Master-Thesis

Aufklärung doloser Handlungen - Innentätern auf der Spur

Erweiterungsmöglichkeiten der Post-Mortem-Forensik zur schnelleren Aufklärung von Vorfällen

Masterarbeit zur Erlangung des Grades eines

Master of Engineering

der Hochschule Wismar

eingereicht am: 27.09.2019

von: Felix Wanner geboren am 01.11.1987

in Schwäbisch Gmünd

Studiengang: IT-Sicherheit und Forensik

Erstgutachter: Frau Prof. Dr.-Ing. Antje Raab-Düsterhöft

Zweitgutachter: Herr Dipl. Ing. Hans-Peter Merkel

Aufgabenstellung

Diese Master-Thesis soll eine Hilfestellung bieten, um für eine bessere Informationssicherheit zu sorgen und für das Thema Innentäter zu sensibilisieren. Dabei soll ein Testsystem aus virtuellen Maschinen aufgebaut werden, um im Versuchsaufbau ein kleines Netzwerk mit sensiblen Daten und einem Innentäter zu simulieren. Der Innentäter versucht auf den Server mit sensiblen Daten zuzugreifen und diese auf einen USB-Stick zu kopieren. Ebenso soll ein Remote-Zugang eingerichtet werden, damit der Mitarbeiter über ein Remote-Access-Tool von einem anderen Standort auf seine Systeme zugreifen kann und so auch unerlaubt Daten übertragen kann.

Anschließend erfolgt eine forensische Untersuchung der virtuellen Maschine des Innentäters. Nach einer ersten Analyse sollen weitere Schritte implementiert werden, die einen Angriff frühzeitig erkennen soll, und so auch Gegenmaßnahmen ergriffen werden können. Es wird anhand aktueller Fachliteratur geprüft, welche Anpassungen in Betriebssystemen und -abläufen sinnvoll sind und wie Unternehmen diese implementieren können.

Die Arbeit soll Antworten auf folgende Fragen liefern:

- Wie erkennen Unternehmen, dass Unternehmensdaten gestohlen wurden?
- Was können Unternehmen tun, damit Unternehmensdaten nicht gestohlen werden?
- Wie müssen sich Unternehmen nach einem Vorfall richtig verhalten?
- Wie kann die Zeit zur Erkennung reduziert werden?
- Wie erreichen Unternehmen die „Forensic Readiness“?

Task definition

This master thesis should provide a little help to get a better information security and to raise awareness of the threat of insiders. A test system consisting of virtual machines will be set up to simulate a small network with sensitive data and an insider who will try to steal sensitive information in the experimental set-up. The insider tries to access the server with sensitive data and copy it to a USB stick. Similarly, a remote access should be set up so that the employee can access his

systems from another location via a remote access tool and thus also be able to transfer data without authorization. Subsequently, a forensic investigation of the virtual machine of the interior decorator takes place. After an initial analysis, further steps are to be implemented to detect an attack early on, and so also countermeasures can be taken. Using state-of-the-art literature, it will be examined which adjustments in operating systems and workflows make sense and how companies can implement them.
The thesis should provide answers to the following questions:

- How do companies recognize that company data has been stolen?
- What can companies do to prevent corporate data from being stolen?
- How do companies behave properly after an incident?
- How can the time for detection be reduced?
- How do companies achieve forensic readiness?

Abstract

Unternehmen sind oft der Gefahr schadhafter Handlungen durch Innentätern ausgesetzt. Dabei wird die schadhafte Handlung oft zu spät, oder gar nicht erkannt. Wird eine forensische Analyse dabei nicht zeitnah durchgeführt, können wichtige Beweise bereits überschrieben worden sein. Deshalb wurde in dieser Arbeit geprüft, wie die Post-Mortem-Analyse erweitert werden kann, um Vorfälle schneller zu entdecken und aufzuklären. Dabei wurde das installierte Testsystem nach einem simulierten Vorfall forensisch untersucht. Im Anschluss erfolgte eine Anpassung in den Audit-Einstellungen und eine permanente Weiterleitung der Ereignisse und Protokolle an ein zentrales Log-Management. Hierbei wurden zwei Lösungen verglichen. Nach der Anpassung der Audit-Einstellungen wurde der Test wiederholt. Das Ergebnis zeigte, dass durch ein zentrales Log-Management und ein implementiertes SIEM Datenabflüsse erkannt werden können und die integrierten Anwendungen in Security Onion ein hilfreicher Zusatz sein können.

Abstract

Companies are often exposed to the risk of harmful acts by an insider. The harmful action is often too late, or not recognized at all. If a forensic analysis is

not carried out in a timely manner, important evidence may already have been overwritten. Therefore, this work examined how to extend post-mortem analysis to detect and investigate incidents more quickly. The installed test system was forensically examined after a simulated incident. Subsequently, an adjustment in the audit settings and a permanent forwarding of the events and logs to a central log management took place. Two solutions were compared. After adjusting the audit settings, the test was repeated. The result showed that centralized log management and implemented SIEM can detect data outflows and that the built-in applications in Security Onion can be a helpful addition.

Inhalt

1. Einleitung

Unternehmen sind täglich der Gefahr von Hackern ausgesetzt, die es auf Daten des Unternehmens abgesehen haben. Jedoch kommt der Täter nicht immer von außen. Sogenannte Innentäter kennen das Unternehmen, die Daten, die sie wollen und auch eventuelle Schwachstellen im Unternehmen, und können so oft „unter dem Radar“ Daten abgreifen und diese beispielsweise bei einem neuen Arbeitgeber nutzen, um daraus Vorteile zu erlangen oder gar ihr eigenes Unternehmen gründen.[1]

Kriminelle Mitarbeiter richten in Unternehmen deutlich mehr Schaden an als externe Täter. Im Jahr 2018 gab es laut dem Gesamtverband der Deutschen Versicherungswirtschaft (GDV) mit Wirtschaftsstraftaten einen Versicherungsschaden von 225 Millionen Euro. Innentäter waren für 75 Prozent des Schadens verantwortlich. Insgesamt gab es im Jahr 2018 2.400 Vertrauensschadensversicherungen, für die die Versicherungen eingesprungen sind (siehe Abbildung 1). Rüdiger Kirsch, Vorsitzender der Arbeitsgruppe für Vertrauensschadensversicherungen des GDV, geht davon aus, dass jedes Jahr fünf bis zehn Prozent der deutschen Unternehmen von eigenen Mitarbeitern betrogen werden. Die Täter, die meist männlich und in Führungspositionen tätig sind, haben dabei verschiedenste Betrugsmaschen wie Diebstahl, Bestechung, Preisabsprachen oder Schwarzgeld.[2] Die Dunkelziffer dürfte jedoch deutlich höher sein, da nicht jeder Fall entdeckt oder zur Anzeige gebracht wird.

Da Angreifer von innen, also sogenannte Innentäter im Vergleich zu Hackern keine Zugriffsrechte „erarbeiten“ müssen, verfügen Innentäter bereits über legitime Zugriffe.[3] Dies macht eine forensische Untersuchung bei einem vermuteten Datenabfluss sehr kompliziert. Da aus eigener Erfahrung bei vielen kleinen und mittelständischen Unternehmen die möglichen Log-Mechanismen diverser Betriebssysteme und Programme nur auf die Minimalkonfiguration des Herstellers eingestellt sind, können Unternehmen Angriffe durch Innentäter oft nicht erkennen. Wenn Angriffe vermutet werden, dann kann dies vor Gericht meist nur durch Indizienbeweise dargelegt

[1] Vgl. Schonscheck, 2017.

[2] Vgl. Channelpartner, 2019.

[3] Vgl. Schonscheck, 2017.

werden. Ein zentrales Log-Management mit einer gewissen Intelligenz könnte bei solchen Fällen helfen und rechtzeitig auf Gefahren hinweisen.[4]

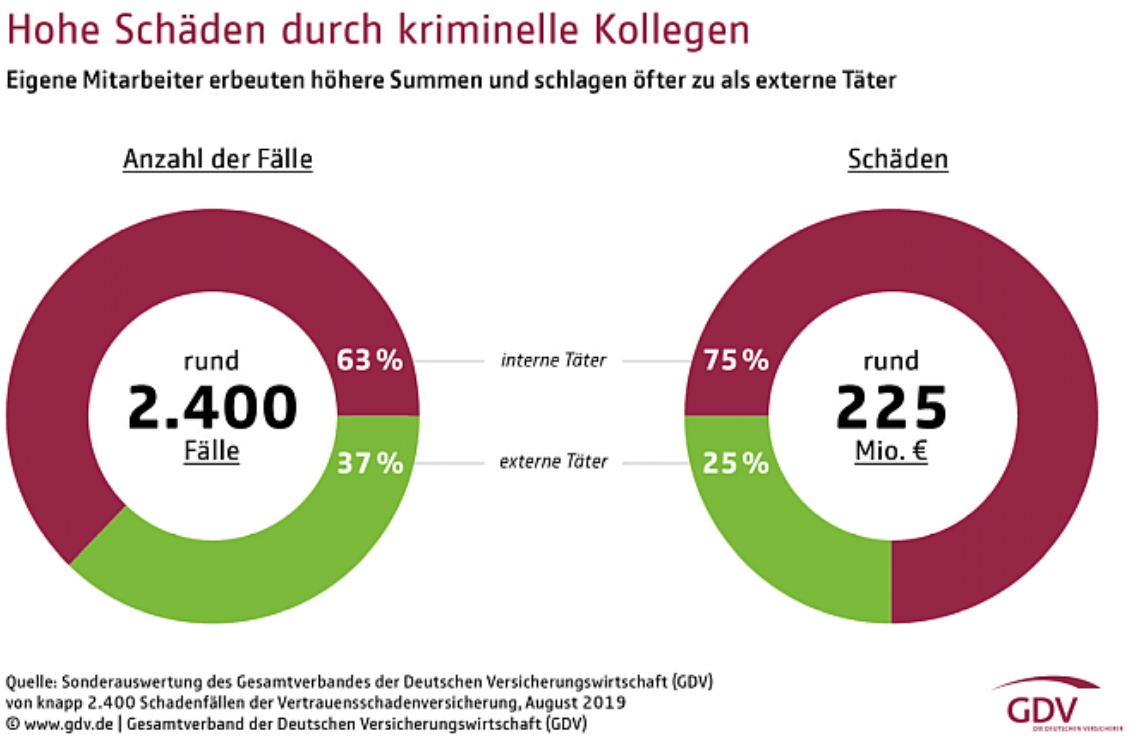


Abbildung 1: Sonderauswertung des GDV zu Innentätern[5]

Diese Master-Thesis soll eine Hilfestellung bieten, um für eine bessere Informationssicherheit zu sorgen und für das Thema Innentäter zu sensibilisieren. Dabei soll ein Testsystem aus virtuellen Maschinen aufgebaut werden, um im Versuchsaufbau ein kleines Netzwerk mit sensiblen Daten und einem Innentäter zu simulieren. Der Innentäter versucht auf den Server mit sensiblen Daten zuzugreifen und diese auf einen USB-Stick zu kopieren. Ebenso soll ein Remote-Zugang eingerichtet werden, damit der Mitarbeiter über ein Remote-Access-Tool von einem anderen Standort auf seine Systeme zugreifen kann und so auch unerlaubt Daten übertragen kann.

Anschließend erfolgt eine forensische Untersuchung der virtuellen Maschine des Innentäters. Nach einer ersten Analyse sollen weitere Schritte implementiert werden, die einen Angriff frühzeitig erkennen und so auch Gegenmaßnahmen ergriffen werden können. Es wird anhand aktueller Fachliteratur geprüft, welche Anpassungen in

[4] Vgl. Sanders, 2016.

[5] Brüss, 2019.

Betriebssystemen und -abläufen sinnvoll sind und wie Unternehmen diese implementieren können.

Die Arbeit soll Antworten auf folgende Fragen liefern:

- Wie erkennen Unternehmen, dass Unternehmensdaten gestohlen wurden?
- Was können Unternehmen tun, damit Unternehmensdaten nicht gestohlen werden?
- Wie müssen sich Unternehmen nach einem Vorfall richtig verhalten?
- Wie kann die Zeit zur Erkennung reduziert werden?
- Wie erreichen Unternehmen die „Forensic Readiness“?

Nicht nur Unternehmen, die eine ISO 27001-Zertifizierung wollen, sind dazu verpflichtet, ein zentrales Log-Management aufzubauen. Das IT-Sicherheitsgesetz, der IT-Grundschutz, Anforderungen der BAFIN für Versicherungen und Banken, und viele weitere Normen und Gesetze verpflichten Unternehmen ihre Risiken für den Geschäftsbetrieb zu erkennen und zu minimieren. Dies umfasst auch Maßnahmen zur Erkennung von Bedrohungen. Um Bedrohungen erkennen zu können, müssen Unternehmen eine Inventarisierung geschäftsrelevanter Vermögenswerte, sogenannter Assets durchführen. Hierbei sind nicht nur Maschinen, Hard- und Software zu betrachten, sondern auch immaterielle Vermögenswerte, wie z. B. intellektuelles Eigentum. Diese können aus Erfindungen, Geschmacksmustern, Bauplänen, Software, automatisierten Prozessen bestehen.

Bei der Analyse der bestehenden Fachliteratur und aktueller Leitfäden fiel auf, dass es keine direkte Literatur zur Aufklärung von Innentätern mit technischen Möglichkeiten gibt. Auch im Bereich der IT-Forensik gibt es viel Fachliteratur, die jedoch meist nur einzelne Aspekte betrachtet.

Technische Lösungen mit Logging-Mechanismen und einer Intelligenz dahinter gibt es schon länger. Diese Lösungen (wie z. B. Splunk) werden als Security Information and Event Management (SIEM) angeboten. Die Kosten für solch eine Lösung übersteigen selbst bei kleinen Unternehmen schnell fünfstellige Beträge. Für größere Unternehmen natürlich entsprechend mehr. Werden jedoch diese Kosten mit den möglichen Kosten eines Abflusses unternehmenskritischer Daten verglichen, besteht hier ein großer Unterschied. Ein Datenverlust, mutwillige Manipulation oder der Diebstahl von Geschäftsdaten kann Unternehmen hohe Geldbeträge kosten, zu Reputationsschäden führen, oder in die Insolvenz führen.

Im Rahmen dieser Masterarbeit sollen zunächst die Rahmenbedingungen definiert und die Grundlagen einer forensischen Untersuchung ausgearbeitet werden. Diese Grundlagen werden anhand von Testfällen in der virtuellen Testumgebung nachgestellt. Anschließend sollen gängige Möglichkeiten für ein zentrales Log-Management geprüft und in den virtuellen Systemen implementiert werden, um eine Basis für spätere forensische Analysen zu haben. Da für das Log-Management entweder ein reines ELK[6], bestehend aus Elasticsearch, Logstash und Kibana, oder eine bereits fertige Sicherheitslösung „Security Onion“ genutzt werden soll, werden diese vorgestellt und verglichen.

Nach der Implementierung einer ELK-Lösung sollen die Vorfälle ein weiteres Mal durchgeführt werden und anschließend eine forensische Untersuchung mit Hilfe der implementierten ELK-Lösung geprüft werden.

In den Grundlagen wird auf Begrifflichkeiten zum weiteren Verständnis dieser Arbeit eingegangen. Anschließend wird auf den Versuchsaufbau eingegangen und anhand von Beispielen gezeigt wie vorgegangen wird. Die forensischen Lösungsansätze präsentieren eine praktische Auswertung der durchgeführten Versuche. Die anschließend durchgeführten Maßnahmen zur Steigerung der Aufklärungsquote beschäftigen sich mit Optimierungsmaßnahmen der Audit- und Eventlogs und deren Anbindung an ein zentrales Log-Management, in dem die Daten gesammelt und ausgewertet werden. Damit ein Vergleich stattfinden kann, werden die Tests ein weiteres Mal durchgeführt und dann anhand eines Vorher-Nachher-Vergleichs gegenübergestellt.

[6] Im Nachfolgenden werden ELK-Stack und Elastic-Stack synonym verwendet.

2. Grundlagen

Zur Verständlichkeit werden in den Grundlagen die wichtigsten Begriffe und Zusammenhänge erläutert, um dem Leser ein besseres Grundverständnis der nachfolgenden Themen zu geben.

2.1 Logdateien und Protokollierung

Logdateien sind Aufzeichnungen von Ereignissen, die in datenverarbeitenden Systemen und Anwendungen generiert werden. Jedes Ereignis schreibt hierzu einen Eintrag in die Logdatei.

Bei einer forensischen Untersuchung von Serversystemen ist die Wahrscheinlichkeit hoch, dass Logdateien analysiert werden müssen. In diesen können externe Zugriffe auf Websites, Angriffe auf die Firewall und auch fehlgeschlagene und erfolgreiche Anmeldungen auf die zu untersuchenden Systeme angesehen werden. Ebenso können Logdateien auch Einträge enthalten, die nichts mit einem von außen wirkendem Zugriff zu tun haben. Systemdienste, Cronjobs, Anwendungen, Hardware, Software und Fehler bei der Ausführung von Diensten und Programmen können ebenso Einträge in Logdateien schreiben.[7]

In modernen Windows-Betriebssystemen werden die Logdateien unter *C:\Windows\System32\winevt\Logs* gespeichert. In diesem Verzeichnis befinden sich alle möglichen Logdateien. Die wichtigsten hierbei sind die Anwendungs-, Sicherheits- und Systemlogdateien.

Der aktuelle Speicherort kann in der Windows-Registry in nachfolgendem Pfad ausgelesen und ggf. geändert werden: *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog*.

In dem Speicherort für die Logdateien befinden sich nachfolgende Dateien:

• Application: Zeigt anwendungsspezifische Meldungen wie Informationen Fehler und Warnungen an, die das jeweilige Programm meldet. Wird ein Dienst gestartet oder beendet wird ein Eintrag in die Ereignisanzeige geschrieben. In jedem Eintrag Ebene (Information, Fehler oder Warnung), Datum und Uhrzeit, Quelle (welches Programm

[7] Vgl. Kuhlee, 2012, S.128f.

oder welcher Dienst), die Ereignis-ID und eine Aufgabenkategorie enthalten. Abbildung 2 zeigt ein Beispiel einer Meldung der Application.evtx.

Protokollname: Application
Quelle: Application Hang
Datum: 04.09.2019 10:28:09
Ereignis-ID: 1002
Aufgabenkategorie:(101)
Ebene: Fehler
Schlüsselwörter: Klassisch
Benutzer: Nicht zutreffend
Computer: DESKTOP-5002M9M
Beschreibung:
Das Programm firefox.exe Version 68.0.2.7164 hat die Interaktion mit Windows beendet und wurde geschlossen. Überprüfen Sie den Problemverlauf in der Systemsteuerung "Sicherheit und Wartung", um nach weiteren Informationen zum Problem zu suchen.
Prozess-ID: 3d28
Startzeit: 01d562f170ecc2a9
Beendigungszeit: 10
Anwendungspfad: C:\Program Files\Mozilla Firefox\firefox.exe
…

Abbildung 2: Beispielmeldung der Application.evtx (eigene Darstellung)

• Security: Zeigt sicherheitsrelevante Informationen für das Betriebssystem an. Darunter fallen die Zuweisung von Benutzerrechten, An- und Abmeldungen und Systemintegritätsdienste. In nachfolgendem Beispiel wurde die Event-ID 4624 für eine erfolgte Anmeldung erzeugt. In den weiteren Informationen des Events können der Benutzername, die Art der Anmeldung, Datum und Uhrzeit, die Aufgabenkategorie und viele weitere Informationen erkannt werden. Die Art der Anmeldung kann bei einer forensischen Untersuchung durchaus hilfreich sein, da diese anzeigt, wie die Anmeldung des Benutzers erfolgt ist. Ein Beispiel ist in Abbildung 3 zu finden. Windows unterscheidet nach

- lokalen, interaktiven Anmeldung mit Tastatur und Bildschirm,
- Anmeldung über einen Dienst,
- über das Netzwerk (über eine Netzwerkfreigabe),
- über die Konsole,

- über Remoteunterstützung oder Remote Desktop
- und weitere, eher seltene Arten wie „NetworkCleartext“ oder „CachedInteractive“.

Protokollname: Security
Quelle: Microsoft-Windows-Security-Auditing
Datum: 04.09.2019 16:01:06
Ereignis-ID: 4624
Aufgabenkategorie: Logon
Ebene: Informationen
Schlüsselwörter: Überwachung erfolgreich
Benutzer: Nicht zutreffend
Computer: DESKTOP-5002M9M
Beschreibung:
Ein Konto wurde erfolgreich angemeldet.
…

Abbildung 3: Beispielmeldung der Security.evtx (eigene Darstellung)

• System: zeigt Systemrelevante Informationen wie Fehler bei der DNS-Auflösung, Treiberprobleme, Kernelfehler und viele weitere an (Beispielmeldung in Abbildung 4).

