abbildung 5.14: LAPS Passwort auslesen

Im Feld "New expiration time" kann man eine neue Zeit setzen, wann das Passwort gewechselt werden soll.

5.3.2 Mit Powershell

Die Powershell muss als Benutzer gestartet werden, welcher die Berechtigung hat das Passwort auszulesen oder zurückzusetzen. Powershell als ein anderer Benutzer starten kann man gleich wie LAPS im Kapitel "Mit dem GUI" als anderer Benutzer gestartet wurde.

Für das Auslesen und Zurücksetzen gibt es folgende Befehle:

```
Get-AdmPwdPassword -ComputerName <Computer Name>
Reset-AdmPwdPassword -ComputerName <Computer Name>
```

5.4 Best Practices

Idealerweise sollten nur ausgewählte IT Mitarbeitende die Berechtigung erhalten, Passwörter auslesen zu können. Alle lokalen Administratorrechte von AD Benutzern sollten entfernt werden und nur noch LAPS Passwörter verwendet werden. Dadurch kann man verhindern, dass es einen Benutzer gibt, welcher auf allen Systemen berechtigt ist.

Falls ein Mitarbeitender ohne LAPS Berechtigung lokale Administratorrechte braucht, kann diesem das LAPS Paswort gegeben werden. Dann sollte man aber auch das "Expire Date" auf das Datum setzen, wo das Passwort nicht mehr gebraucht wird. Zum Beispeil am nächsten Tag.

5.5 Intergration in Wazuh

In Wazuh existiert eine Regel, welche jedes auslesen meldet. Die Regel hat die ID 110010 und der Agent Name ist der **Domain Controller**. Es ist nicht der Computer, auf welchem das Passwort ausgelesen wurde.

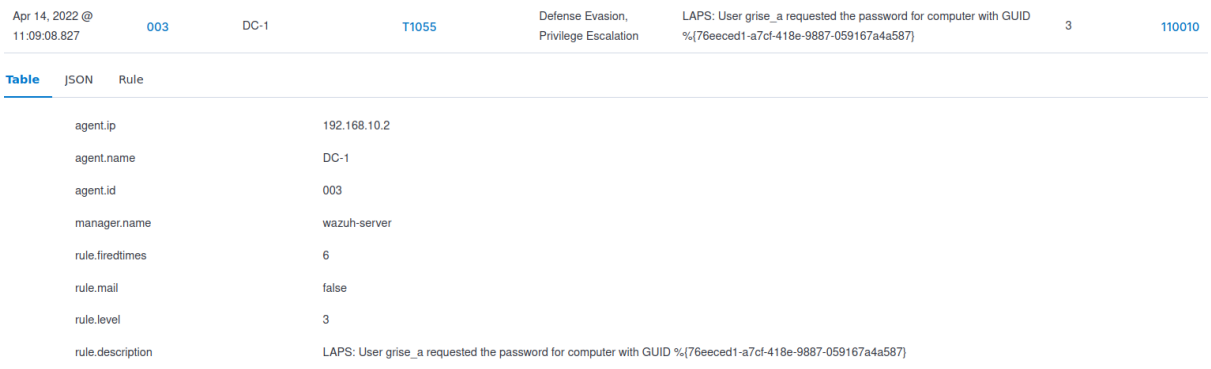


Abbildung 5.15: LAPS Wazuh Alert

Somit weiss man wer für welchen Computer das Passwort ausgelesen hat. Man kann jedoch nicht feststellen, von welchem Computer aus das Passwort ausgelesen wurde.

Zusätzlich wird nur die GUID des Computers angezeigt, für welchen man das Passwort ausgelesen hat. Um den Computernamen zu finden, kann man folgenden Powershell Befehl verwenden:

```
#GUID mit { } eingeben!
Get-ADObject -Identity "<GUID>"
```

Zusätzlich gibt es noch eine Regel, welche einen Alert generiert, sobald 20 LAPS Passwörter in 10 Minuten ausgelesen wurden.

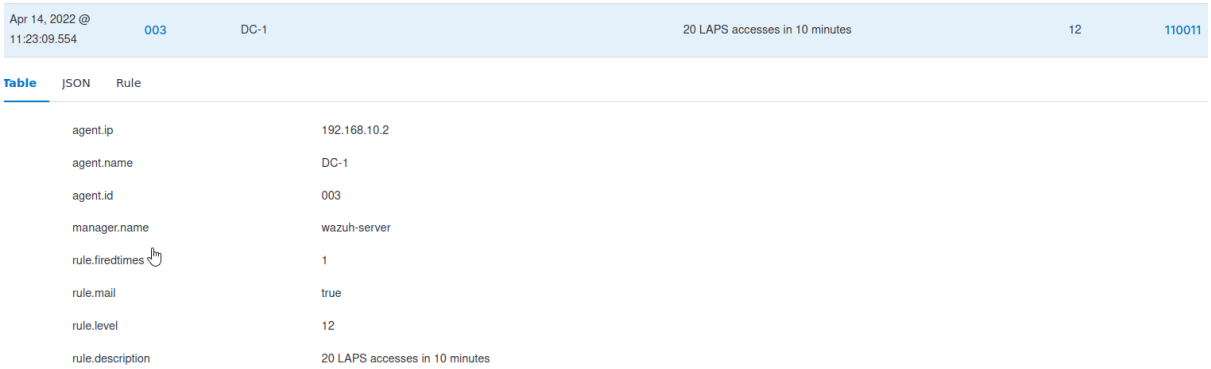


Abbildung 5.16: LAPS Wazuh Alert 2

KAPITEL 6

Updates

6.1 Einleitung

Updates gehören zu den effektivsten Möglichkeiten, sich gegen Angreifer zu schützen. Für Angreifer ist es ein goldenes Los, Software zu entdecken, welche nicht aktualisiert wurde und tendenziell sogar ein Common Vulnerabilities and Exposures (CVE)[1] dazu existiert.