Protokollname: System
Quelle: Service Control Manager
Datum: 11.08.2019 18:50:38
Ereignis-ID: 7001
Aufgabenkategorie: Keine
Ebene: Fehler
Schlüsselwörter: Klassisch
Benutzer: Nicht zutreffend
Computer: DESKTOP-5002M9M
Beschreibung:
Der Dienst "hvsics" ist vom Dienst "CmService" abhängig, der aufgrund folgenden Fehlers nicht gestartet wurde:
Der Abhängigkeitsdienst oder die Abhängigkeitsgruppe konnte nicht gestartet werden.
…

Abbildung 4: Beispielmeldung der System.evtx (eigene Darstellung)

Neben den typischen Ereignisprotokollen gibt es noch weitere, die meist noch konfiguriert werden müssen. Da diese meist nur für eine Anwendung oder einen Dienst sind, wird auf eine weitere Beschreibung verzichtet:

- Windows PowerShell
- Microsoft-Windows-PowerShell/Operational
- Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational
- Microsoft-Windows-SmbClient/Security
- Microsoft-Windows-SMBServer/Security
- Microsoft-Windows-TaskScheduler/Operational
- Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational
- Microsoft-Windows-Windows Defender/Operational
- Microsoft-Windows-Windows Firewall With Advanced Security/Firewall
- Microsoft-Windows-Winlogon/Operational
- Microsoft-Windows-WinRM/Operational
- Microsoft-Windows-WMI-Activity/Operational.

Windows-Betriebssysteme nutzen Event-IDs, um Ereignisse einer gewissen Kategorie zuzuweisen. Laut Schlede sind nachfolgende Ereignis-IDs besonders wichtig:

Tabelle 1: Wichtige Ereignis-IDs[8]

ID	Meldung	Kategorie	Unterkategorie
4777	Ein Konto wurde für die Anmeldung zugeordnet	Kontoanmeldung	Überprüfung der Anmeldeinformation
4771	Kerberos-Vorbestätigung ist fehlgeschlagen	Kontoanmeldung	Kerberos-Authentifizierungsdienst
4772	Kerberos-Vorbestätigung ist fehlgeschlagen.	Kontoanmeldung	Kerberos-Authentifizierungsdienst
4723	Es wurde versucht, ein Kontokennwort zu ändern.	Kontoverwaltung	User Account Management
4738	Ein Benutzerkonto wurde geändert.	Kontoverwaltung	User Account Management
4740	Ein Benutzerkonto wurde gesperrt.	Kontoverwaltung	User Account Management
4780	Die ACL wurde für Konten festgelegt, die Mitglieder der Gruppenadministratoren sind.	Kontoverwaltung	User Account Management
4649	Ein Replay-Angriff wurde festgestellt.	Anmelden/Abmelden	Andere An-/Abmelde-Ereignisse

[8] Schlede, 2012.

5378	Die angeforderte Anmeldeinformationen-Delegierung wurde durch die Richtlinie nicht zugelassen.	Anmelden/Abmelden	Andere An-/Abmelde-Ereignisse
4621	Administratorsystem vom CrashOnAuditFail wiederhergestellt. Benutzer, die keine Administratoren sind, können sich nun anmelden.	System	Security-Status ändern

In Linux-Betriebssystemen werden Logdateien typischerweise in /var/log abgespeichert. Sind die entsprechenden Logdateien nicht zu finden, kann in der Konfigurationsdatei des Programms in /etc eine Konfigurationsänderung wie z. B. eine Logpfad-Änderung vorgenommen werden. Werden Windows- und Linux-Logdateien verglichen, sind deutliche Unterschiede zu erkennen.[9]

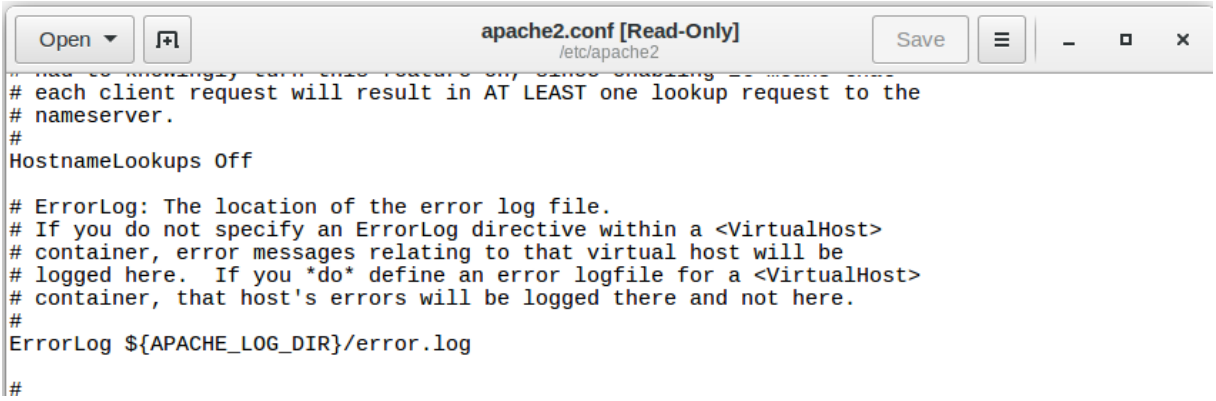


Abbildung 5: Beispielhafte Konfigurationsanpassung für Apache2 (eigene Darstellung)

Im Linux-Logverzeichnis liegen unterschiedliche Ordner der jeweiligen Programme und deren Logdateien. Die Logeinträge werden als Text in die Logdatei geschrieben. Ein Auszug davon ist in Abbildung 6 zu erkennen.

[9] Vgl. Riegel, 2019.

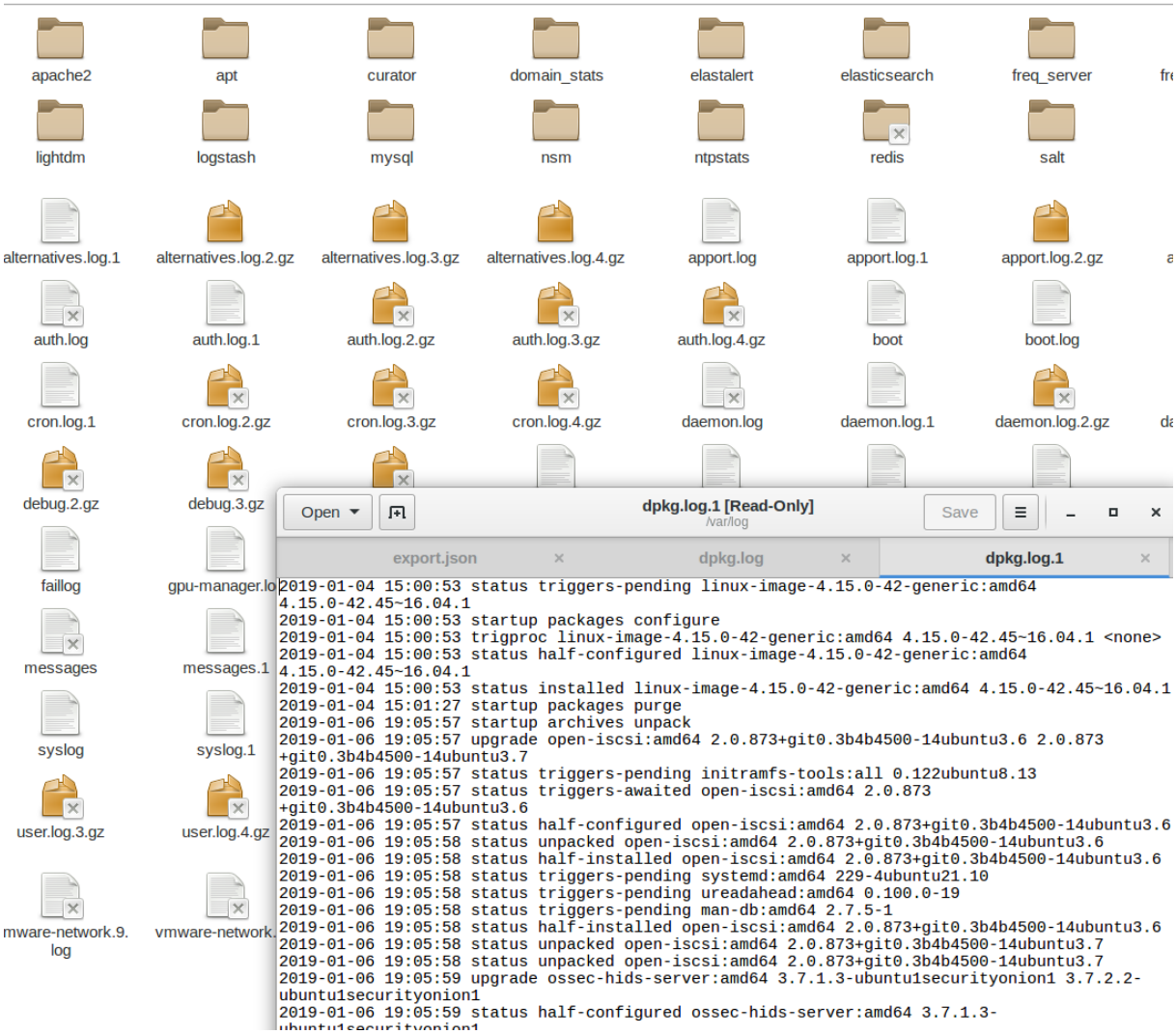


Abbildung 6: Auszug aus Linux-Logverzeichnis und Logdatei (eigene Darstellung)

Bei Datenbanken können Log-Dateien betrachtet in drei Kategorien unterteilt werden:

- Performance-Logs
- Sicherheits-Logs
- Stabilitäts-Logs.[10]

Neben der normalen Logaufzeichnungsfunktion bieten sogenannte Audittrails oder Transaktionslogs die Möglichkeit sämtliche Kommunikation mit einer Datenbank aufzuzeichnen.

In unternehmenskritischen Bereichen können diese eingesetzt werden, um jegliche Manipulation zu erkennen.[11]

[10] Vgl. Wyllie, 2009.

[11] Vgl. Van Randen, 2016, S. 96f.

Um Vorfälle erkennen zu können, müssen die Logdateien bzw. die Auditfunktion so angepasst werden, dass die Bedrohung entsprechend kategorisiert und behoben werden kann. Da Windows und Linux unterschiedliche Arten der Protokollierung nutzen, ist ein zentrales Log-Management mit einer Normalisierung der Daten notwendig, damit die entsprechenden Felder wie IP-Adressen, Datum und Uhrzeit, Benutzername etc. über verschiedene Systeme hinweg vergleichbar ist.

Neben organisatorischen und technischen Vorgaben stellen der Gesetzgeber und andere Organisationen weitere Anforderungen an die Protokollierung. Im Bundesdatenschutzgesetz und der Datenschutzgrundverordnung wird im §76 geregelt, dass in automatisierten Verarbeitungssystemen Verantwortliche und Auftragsverarbeiter die Erhebung, Veränderung, Abfrage, Offenlegung und Übermittlung, Kombination und Löschung von Verarbeitungsvorgängen protokollieren müssen. In diesem Protokoll müssen die Begründung, das Datum und die Uhrzeit des Vorgangs und die Identität der abfragenden Person und die Identität des Empfängers dokumentiert werden. Zur Überprüfung der Rechtmäßigkeit der Datenverarbeitung, der Eigenüberwachung, zur Gewährleistung der Integrität und Sicherheit der personenbezogenen Daten und für Strafverfahren dürfen der oder die Datenschutzbeauftragte, der Bundesbeauftrage, die betroffene Person, oder der Verarbeiter der Daten diese Daten verwenden und spätestens am Ende des folgenden Jahres nach Generierung löschen.[12]

Durch die Protokollierung soll eine Aufrechterhaltung von Datenschutz und -sicherheit gewährleistet werden und darf nicht zur automatisierten Verhaltens- und Leistungskontrolle von Mitarbeitern genutzt werden. Die Protokolldaten dürfen nur für einen gewissen Zweck verwendet werden und unterliegen somit einer Zweckbindung, da in Protokollen ein Einblick in Tätigkeiten von Mitarbeitern möglich ist. Durch den Grundsatz der Erforderlichkeit kann ein Protokollierungsverfahren gestaltet werden. Das Protokollierungsverfahren muss Art, Umfang und Dauer des Protokollierungszwecks beschränken. In der technischen Ausgestaltung und Auswahl ist das Gebot der Datenvermeidung und -sparsamkeit zu befolgen und die Möglichkeiten der Anonymisierung und Pseudonymisierung zu berücksichtigen.[13]

---

[12] Vgl. BDSG, 2018, §76.

[13] Vgl. https://www.baden-wuerttemberg.datenschutz.de/technik/orientierungshilfe_protokollierung_ak_technik_/ (Stand 07.09.2019)

Das Verfahren der Verarbeitung personenbezogener Daten soll durch den Zweck der Protokollierung transparent gemacht werden. Damit soll ein Verstoß gegen die Verarbeitung personenbezogener Daten vermieden werden und die Ordnungsmäßigkeit der Verarbeitung nachgewiesen werden können. Da es gesetzliche Anforderungen an die Protokollinhalte gibt muss ersichtlich sein, wer wann welche Daten verarbeitet hat. Protokolldaten müssen zweckgebunden, vollständig und datensparsam eingerichtet werden, um den allgemeinen Anforderungen an Datenschutz und Datensicherheit, sowie einer Beweissicherheit und Revisionssicherheit zu genügen. Dabei ist eine automatisierte Leistungs- und Verhaltenskontrolle von Mitarbeitern auszuschließen. Im Protokoll sind die Person, ein Zeitbezug und die durchgeführte Tätigkeit korrekt zu dokumentieren. Um einen bestmöglichen Ausgleich des Konflikts zwischen Vollständigkeit und Datensparsamkeit zu finden, muss der Konflikt vor dem Hintergrund der verfahrensspezifischen Bedingungen betrachtet werden. Die erhobenen Protokolldaten müssen manipulationssicher gespeichert sein und dürfen nur Berechtigten zugänglich sein. Durch geeignete Tests ist die ordnungsgemäße Funktion des Verfahrens sicherzustellen.[14]

In der Praxis ist dies durch den PDCA[15]-Zyklus leicht zu realisieren. Dabei wird in der Planungsphase (Plan) geschaut welche Aktionen protokolliert werden müssen. Anschließend wird in der Do-Phase die Aktion durchgeführt. In der Check-Phase wird das Ergebnis kontrolliert. Wenn alles korrekt protokolliert wurde, kann in der Act-Phase mit einer anderen Aktion weitergemacht werden, ansonsten ist der Zyklus zu wiederholen und die Logquelle anzupassen.

Die ordnungsgemäße Funktion ist regelmäßig, spätestens jedoch bei einer Änderung des Systems, erneut zu prüfen.[16] Gerade bei Hard- und Software ändern Hersteller oft Feldnamen von Protokollierungsereignissen, was bei einer weiteren Verarbeitung der Logdatei zu Fehlern führt. Je nach eingesetztem System für die Verarbeitung der

[14] Vgl. https://www.baden-wuerttemberg.datenschutz.de/technik/orientierungshilfe_protokollierung_ak_technik_/ (Stand 07.09.2019)

[15] PDCA steht für Plan, Do, Check, Act und beschreibt eine koordinierte und Lösungsfindung und –kontrolle, siehe auch BSI, 2008, S. 14.

[16] Vgl. https://www.baden-wuerttemberg.datenschutz.de/technik/orientierungshilfe_protokollierung_ak_technik_/ (Stand 07.09.2019)

Logdatei kann der fehlerhafte Protokolleintrag nicht in die Datenbank übernommen werden, was den Grundsätzen der Protokollierung widerspricht. Meldet das System nach einem Update weitere Felder, ist dies durch den Datenschutzbeauftragten auf die Ordnungsmäßigkeit der Datenverarbeitung zu prüfen und muss ggf. vom Beauftragten für die Protokollierung angepasst werden. Da in Protokollen Aktivitäten der Maschinen, Administratoren, Nutzer und Anwendern stehen, ist zwischen diesen zu unterscheiden. Da Administratoren besonderen Einfluss auf Strukturen eines IT-Systems ausüben können, ist deren Aktivität besonderer Kontrolle zu schenken. Mit dieser Berechtigung können üblicherweise Installationen, Deinstallationen, Konfigurationsänderungen und Rechteänderungen durchgeführt werden. Im Gegensatz zu administrativen Tätigkeiten, die der Systemüberwachung dienen, liegt der Fokus bei Benutzern auf einer Verfahrensüberwachung.

Da Protokolldaten sensible Daten enthalten, ist auf die Schutzziele der Informationssicherheit (Verfügbarkeit, Vertraulichkeit und Integrität) nach Stand der Technik zu achten. Der aktuelle Stand der Technik, wie es meist in Gesetztestexten oder ISO-Normen nachzulesen ist, wird nach der Drei-Stufen-Theorie festgelegt (siehe Abbildung 7). Hierbei wird der Stand der Technik von allgemein anerkannten Regeln der Technik (aaRdT) und dem „Stand der Wissenschaft und Forschung“ (SdWF) abgegrenzt.

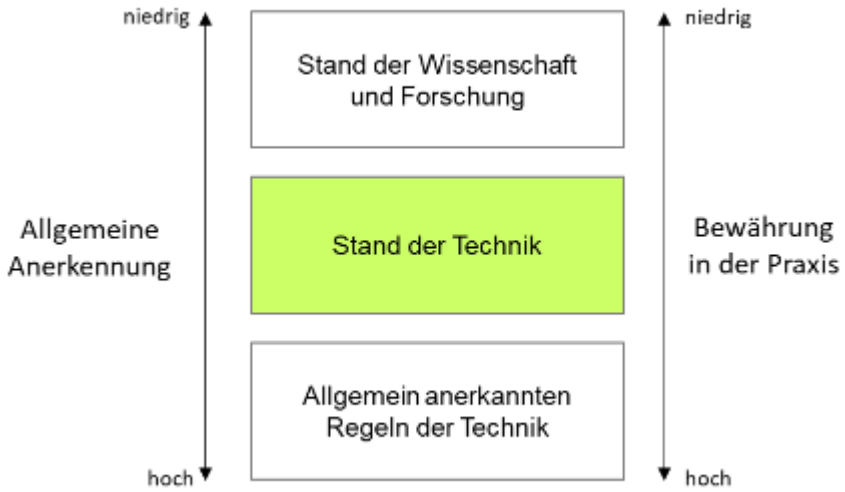


Abbildung 7: Drei-Stufen-Theorie nach Kalkar-Entscheidung[17]

[17] https://www.teletrust.de/fileadmin/docs/fachgruppen/2019-06_TeleTrusT_Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DEU.pdf (Stand 07.09.2019)

Der Stand der Technik ist zwischen dem innovativen Stand der Wissenschaft und Forschung und den allgemein anerkannten Regeln der Technik eingeordnet. Alle drei Technologiestände sind dem Konflikt der allgemeinen Anerkennung und der Bewährung in der Praxis ausgesetzt. Da die Systematik der Gesetze eine Unterscheidung zwischen objektiven und subjektiven Tatbestandsmerkmalen macht, ist der Stand der Technik rein objektiv zu verstehen.

Damit lässt sich sagen, dass der Stand der Technik als „die im Waren- und Dienstleistungsverkehr verfügbaren Verfahren, Einrichtungen oder Betriebsweisen, deren Anwendung die Erreichung der jeweiligen gesetzlichen Schutzziele am wirkungsvollsten gewährleisten kann“ bezeichnet werden kann.[18]

Neben diesen Anforderungen stellt das IT-Sicherheitsgesetz, das 2015 durch den deutschen Bundestag verabschiedet wurde, für Unternehmen kritischer Infrastrukturen eine weitere Anforderung dar.[19] Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ordnet nachfolgende kritische Infrastrukturen ein:

- Transport und Verkehr (inkl. Luftfahrt, Seeschifffahrt, Binnenschifffahrt, Bahn, Nahverkehr, Straße und Postwesen)
- Energie (Elektrizität, Kernkraftwerke, Gas und Mineralöl)
- Gefahrstoffe (Chemie und Biostoffe, Gefahrguttransport und Rüstungsindustrie)
- Informationstechnik und Telekommunikation
- Finanz-, Geld- und Versicherungswesen (Banken, Versicherungen, Finanzdienstleister und Börsen)
- Versorgungssektor (Gesundheit, Notfall- und Rettungswesen, Katastrophenschutz, Lebensmittelversorgung, Wasserversorgung und -entsorgung).[20]

Demnach sind diese Betreiber verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Informationssicherheit, also Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der Daten der verarbeitenden Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der kritischen Infrastrukturen wichtig sind. Auch hier muss der

[18] https://www.baden-wuerttemberg.datenschutz.de/technik/orientierungshilfe_protokollierung_ak_technik_/ (Stand 07.09.2019)

[19] Vgl. https://www.security-insider.de/was-ist-das-it-sicherheitsgesetz-a-644438/ (Stand 07.09.2019)

[20] Vgl. Greve, 2009.

Stand der Technik eingehalten werden. Ebenso sind organisatorische und technische Vorkehrungen angemessen zu treffen, die nicht außer Verhältnis zu den Folgen eines Ausfalls oder Störung der kritischen Infrastruktur stehen. Sollten die Anforderungen des BSI für Betreiber kritischer Infrastrukturen oder deren Branchenverbände nicht ausreichen, können branchenspezifische Sicherheitsstandards vorgeschlagen werden.[21]

Tritt bei einem Unternehmen, das zur kritischen Infrastruktur zählt, eine IT-Störung auf, muss geprüft werden, ob das Problem mit Maßnahmen nach Stand der Technik abgewehrt werden konnte. War es lediglich eine gewöhnliche IT-Störung wie ein Hardwareausfall, ein Festplattenfehler, SPAM oder gewöhnliches Phishing ist keine Meldung an das BSI nötig. Sollte es jedoch eine außergewöhnliche IT-Störung sein, ist das BSI unverzüglich, also ohne schuldhaftes Zögern, zu informieren.

Bei einer erheblichen IT-Störung nach §8b Ab. 4 Nr. 2 BSIG ist die Störung dann erheblich, wenn:

- Es immer weiterführende negative Auswirkungen bei einer Nicht-Behandlung gibt
- Weitere Ressourcen (Personal und Mittel) eingesetzt werden müssen, die über die Aufwände des normalen Regelbetriebs hinausgehen
- Die Behandlung durch spezielle Incident-Responder durchgeführt werden muss
- Wichtige IT-Systeme oder Komponenten isoliert oder abgeschaltet werden müssen, um weiteren Schaden zu verhindern
- Der Bewältigungszeitraum eine Änderung der Betriebsprozesse erfordert
- Ein höher finanzieller Schaden verursacht wird
- Ein vermuteter Advanced Persistent Threat (APT) vermutlich vorliegt und das Unternehmen somit Ziel eines neuartigen und außergewöhnlichen Angriffs ist
- Besondere Berufspflichten für solche IT-Störungen gegenüber der Unternehmensleitung vorliegen.[22]

[21] Vgl. https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html (Stand 09.09.2019)

[22] Vgl. https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/FAQ/FAQ_zur_Meldepflicht/faq_meldepflicht_node.html (Stand 07.09.2019)

2.2 Zugang, Zutritt und Zugriff

Der Zutritt und dementsprechend eine Zutrittskontrolle verhindern das ungewollte Betreten eines Unternehmens oder einer datenverarbeitenden Anlage.[23] Hiermit sind also physische Barrieren gemeint, die Unbefugten den Zutritt durch Maßnahmen wie Mauern, Türen, Fenster, einen Sicherheitsdienst oder weitere technische Zutrittskontrollsysteme verwehrt. In der Praxis gibt es die Möglichkeit über einen Fingerabdruck, Iris- oder Venenscan, Gesichtserkennung oder weitere Merkmale eine Person zu identifizieren und entsprechend einer hinterlegten Berechtigungsmatrix den Zutritt auf gewisse Räume zu beschränken.

Beim Zugang bzw. der Zugangskontrolle hat der Nutzer also schon die Möglichkeit bis an datenverarbeitende Systeme, was Systeme jeglicher Art mein, zu gelangen. Zugangssysteme müssen also für eine Sicherheit durch Passwortschutz, Passwortrichtlinien, biometrische Verfahren, PIN-Verfahren und weitere Möglichkeiten sorgen, um die Sicherheit der Systeme abzusichern.[24]

Die Zugriffskontrolle sorgt dafür, dass nur die Personen auf Daten zugreifen können, die dazu auch berechtigt sind. Die Berechtigung und ein entsprechendes Berechtigungskonzept sollen dafür sorgen, dass personenbezogene Daten bei der Verarbeitung vor unbefugten Zugriffen geschützt sind.

2.3 Innentäter versus Außentäter

Wie bereits in der Einleitung erläutert, verfügen Unternehmen über sensible Unternehmensdaten, die schützenswert sind und vor missbräuchlichem Gebrauch bewahrt werden müssen. Werden Angriffsmöglichkeiten auf diese analysiert, kann der Angriff von innerhalb des Unternehmens, oder von außerhalb erfolgen. Dementsprechend erfolgt eine Unterteilung der Täter auf Innen- und Außentäter. Unternehmen bestehen aus Mitarbeitern, die für das Unternehmen arbeiten oder Dienstleistern, die über Verträge für das Unternehmen arbeiten. Werden dolose Handlungen durch diesen Personenkreis durchgeführt, werden diese als Innentäter

[23] Vgl. Mühlich, 2019.

[24] Vgl. ebd.

bezeichnet. Im Gegensatz dazu gibt es externe Dritte, die nicht für das Unternehmen arbeiten. Hiermit kann beispielsweise ein Hacker gemeint sein.

Im Vergleich zu Außentätern, die dementsprechend nicht für das Unternehmen arbeiten, genießen Mitarbeiter oder Dienstleister einen Vertrauensbonus, den Fremde nicht haben. Innentäter verfügen meist über Zugangs- und Zutrittsmöglichkeiten in das Unternehmen. Somit sind Angriffe auf die DV-Anlagen[25] allein durch den Informationsvorsprung deutlich einfacher, als von Personen außerhalb des Unternehmens.

Im Leipziger Verlaufsmodell für wirtschaftskriminelles Handeln werden drei Stufen beschrieben. Der Mitarbeiter steht vor einer Situation, die potenziell ausnutzbar ist. In der ersten Stufe kann es sein, dass der Mitarbeiter die Situation nicht erkennt und demnach auch die Tat nicht ausführen kann. Erkennt er die Situation, kann in Stufe zwei die Sicherheitslücke melden und beheben (lassen). Wird die Sicherheitslücke nicht behoben, kann der Mitarbeiter die Situation ignorieren oder ausnutzen.[26]

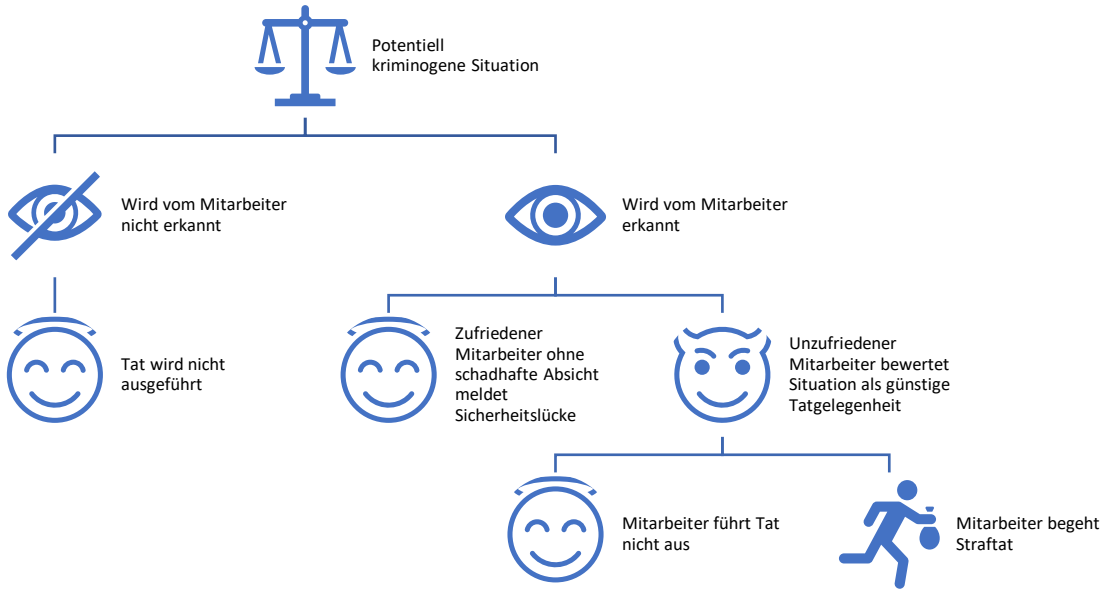


Abbildung 8: Leipziger Verlaufsmodell wirtschaftskriminellen Handelns (eigene Darstellung in Anlehnung an Schneider 2019)[27]

Kommt es zu Schäden durch Innentäter, werden meist folgende Szenarien unterschieden:

[25] DV-Anlagen = Datenverarbeitende Anlagen, also alle Systeme wie Server, Computer, Client, Smartphone, NAS, …

[26] Vgl. Schneider, 2019

[27] Vgl. ebd.

- Beeinträchtigung von IT-Infrastrukturen, z. B. durch Ransomware
- Datenverluste von Kundendaten
- Datenverluste geistigen Eigentums
- Betrugsversuche
- Manipulation von Produktions- und /oder Qualitätssicherungssystemen (Sabotage).[28]

Die große Schwierigkeit bei der Erkennung von Datendiebstahl oder Datenmanipulation ergibt sich aus der Tatsache, dass auch berechtigte Zugriffe auf Dokumente im Rahmen der Arbeitstätigkeit erfolgen können und eine Differenzierung zwischen normalem und schadhaftem Verhalten somit schwer ist.

Neben berechtigten Datenzugriffen können Innentäter auch durch missbräuchlich erlangte Zugriffsmöglichkeiten oder durch Fehler in der Sicherheitsarchitektur auf Systeme zugreifen.[29]

Angriffe von Innentätern sind meist schon wegen augenscheinlich berechtigter Datenzugriffe, missbräuchlich erlangter Berechtigungen oder durch Fehler in der Sicherheitsarchitektur schwer zu erkennen.

2.4 Dolose Handlungen

Handlungen, die für das Unternehmen schadhaft sind, werden als dolose Handlungen bezeichnet. Dabei können es Handlungen sein, die eine direkte schadhafte Wirkung auf das Unternehmen haben, oder auch Handlungen, die indirekt Schaden verursachen. Hiermit kann z. B. ein Image- oder Kundenschaden gemeint sein.[30]

Im Fokus doloser Handlungen steht der Zweck der persönlichen Bereicherung. Hierunter fallen Straftatbestände und Delikte aus der Wirtschaftskriminalität, denen Diebstahl, Betrug, Untreue, Urkundenfälschung, Unterschlagen und Computerkriminalität unterliegen.

Bei eigenen Fällen konnten z. B. ein doppeltes Buchhaltungssystem aufgedeckt werden, das genutzt wurde, um den Innentätern Millionenbeträge Firmengeld auf das eigene Konto zu überweisen und Wirtschaftsprüfer und Banken jahrelang zu betrügen.

---

[28] Vgl. Bartsch, 2018 S. 75.

[29] Bartsch 2018, S. 75.

[30] Vgl. http://www.forum-wirtschaftskriminalitaet.org/einfuehrung/begriffe/dolose-handlungen.html (Stand 13.07.2019)

Geistiges Eigentum gehört zu den Kronjuwelen jedes Unternehmens. Dieses gilt es vor unberechtigtem Zugriff zu schützen, um somit auch die meist jahrelange Arbeit und den Fortbestand des Unternehmens zu sichern.

Das geistige Eigentum kann als immaterieller Vermögenswert, ebenso als Ergebnis einer zufälligen, oder infolge zielstrebiger geistiger Anstrengungen gesehen werden.[31]

Ein Beispiel für eine dolose Handlung nennt Rüdiger Hirsch im aktuellen Report zur Innentäterschaft. Hier führt er ein Beispiel einer Co-Geschäftsführerin an, die in alleiniger Verantwortung die Buchhaltung des Unternehmens führte und sich innerhalb von zwölf Jahren 750.000 € auf ihr privates Konto überwies, um ihre Kaufsucht zu befriedigen.[32]

2.5 Vorfall

Als Vorfall oder Incident werden außergewöhnliche Ereignisse bezeichnet, die meist negativ sind. Hierbei wird der Vorfall erst einmal wertneutral betrachtet, da dies entweder eine normale Betriebsstörung oder ein Systemeinbruch sein kann. Im Rahmen des Incident Response, also der Reaktion auf den Vorfall, muss anschließend geprüft werden, um was es sich tatsächlich handelt.[33]

Sicherheitsvorfälle müssen schnell erkannt und effizient bearbeitet werden, damit es keine größeren Schäden gibt, oder Schäden ganz vermieden werden können. Hierzu ist ein erprobtes und vorgegebenes Verfahren zur Behandlung von Sicherheitsvorfällen notwendig. Die Behandlung der Sicherheitsvorfälle wird oft als Security Incident Handling oder Security Incident Response bezeichnet.[34]

Ein Sicherheitsvorfall kann große Schäden für das Unternehmen oder die Institution haben und muss dementsprechend rechtzeitig erkannt oder gar vermieden werden.

Als Sicherheitsvorfall ist nicht nur ein Hackerangriff zu verstehen, sondern z. B. auch eine Fehlkonfiguration von Systemen, die es unberechtigten Dritten erlaubt, auf

[31] Mittelstaedt, 2018.

[32] Vgl. Brüss, 2019.

[33] Vgl. Geschonneck, Computer-Forensik 2014, S. 45.

[34] BSI, 2019, S. 315f.

Systeme zuzugreifen. Hacking, Malware, Zero-Day-Exploits, Advanced Persistent Threats sind hierbei nur ein paar Beispiele für einen Sicherheitsvorfall.[35]

Werden Systeme nicht regelmäßig aktualisiert oder Systemparameter sicherheitskritisch verändert, kann dies ebenso zu einem Verstoß interner Richtlinien führen wie eine Fehlhandlung eines Benutzers. Hierbei sind neben den internen Mitarbeitern auch Administratoren und externe Dienstleister gemeint.[36]

Ein ungeeigneter Umgang mit Sicherheitsvorfällen kann zu großen Schäden oder einer Katastrophe in Unternehmen führen. Beispiele hierfür können auffällige Einträge in Protokolldateien der Firewall sein, in der Anzeichen für einen Einbruchsversuch sind, oder Sicherheitslücken veralteter Systeme, die Angreifer ausnützen.[37]

Beispiele für nicht erkannte Sicherheitsvorfälle können folgende sein:

- Ein Benutzer hält eine langsame Internetverbindung in der Firma für normal, obwohl ein Schadprogramm im Hintergrund die Verbindung durch eine Umleitung verlangsamt.
- Ein Produktionsleiter bemerkt die heimlich geänderten Daten der Produktions- und Steuerungsanzeigesysteme nicht und wundert sich über seltsame Werte der SCADA-Steuerung.
- Nach einem Einbruchsdiebstahl in einer Filiale wird der Angriff als Beschaffungskriminalität abgetan, obwohl der Einbruch dazu genutzt wurde im an Notebooks mit vertraulichen Informationen und Zugangsdaten der IT-Systeme zu gelangen.[38]

Bei der Behandlung von Sicherheitsvorfällen ist es stets wichtig die Daten als Beweisspuren anzusehen und dementsprechend vorsichtig zu behandeln. Hierbei müssen die Daten vor unbeabsichtigter Manipulation geschützt werden.

Die Ziele nach einem tatsächlichen Vorfall sind in der Regel folgende:

- Erkennung der Methode oder der Schwachstelle, die zum Vorfall geführt haben könnte

[35] Vgl. BSI, 2019, S. 315f.

[36] Vgl. ebd.

[37] Vgl. BSI 2019, Seite 320f

[38] Vgl. ebd.

- Ermittlung des entstandenen Schadens
- Identifikation des Angreifers
- Beweissicherung für gerichtliche Zwecke.[39]

Zusammenfassend kann das Vorliegen eines Vorfalls mit einem BSI-Schaubild (Abbildung 9) veranschaulicht werden:

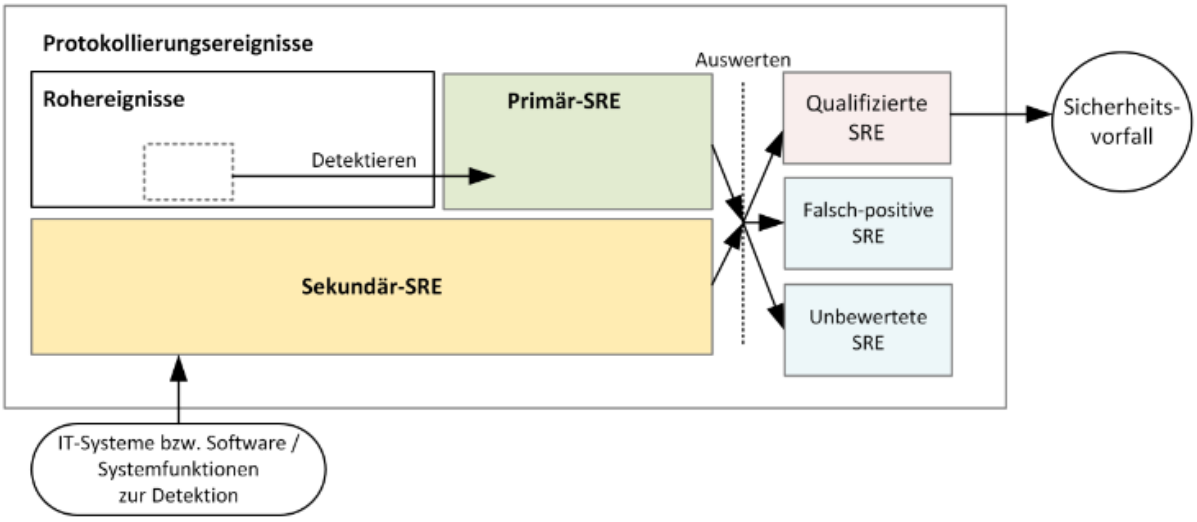


Abbildung 9: Mengendiagramm von Ereignissen[40]

Protokollierungsereignisse werden dabei in Rohereignisse, primäre Sicherheitsrelevante Ereignisse (SRE) und sekundäre SRE eingeteilt. Nach der Auswertung werden diese in qualifizierte SRE, falsch-positive-SRE und unbewertete SRE eigeteilt.

Rohereignisse sind Ereignisse, die selbst noch keinen Sicherheitsvorfall ergeben. Sobald weitere Kontextinformationen einfließen, kann ein eventueller Vorfall erkannt werden.

Primäre sicherheitsrelevante Ereignisse werden über verschiedene Verfahren zur Detektion erkannt und sind im Schaubild als „Primär-SRE“ gekennzeichnet. Diese beinhalten immer einen direkten Bezug auf einzelne oder mehrere Rohereignisse.[41]

False-positive SRE sind Ereignisse, die als Vorfall klassifiziert wurden, aber tatsächlich keine waren. Vergleichbar wie bei einem SPAM-Filter, der eine legitime Nachricht als

[39] Vgl. Geschonneck, Computer-Forensik 2014, Seite 65

[40] Vgl. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_Protokollierung_und_Detektion_Version_1_0.pdf?__blob=publicationFile&v=4 (Stand 05.09.2019)

[41] Vgl. ebd.

SPAM einordnet. Die Nachricht wird bei diesem Beispiel als schadhaft eingestuft, obwohl sie es gar nicht ist.

Qualifizierte SRE sind Ereignisse, die nach einer Prüfung durch einen Analysten als Sicherheitsvorfall eingestuft werden.

Unbewertete SRE sind SRE, die noch nicht bewertet wurden. Bei diesen ist bei einer Überlastung der Analysten auf eine Priorisierung zu achten, damit existenzbedrohende Vorfälle nicht „verschlafen“ werden.

2.6 Post-Mortem-Analyse

Bei der Post-Mortem-Analyse wird eine zuvor erstellte forensische Datensicherung nach einem Vorfall ausgewertet. Da die Daten bereits gesichert und nicht mehr flüchtig sind, können diese ohne Zeitdruck ausgewertet werden und ohne die Sorge dabei, wichtige Beweise zu vernichten. In der Praxis hat sich die Anfertigung einer Master- und Arbeitskopie bewährt. Wenn möglich sollte auch der Datenträger bis zur vollständigen Klärung weiterer juristischer Schritte nicht mehr benutzt werden.[42]

Damit die Analyse später auch gerichtsverwertbar ist, sollten nachfolgende Punkte bereits im Vorfeld geprüft werden:

- Akzeptanz: Methoden und Schritte der Analyse müssen in der Fachwelt beschrieben und allgemein akzeptiert sein.
- Glaubwürdigkeit: Die Funktionalität und Robustheit der Methoden gelten als Anforderung. Das Ergebnis muss nachvollziehbar und glaubwürdig sein.
- Wiederholbarkeit: Die Methoden und Hilfsmittel müssen bei einer Prüfung durch einen Dritten das gleiche Ergebnis liefern. Die Reproduzierbarkeit muss gegeben sein und mit gleichen Schritten das gleiche Ergebnis liefern.
- Integrität: Spuren dürfen nicht unbemerkt verändert werden. Deshalb ist eine Sicherstellung der Integrität z. B. durch einen Hashwert sicherzustellen. Die Ursprungsdaten dürfen nicht verändert werden.
- Ursache und Auswirkung: Die Methoden müssen nachvollziehbare Verbindungen zwischen Personen, Ergebnissen und Beweisspuren ermöglichen.

[42] Vgl. Geschonneck, Computer-Forensik 2014, S. 104f.

- Dokumentation: Jeder Prozessschritt muss angemessen dokumentiert sein.[43]

Bei der Post-Mortem-Analyse werden File Slacks, MAC-Time, NTFS-Streams, versteckte, gelöschte und unbekannte Dateien, sowie Systemprotokolle analysiert. Dabei wird im ersten Schritt versucht, so viele Beweisspuren wie möglich wiederherzustellen. Das bedeutet, dass neben den vorhandenen Dateien auch gelöschte Dateien wiederhergestellt werden, versteckte Dateien aufgefunden und wiederhergestellt werden und verschlüsselte Dateien entschlüsselt werden. Diese sind zwar nicht immer zu entschlüsseln, aber durch den Einsatz diverser Programme kann die Entschlüsselung ermöglicht werden. Programme für die forensische Untersuchung können durch einen erstellten Suchindex die Suche innerhalb der forensischen Kopie deutlich vereinfachen und ersparen dem Ermittler wertvolle Zeit. Hierbei ist wichtig, dass alle Bereiche indexiert werden, also auch der File Slack, unbelegte und belegte Bereiche, sowie Metadaten der Dateisysteme. Über Hashwerte kann ein Abgleich mit bereits bekannten Dateien ermöglich werden. Hierbei können White- oder Blacklist-Verfahren genutzt werden, um die zu untersuchenden Dateien einzuschränken. Beim File Carving werden alle lesbaren vorhandene Dateien oder auch gelöschte Dateien und Dateifragmente auf der forensischen Kopie wiederhergestellt. Über eine Dateikategorisierung können die Dateien weiter eingeschränkt werden. Liegt der Fokus der Untersuchung auf Bilddateien, können andere Formate exkludiert werden und ermöglichen dem Ermittler so eine kleinere zu untersuchende Datenmenge.[44]

Neben der reinen Analyse eines Datenträgers können auch weitere Systeme analysiert werden. In Firmen können wertvolle Informationen in Routern, Firewalls, Syslog-Servern, etc. gespeichert sein.