Daher ist es wichtig, möglichst zeitnah aktuelle Updates zu installieren. Viele Softwarehersteller bieten eine automatische Updatefunktion, welche die neusten Updates direkt installiert.

6.2 Windows Updates

Windows Updates können direkt in den Systemeinstellungen heruntergeladen und installiert werden. Dies muss jedoch standardmässig von den Benutzern gemacht werden. Diese Updates können über die Group Policy erzwungen werden, damit sichergestellt werden kann, dass die System immer auf aktuellen Stand sind.

Wichtige Anmerkung:
Bei unternehmenskritischen Systemen muss immer zuerst überprüft werden, ob alle Funktionen nach dem Update noch funktionieren.

6.2.1 GPO für Clients

Falls unternehmenskritische Clients vorhanden sind, sollte Windows Server Update Services (WSUS) verwendet werden. Siehe Kapitel WSUS.

Im Group Policy Management muss eine neue Group Policy erstellt werden, welche mit der OU verknüpft ist, die alle Windows Geräte enthält.

[1] Link: https://www.cve.org/

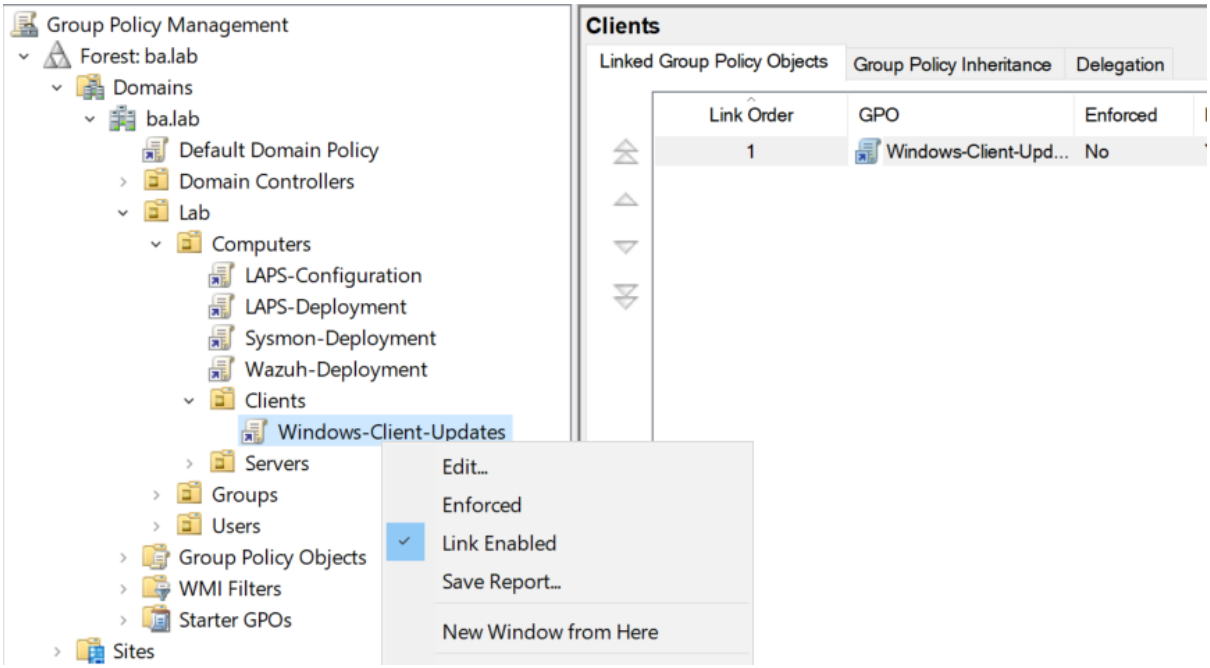


Abbildung 6.1: Neue GPO für Windows Client Updates

Mit **Rechtsklick** → **Edit** kann die neue Group Policy bearbeitet werden. Unter **Computer Configuration** → **Policies** → **Administrative Templates** → **Windows Components** → **Windows Update** findet man alle Policies bezüglich Windows Updates. Für Clients werden folgende Policies eingerichtet:

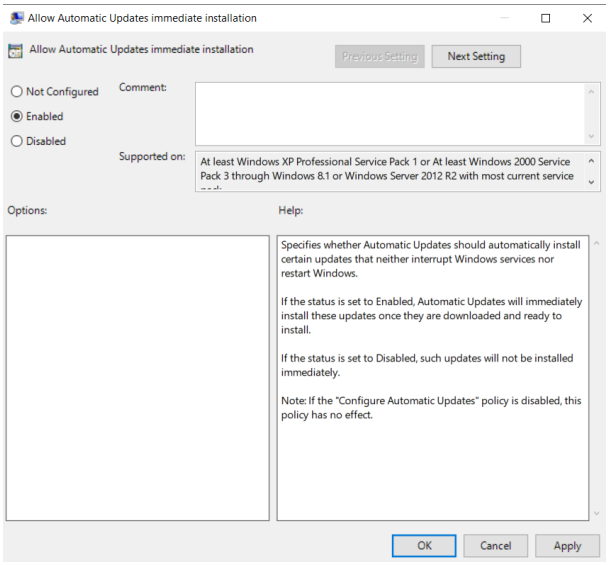


Abbildung 6.2: GPO Client Updates 1

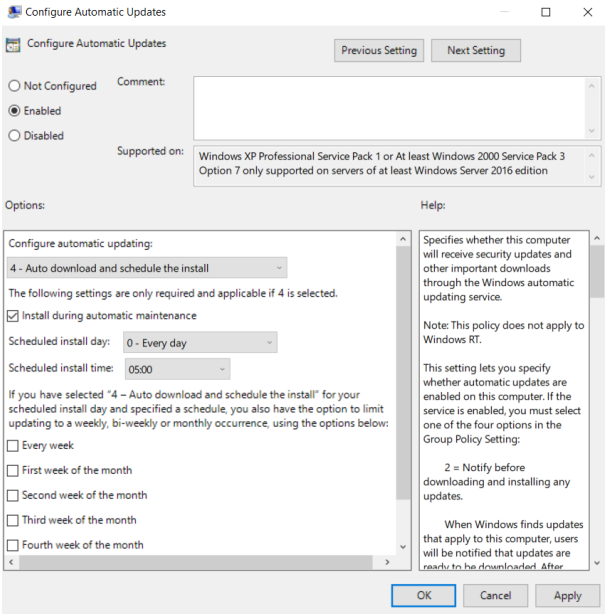


Abbildung 6.3: GPO Client Updates 2

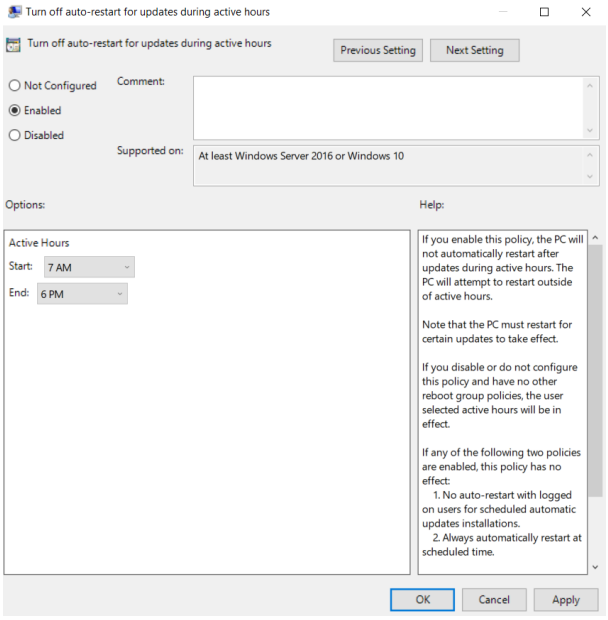


Abbildung 6.4: GPO Client Updates 3

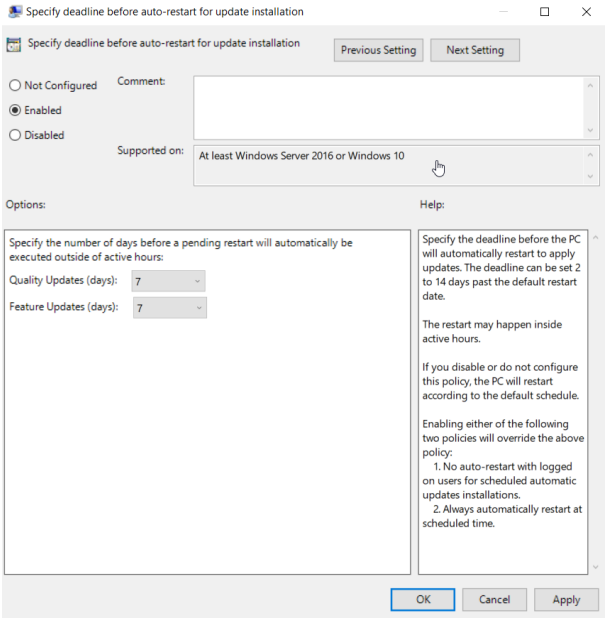


Abbildung 6.5: GPO Client Updates 4

Mit diesen Einstellungen werden die Updates am Morgen, um 05:00 Uhr, heruntergeladen und installiert. Die Benutzer müssen spätestens nach 7 Tagen ihre Computer neu starten. Ausserdem werden die Computer nur ausserhalb der definierten Arbeitszeit automatisch neu gestartet.

Diese Einstellungen sollen nicht strikt übernommen werden, sondern den Bedürfnissen des Betriebs angepasst werden. Wichtig ist jedoch, dass die Updates automatisch installiert werden und das die Computer nach Updates neugestartet werden müssen.

6.2.2 GPO für Server

Falls unternehmenskritische Server vorhanden sind, sollte Windows Server Update Services (WSUS) verwendet werden. Siehe Kapitel WSUS.

Updates für Server sollten installiert werden, wenn Sie nicht in Verwendung sind, da sie für kurze Zeit nicht verfügbar sein werden. Daher ist die Group Policy für Server anders als für Clients. Für Server die 24/7 verwendet werden, muss ein "Maintenance Window" gesetzt und alle Benutzer informiert werden.

Im Group Policy Management muss eine neue Group Policy erstellt werden, welche mit der OU verknüpft ist, die alle Windows Geräte enthält.