Damit eine forensische Datensicherung auch alle relevanten Daten enthält, sollte unbedingt auf eine logische Sicherung verzichtet werden.

Bei der Sicherung von DV-Systemen sollte grundsätzlich eine bit-für-bit Kopie erstellt werden, die anschließend nicht forensisch bearbeitet wird. Aus dieser Kopie ist eine Arbeitskopie zu erstellen. Für die Originalsicherung ist ein Hashwert der Datensicherung zu erzeugen, der die Integrität der Daten sicherstellt und es

[43] Vgl. Geschonneck, Computer-Forensik 2014, S. 67.

[44] Vgl. Geschonneck, Computer-Forensik, 2014, S. 105f.

sachverständigen Dritten erlaubt, die Unversehrtheit der Datensicherung zu bestätigen. Bei einem Papierstapel fällt ein fehlendes Blatt meist nicht auf, bei einem Hashwert wäre dies direkt erkennbar.[45]

2.7 Klassifikation von Informationen

Unternehmen müssen die Informationen, die sie haben, kennen und sich über deren Bedeutung im Klaren sein. Damit ein einfacher und sicherer Datenaustausch stattfinden kann, muss ein Klassifikationsschema für die Art der Information vorhanden sein. Dieses gibt in Abstufung die Wertigkeit der Information wieder und ermöglicht Mitarbeitern eine einfache Einstufung des Dokuments in die jeweilige Kategorie. Dabei sollte die Klassifizierung so einfach und übersichtlich sein, dass Mitarbeiter ohne großen Aufwand und ohne eine explizite Kennzeichnung, die korrekte Einstufung vornehmen können. Hier bietet sich die Erstellung der Klassifikation nach den Grundwerten der Informationssicherheit (Vertraulichkeit, Verfügbarkeit und Integrität) an.[46]

Zur Klassifizierung der Vertraulichkeit wird häufig zwischen offen, intern, vertraulich und streng vertraulich abgestuft. Die Verfügbarkeit kann beispielsweise die Zeit bis zur Wiederherstellung oder tolerierbare Ausfallzeit beziffern, also eine Stunde, ein Tag, ein Monat. Schwieriger wird es bei der Klassifizierung der Integrität. Hier kann eine Unterscheidung in essenziell, wichtig und normal getroffen werden. Kriterien können hier die mögliche Auswirkung auf einen Integritätsverlust sein, der für den Aufwand der Wiederherstellung der Integrität benötigt wird.[47]

2.8 Log-Management und SIEM

Aufgrund der zunehmenden Professionalisierung von Cyberangriffen und Vorschriften durch das IT-Sicherheitsgesetz, führen viele Unternehmen ein zentrales Log-Management ein, das Logdateien aller möglichen Systeme an einem zentralen Punkt zusammenführt und es anschließend einem Security Information and Event Management (SIEM) ermöglich, diese systematisch nach Angriffen zu durchsuchen.[48]

---

[45] Vgl. Klapproth, 2017, S. 325f.

[46] Vgl. Informationstechnik, 2017, S. 121f.

[47] Vgl. ebd.

[48] Vgl. Bartsch, 2018, S. 271f.

Eine zentrale Verwaltung von Logdateien ermöglicht es z. B. bei fehlgeschlagenen Anmeldungen einen gesamtheitlichen Zusammenhang zu bekommen. Während eine fehlerhafte Anmeldung an einem DV-System noch kein Grund zur Panik sein muss, ist die Situation ganz anders, wenn diese fehlerhafte Anmeldung zeitglich bei allen Systemen im Netzwerk geschieht. Eine zentrale Lösung hilft somit bei der Klärung wichtiger W-Fragen der Forensik. So lässt sich schon während eines Angriffs erkennen:

- Woher stammen die Anmeldeversuche?
- Welcher Benutzername wird dazu genutzt?
- Welche Systeme sind betroffen?
- Wann und wie lange erfolgten die Anmeldeversuche?

Ebenso können die Logdateien auch dazu genutzt werden, um die erfolgte Anmeldung und die anschließende laterale Bewegung im Netzwerk zu beobachten und nachzuvollziehen.

Durch verschiedene Einstellungen und die Detaillierung der Logdatei können so auch neu installierte Dienste, geänderte Registry-Einträge, neue Benutzer oder Benutzer höheren Privilegien, sowie ungewöhnliche Datei- und Netzwerkzugriffe schnell erkannt werden.

Bevor ein Unternehmen ein zentrales Log-Management und/oder eine SIEM-Lösung implementiert, sind davor einige wichtige Themen zu beachten. So sind neben den technischen Möglichkeiten und Herausforderungen auch datenschutzrechtliche Themen zu beachten. Demnach ist es ratsam, den Betriebsrat und den Datenschutzbeauftragten frühzeitig ins Boot zu holen und auch den Mitarbeitern gegenüber Prozesse transparent darzustellen.[49]

Bei der technischen Einführung eines zentralen Log-Managements sollte mit einer Hard- und Softwareinventarisierung begonnen werden, um auch sicherzustellen, dass alle relevanten Logquellen mit in die Implementierungsüberlegungen einfließen. Anschließen sollte überlegt werden, welche Log-Meldungen überhaupt relevant sind.

Damit ein zentrales Log-Management und ein SIEM korrekt funktioniert, muss in der Assetanalyse geprüft werden, welche Systeme und Programme relevant sind und

[49] Vgl. Bartsch, 2018, S. 271f.

welchen Inhalt diese liefern müssen. Neben Betriebssystemen wie Windows und Linux können Datenbanken, Applikationsserver, Webserver, Router, Switche, IDS, IPS, Antivirenscanner, Schwachstellenscanner und viele weitere wichtige Hinweise liefern.

Abbildung 10 zeigt, welchen Weg eine Logdatei beispielhaft beschreiten muss, um in einem zentralen Log-Management oder SIEM durchlaufen muss.

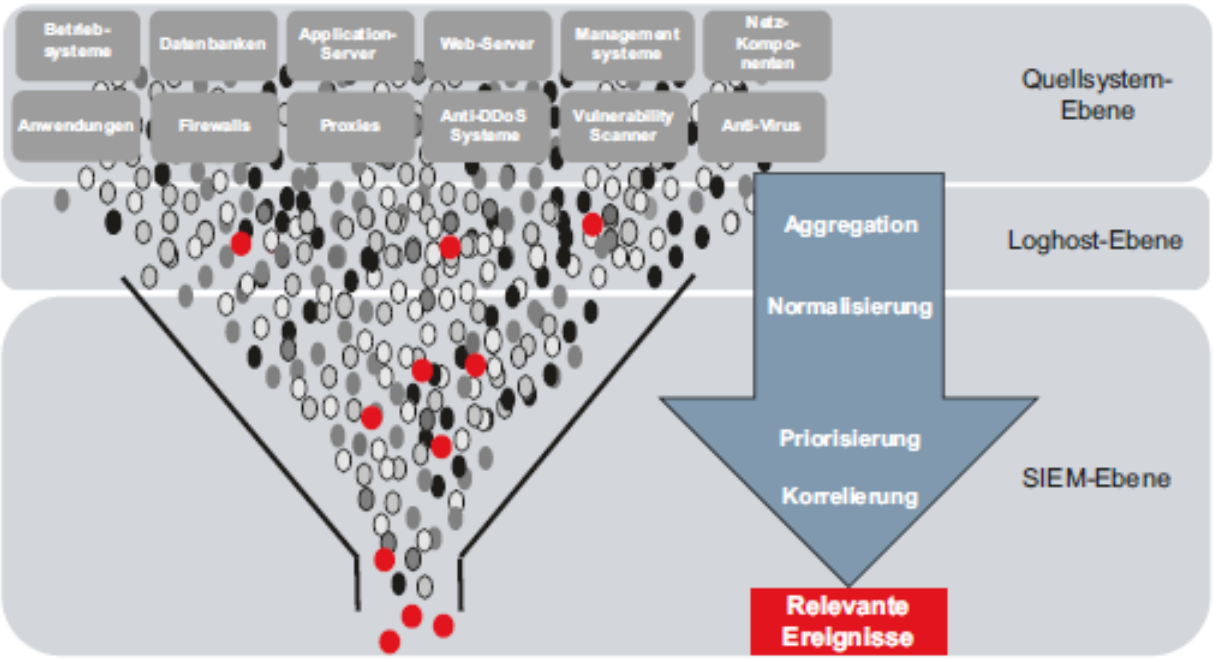


Abbildung 10: Zusammenspiel Log-Management und SIEM (schematische Darstellung)[50]

Aggregation

Bei der Aggregation werden verschiedene Einzelgrößen hinsichtlich eines gleichartigen Merkmals zusammengefasst, um daraus weitere Erkenntnisse und Zusammenhänge zu gewinnen.[51]

Normalisierung

Die Normalisierung beschreibt die Aufteilung von Daten in verschiedene Felder und Tabellen. Speziell bei Logdateien von unterschiedlichen Betriebssystemen und Applikationen können Daten wie IP-Adresse, Nachricht, Event-ID, etc. in unterschiedlichen Feldern gespeichert sein. Bei der Normalisierung werden z. B. alle Felder mit einer IP-Adressen eindeutig benannt, damit in der Datenbank keine Anomalie vorliegt. Im Vergleich zu relationalen Datenbanken, bieten NoSQL-

[50] Bartsch 2018, S. 276.

[51] Vgl. https://wirtschaftslexikon.gabler.de/definition/aggregation-30653 (Stand 03.09.2019)

Datenbanken wie Elasticsearch, die Möglichkeit an, dass Felder, die vorher nicht bekannt waren, übernommen werden. Über eine Konfiguration kann dieser „strict-mode“ angepasst werden.

Priorisierung

Da nicht jedes Ereignis gleichwertig ist, kann eine Priorisierung von Ereignissen oder auch von Systemen vorgenommen werden.

Korrelation

Die Korrelation misst die statistische Stärke einer Beziehung von zwei oder mehr Variablen zueinander.[52] Bei Ereignissen kann die Korrelation Beziehungen mehrerer Merkmale in Verbindung bringen und in Echtzeit Sicherheitsvorfälle erkennen. Fehlerhafte Anmeldungen des Anmeldeservers können mit erlaubten Zugriffen der Firewall korreliert werden, um zu erkennen, dass es einen Missbrauch bei einem externen Mitarbeiter-Account gibt.[53]

Wurden diese Schritte durchlaufen, kann eine Klassifizierung des Vorfalls vorgenommen werden.

3. Konzept

Um eine möglichst realistische Umgebung eines Unternehmens zu simulieren, wird im Versuch ein Netzwerk aufgebaut, das aus einem Fileserver, einem Proxy und einem Client besteht. Das komplette System wird in VMWare, einer Virtualisierungslösung, abgebildet.

Die Installation der einzelnen Systeme wird zur Reproduzierbarkeit der Ergebnisse dokumentiert und in der angehängten Systemdokumentation niedergeschrieben.

Bei der Installation wurde darauf geachtet, dass alle Systeme auf dem aktuellen Stand sind. Deshalb erfolgte nach jeder Installation ein Update.

Der Client soll und darf in diesem Versuchsaufbau mit dem Server kommunizieren und kann hier auch auf einzelne Ordnerfreigaben zugreifen. Über den Proxy ist ein Zugriff ins Internet möglich.

---

[52] Vgl. https://de.statista.com/statistik/lexikon/definition/77/korrelation/ (Stand 03.09.2019)

[53] Vgl. https://www.secupedia.info/wiki/SIEM (Stand 03.09.2019)

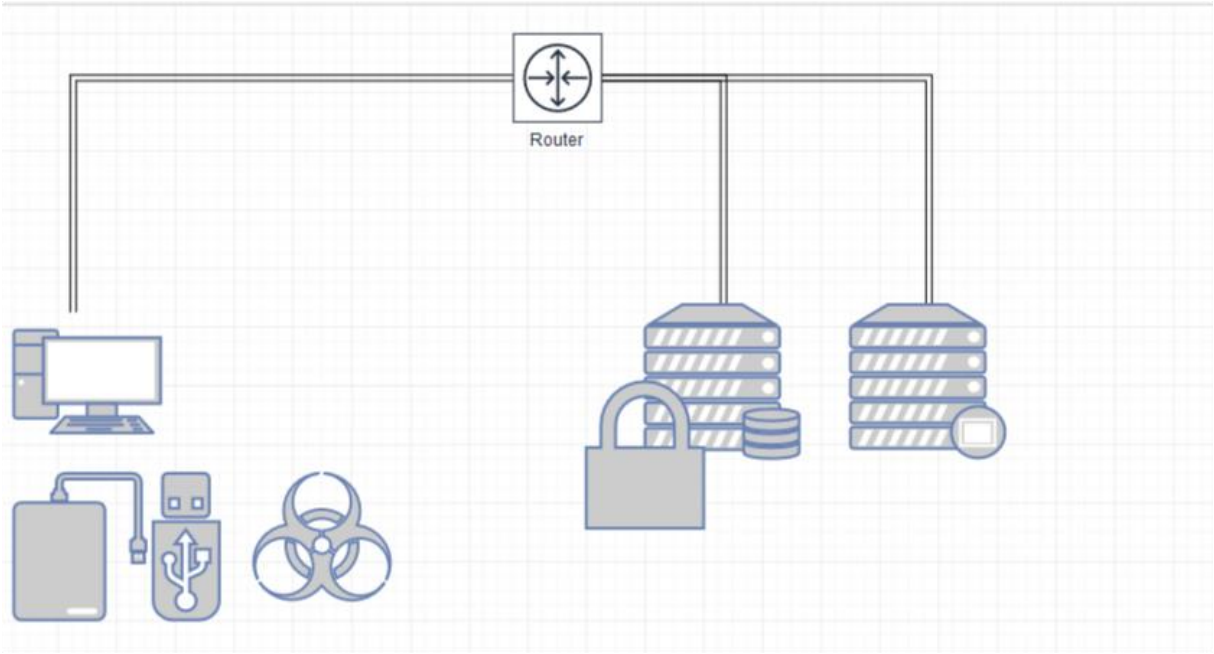


Abbildung 11: Versuchsaufbau vor Anpassung (eigene Darstellung)

Im ersten Versuch (siehe Abbildung 11) wird mit den Standardeinstellungen bzgl. des Logmechanismen bzw. Auditmechanismen ein Datendiebstahl simuliert. Bei dem Datendiebstahl wird ein USB-Stick an den Client angeschlossen und anschließend ein Datendiebstahl durchgeführt.

Nach dem erfolgten Datendiebstahl werden die virtuellen Maschinen forensisch analysiert und Spuren ausgewertet.

Nach erfolgter Auswertung wird der zweite Datendiebstahl über eine Schadsoftware durchgeführt, die Daten über das Internet an den Angreifer leitet. Auch hier wird nach erfolgtem Datendiebstahl eine forensische Analyse durchgeführt und die Spuren ausgewertet.

Nach der durchgeführten Post-Mortem-Analyse werden Maßnahmen zur Steigerung der Aufklärungsquote durchgeführt. Hier werden Empfehlungen von renommierten Firmen und Instituten berücksichtigt und eingearbeitet. Die Systeme werden an ein zentrales Log-Management angebunden und erneut getestet.

Beim zentralen Log-Management werden zwei Systeme eingesetzt. Eine Ubuntu-Installation mit nachinstalliertem ELK-Stack, bestehend aus Elasticsearch, Logstash und Kibana und einer bereits fertigen Lösung „Security Onion“.

Die Log-Daten der angebundenen Systeme (Client, Server und Proxy) werden direkt an beide Lösungen geschickt und können dort ausgewertet werden.

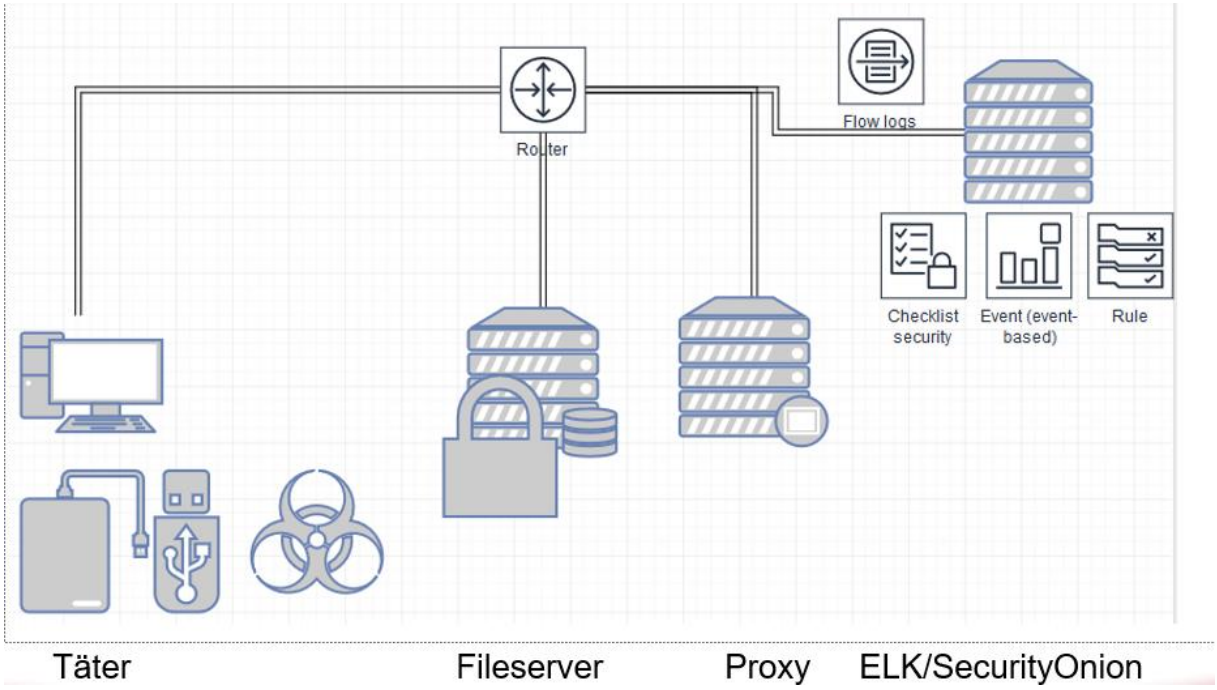


Abbildung 12: Versuchsaufbau nach Anpassung (eigene Darstellung)

Um den Datenverkehr zentral zu analysieren und zu filtern, wurde Endian Firewall Community-Edition als virtuelle Maschine installiert. Der Internetverkehr der anderen Systeme wird durch den Proxy geleitet und kann bei Bedarf gefiltert werden.

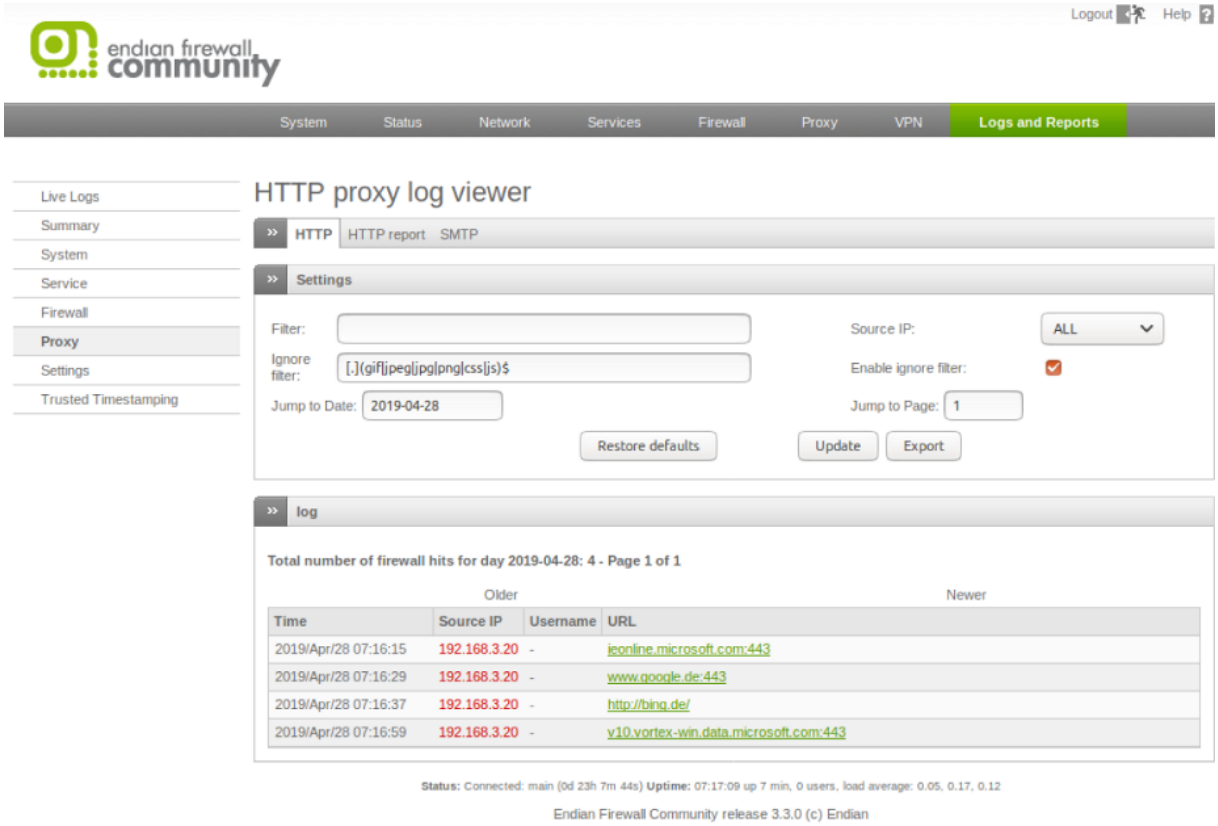


Abbildung 13: Endian Firewall mit aktiviertem Proxy (eigene Darstellung)

Die Endian Firewall-VM verfügt über drei Netzwerkkarten, wovon eine mit dem Internet verbunden ist. Die Netzwerkkarte (eth0), die mit dem Netzwerk des Versuchsaufbaus verbunden ist, hat keine direkte Verbindung in das Internet. Sämtlicher Verkehr aller virtuellen Maschinen muss somit über die Netzwerkkarte eth1 der Endian Firewall geroutet werden.