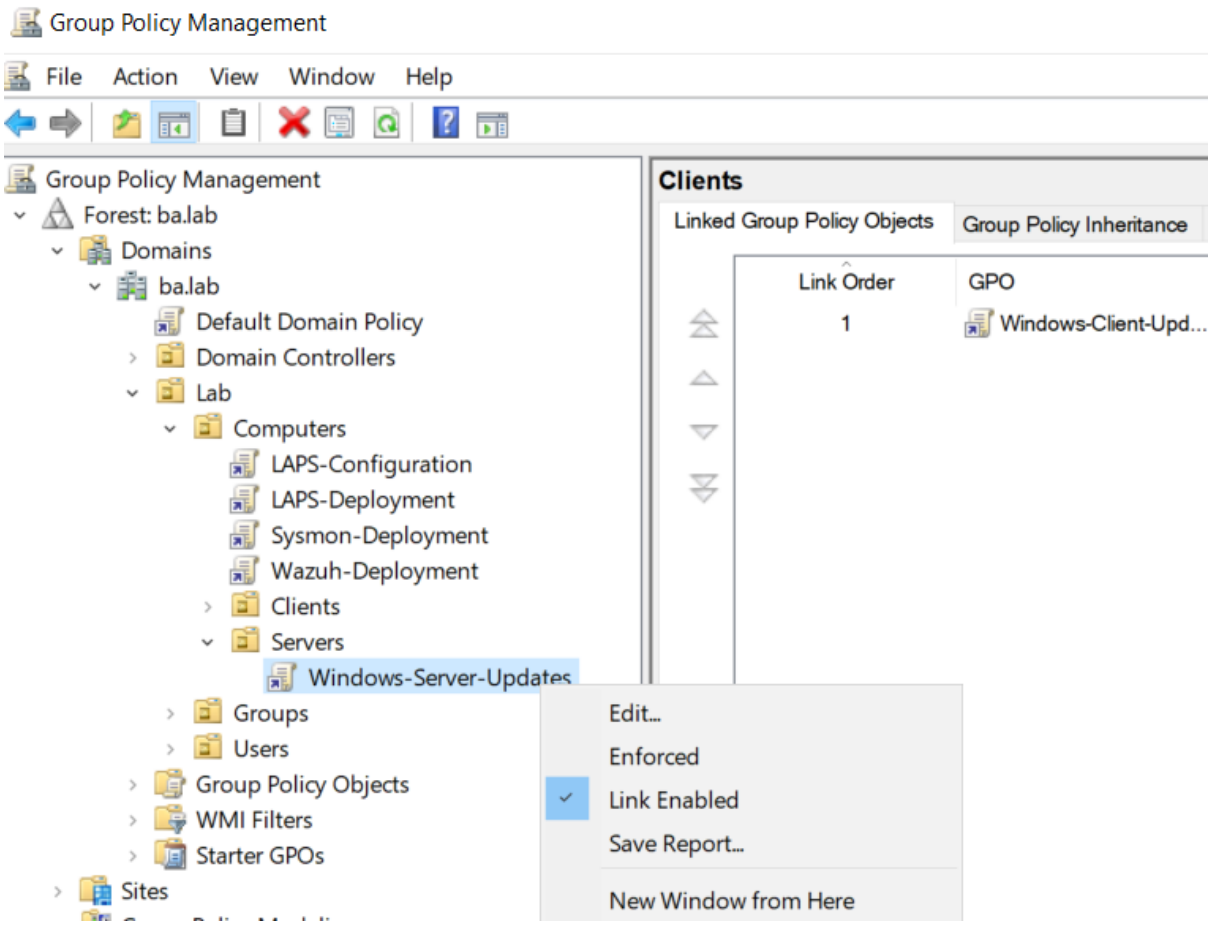


Abbildung 6.6: Neue GPO für Windows Server Updates

Mit **Rechtsklick** → **Edit** kann die neue Group Policy bearbeitet werden. Unter **Computer Configuration** → **Policies** → **Administrative Templates** → **Windows Components** → **Windows Update** findet man alle Policies bezüglich Windows Updates. Für Server werden folgende Policies eingerichtet:

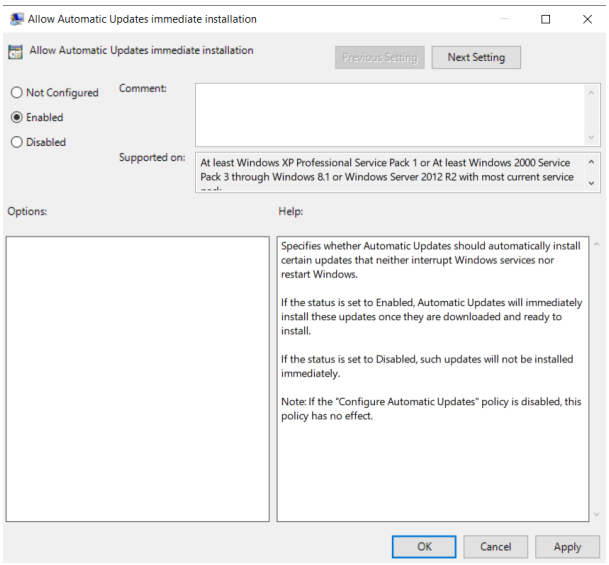


Abbildung 6.7: GPO Server Updates 1

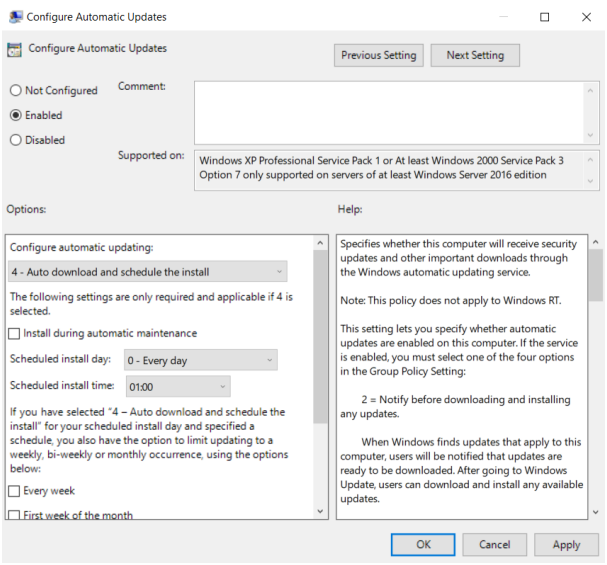


Abbildung 6.8: GPO Server Updates 2

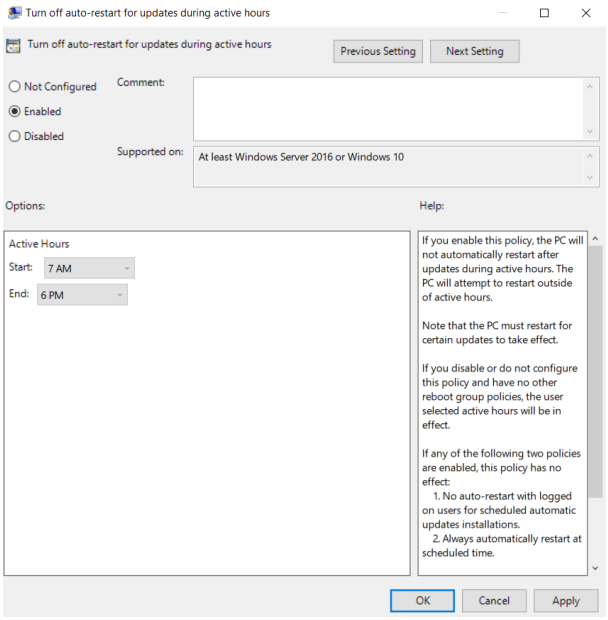


Abbildung 6.9: GPO Server Updates 3

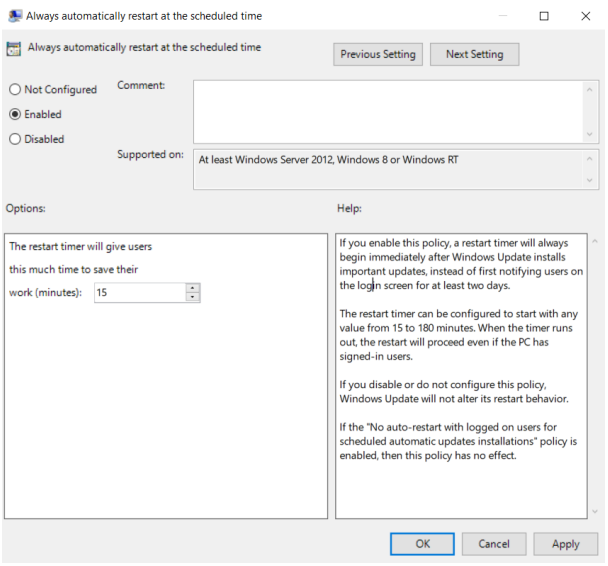


Abbildung 6.10: GPO Server Updates 4

Die Updates werden auf den Servern in der Nacht, um 01:00 Uhr, installiert und die Server anschliessend neu gestartet. Für unternehmenskritische Server sollten die Updates zuerst getestet werden und manuell installiert werden.

6.2.3 Windows Server Update Services (WSUS)

Falls neben den regulären auch unternehmenskritische Systeme vorhanden sind, ist es empfohlen sich einen WSUS Server einzurichten. Dieser bietet die Möglichkeit, Computer und Server in Gruppen einzuteilen und genauer zu definieren, welche Gruppe wann welche Updates erhält. WSUS ist eine Serverrolle auf Windows Server und kann über den Server Manager installiert werden.

In diesem Guide wird nicht genauer auf die Verwendung von WSUS eingegangen. Microsoft bietet gute Anleitungen[2], wie WSUS installiert und eingerichtet werden kann.

6.3 Updates weiterer Software

Für weitere Software, welche nicht zentral verwaltet werden kann, sollte ein Update-Konzept erstellt werden. Dies ist besonders wichtig für Software, welche sich nicht automatisch aktualisiert.

6.3.1 Update Konzept

Im Update Konzept sollten alle Computer welche die Software installiert haben inventarisiert werden. Damit hat man einen Überblick und kann sich vergewissern, dass keine der Computer auf einer alten Softwareversion bleiben. Jede Software sollte einen "Owner" haben. Dieser kann sich bei den Verteilerlisten der Softwarehersteller anmelden um Informationen über die neusten Updates zu erhalten. Der "Owner" ist auch intern die Anlaufstelle für Probleme, welche er gegebenfalls auch mit externen Partnern löst.

[2]Link: https://docs.microsoft.com/de-de/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus

KAPITEL 7

Firewall

Firewalls sind seit 25 Jahren die erste Sicherheitsstufe in einem Netzwerk. Firewalls kommen in allen Arten und Formen. Ob Hardware oder Software, der Anwendungsbereich bleibt gleich. Das Ziel einer Firewall ist es den Netzwerkverkehr zu überprüfen und gegebenfalls zu blockieren.