In der nachfolgenden Tabelle sind die installierten Systeme und deren Eigenschaften abgebildet:

Tabelle 2: Übersicht der Systeme (eigene Darstellung)

System (IP)	IP	Beschreibung	Benutzer
Endian Firewall	192.168.3.15 (eth0)	Firewall-Lösung mit integriertem Proxy und IDS	Admin
Ubuntu ELK	192.168.3.240	Ubuntu 18.04 mit installiertem ELK	ELK
Security Onion	192.168.3.241	Standard Security Onion-Installation	SO
Windows 2016	192.168.3.20	Windows 2016-Server mit Active-Directory und Netzwerkfreigabe	Administrator Mitglied in der AD
Windows 7	192.168.3.50	Innentäter-VM mit Netzlaufwerk *w:*, das auf Netzwerkfreigabe des Servers verweist.	Innen Mitglied in der AD

4. Forensische Lösungsansätze

In diesem Kapitel werden grundsätzliche forensische Lösungsmöglichkeiten zur Erkennung von Innentätern und Verhinderung von Datendiebstahl dargestellt und anhand von praktischen Beispielen, die während des Versuchsaufbaus gemacht wurden, beschrieben.

4.1 Post-Mortem-Analyse

4.1.1 Datei- und Ordnerzugriffe

Bei der Post-Mortem-Analyse werden Spuren von Datei- und Ordnerzugriffen in nachfolgenden Bereichen gesucht:

Open/Save MRU[54]

Beschreibung:

Eine der einfachsten Möglichkeiten in der forensischen Analyse ist die Überprüfung der MRU-Daten. Windows speichert beim Öffnen und Speichern von Daten über die Windows-Dialogbox den Namen der entsprechenden Datei. Da viele Anwendungen diese Dialogbox nutzen, können hier wichtige Spuren enthalten sein, die das Verhalten des Nutzers zeigen.

Speicherort

XP:

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\

OpenSaveMRU

Win7/8/10:

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\

OpenSavePIDlMRU[55]

Systeme, bei denen der Vorfall noch nicht lange her ist, können durch die MRU-Daten interessante Hinweise liefern. Hat der Innentäter über einen Windows-Dialog eine Datei geöffnet oder gespeichert, kann dies so schnell erkannt werden und weitere Hinweise für die Untersuchung liefern.

Recent Files – Zuletzt verwendete Dateien

Beschreibung:

Dieser Registry-Schlüssel zeigt die letzten Dateien und Ordner an, und wird meist auch im Startmenü angezeigt.

Speicherort

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

Beschreibung:

[54] Zuletzt aufgerufene Dateien (engl.= Most Recently Used)

[55] Vgl. http://www.forensicswiki.org/wiki/OpenSavePidlMRU (Stand 09.09.2019)

Zeigt bis zu letzte 150 Dateien oder Ordner an. Die Reihenfolge wird chronologisch abgespeichert.[56]

Im Versuchsaufbau wurde versucht eine Datei zu lesen (Lesen.txt), eine Datei zu manipulieren (Manipulieren.txt), zu kopieren (Kopieren.txt) und zu löschen (Löschen.txt). Bei der Analyse der Recent Files fällt auf, dass ersichtlich ist, dass die Freigabe des Servers (Netzlaufwerk w:\) geöffnet wurde, anschließend die Datei „Manipulieren.txt“ und danach die „Lesen.txt“. Die Dateien „Kopieren.txt“ und „Löschen.txt“ werden nicht angezeigt.

Tabelle 3: Auswertung der zuletzt verwendeten Dateien (eigene Darstellung)

Recent Files (3)	
Lesen.txt	Accessed before Manipulieren.txt Estimated access time before Mon May 20 11:30:16 CEST 2019
Manipulieren.txt	Accessed after Lesen.txt Accessed before Freigabe (\\server) (W:) Last access time Mon May 20 11:30:16 CEST 2019
Freigabe (\\server) (W:)	Accessed after Manipulieren.txt Last access time Mon May 20 11:30:16 CEST 2019

Windows-Taskleiste

Beschreibung

Die Windows Taskleiste erlaubt Benutzern den Schnellzugriff auf Programme und Dateien. Hierbei werden die zuletzt verwendeten Dateien in der Windows-Standardkonfiguration automatisch oben links angezeigt. Für jede Datei, die in der „Automatic Destinations“ gespeichert wird, existiert eine Anwendungs-ID und der Pfad, unter der die Datei aufgerufen wurde.

Speicherort

Win7/8/10:

C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

Beschreibung

Über ein Betrachter-Programm können die Daten ausgelesen werden. Jeder Aufruf wird mit einer separaten LNK-Datei numerisch und historisch abgespeichert. Der letzte Aufruf hat dabei die höchste Nummer.[57]

[56] Vgl. https://www.sans.org/security-resources/posters/windows-forensic-analysis/170/download (Stand 09.09.2019)

[57] Vgl. https://www.sans.org/security-resources/posters/windows-forensic-analysis/170/download (Stand 09.09.2019)

Shell Bags **Beschreibung** Über die Shell Bags können aufgerufene Ordner vom lokalen System, oder angeschlossenen Wechseldatenträgern oder Zugriffe von anderen Systemen nachvollzogen werden. Mit dieser Möglichkeit können auch gelöschte oder überschriebene Ordner nachgewiesen werden. **Speicherort** Explorer Zugriff: • USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags • USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU Desktop Zugriff: • NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU • NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags **Beschreibung** Speichert Informationen über die zuletzt aufgerufenen Ordner ab, die der Benutzer aufgerufen hat.

Tabelle 4: Auswertung der Shellbags (eigene Darstellung)

Shellbags (10) (Auszug)	
Computer	GUID 20d04fe0-3aea-1069-a2d8-08002b30309d Last Explored Mon May 20 14:21:21 CEST 2019 Sort Index 0x50 User Name innen
Computer\E:	Last Explored Mon May 20 11:53:44 CEST 2019 User Name innen
Computer\W:	User Name innen
	…

Bei der Auswertung der Shellbags kann nachgewiesen werden, dass der Benutzername „innen“, der Benutzername des Innentäters, auf das E-Laufwerk, den Wechseldatenträger, und das Laufwerk W: zugegriffen hat. Zudem kann nachgewiesen werden, dass der Benutzer den Ordner aufgerufen hat und von der Existenz des Ordners weiß. Da der Shellbag-Eintrag für jeden Benutzer in der eigenen

.dat-Datei generiert wird, kann der Aufruf zwischen verschiedenen Benutzern des Systems unterschieden werden.[58]

Shortcut (LNK) Files

Beschreibung

Die LNK-Dateien werden automatisch durch Windows generiert und zeigen die letzten Dateizugriffe auf lokale oder externe Dateien an.

Speicherort

XP:

• C:\%USERPROFILE%\Recent

Win7/8/10:

• C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\

• C:\%USERPROFILE%\AppData\Roaming\Microsoft\Office\Recent\

In obigem Speicherort werden lediglich die Hauptspeicherorte angezeigt. Darüber hinaus werden LNK-Dateien noch an anderen Orten gespeichert.

Beschreibung

Datum und Uhrzeit, zu der die Datei das erste Mal geöffnet wurde, wird in der Erstellzeit der Datei gespeichert. Der letzte Aufruf wird in der letzten Änderungszeit gespeichert.

Die internen LNK-Zieldateiinformationen (Internal LNK File Information) zeigen die MAC-Zeiten der Zieldatei an, Informationen über das Volume, also Name, Typ und Seriennummer, sowie Informationen über die Netzwerkfreigabe und das System.[59]

Prefetch

Beschreibung

Prefetching lädt Inhalte in den Speicher, bevor diese tatsächlich benötigt werden, um die Zugriffszeiten bei Bedarf zu erhöhen. Die Daten werden mit der Dateiendung .pf abgelegt und liefern für die Forensik wichtige Hinweise. Der Dateiname enthält den Namen der ausführbaren Datei, einen Bindestrich und anschließend acht Zeichen Hashwert. Wenn derselbe Dateiname in unterschiedlichen Ordnern vorhanden ist, werden verschiedene Hashwerte, und damit auch verschiedene Prefetch-Dateien erzeugt.

• Limitierung auf 128 Dateien bei XP und Win7

• Limitierung auf 1024 Dateien bei Win8-10.

Die Dateien werden in folgendem Format abgelegt: (Dateiname)-(hash).pf.

Speicherort

WinXP/7/8/10:

C:\Windows\Prefetch[60]

---

[58] Vgl. https://www.magnetforensics.com/blog/forensic-analysis-of-windows-shellbags/ (Stand 08.09.2019)

[59] Vgl. https://forensicswiki.org/wiki/LNK (Stand 09.09.2019)

[60] Vgl. https://forensicswiki.org/wiki/Prefetch und http://blog.digital-forensics.it/2015/06/a-first-look-at-windows-10-prefetch.html (Stand 09.09.2019)

Last-Visited MRU

Beschreibung

Verweist auf Programme, Dokumente, Netzwerkverzeichnisse und andere Orte, die zuletzt geöffnet wurden und erlaubt es dem Benutzer schnell auf die letzten Orte und Dateien zuzugreifen.[61]

Speicherort

XP:

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32

LastVisitedMRU

Win7/8/10:

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\[62]

IE|Edge file://

Beschreibung

Der Verlauf des Internet Explorers zeichnet Dateizugriffe auf lokale Dateien, Wechseldatenträger und Netzwerkfreigaben ist, und eignet sich damit als gutes Mittel für die forensische Analyse.

Speicherort

Internet Explorer:

• IE6-7:

%USERPROFILE%\Local Settings\History\ History.IE5

• IE8-9:

%USERPROFILE%\AppData\Local\Microsoft\Windows\History\History.IE5

• IE10-11:

%USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat

Beschreibung

Speichert index.dat-Einträge als: ***file:///C:/Verzeichnis/Dateiname.ext.*** Dies bedeutet jedoch nicht, dass diese Datei im Browser geöffnet wurde.[63]

Office Recent Files

Beschreibung

MS Office-Programme verfolgen ihr eigenes Verzeichnis der zuletzt geöffneten Dateien, um die es für Benutzer einfacher zu machen die zuletzt geöffneten Dateien zu finden.

Speicherort

NTUSER.DAT\Software\Microsoft\Office\VERSION

• 14.0 = Office 2010 • 11.0 = Office 2003

• 12.0 = Office 2007 • 10.0 = Office XP

NTUSER.DAT\Software\Microsoft\Office\VERSION\UserMRU\LiveID_####\FileMRU

[61] Vgl. https://forensicswiki.org/wiki/MRU (Stand 03.09.2019)

[62] Vgl. https://forensicswiki.org/wiki/List_of_Windows_MRU_Locations (Stand 03.09.2019)

[63] Vgl. https://forensicswiki.org/wiki/Internet_Explorer (Stand 06.08.2019)

• 15.0 = Office 365

Beschreibung

Ähnlich wie bei den zuletzt geöffneten Dateien, werden die letzten Dateien nachverfolgt, die von einer MS Office-Anwendung geöffnet wurden. Der zuletzt hinzugefügte MRU-Eintrag, ist der Zeitpunkt, zu dem die letzte Datei von einem bestimmten MS Office-Anwendung geöffnet wurde.

4.1.2 Spuren des Benutzers

In diesem Unterkapitel werden Möglichkeiten zur Erkennung von An- und Abmeldung an Systemen gezeigt, sowie Änderungen am Benutzeraccount.

In der Ereignisanzeige liefert eine erfolgte oder fehlerhafte An- und Abmeldung folgende Event-IDs:

Tabelle 5: Event-IDs von An- und Abmeldungen[64]

Event-ID	Beschreibung
4624	Erfolgreiche Anmeldung
4625	Erfolglose Anmeldung
4634|4647	Erfolgreich Abmeldung
4648	Anmeldung mit expliziten Anmeldeinformationen (Runas)
4672	Kontoanmeldung mit Superuser-Rechten (Administrator)
4720	Ein Konto wurde erstellt

Neben der Ereignisanzeige liefern nachfolgende Quellen weitere Spuren.

Login-Daten:

Letzte Anmeldung

Beschreibung

Listet die lokalen Benutzer und deren Daten auf.

Speicherort

• C:\windows\system32\config\SAM

• SAM\Domains\Account\Users

Beschreibung

Zeigt die letzte Anmeldung an. Anmeldungen in dem Active-Directory werden hier nicht aufgelistet.

Letzte Passwortänderung

Beschreibung

Zeigt die letzte Passwortänderung an.

[64] Vgl. https://www.sans.org/security-resources/posters/windows-forensic-analysis/170/download (Stand 09.09.2019)

Speicherort
• C:\windows\system32\config\SAM • SAM\Domains\Account\Users

Tabelle 6: Auswertung der angemeldeten Benutzer (eigene Darstellung)

User Accounts (3) (Auszug)	
Administrator	

Account expiration date	(not set)
Last failed login	Mon May 20 14:39:59 CEST 2019
	(never) (RegBack)
Last login date	Sun Nov 21 04:47:20 CET 2010
Login count	6
Password reset date	Sun Nov 21 04:57:24 CET 2010
Privilege level	Administrative user
Profile image path	C:\Users\administrator
RID unique identifier	500
SID	S-1-5-21-2084798845-2714014776-2354216658-500
User description	Vordefiniertes Konto für die Verwaltung des Computers bzw. der Domäne
User name	Administrator

Test

Account expiration date	(not set)
Last failed login	Sun Apr 28 08:59:25 CEST 2019
Last login date	Sun Apr 28 09:07:27 CEST 2019
Login count	5
Password reset date	Wed Mar 13 09:35:39 CET 2019
Privilege level	Administrative user
Profile image path	C:\Users\Test

	RID unique identifier: 1000 SID: S-1-5-21-4178458577-3565549689-3224368756-1000 User name: Test

In dieser Übersicht wird ersichtlich, dass der Benutzername des Innentäters nicht angezeigt wird, da dieser zentral durch die eingesetzte Active Directory verwaltet wird. Eine Anmeldung durch einen der lokalen Benutzer erfolgte zum „Tatzeitpunkt“, den 20.05.2019 nicht. In der Active Directory sind diese Anmeldungen nachvollziehbar.

Remote-Desktop

Beschreibung

Zeigt Anmeldungen mit dem Remote Desktop Protokoll (RDP) an.

Speicherort

Security Log

Win7/8/10:

%SYSTEM ROOT%\System32\winevt\logs\Security.evtx

Beschreibung

• Win7/8/10 – Beschreibung

- Event ID 4778 – Session Connected/Reconnected

- Event ID 4779 – Session Disconnected

Zeigt den Hostnamen und die IP-Adresse des Remote-Systems an. Bei Workstations und Servern wird häufig die Sitzung der Konsole beendet (Event-ID 4779) und anschließend die RDP-Verbindung aufgebaut (Event-ID 4778).

4.1.3 Externe Datenträger

Wenn externe Datenträger an Systemen eingesetzt und benutzt werden, kann das über nachfolgende Möglichkeiten herausgefunden werden.

USB-Geräte

Beschreibung

Zeigt eingesteckte USB-Geräte am System an.

Speicherort

• SYSTEM\CurrentControlSet\Enum\USBSTOR

• SYSTEM\CurrentControlSet\Enum\USB

Beschreibung

Hersteller, Produkt, Version, etc. sind hier erkennbar. Jedes USB-Gerät wird separat mit eigenen Identifikationsnummern ausgewiesen. Die Zeit, zu der das Gerät eingesteckt wurde, ist erkennbar.

USB-Geräte

Beschreibung

Bestimmt die zeitliche Verwendung bestimmter USB-Geräte, die mit einem Windows-Computer verbunden sind.

Speicherort *First Time*

Plug and Play Log Datei:

XP:

C:\Windows\setupapi.log

Win7/8/10:

C:\Windows\inf\setupapi.dev.log

Beschreibung

Ermöglicht die Suche nach einer Geräteseriennummer und der Uhrzeit.

Speicherort *First, Last, and Removal Times*

(Win7/8/10 Only)

System Hive:

\CurrentControlSet\Enum\USBSTOR\Ven_Prod_Version\USBSerial#\Properties

{83da6326-97a6-4088-9453-a19231573b29}**####*

0064 = First Install (Win7-10)

0066 = Last Connected (Win8-10)

0067 = Last Removal (Win8-10)

User

Beschreibung

Ermöglicht die Suche nach einem Benutzer, der das eindeutige USB-Gerät verwendet hat.

Speicherort

- **SYSTEM\MountedDevices**
- **NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2**

Beschreibung

Diese GUID wird als Nächstes verwendet, um den Benutzer zu identifizieren, der das Gerät angeschlossen hat. Das letzte Datum dieses Schlüssels entspricht auch dem letzten Einstecken des Geräts an das System durch diesen Benutzer. Auf die Nummer wird im persönlichen Mountpoints-Schlüssel des Benutzers in der NTUSER.dat verwiesen.[65]

PnP Events

Beschreibung

Wenn ein Plug and Play Gerät installiert wird, schreibt der PnP-Dienst ein Event 20001 in die system.evtx und liefert dabei einen Status mit.

Speicherort *System Logdatei*

Win7/8/10:

[65] Vgl. https://www.sans.org/security-resources/posters/windows-forensic-analysis/170/download (Stand 09.09.2019)

%system root%\System32\winevt\logs\System.evtx

Beschreibung

Event ID: 20001 – Plug and Play Treiberinstallation versucht

Zeitstempel

Geräteinformation

Geräteseriennummer

Status[66]

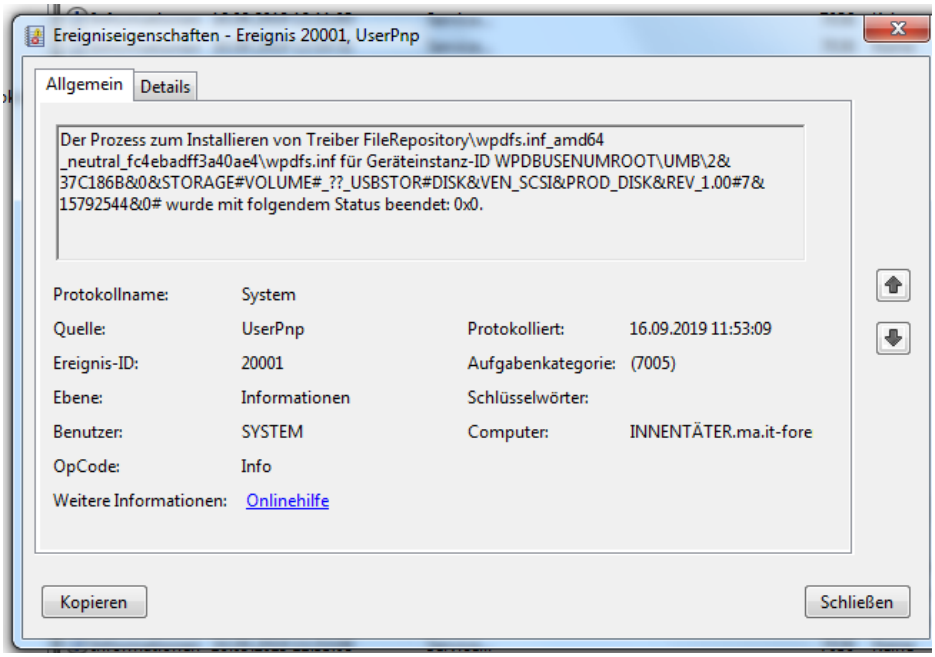


Abbildung 14: Nachweis der Treiberinstallation in Ereignisanzeige (eigene Darstellung)

Volume Serial Number

Beschreibung

Volume Serial Number der Dateisystempartition auf dem USB-Gerät. Entspricht nicht der auf dem Gerät fest kodierten Seriennummer!

Speicherort

SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ENDMgmt

Beschreibung

Wenn die Volume Serial Number und der Volume Name bekannt sind, kann eine Korrelation zwischen LNK-Dateien und den zuletzt verwendeten Dateien gemacht werden.