7.1 Umfang

In diesem Dokument wird auf die Netzwerkfirewall eingegangen. Für die persönliche Firewall wird die Windows Firewall empfohlen. Diese wird automatisch von Windows verwaltet, ist Teil des OS-Schutzkonzept und wird darum in diesem Dokument nicht weiter behandelt.

7.2 Funktionsweise

Eine Layer 3 Netzwerkfirewall-Regel besteht aus vier Teilen:

- Herkunftsadresse
- Zieladresse
- Protokoll
- Zulassen / Blockieren

Ausserdem wird eine Regel immer entweder für eingehenden oder ausgehenden Verkehr definiert. Für die Herkunft und Zieladressen können auch ganze Bereiche von IP-Adressen angegeben werden. Viele Firewalls funktionieren nach dem Top-Down Prinzip. Die Regeln werden von oben nach unten für jedes Packet geprüft und bei der ersten Übereinstimmung angewendet, gibt es keine Übereinstimmung wird die Standardaktion ausgführt.

7.3 Default Deny

In einem Netzwerk sollten keine Annahmen getroffen werden. Basierend darauf kann auch keinem Gerät standardmässig vertraut werden. Die Firewall soll so eingerichtet werden, dass spezielle Operationen wie Netzwerkverkehr vom Internet nach intern freigeschaltet werden muss. Es sollten strenge Regeln implementiert und die Ausnahme speziell einrichtet werden. Dies wird Whitelist Policy[1] gennant. Das genannte Verhalten

[1] https://en.wikipedia.org/wiki/Whitelist

ist bei den meisten Produkten ein Standard. Auf jeden Fall sollte es aber überprüft werden.

Explizite Regeln sollten zuerst eingreifen. Eine Default Deny Regel sollte immer am Schluss aller Regeln einsetzten und sieht folgendermassen aus:
Herkunftsadresse: ANY
Zieladresse: ANY
Protokoll: ANY
Blockieren

7.4 Unternehmenskritische Infrastruktur

Unternehmenskritische Infrastruktur sollte nicht mit allen anderen Geräten im selben Netzwerk sein, sondern in einem dedizierten LAN Segment. Das Segment sollte mit einer Firewall abgeschottet sein und nur benötigte Verbindungen geöffnet werden.

7.5 Betrieb einer Firewall

Eine Firewall übernimmt den Grossteil ihrer Arbeit selbst. Das Updaten der Firmware wird nicht von der Firewall selbst übernommen und muss meist manuell gemacht werden. Eine Firewall ist eine äusserst kritische Komponente eines Netzwerk und sollten dadurch auch regelmässig gepatcht werden.

Bei einem Ausfall einer Firewall muss nicht zwingend ein Security Incident eingetroffen sein, aber es kann sein das der produktive Betrieb des Unternehmens eingeschränkt wird.

7.6 Audits

Es ist empfehlenswert in regelmässigen Abständen Audits von unternehmenskritischer Infrastruktur zu halten. Dies betrifft auch eine Firewall, respektiv deren Konfiguration. Idealerweise werden Audits jährlich durchgeführt, solche Audits können auch von Dienstleister durchgeführt werden. Externe Dienstleister bringen bei Audits oftmals einen grossen Mehrwert, da diese viele Erfahrungen mit diversen Kunden machen.

7.7 Intergration in Wazuh

Viele Firewall Hersteller haben ihr eigenes Betriebssystem auf den Geräten installiert. Durch diese Vielzahl an Systemen ist es für Wazuh nicht möglich einen Wazuh Agent für jedes Betriebssystem zu entwicklen.
Daher bietet Wazuh die Möglichkeit, Agentless via rsyslog[2] die Logdateien auszulesen und zu verarbeiten.

Ausserdem exisiteren bereits im Standard-Ruleset Regeln für einige Firewall-Hersteller[3], wie zum Beispiel Cisco, JunOS oder CheckPoint Smart-1.

In diesem Guide wird das Einrichten von Agnetless Verbindungen zu Firewalls und anderen Geräten nicht genauer erläutert. In der Dokumentation von Wazuh[4] gibt es gute Anleitungen wie solche Systeme in Wazuh aufgenommen werden können.

[2] Link: https://github.com/rsyslog/rsyslog
[3] Link: https://documentation.wazuh.com/current/user-manual/ruleset/getting-started.html
[4] Link: https://documentation.wazuh.com/current/user-manual/capabilities/agentless-monitoring/index.html

KAPITEL 8

Backup

8.1 Einleitung

Ein Backup ist eine Sicherungskopie und kann aus Nutzdaten, Systemdaten oder gar ganzen Datenträgerabbildungen bestehen. Im normalen, operativen Betrieb wird ein Backup selten benötigt. Ein Backup wird in nicht alltäglichen Situationen, wie Datenverlust (z.B. Missclick) oder Ransomware, von sehr grossem Nutzen. Trotz des enormen Mehrwertes des Backups geht es in KMUs oft vergessen. Dies kann schon bei kleinen Vorfällen schwerwiegende wirtschaftliche Folgen herbeiziehen.

8.2 Allgemeine Tipps zum Backup

Bevor dieser Guide ins Detail vom Backup geht, wird noch ein wichtiger Punkt aufgegriffen.

Das Backup ist gleich sensibel wie die darin enthaltenen Daten. Oft als unkritisch klassifiziert – das Backup sollte gleich wie die Daten darin behandelt werden. In der Schlussfolgerung, wenn die Daten verschlüsselt werden, sollte dies das Backup auch. Es sollte verschlüsselt übermittelt werden, verschlüsselt gespeichert und bei sehr kritischen Daten in einer Form verschlüsselt bearbeitet, resp. im Memory gelagert werden.