Drive Letter and Volume Name

Beschreibung

Zeigt den letzten Laufwerksbuchstaben an.

Speicherort

XP:

• Find **ParentIdPrefix** – **SYSTEM\CurrentControlSet\Enum**

[66] Vgl. https://www.sans.org/security-resources/posters/windows-forensic-analysis/170/download (Stand 09.09.2019).

USBSTOR

• Using **ParentIdPrefix** Discover Last Mount Point

– **SYSTEM\MountedDevices**

Win7/8/10:

• **SOFTWARE\Microsoft\Windows Portable Devices\Devices**

• **SYSTEM\MountedDevices**

- Examine Drive Letters looking at Value

Data Looking for Serial Number

Beschreibung

Identifizierung USB-Geräts, das zuletzt einem bestimmten Laufwerkbuchstaben zugeordnet wurde. Diese Technik funktioniert nur für das zuletzt zugeordnete Laufwerk. Es enthält keine historischen Aufzeichnungen für jeden Laufwerkbuchstaben, der einem Wechsellaufwerk zugeordnet wurde.[67]

Tabelle 7: Auswertung externer Datenträger (eigene Darstellung)

USB Mass Storage Devices (1)

SanDisk Cruzer Force USB Device	Class ID	Disk&Ven_SanDisk&Prod_Cruzer_Force&Rev_1.27
	Connect Date	Mon May 20 11:29:49 CEST 2019
	Connected by	innen
	Friendly Name	SanDisk Cruzer Force USB Device
	Last Assigned Drive Letter	E:
	Product ID	557D
	Serial Number	4C530012570128106055
	Vendor ID	0781 (SanDisk Corp.)
	Volume GUID	d9cfc69e-7091-11e9-8c72-c0b6f9fa088d
	Volume Name	Innentäter

[67] Vgl. https://www.sans.org/security-resources/posters/windows-forensic-analysis/170/download (Stand 09.09.2019)

Mit diesen Möglichkeiten kann nachgewiesen werden, dass der Benutzer des Innentäters einen SanDisk USB-Speicher benutzt hat, dem das Laufwerk E: zugewiesen wurde.

Seit Windows 10 werden im Security-Log neue Einträge für installierte Geräte erzeugt:

Tabelle 8: Neue Event-IDs in Windows 10[68]

Event-ID	Beschreibung
6416	Ein neues externes Gerät wurde vom System erkannt.
6419	Es wurde eine Anforderung zum Deaktivieren eines Geräts gestellt.
6420	Ein Gerät wurde deaktiviert.
6421	Es wurde eine Anforderung zum Aktivieren eines Geräts gestellt.
6422	Ein Gerät wurde aktiviert.
6423	Die Installation dieses Geräts ist durch die Systemrichtlinie verboten.
6424	Die Installation dieses Geräts wurde erlaubt, nachdem es zuvor durch die Richtlinie verboten worden war.

Shortcut (LNK) Dateien

Beschreibung

LNK-Dateien werden automatisch durch Windows generiert und speichern dabei die letzten Dateiaufrufe von Dateien ab. Hierbei spielt es keine Rolle, ob die Datei lokal abgespeichert wurde oder nicht. Dateien, die im Netzwerk aufgerufen wurden, können hier nachgewiesen werden.

Speicherort

XP:

• %USERPROFILE%\Recent

Win7/8/10

• %USERPROFILE%\AppData\Roaming\Microsoft\Windows\

Letzte Office-Dokumente:

• %USERPROFILE%\AppData\Roaming\Microsoft\Office\Recent

Beschreibung:

• Datum und Uhrzeit zu der die Datei das erste Mal geöffnet wurde

- Erstelldatum der LNK-Datei

• Datum und Uhrzeit zu der die Datei das letzte Mal geöffnet wurde

- Änderungsdatum der LNK-Datei

• LNK-Zieldatei (Internal LNK File

Information) Data:

- MAC-Zeiten der Zieldatei

- Volume Information (Name, Typ, Seriennummer)

[68] Vgl. https://www.forensicswiki.org/wiki/USB_History_Viewing (Stand 05.08.2019)

- Informationen über die Netzwerkfreigabe
- Original Speicherort
- Name des Systems

4.2 IDS/IPS

Ein Intrusion-Detection-System (IDS) zeigt Einbruchsversuche in Systeme anhand definierter Regeln an. Hierbei werden folgende IDS-Typen unterschieden:

- Hostbasierte Intrusion Detection System
- Netzwerkbasiertes Intrusion Detection System
- Hybrides Intrusion Detection System.

Im Gegensatz zu einem Intrusion Prevention System (IPS) meldet das IDS lediglich den Einbruchsversuch und wehrt dabei den Angriff nicht ab und kann diesen somit auch nicht verhindern. Je nach IDS-Typ ist die Software entweder direkt auf dem System installiert oder auf einem anderen Gerät. Beim hostbasierten IDS ist das IDS direkt auf dem zu überwachenden System installiert und prüft dort Dienste, Dateien und Zugriffe und kann anhand vorher definierter Regeln daraus Alarme ableiten. Das Netzwerkbasierte IDS liest alle Pakete im Netzwerk mit und versucht daraus Auffälligkeiten anhand definierter Regeln zu ermitteln und löst dann den Alarm aus. Das hybride System ist ein Mix aus beiden und bietet somit den besten Schutz. Der Netzwerkverkehr wird durch das netzwerkbasierte IDS durchleuchtet und der Host prüft sich selbst.[69]

4.3 Data-Leakage-Prevention

Aufgabe einer Data-Leakage-Prevention (DLP) ist es, den Abfluss von Informationen zu verhindern. Dabei muss diese im Unternehmen so implementiert sein, dass alle Informationen ausschließlich durch das DLP-System nach „außen“ gelangen können. Maßnahmen, mit dem das DLP-System die Funktionsfähigkeit sicherstellt, sind ganz klassische Wasserzeichen auf Dokumenten und das Prüfen von E-Mails nach Markierungen. Bei den Wasserzeichen und Markierungen erfolgt eine eindeutige Zuordnung zu einer Person, die die Daten durch das DLP-System geschleust hat.

[69] Vgl. https://www.security-insider.de/was-ist-ein-intrusion-detection-system-ids-a-612870/ (Stand 28.05.2019)

Somit kann auch im Falle einer Veröffentlichung von Dokumenten leicht nachvollzogen werden, wer diese Dokumente veröffentlicht hat.[70]

4.4 Zentrales-Log-Management und SIEM

Wie in der Einleitung erklärt, sind Logdateien eine Sammlung von Ereignissen, die ein datenverarbeitendes System in der Logdatei speichert. Viele dieser Ereignisse sind sicherheitsrelevant. Dies können Meldung der Firewall, des Antivirenprogramms, des IDS und natürlich auch von Servern, Workstations, Netzwerkgeräten oder Anwendungen sein.[71] Ein paar typische Anwendungsbeispiele für ein zentrales Log-Management sind folgende:

- Meldungen von Sicherheitsgateways hinsichtlich blockierter Verbindungsversuche
- Zentrale Sammelstelle für Warnmeldungen bei der Überschreitung von Datenkontingenten
- Archiv für forensische Untersuchungen nach einem Angriff auf IT-Systeme.[72]

Bei der Überwachung eines Informationsverbundes sind Quellen folgender Logdateien besonders relevant:

- Aktive Netzkomponenten (wie z. B. Router, Switche),
- Betriebssysteme,
- Applikationen und Dienste (wie Webserver, Mailserver, Fileserver),
- Sicherheitskomponenten im Netz (wie Firewall, Proxy, IDS),
- Sicherheitskomponenten auf Hosts (wie Sicherheitsgateways, Virus-Scanner),
- Physikalische Zutrittssysteme.

Die Anzahl und die Menge unterschiedlicher Logdateien sorgte dafür, dass Log-Management-Software entwickelt wurde, die Logdateien von der Erzeugung bis zur Verwertung verarbeitet.

---

[70] Vgl. Dörsam, 2017, S. 28.

[71] Vgl. https://csrc.nist.gov/publications/detail/sp/800-92/final (Stand 25.07.2019)

[72] Vgl. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b05/b05022.html?nn=6610630 (Stand 13.08.2019)

Die Logdateien werden dabei erzeugt, übermittelt, zentral gespeichert, analysiert und wieder entsorgt. Um Sicherheitsvorfälle erkennen zu können, müssen Logdateien eine Zeit lang gespeichert und auswertbar sein. Die zentrale Speicherung sorgt dafür, dass der Angreifer Spuren schlechter verwischen kann. Durch die regelmäßige Loganalyse können Sicherheitsvorfälle, Richtlinienverstöße, schadhafte Aktivitäten und operationale Probleme erkannt werden. Im Rahmen eines Audits oder einer forensischen Analyse können diese Logdateien herangezogen und ausgewertet werden. Da bei der Verwaltung von Logdateien einige Probleme auftreten können, sind Vertraulichkeit, Verfügbarkeit und Integrität der Logdateien stets zu beachten.[73] Bei der Verarbeitung der Logdateien ist darauf zu achten, dass Softwareänderungen dafür sorgen können, dass Logeinträge nach dem Update anders sind, oder Daten in anderen Feldern stehen. Ebenso muss dafür gesorgt werden, dass alle Systeme dieselbe Zeitquelle haben, damit eine spätere Korrelation möglich ist.[74] Zudem ist darauf zu achten, dass die Daten aggregiert und korreliert werden und aus diesen Daten Alarme ausgelöst werden. Bei einem Sicherheitsvorfall kann die Computerforensik mit den vorhandenen Protokolldateien den bereits aufgetretenen Sicherheitsvorfall rekonstruieren und daraus den entstandenen Schaden ermitteln.[75] Damit ein Unternehmen angemessen auf einen Sicherheitsvorfall reagieren kann, muss ein Alarmierungskonzept erstellt werden, das die Meldewege bei einem eingetretenen Sicherheitsvorfall genau beschreibt und so Personen informiert werden können, die über den Sicherheitsvorfall informiert sein müssen. Bei der Alarmierung sollte darauf geachtet werden, dass der Alarm nicht nur auf einer Management-Konsole angezeigt wird, sondern Alarme auch über E-Mail, SMS oder ein angebundenes Ticketsystem verschickt werden, damit schnellstmöglich auf den Vorfall reagiert werden kann.[76]

---

[73] Vgl. https://csrc.nist.gov/publications/detail/sp/800-92/final (Stand 25.07.2019)

[74] Vgl. https://csrc.nist.gov/publications/detail/sp/800-92/final (Stand 25.07.2019)

[75] Vgl. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02499.html?nn=6610630 (Stand 19.07.2019)

[76] Vgl. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02499.html?nn=6610630 (Stand 19.07.2019)

Planung der Protokollierung:

In der Vorbereitungsphase sollten alle Systeme identifiziert werden, die an das zentrale Log-Management angebunden werden sollen. Eine bereits vorhandene Hard- und Softwareinventarisierung kann hierbei überaus nützlich sein. Anschließend erfolgt eine Auswahl von Ereignissen, die zum Beispiel fehlgeschlagene Anmeldeversuche auf Systemen anzeigt. Anschließend kann die Anbindung erfolgen. Für die technische Umsetzung ist zu beachten, dass Logdateien unterschiedlichster Systeme Daten in unterschiedlichsten Formaten und Arten liefern. Deshalb ist eine Normalisierung nötig, die beispielsweise alle Datenfelder mit einem Zeitstempel oder einer IP-Adresse in ein einheitliches Format und in einheitliche Felder schreibt.

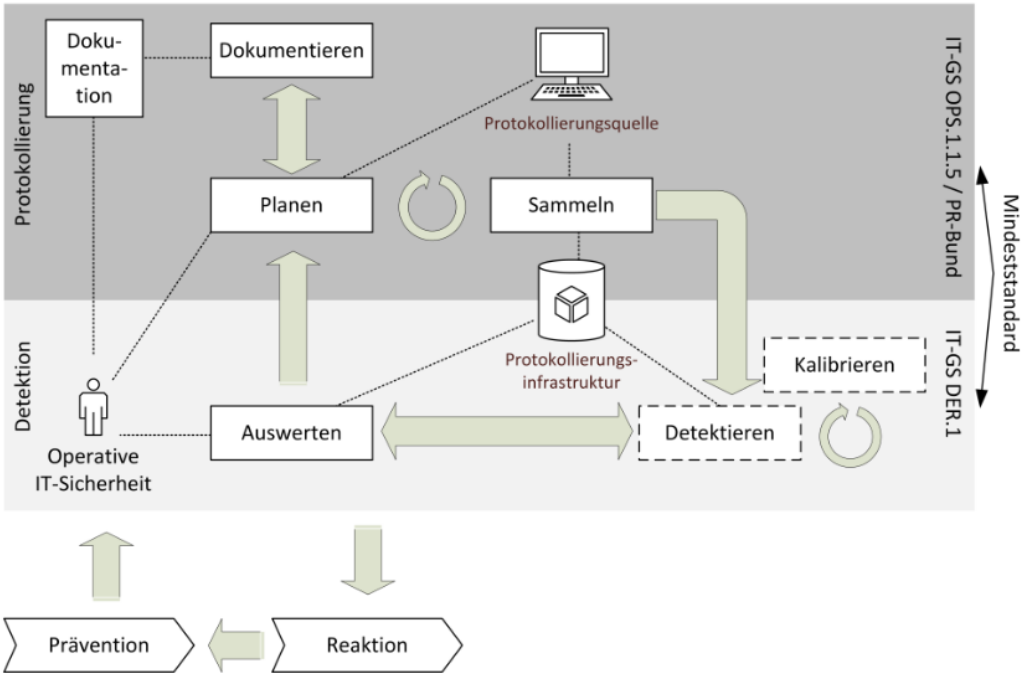


Abbildung 15: Prozesse der Protokollierung und Detektion (BSI)[77]

Erfolgt keine Normalisierung, sind die nachfolgenden Schritte der Filterung Aggregation, Kategorisierung und Korrelation schwierig bis unmöglich. Bei der Normalisierung werden Daten, die im Syslog-, SNMP-, Netflow-, IPFIX, MS-Eventlogformat oder sonstigen Formaten gemeldet werden in ein einheitliches Format gebracht. Über die Filterung können Ereignisse, die keinen sicherheitsmehrwert

[77] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_Protokollierung_und_Detektion_Version_1_0.pdf?__blob=publicationFile&v=4 (Stand 05.09.2019)

haben, bereits ausgeschlossen werden, bevor diese in der zentralen Datenbank abgespeichert werden.[78]

Das BSI beschreibt in den Mindeststandards zur Protokollierung die Abbildung 15. Ein Schritt, der bei dem BSI-Schaubild vergessen wurde, ist die Anreicherung (engl.: enrichment) von Daten, bei der zusätzliche Daten abgespeichert werden. Durch diese kann beispielsweise zu einer IP-Adresse noch eine Geolokation abgespeichert werden, die eine spätere Auswertung von Verbindungen erleichtert. Laut BSI-Grundschutzkatalog ist auf folgende Ereignisse besonders zu achten:

- Fehlgeschlagene Anmeldeversuche
- Sperrung von Benutzerkonten
- Anmeldung von Benutzern und Administratoren zu ungewöhnlichen Zeiten
- Ausfall oder Störung von Hardware
- Fehlfunktionen oder Überlastung von Software
- Netzauslastung und -überlastung
- Daten von Warn- und Informationssystemen wie dem Intrusion Detection System
- Zugriffe auf aktive Netzkomponenten.[79]

Da Protokolldaten sensible, datenschutzrelevante Daten enthalten können, sind besondere Punkte für den Datenschutz und die Archivierung zu beachten. Zur Mindestanforderung an die Protokollierung administrativer Aktivitäten gehören nachfolgende Punkte:

- Systemgenerierung und Modifikation von Systemparametern
- Einrichten von Benutzern
- Erstellung von Rechteprofilen
- Einspielen und Änderung von Anwendungssoftware
- Änderungen in der Dateiorganisation

---

[78] Vgl. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_Protokollierung_und_Detektion_Version_1_0.pdf?__blob=publicationFile&v=4 (Stand 05.09.2019)

[79] Vgl. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02500.html?nn=6610630 (Stand 19.07.2019)

- Durchführen von Datensicherungsmaßnahmen
- Sonstiger Aufruf von Administrations-Tools
- Versuche unbefugten Einloggens und Überschreitung von Befugnissen.[80]

Werden alle Protokolldaten zentral analysiert, können komplexe Zusammenhänge bei Betriebsstörungen oder Sicherheitsvorfällen erkannt werden.[81] Da es besonders in der Anfangsphase viele False-Positives, also Vorfälle gibt, die eigentlich gar keine sind, müssen Alarme und Fehlalarme gut dokumentiert werden. Ebenso lohnt sich ein Purple-Team-Assessment, bei dem sich Pentester (Red-Team) und IT-Sicherheitsexperten (Blue-Team) gemeinsam das System anschauen und so blinde Flecken im System aufdecken können. So kann eine Password-Spray-Attacke leicht als "blinder Fleck" erkannt und behoben werden. Das Center for Internet Security (CIS) befasst sich mit der Erstellung von Empfehlungen und Leitfäden zur IT-Sicherheit und empfiehlt für die Wartung, das Monitoring und die Analyse von Audit-Logs noch folgende Themen:

- Zeitquellen: Es sind mindestens drei synchronisierte Zeitquellen zu verwenden, damit die Zeitstempel bei allen Quellen konsistent sind.
- Audit-Funktion aktivieren: Es muss sichergestellt werden, dass das Logging bei allen (relevanten) Systemen und Geräten aktiviert ist.
- Detailliertes Logging aktivieren: Das erweiterte Logging bietet weiterführende Informationen zu Systemen wie Quell- und Zieladresse, Zeitstempel, Benutzer, und vieles mehr.
- Adäquate Speicherung von Logdateien: Alle Logdateien haben ausreichend Speicherplatz zur Datenspeicherung.
- Zentrales Log-Management: Alle relevanten Logdateien müssen aggregiert und im zentralen Log-Management analysiert werden.
- SIEM oder analytische Log-Tools: Bereitstellung eines Security Information und Event Management (SIEM) oder Loganalyse-Tool zur Log-Korrelation und -analyse.

---

[80] Vgl. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02500.html?nn=6610630 (Stand 19.07.2019)

[81] Vgl. ebd.

- Regelmäßiges Prüfen von Logdateien: Logdateien müssen regelmäßig geprüft und ausgewertet werden, um Anomalien zu erkennen
- Regelmäßiges prüfen und erweitern des SIEM: Daten müssen regelmäßig geprüft und ausgewertet werden, um wichtige Ereignisse besser filtern zu können.[82]

Das National Institute for Standards and Technology (NIST) empfiehlt darüber hinaus noch die Anbindung der VPN-Server, der Authentifizierungsserver (also z.B. den Active-Directory-Server).[83] Im Gegensatz zum zentralen Log-Management nimmt das SIEM nur sicherheitsrelevante Logdateien entgegen und verwertet diese. Das zentrale Log-Management kann zu einer Entlastung des SIEM führen, wenn es Events bereits vorfiltert und nur relevante Daten weiterleitet. Ein SIEM bietet noch zusätzliche Informationen wie den Indicator of compromise (IOC), Schwachstellen und zusätzliche Verkehrsdaten des Netzwerks.[84]

Die Abkürzung SIEM stellt eine Kombination von Security Event Management (SEM) und Security Information Management (SIM) dar und nutzt Verfahren des maschinellen Lernens und der künstlichen Intelligenz.[85] Bei der Implementierung von Firewalls und Systemaudits in ein SIEM, sorgen diese für eine große Menge von Ereignisdaten. Damit die großen Datenmengen auch zeitnah verarbeitet werden können, muss nach Engpässen gesucht werden, die dann behoben werden müssen. Wichtig hierbei ist, dass auch die Wirtschaftlichkeit beachtet werden muss.[86]

Bei der installierten Elastic-Stack-Lösung werden durch das SIEM die Anmeldungen der Systeme korreliert und können anschließend ausgewertet werden. Ein Test mit einem nicht existenten Benutzer „asd“ zeigt in Abbildung 16 direkt eine fehlerhafte Anmeldung des Innentäter-Clients mit der IP-Adresse „192.168.3.100“ an. Durch diese Funktion können Bruteforce-Attacken, bei denen Benutzer- und Passwortkombinationen getestet werden, direkt erkannt werden.

---

[82] Vgl. CIS Controls Version 7 Seite 22f

[83] Vgl. https://csrc.nist.gov/publications/detail/sp/800-92/final Stand 03.06.2019

[84] Vgl. https://www.t-systems.com/at/de/newsroom/blog/security/securityservices/zentrales-log-management-vs--siem-766564 Stand 03.06.2019

[85] Vgl. https://www.security-insider.de/was-ist-ein-siem-a-772821/ Stand 03.06.2019

[86] https://www.security-insider.de/siem-systeme-richtig-konfigurieren-und-einsetzen-a-357534/index5.html Stand 03.06.2019

Authentications

Showing: 5 Users

User	Successes	Failures	Last Success	Last Successful Source	Last Successful Destin...	Last Failure	Last Failed Source	Last Failed Destination
SERVER$	40	0	3 minutes ago	::1	Server	--	--	--
INNENTÄTER$	16	0	2 minutes ago	192.168.3.100	Server	--	--	--
Administrator	11	0	8 minutes ago	192.168.3.100	Server	--	--	--
ANONYMOUS-ANMELDUNG	2	0	13 minutes ago	192.168.3.100	Server	--	--	--
asd	0	2	--	--	--	2 minutes ago	192.168.3.100	Server

Abbildung 16: Anmeldungen in Elastic-SIEM (eigene Darstellung)

Da sich in einem üblichen Geschäftsbetrieb gewisse Kennzahlen für Anmeldungen und fehlerhafte Anmeldungen schätzen lassen, kann über ein Dashboard ein direkter Vergleich zwischen erfolgreichen und fehlerhaften Anmeldungen gemacht werden (siehe Abbildung 17).

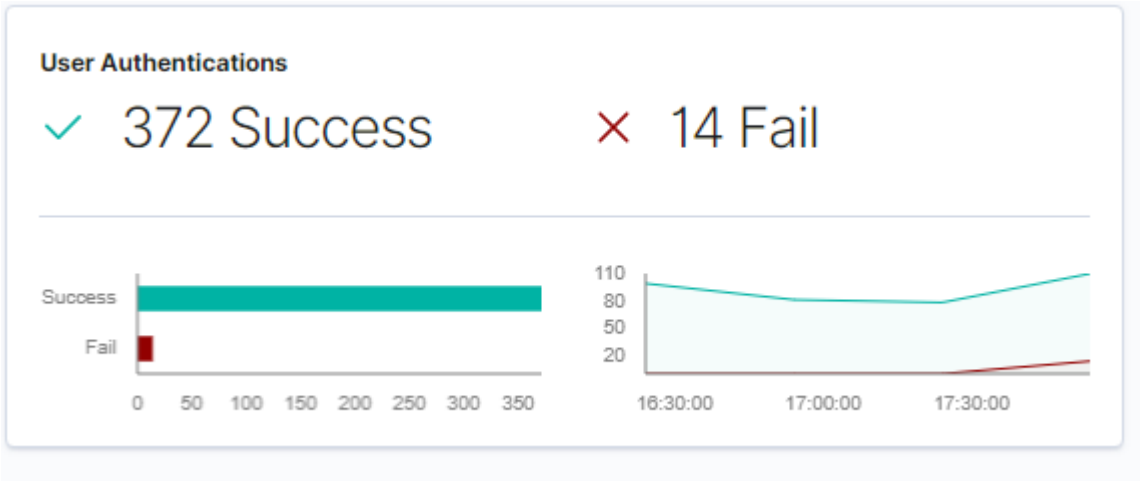


Abbildung 17: Vergleich erfolgreiche und fehlerhafte Anmeldungen in ELK-Dashboard (eigene Darstellung)

Werden Programme benutzt, die in einem normalen Geschäftsbetrieb keine Verwendung finden, können diese über die ungewöhnlichen Prozesse direkt erkannt werden. Bei der Implementierung eines zentralen Log-Managements oder eines SIEMs, können False-Positives auftreten, die jedoch nach einer Kontrolle durch einen Analysten im System eingepflegt werden können. Diese Prozesse werden anschließend nicht mehr als ungewöhnliche Prozesse im System angezeigt.

Uncommon Processes

Showing: 35 Processes

Name	Number of Hosts	Number of Instances
FastTray.exe	1	1
GoogleChromePortable.exe	1	1
SearchIndexer.exe	1	1
auditbeat.exe	1	1
wmpnetwk.exe	1	1
FastProxy.exe	1	2
SearchFilterHost.exe	1	2
SearchProtocolHost.exe	1	2
VGAuthService.exe	1	2
VSSVC.exe	1	2

Rows: 10

Abbildung 18: Ungewöhnliche Prozesse in Elastic-SIEM (eigene Darstellung)

Da sämtliche Ereignisse der Systeme zentral gespeichert werden, kann eine Übersicht der verschiedenen Aktionen generiert werden. Dies ermöglicht einen schnellen Überblick über die verschiedenen Meldungen der angebundenen Systeme (siehe Abbildung 19).

Events

Showing: 343.246 Events

Timestamp	Host Name	Module/Dataset	Event Action	User
Sep 16, 2019 @ 11:06:21.382	Server	--/--	Filterplattformverbindung	--
Sep 16, 2019 @ 11:06:21.157	INNENTÄTER	--/--	Sensible Verwendung von Rechten	--
Sep 16, 2019 @ 11:06:20.973	INNENTÄTER	--/--	Filterplattformverbindung	--
Sep 16, 2019 @ 11:06:20.973	INNENTÄTER	--/--	Filterplattformverbindung	--
Sep 16, 2019 @ 11:06:20.656	INNENTÄTER	--/--	Sensible Verwendung von Rechten	--
Sep 16, 2019 @ 11:06:20.596	Server	--/--	Filterplattformverbindung	--
Sep 16, 2019 @ 11:06:20.226	INNENTÄTER	--/--	Filterplattformverbindung	--

Abbildung 19: Ereignisse der verschiedenen Systeme (eigene Darstellung)

Da das Log-Management und ein SIEM Gemeinsamkeiten und Unterschiede haben, zeigt Tabelle 9 einen Vergleich beider Systeme.

Tabelle 9: Vergleich Log-Management und SIEM[87]

	Log-Management	**SIEM**
Was:	Sammeln und Auswerten von Logdaten in Echtzeit	
Nutzer:	Technisches Personal	Management
Anwendung:	Datenanalyse und Fehlersuche	Sicherheitsmonitoring, Vorfälle erkennen, Compliance-Nachweis (ISO27001)
Logquelle:	Ausgewählte Anwendungen	Alle sicherheitsrelevanten Logdateien, System- und Anwendungsebene
Technische Optimierung:	-	Zuverlässigkeit des Systems, strenge Klassifizierung und Normalisierung
Organisatorische Prozesse:	Agil, Nutzung bei Bedarf	Benötigt neue IT-Sicherheitsprozesse für Vorfallbehandlung

[87] Vgl. https://blog.to.com/log-management-vs-siem-gemeinsamkeiten-und-unterschiede/ (Stand 20.09.2019)

5. Maßnahmen zur Steigerung der Aufklärungsquote

5.1 Grundlagen

In diesem Kapitel werden Maßnahmen und Grundlagen zur Steigerung der Aufklärungsquote beschrieben.

5.1.1 Erkennung von Datendiebstahl

Unter Diebstahl wird heimliches Entwenden fremden Eigentums verstanden. Unter Entwenden versteht der Duden die Ausnutzung einer Gelegenheit Dinge unbemerkt wegzunehmen und (mühelos) an sich zu bringen bzw. stehlen.[88] Stehlen wiederum bedeutet, dass fremdes Eigentum, also etwas, was einem nicht gehört, heimlich, unbemerkt an sich zu nehmen und in seinen Besitz zu bringen[89]. Besitz wiederum ist die tatsächliche Herrschaft über eine Sache.[90]

Zumindest laut allgemeiner Definition wäre demnach ein Datendiebstahl ein unbemerktes, heimliches entwenden von einer Sache, um anschließend diese im Besitz und damit die tatsächliche Herrschaft darüber zu haben.

Da Daten bei einem Kopiervorgang dupliziert werden, und somit mehrfach vorhanden sind, kann sich hier der Besitz der „Sache“, also der Daten trennen. Kopiert ein Innentäter Daten auf einen USB-Stick sind diese auf der Quelle, zum Beispiel der lokalen Festplatte, vorhanden und auf dem USB-Stick. Lässt der Innentäter die Daten auf der lokalen Festplatte hat der Innentäter im Nachgang die Daten des USB-Sticks in seiner „Gewalt“ und ist damit der Besitzer dieser Daten.

Im Vergleich zu einem normalen, dinglichen Diebstahl, liegt hier der Unterschied, dass Daten anschließend mehrfach vorhanden sein können. Zumindest, wenn die Daten lediglich kopiert und nicht gelöscht oder verschoben werden.

Da Windows, wie im letzten Kapitel dargelegt wurde, zumindest im Standard den Kopiervorgang nicht nachweisen kann, sondern lediglich den Besuch des Ordners und die Installation bzw. die Zuweisung des Laufwerkbuchstabens zum USB-Stick, ist der

[88] Vgl. https://www.duden.de/rechtschreibung/entwenden

[89] Vgl. https://www.duden.de/rechtschreibung/stehlen>

[90] Vgl. https://wirtschaftslexikon.gabler.de/definition/besitz-27446

Datendiebstahl nicht erkennbar. Sobald die Windows-Auditmechanismen aktiviert werden, können wichtige Indizien gesammelt werden.

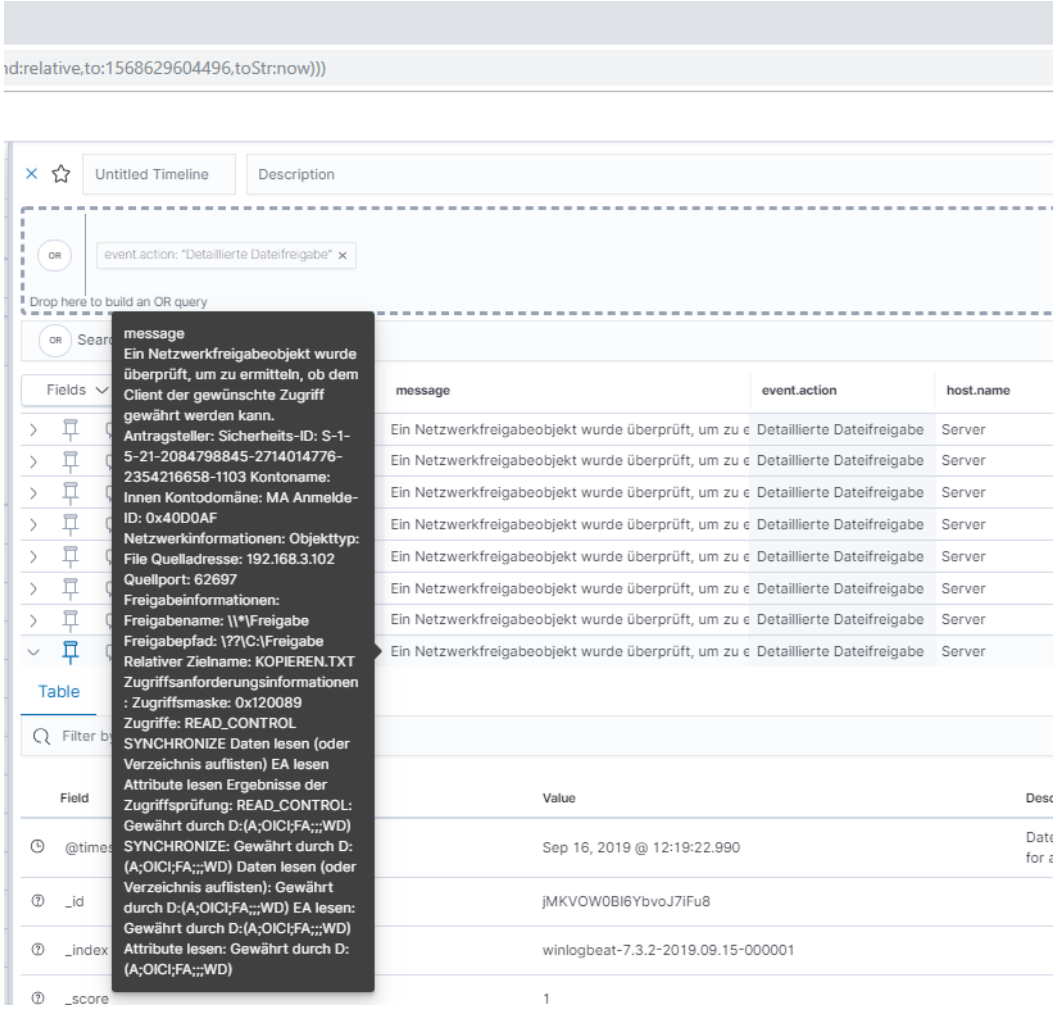


Abbildung 20: Nachgewiesener Zugriff auf Datei (eigene Darstellung)

In Abbildung 20 wird gezeigt, wie durch ein SIEM und aktivierte Auditlogs in Windows ein Zugriff auf Dateien nachgewiesen werden kann. Im Gegensatz zu letzten Zugriffszeiten, die das NTFS anzeigt, kann über diese Möglichkeit eine komplette Historie von zugegriffenen Daten abgebildet werden. Diese Informationen bleiben bis zum Löschen der Logdaten in der Datenbank und können so auch lange nach dem Vorfall ausgewertet werden. Bei einer forensischen Analyse des Computers kann dieser Hinweis bereits überschrieben sein.

5.1.2 Verhinderung von Datendiebstahl

Verhinderung von Datendiebstahl hat gemäß der Definition die Bedeutung, dass ein unbemerktes, heimliches Entwenden von Daten geschieht, was bei einem Kopiervorgang unzutreffend ist. Treffender wäre hier die unbefugte Datenbeschaffung.

Windows bietet in Pro- und Enterprise-versionen EFS (Encrypting File System) an, mit dem Daten mit dem öffentlichen Schlüssel aus dem Schlüsselpaar verschlüsselt werden und mit dem privaten Schlüssel entschlüsselt werden können. Sensible Daten könnten so mit wenig Aufwand vor unbefugten Dritten unlesbar gemacht werden. Da sich die Zertifikate auch exportieren lassen, könnten sehr sensible Daten, die nur einem kleinen Personenkreis zur Verfügung stehen sollen, durch dieses Zertifikat abgesichert werden.[91] Mit EFS lässt sich der Datendiebstahl nicht verhindern, sorgt aber dafür, dass der Täter unbrauchbare, nichtlesbare Daten hat. Beim Einsatz von EFS ist darauf zu achten, dass das Zertifikat, mit dem die Daten entschlüsselt werden können, gut geschützt und gut gesichert ist. Ein verschlüsselter USB-Stick (z. B. durch Bitlocker) kann ein guter Speicherort für das sensible Zertifikat sein.

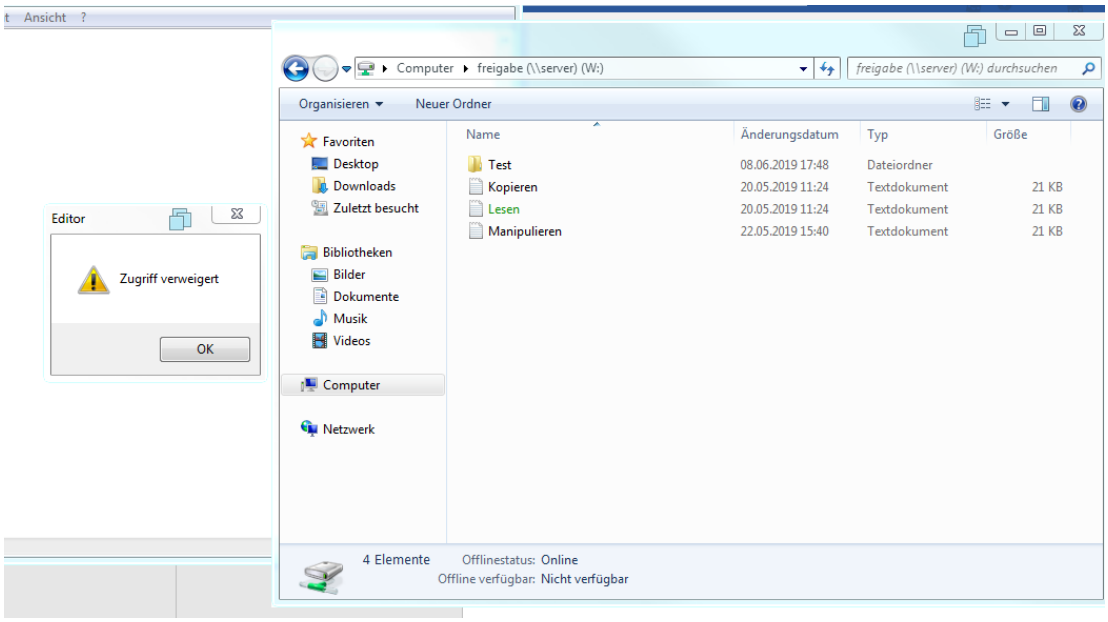


Abbildung 21: Öffnen einer verschlüsselten Datei „Lesen.txt“ (eigene Darstellung)

Ändert ein Administrator das Kennwort eines Benutzers, um so auf seine Daten zuzugreifen, verweigert EFS den Zugriff auf die Daten. Ebenso ist bei Verlust des privaten Schlüssels, oder Ablauf des privaten Schlüssels kein Zugriff auf die Daten

[91] Vgl. https://www.der-windows-papst.de/wp-content/uploads/2018/01/Windows-EFS-Verschl%C3%BCsselung.pdf (Stand 21.08.2019)

möglich. Abbildung 21 zeigt, dass der Zugriff verweigert wird bei der Öffnung einer verschlüsselten Datei.

Die Kombination von Bitlocker zur Laufwerksverschlüsselung und EFS zur Dateiverschlüsselung kann einen effektiven Datendiebstahl bei Einzelnutzern verhindern, da der Täter bei dem Diebstahl des kompletten Notebooks oder Servers lediglich verschlüsselte Daten vorliegen hat. Ohne das richtige Zertifikat oder Kennwort ist kein Zugriff auf die Daten möglich. In größeren Organisationen kann diese Kombination den Kreis der potenziellen Täter deutlich verringern.

Mit diesen Maßnahmen kann ein Diebstahl zwar nicht verhindert werden, jedoch können dessen Auswirkungen deutlich verringert werden.

Neben einer Verschlüsselung von Daten und Datenträgern, hilft ein Berechtigungskonzept innerhalb der Organisation. Damit können unbefugte, die keine administrativen Rechte haben, nicht auf die Daten zugreifen, von denen sie über die NTFS-Rechtevergabe ausgeschlossen wurden.

Hierbei kann ein Administrator folgende Zugriffe anpassen:

- Vollzugriff
- Ändern
- Lesen/Ausführen
- Ordnerinhalt auflisten (gilt nur für Ordner)
- Lesen
- Schreiben.

Diese Zugriffe können für Dateien und Ordner angepasst werden.

Eine weitere Möglichkeit besteht darin, USB-Geräte per Gruppenrichtlinie zu verbieten. Die Richtlinie in Windows wird in Abbildung 22 gezeigt. Spezielle Geräts-IDs können hier erlaubt werden, die zuvor z. B. durch die Geschäftsleitung genehmigt wurden.

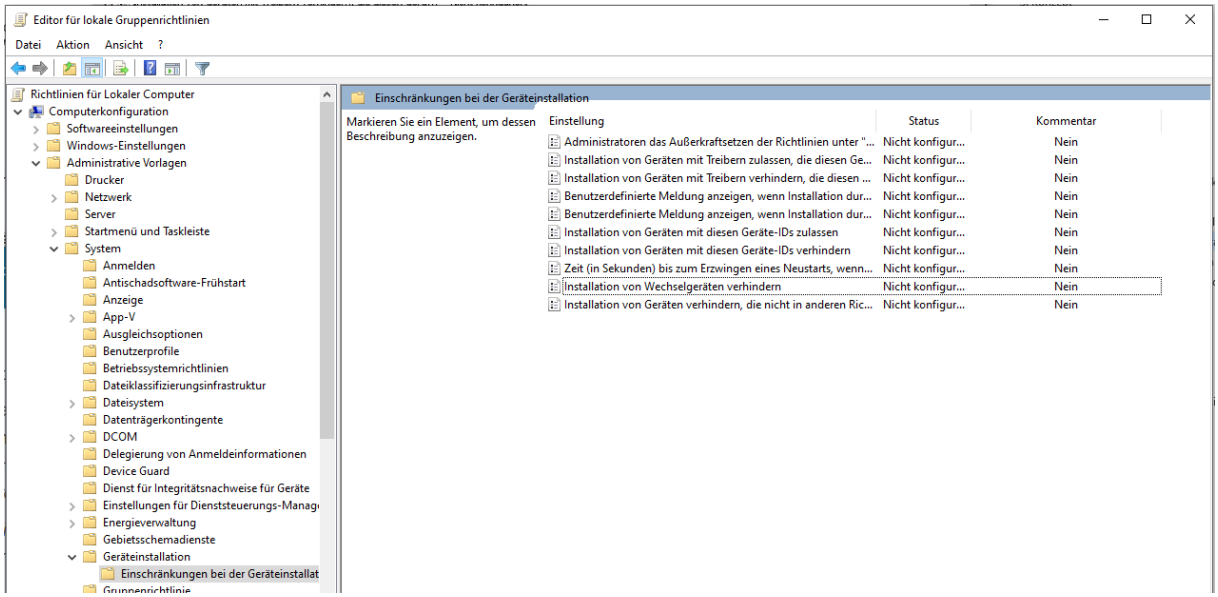


Abbildung 22: Richtlinie in Windows zur Einschränkung von Geräteinstallationen (eigene Darstellung)

Mit dieser Richtlinie kann die Installation von Wechseldatenträgern für alle Benutzer verboten werden. Wird ein Gerät versucht zu installieren, wird kein Treiber durch die Richtlinie zugelassen und ein Hinweistext kann dem Mitarbeiter den Hinweis liefern, dass die Installation verboten ist.[92]

Eine weitere Möglichkeit Daten von einem System zu kopieren, ist der Einsatz von Remote Desktop. Durch die Zwischenablage und verbundene Laufwerke, können Daten von einem System auf das andere kopiert werden. Auch hier bietet die Gruppenrichtlinie Möglichkeiten an.