8.3 Backup Plan

Ein Backup sollte keine zufällige Sache sein. Ein Backup sollte regelmässig, vollständig und geplant sein. Alle nachfolgenden Punkte sollten im Backup Plan berrücksichtigt werden.

8.3.1 spezifische Daten

Ein Backup macht in den meisten Fällen Sinn, wenn spezifische Daten existieren. Backups können schnell zu einem grossen Kostenpunkt werden, denn diese konsumieren enorm viel Speicher. Daher sollte es vermieden werden unnötige Daten zu backupen. Es wäre zum Beispiel denkbar wöchentlich ein Full-Backup zu machen und jeden Tag den inkrement.

Die nachfolgenden Beispiele visualisieren, welche Geräte / Daten für ein Backup geeignet sind.

Beispiel 1:
Ausgangslage: Ein Fileshare mit kritischen Daten, von 100 Usern verwendet, wird gebackupt.
Erläuterung: Der oben beschriebene Sachverhalt bestätigt, dass hier ein Backup sinnvoll ist. Denn der Ausfall dieses Server könnte für die Firma den produktiven Betrieb beeinträchtigen. Die Daten könnten durch Verlust

grossen Sachschaden bedeuten.

Beispiel 2:
Ausgangslage: Ein Notebook mit einer standard Firmeninstallation wird gebackupt. Der Benutzer liest seine E-Mails und arbeitet auf dem Gerät in Sharepoint.
Erläuterung: Dieses Gerät zu backupen macht keinen Sinn da es weder spezifische Daten beherbergt, noch einen speziellen Wert für das Unternehmen bringt. Der Plan bei einem Notfall sollte hier sein das Gerät neu zu installieren.

Es ist wichtig seine Mitarbeitenden zu schulen, wie diese sich im Umgang mit Daten verhalten sollen. Möglich wäre eine Regel die besagt alle kritischen Geschäftsdaten werden auf einem Fileshare abgelegt der gebackupt wird. Damit ist es nicht nötig jeden Client einzeln zu backupen.

8.3.2 Aufbewahrungsdauer / Retention Policy

Bei Datensicherungen ist es wichtig nicht nur die neuste Version zu behalten, da vielleicht diese nicht vollständig ist. Die Aufbewahrungsdauer muss in der Firma mit dem Management geklärt werden, da es sich direkt auf die Kosten des Backups auswirkt. Backup Aufbewahrungsdauer können wie folgt aussehen:

Intervall	Dauer	Art von Backup
Täglich	1 Woche	Inkrementell
Wöchentlich	1 - 4 Wochen	Full Backup
Monatlich	1 Monat - 2 Jahre	Full Backup
Jährlich	2 - 10 Jahre	Fullbackup

Tabelle 8.1: Backup Aufbewahrungsdauer

8.3.3 Datenspeicherort

Das Backup sollte auch in einem Disaster Fall noch zur Verfügung stehen. Dies könnte auch eine Naturkatastrophe bedeuten, wie Überschwemmung des Datacenters. Es wird empfohlen Backups an mehreren physikalisch getrennten Orten zu lagern. Ausserdem empfiehlt es sich auch ein Backup Offline zu lagern, im Falle der Kompromittierung des Firmennetzwerkes. Es wird vermehrt beobachtet, dass Ransomware zuerst das Backup kompromittiert, auch dieser Trend sollte in der Entscheidung des Lagerortes einfliessen. Die Backups sollten immer wieder mal überprüft werden um zu sehen, ob soetwas nicht schon passiert ist.

8.3.4 Datenschutz

Aus Datenschutzgründen muss abgeklärt werden, welche Daten in welchem Land gespeichert werden dürfen. Dies ist vorallem bei Cloudanbieter kritisch und sollte im vorhinein klar vereinbart werden. Der Datenspeicherort sollte gegebenfalls mit juristischer Unterstützung geklärt werden.

Oftmals gibt es für Daten eine Mindest- und/oder Maximalspeicherdauer. Diese muss auch für die verschiedenen Geschäftsdaten abgeklärt werden, damit keine juristischen Probleme entstehen.

8.4 Emergencyplan

In einem Notfall ist es wichtig einen "Emergencyplan" zu haben. Die wichtigsten Elemente in einem Notfallplan sind die Prioritäten der Geschäftsprozesse und deren Abhängigkeit an Daten.

Das Recovery Time Objective (RTO) ist die Zeitspanne, innerhalb derer ein Geschäftsprozess nach einer Katastrophe wiederhergestellt werden muss, um unannehmbare Folgen einer Unterbrechung des operativen Betriebs zu vermeiden.

Der Notfallplan eines Unternehmens sollte mindestens einmal jährlich validiert werden und im Idealfall ein ähnliches Szenario durch gespielt. Der Notfallplan sollte mit dem höheren Management des Unternehmens erarbeitet und anschliessend abgesegnet werden.

8.5 Wiederherstellen des Backups

Es scheint trivial, dass ein Backup wiederherstellbar sein sollte. Leider kann es auch hier technisches Versagen geben. Es wird stark empfohlen in regelmässigen Abständen das wiederherstellen der Daten zu testen. Das beste Backup bringt ohne einen funktionierenden Restore nichts.

KAPITEL 9

Verzeichnisse

Abbildungsverzeichnis

Tabellenverzeichnis

Literatur

[Gra22] Paul A. Grassi. *Digital Identity Guidelines*. Techn. Ber. DOI: 10.6028/NIST.SP.800-63b. Gaithersburg, Maryland, United States: NIST, Apr. 2022.

KAPITEL 10

Anhang

Glossar

Antivirus Ein Antivirus (AV) ist eine Software, die Schadsoftware wie zum Beispiel Viren, Würmer oder Trojanische Pferde aufspüren, blockieren und beseitigen soll. 2, 4, 5, 21, 22, 51

Certification Authority Die Certification Authoritity (CA) ist eine Stelle, welche digitale Zertifikate ausstellt. Somit ist es möglich bei der Kommunikation zweier Parteien die Integrität durch zuverlässige dritte Partei zu haben. 51

Common Vulnerabilities and Exposures Das Common Vulnerabilities and Exposures Referenzier-System wird durch die Mitre Corporation gepflegt und ist dem US National Cybersecurity FFRDC unterstellt. CVEs sind bekannt gewordene Attacken welche dokumentiert und veröffentlich werden. Sie beinhalten die geschätzte Herkunft der Angreifer, den Angriffsweg und Möglichkeiten, sich gegen solch einen Angriff zu schützten. 34, 51

Dynamic Host Configuration Protocol Das Dynamic Host Configuration Protocol (DHCP) ist ein Protokoll im Netzwerk. Es ermöglicht die Zuweisung von Netzwerkkonfigurationen, wie IP-Adressen und Gateway, an Clients durch einen Server. 51

Graphical user interface Ein Graphical user interface, auch Grafische Benutzeroberfläche genannt, ist eine Schnittstelle für Benutzer, um mit einem elektronischen Gerät grafisch zu interagieren . 51

Group Policy Object Ein Group Policy Object (GPO) ist eine Sammlung von Richtlinieneinstellungen. Ein GPO hat einen eindeutigen Namen, z. B. eine GUID. Gruppenrichtlinieneinstellungen sind in einem GPO enthalten. 51

Identity and Access Management Identitäts- und Zugriffsmanagement (IAM) können Administratoren autorisieren, wer auf bestimmte Ressourcen zugreifen darf. So ist es möglich die Kontrolle und Transparenz zentral zu verwalten. Für Unternehmen mit komplexen Organisationsstrukturen, Hunderten von Teams und vielen Projekten bietet IAM eine einheitliche Sicht auf die Sicherheitsrichtlinien in Ihrem gesamten Unternehmen mit integrierter Prüfung zur Vereinfachung der Compliance-Prozesse. 2, 4, 6–12, 51

Local Administrator Password Solution Die Local Administrator Password Solution (LAPS) ermöglicht die Verwaltung der Passwörter lokaler Accounts von Computern, die der Domäne angeschlossen sind. Die Passwörter werden im Active Directory (AD) gespeichert. 2, 4, 23–33, 51

National Institute of Standards and Technology Das National Institute of Standards and Technology ist eine Amerikanische Bundesbehörde, welche für Standardisierungsprozesse zuständig ist. 51

Network Time Protocol Das Network Time Protocol (NTP) wird häufig zur Synchronisierung von Computeruhren im Netzwerk verwendet. 51

Operating System Ein Operatingsystem (OS), auch Betriebssystem genannt, ist eine Systemsoftware, die Computerhardware und Softwareressourcen verwaltet und allgemeine Dienste für Computerprogramme bereitstellt. 51

Organizational Unit Mit Organizational Units (OUs) in einer von Active Directory (AD) verwalteten Domäne können Objekte wie Benutzeraccounts, Serviceaccounts oder Computer logisch gruppieren. 51

Recovery Time Objective Das Recovery Time Objective (RTO) ist die Zeitspanne, innerhalb derer ein Geschäftsprozess nach einer Katastrophe wiederhergestellt werden muss, um unannehmbare Folgen einer Unterbrechung des operativen Betriebs zu vermeiden. 42, 51

Trusted Platform Module Das Trusted Platform Module ist ein optionaler Hardware-Chip auf der Hauptplatine in einem Computer. IM TPM Chip werden Kryptografische Schlüssel hinterlegt, welche dann von Software verwendet werden können. 13, 51

Windows Server Update Services Der Windows Server Update Services ist eine Serverrolle für Windows Server mit welcher die Windows Updates zentral Verwaltet werden können. Die Rolle bietet die Möglichkeit, Updates zentral herunterzuladen und auf alle Windows Geräte zu verteilen. Zusätzlich kann genau gestueret werden, welche Computer und Server welche Updates erhalten sollen. 3, 34, 36, 38, 51

Abkürzungsverzeichnis

AV Antivirus. 2, 4, 5, 21, 22

CA Certification Authority. 6

CVE Common Vulnerabilities and Exposures. 34

DHCP Dynamic Host Configuration Protocol. 6, 7

DNS Certification Authority. 6, 7

GPO Group Policy Object. 2, 3, 19, 23–26, 34–38, 45, 46

GUI Graphical user interface. 3, 25–27, 31, 45

IAM Identity and Access Management. 2, 4–12

LAPS Local Administrator Password Solution. 2–5, 23–33, 45, 46

NIST National Institute of Standards and Technology. 9

NTP Network Time Protocol. 6, 7

OS Operating System. 13, 39

OU Organizational Unit. 10, 15, 24, 29, 30, 34, 36

RTO Recovery Time Objective. 42

TPM Trusted Platform Module. 13, 14, 19, 45

WSUS Windows Server Update Services. 3, 34, 36, 38

Ende Anhang