5.1.3 Richtiges Handeln nach einem Vorfall

Das Center for Internet Security (CIS) rät in den CIS Top 20, den 20 wichtigsten Maßnahmen für ein abgesichertes Unternehmensnetzwerk, als Basisanforderung folgende sechs Elementare Punkte:

- Inventarisierung und Steuerung von Hardware Assets
- Inventarisierung und Steuerung von Software Assets
- Kontinuierliches Schwachstellenmanagement
- Kontrollierte Nutzung administrativer Rechte

[92] Vgl. https://www.tecchannel.de/a/windows-praxis-usb-nutzung-per-gruppenrichtlinie-reglementieren,2034183,4 (Stand 09.09.2019)

- Sichere Konfiguration von hard- und Software auf mobilen Geräten, Laptops, Workstations und Servern
- Wartung, Monitoring und Analyse von Auditlogs.[93]

Anhand dieser Punkte kann anschließend ein Incident Response Plan (IRP) erarbeitet werden, der die Reaktion nach einem Vorfall als schriftliche Anweisung beschreibt. Durch den IRP wissen zuständige Personen, wie sie bei potenziellen Szenarien zu reagieren haben. Durch diese können Datensicherheitsverletzungen, Denial of Service (DoS), Distributed Denial of Service (DDoS), Sicherheitslücken in der Firewall, der Ausbruch und die Verbreitung von Malware und auch Bedrohungen durch Insider frühzeitig geplant und geübt werden.[94]

Bei einem IRP gibt es sechs wichtige Schritte, die das SANS-Institut beschreibt[95]:

In der **Vorbereitungsphase** wird das Team auf mögliche Vorfälle vorbereitet. Dabei werden Vorfälle von einem Stromausfall, über Hardwarefehler bis hin zum Verstoß von Unternehmensrichtlinien oder Hackerangriffen vorbereitet. Unabhängig vom Grund des Vorfalls ist die Vorbereitung der ausschlaggebende Schritt, da dieser Schritt den Grundstein für alle weiteren Schritte legt. In den Richtlinien werden Prinzipien und Regeln der Organisation festgehalten. Ohne klare Richtlinien kann die Organisation rechtlich verwundbar sein.

Im Reaktionsplan werden Pläne und Strategien zur Behandlung von Vorfällen festgelegt. Dabei müssen Vorfälle anhand der Auswirkung auf die Assets priorisiert werden. Fällt beispielsweise der Computer einer Aushilfe aus, hat dies nicht die Auswirkung auf das Unternehmen wie der Ausfall eines Fileservers oder ein Datendiebstahl in der Personalabteilung.

Ein Kommunikationsplan ist nötig, da es nötig sein kann, dass gewisse dritte Parteien informiert oder um Hilfe gebeten werden müssen. Dieser Plan sollte allen Mitgliedern des Teams zugänglich sein.

[93] Vgl. https://www.cisecurity.org/controls/cis-controls-list/ (Stand 25.08.2019)

[94] Vgl. https://www.computerweekly.com/de/definition/Vorfallreaktionsplan-Incident-Response-Plan-IRP (Stand 25.08.2019)

[95] Vgl. https://www.sans.org/reading-room/whitepapers/incident/paper/33901 (Stand 25.08.2019)

Die Dokumentation ist ein elementarer Bestandteil und muss bei jeder Aktion berücksichtigt werden. Hierbei sind alle W-Fragen (Wer, Was, Wann, Wo, Warum und Wie) genauestens zu dokumentieren.

Durch eine geregelte Zugriffskontrolle sollten die Personen, die den Vorfall beheben müssen (Incident Handler) bei Bedarf Zugriffe und Berechtigungen auf Systeme zeitnah durch Administratoren zugewiesen bekommen. Anschließend können diese Berechtigungen, sofern diese nicht mehr zur Behebung notwendig sind, entfernt werden.

Zur effektiven Behebung von Vorfällen sollten vor einem Vorfall alle relevanten Werkzeuge (Hard- und Software) vorbereitet werden, damit kostbare Zeit bei einem Vorfall gespart werden kann.

Durch ein regelmäßiges Training kann richtiges Verhalten geübt werden, damit Fehlverhalten vermieden wird und auch in stressigen Vorfällen jeder weiß, was zu tun ist.

Die zweite Phase der **Identifikation** dient dazu, dass bei der aufgetretenen Abweichung weitere Untersuchungsschritte durchgeführt werden, um sicherzustellen, dass es auch tatsächlich ein Vorfall ist. Dazu werden neben Logdateien weitere Ereignisse, beispielsweise Fehlermeldungen, Meldungen des IDS und der Firewall analysiert. Wird die Abweichung als tatsächlicher Vorfall eingestuft, kann mit der Beweisaufnahme gestartet werden. Es ist stets darauf zu achten, dass die Grundsätze der IT-Forensik beachtet werden.

Der Hauptzweck der **Eindämmungsphase** besteht darin, weitere Schäden zu verhindern und den Schaden zu begrenzen. In dieser Phase gibt es mehrere Schritte die notwendig sind, um den Vorfall vollständig zu beheben und dabei keine Beweise zu vernichten. Insbesondere wenn der Fall an Strafverfolgungsbehörden oder vor Gericht geht, muss sichergestellt sein, dass die Beweise nicht vernichtet wurden. Der erste Schritt in der Eindämmungsphase besteht in einer kurzfristigen Eindämmung, bei der der Fokus darauf liegt, den Schaden so schnell wie möglich zu begrenzen. Beispiele für eine kurzfristige Eindämmung sind die Isolation eines Netzwerks, die Segmentierung betroffener Workstations, das Abschalten des Produktionsservers. Die kurzfristige Eindämmung stellt keine Langzeitlösung dar, sondern soll nur die weitere Verbreitung verhindern und damit den Vorfall zu begrenzen bevor es schlimmer wird. Anschließend wird im zweiten Schritt der Eindämmungsphase ein

Systembackup erstellt. Hierbei wird das forensische Backup mit bekannten Programmen wie dem Forensic Tool Kit (FTK), EnCase oder anderen erstellt.

Wird das Backup mit FTK erstellt, kann das platzsparende E01-Format gewählt werden. Zusätzlich wird automatisch ein Hashwert zur Integritätsfeststellung des Images gebildet.[96] Wird das Backup im laufenden, kompromittierten System erstellt, kann diese Backup für spätere Analysen genutzt werden[97] und kann so auch Inhalte des Arbeitsspeichers enthalten, die bei einem abgeschalteten System nicht vorhanden wären. Im Arbeitsspeicher lassen sich Netzwerkaktivitäten, laufende Prozesse und Verbindungen zu anderen Systemen, Inhalte von Dateien, die noch nicht auf einer Festplatte gespeichert wurden und Passwörter einer Laufwerksverschlüsselung enthalten.[98] Der letzte Schritt vor der nächsten Phase ist die langfristige Eindämmung, bei der die betroffenen Systeme vorübergehend repariert werden können. Dabei wird das betroffene System so repariert, dass es vorübergehend wieder in Betrieb genommen werden kann, während eine saubere Installation des Systems durchgeführt wird. In diesem Schritt werden Hintertüren und Benutzer des Angreifers entfernt und aktuelle Sicherheitsupdates auf diesem und benachbarten Systemen installiert. Damit kann der Geschäftsbetrieb fortgesetzt werden und eine weitere Ausbreitung eingeschränkt werden.[99]

Ausrottung

Diese Phase befasst sich mit der tatsächlichen Entfernung und Wiederherstellung der betroffenen Systeme. Wie bei jeder der vorherigen Phasen der Reaktion auf Vorfälle ist eine kontinuierliche Dokumentation aller ergriffenen Maßnahmen erforderlich, um die Kosten für Arbeitsstunden und andere Ressourcen zu ermitteln, damit die Gesamtauswirkungen auf die Organisation bestimmt werden kann. Es muss auch sichergestellt werden, dass geeignete Maßnahmen ergriffen wurden, um böswillige und andere illegale Inhalte aus den betroffenen Systemen zu entfernen und

[96] Vgl. Willer, 2012.

[97] Vgl. Kral, 2011.

[98] Vgl. Willer, 2012.

[99] Vgl. Kral, 2011.

sicherzustellen, dass diese keinerlei Schadsoftware mehr enthalten. Im Allgemeinen bedeutet das die Neuinstallation eines Systems auf zuvor formatierten Festplatten, um eine erneute Infektion zu verhindern. Diese Phase ist auch der Zeitpunkt, zu dem die Verteidigung verbessert werden sollte, nachdem geprüft wurde, wie das Problem entstanden ist.[100]

In der Praxis eignet sich hierbei die CERT-Taxonomie, bei dem der IT-forensische Prozess in den Vorfall in den Mittelpunkt stellt und davon ausgeht, dass es einen Angreifer gibt und eine Absicht vorliegt. Mit dieser Taxonomie kann ein Angriffsverlauf beschrieben werden, bei dem eine Klassifizierung in Vorfall, Angriff und Ereignis erstellt wird.[101]

In der Wiederherstellungsphase werden betroffene Systeme wieder in die Produktionsumgebung gebracht. Dabei muss sichergestellt werden, dass es nicht zu einem weiteren Vorfall kommt. Die Systeme müssen hierzu getestet, überwacht und validiert werden, um eine erneute Kompromittierung zu verhindern. Wichtige Entscheidungen in dieser Phase sind:

- Datum und Uhrzeit der Inbetriebnahme
- Überprüfung der vollen Funktionsfähigkeit des Systems inkl. Abnahme des Anwendungs- oder Systemverantwortlichen
- Einsatz der Programme zum Testen, Überwachen und Überprüfen des Systems.[102]

Die kritischste Phase ist die „Lessons Learned“-Phase, bei der alle Dokumentationen vervollständigt und analysiert werden, um diese Erkenntnisse bei zukünftigen Vorfällen nutzen zu können. Das Dokument sollte in Form eines Berichts erfasst werden und die wichtigsten W-Fragen (siehe CERT-Taxonomie) beinhalten.

Das übergeordnete Ziel dieser Phase besteht darin, dass die Organisation aus Vorfällen lernen kann und so die Leistungsfähigkeit des Teams verbessern kann. Ebenso dienen diese Erkenntnisse für interne Schulungsunterlagen. Eine

[100] Vgl. Kral, 2011.

[101] Vgl. https://it-forensik.fiw.hs-wismar.de/index.php/CERT-Taxonomie (Stand 10.09.2019)

[102] Vgl. Kral, 2011.

anschließende Diskussion mit anderen Teammitgliedern kann für die Verbesserung der Effektivität nach einem Vorfall durchaus hilfreich sein.[103]

5.1.4 Maßnahmen zur Reduzierung der Reaktionszeit und Forensic Readiness

Die Forensic Readiness ist die Vorbereitung von Organisationen auf eine forensische Untersuchung, um deren Nutzen maximal zu erhöhen und dabei die Kosten der Untersuchung möglichst gering zu halten. Zudem ermöglicht die Vorbereitung die Qualität der Daten und stellt sicher, dass Organisationen vorbereitet sind und mit den Daten gemäß, damit im Falle eines Vorfalls Spuren fachgerecht gesichert und behandelt werden.[104]

Die ISACA, ein Berufsverband für IT-Revisoren, Informationssicherheit und IT-Governance, schlägt folgende zehn Schritte zur Forensic Readiness vor:[105]

- Definieren Sie die Geschäftsszenarien, die digitale Beweise erfordern würden. Dies hilft zu optimieren, wo und wie die Speicherung von Beweissammlungen konzentriert werden kann.
- Identifizieren Sie potenzielle Beweisquellen und die Arten von Beweisen.
- Bestimmen Sie die Anforderungen für die Beweiserfassung.
- Stellen Sie die Fähigkeit zur sicheren Sicherung und Sammlung von Beweisen auf forensisch einwandfreie Weise her.
- Richten Sie eine Richtlinie für die ordnungsgemäße Beweismittelkette, der Chain of Custody (engl.) ein.
- Stellen Sie sicher, dass die Ziele zur Erkennung und Abschreckung schwerwiegender Vorfälle überwacht werden.
- Geben Sie die Umstände an, unter denen die Eskalation einer vollständigen digitalen Untersuchung beginnen soll.
- Schulung und Sensibilisierung der Mitarbeiter in Bezug auf die Reaktion auf Vorfälle, um sicherzustellen, dass sie ihre Rolle im Prozess sowie deren Bedeutung und Sensibilität verstehen.[106]

[103] Vgl. Kral, 2011.

[104] Vgl. Rowlingson, 2004.

[105] Vgl. ebd.

[106] Vgl. (Center for Internet Security®, 2019)

- Dokumentieren Sie Fälle, in denen der Vorfall und seine Auswirkungen beschrieben werden.
- Stellen Sie eine rechtliche Überprüfung sicher, um angemessene Maßnahmen zur Reaktion auf einen Vorfall zu ermöglichen.[107]

Schon nach der ersten Analyse der Umsetzungsmaßnahmen ist ersichtlich, dass Unternehmen die tatsächliche Arbeit vor einem Vorfall machen müssen, um bei einem Vorfall keine wertvolle Zeit zu verlieren und Beweise zu vernichten.

5.2 Umsetzung der Maßnahmen

In diesem Unterkapitel werden die einzelnen Maßnahmen zur schnelleren Aufklärung von Vorfällen beschrieben. Damit die Vorfälle überhaupt erkannt werden können, müssen diverse Anpassungen in den Log-Mechanismen durchgeführt werden und an die installierte ELK- und Security Onion-Lösung weitergeleitet werden. Dort müssen die Events, die durch Winlogbeat und Auditbeat geliefert werden, gefiltert werden. Durch die Dashboards, die in beiden Systemen gebaut wurden, sollen dann Hinweise auf einen Vorfall erkennbar sein, damit schnell Gegenmaßnahmen eingeleitet werden können und so der Vorfall schnell aufgeklärt werden kann.

Da Windows im Standard nicht alle Ereignisse in das Windows-Eventlog schreibt, kann über das Programm „Auditpol.exe“ die aktuelle Konfiguration abgerufen werden (siehe Abbildung 23 und Anlage I):

[107] Vgl. Sule, 2014.

```
Richtlinienänderung
  Richtlinienänderungen überwachen        Erfolg
  Authentifizierungsrichtlinienänderung   Erfolg
  Autorisierungsrichtlinienänderung       Keine Überwachung
  MPSSVC-Richtlinienänderung auf RegelebeneKeine Überwachung
  Filterplattform-Richtlinienänderung     Keine Überwachung
  Andere Richtlinienänderungsereignisse   Keine Überwachung
Kontenverwaltung
  Computerkontoverwaltung                 Erfolg
  Sicherheitsgruppenverwaltung            Erfolg
  Verteilergruppenverwaltung              Keine Überwachung
  Anwendungsgruppenverwaltung             Keine Überwachung
  Andere Kontoverwaltungsereignisse       Keine Überwachung
  Benutzerkontenverwaltung                Erfolg
DS-Zugriff
  Verzeichnisdienstzugriff                Erfolg
  Verzeichnisdienständerungen             Keine Überwachung
  Verzeichnisdienstreplikation            Keine Überwachung
  Detaillierte VerzeichnisdienstreplikationKeine Überwachung
Kontoanmeldung
  Ticketvorgänge des Kerberos-Diensts     Erfolg
  Andere Kontoanmeldungsereignisse        Keine Überwachung
  Kerberos-Authentifizierungsdienst       Erfolg
  Überprüfung der Anmeldeinformationen    Erfolg
```

Abbildung 23: Auszug der überwachten Logereignisse Teil 2 (eigene Darstellung)

Was bei der Durchsicht der Auditpol-Ausgabe auffällt ist, dass viele Kategorien nicht überwacht werden. Erfolg und Fehler sagen aus, dass beispielsweise nur bei erfolgtem oder fehlerhaften Anmeldeversuch ein Protokoll geschrieben wird. Sofern keine Überwachung erfolgt, werden auch keine Ereignisse aufgezeichnet.

Da Microsoft auf der Website bereits Empfehlungen anbietet, wurde folgende Tabelle zur Übersicht eingefügt (siehe Anlage II). Auf der Empfehlung zur Überwachungsrichtlinie wird zwischen drei unterschiedlichen Abstufungen unterschieden. Die Windows-Standard-Installation beschreibt die Audit-Policy nach einer normalen Installation von Windows. Die rechte Spalte („Eine stärkere Empfehlung“) ist die Empfehlung für kritische Systeme oder sensible Daten (siehe Anlage II).

Im Bereich „Zugriff auf Objekte“ findet sich keinerlei Empfehlung. In diesem Bereich sind beispielsweise Zugriffe auf Netzwerkfreigaben oder Wechseldatenträger gemeint. Da diese jedoch für die Aufklärung von Vorfällen wichtig sind, wurde diese Überwachung auf dem Server und dem Client über die Gruppenrichtlinie aktiviert. Somit ist erkennbar, was über eine Netzwerkfreigabe gemacht wird.

Bei der weiteren Recherche von Best-Practices wurden diverse Empfehlungen gefunden. Da Mitre, von der die nachfolgende Tabelle stammt, auch in der Fachwelt bekannt ist, wurde diese übernommen.

Tactic	Technique Name	Technique ID	Data Source 1	Data Source 2	Data Source 3	Data Source 4	Data Source 5
Collection	Audio Capture	T1123	4688 Process Execution	4663 File monitoring	API monitoring		
Collection	Automated Collection	T1119	4688 Process CMD Line	4663 File monitoring	Data loss prevention		
Collection	Clipboard Data	T1115	API monitoring				
Collection	Data from Information Repositories	T1213	Application Logs	Authentication logs	Data loss prevention	Third-party application logs	
Collection	Data from Local System	T1005	4688 Process Execution	4688 Process CMD Line	200-500, 4100-4104 PowerShell logs	4663 File monitoring	5861 WMI
Collection	Data from Network Shared Drive	T1039	4688 Process CMD Line	4688 Process Execution	5140/5145 Share connection	4663 File monitoring	
Collection	Data from Removable Media	T1025	4688 Process Execution	4688 Process CMD Line	4657 Windows Registry	4663 File monitoring	5140/5145 Net Shares
Collection	Data Staged	T1074	4688 Process CMD Line	4688 Process Execution	4663 File monitoring		
Collection	Email Collection	T1114	4688 Process Execution	5156 Firewall Logs	4624 Authentication logs	4663 File monitoring	
Collection	Man in the Browser	T1185	4624 Authentication logs	4688 Process Execution	API monitoring	Packet capture	
Collection	Screen Capture	T1113	4688 Process Execution	4663 File monitoring	API monitoring		

Abbildung 24: Auszug aus Mitre Logging Cheatsheet[108]

In dem Auszug der Tabelle konnten nachfolgende Event-IDs extrahiert werden, die für den in der Thesis relevanten Sachverhalt wertvoll ist. Die extrahierten Event-IDs wurden mit einer Beschreibung der Event-IDs erweitert:

Tabelle 10: Event-IDs mit Beschreibung (eigene Darstellung)

EventID	Beschreibung
4688	A new process has been created: Hierbei sind Benutzername und Prozess, sowie der Pfad erkennbar.
4663	An attempt was made to access an objekt: Hierbei kann der Zugriff auf eine Datei festgestellt werden. Zudem kann die Art des Zugriffs (Lesen, Schreiben, …), sowie Benutzername, Pfad, etc. ausgelesen werden.
5861	WMI: Windows Management Instrumentation (WMI) zeigt Zugriffe auf diverse Quellen

[108] https://www.malwarearchaeology.com/cheat-sheets (Stand 07.05.2019)

5140	A network share object was accessed: Zeigt die IP-Adresse, den Port und die Freigabe an, auf die zugegriffen wurde.
5145	A network share object was checked to see whether client can be granted desired access: Zeigt genaue Informationen an. Z. B. die Datei und der Grund, warum der Dateizugriff erlaubt oder verweigert wurde.
4624	An account was successfully logged on: Zeigt den erfolgten Anmeldevorgang an.

Gemäß der Mitre-Veröffentlichung sollten diese Event-IDs aktiviert sein, damit eine forensische Untersuchung von Daten auf lokalen Datenträgern, Netzlaufwerken und Wechseldatenträgern über die Ereignisanzeige möglich ist. Neben diesen Event-IDs liefert Microsoft noch weitere Event-IDs inklusive einer Einstufung der Kritikalität und der erwarteten Auswirkung bei Eintritt dieses Ereignisses.

Damit alle relevanten Ereignis-IDs in die Ereignisanzeige geschrieben werden, wurde die Auditpolicy gemäß der Microsoft-Empfehlung angepasst und um die weiteren Empfehlungen erweitert (siehe Anlage III).

Die Überwachungsrichtlinien wurden in den Gruppenrichtlinien hinterlegt, sodass jeder Client, der in der Domäne ist, auch dieselben Einstellungen hat (Abbildung 25). Die Überwachungseinstellungen werden zwischen Server und Client regelmäßig synchronisiert und können manuell durch den Befehl „gpupdate /force“ erzwungen werden. Da Microsoft auch Richtlinien zur Handhabung mit Wechseldatenträgern anbietet, wurden Wechseldatenträger auf den Systemen verboten. Ein Innentäter, der Daten über einen USB-Stick abgreifen möchte, könnte an dieser Stelle zwar den USB-Stick einstecken, kann aber keine Daten auf den USB-Stick kopieren, da der USB-Stick erst gar nicht durch Windows installiert wird.

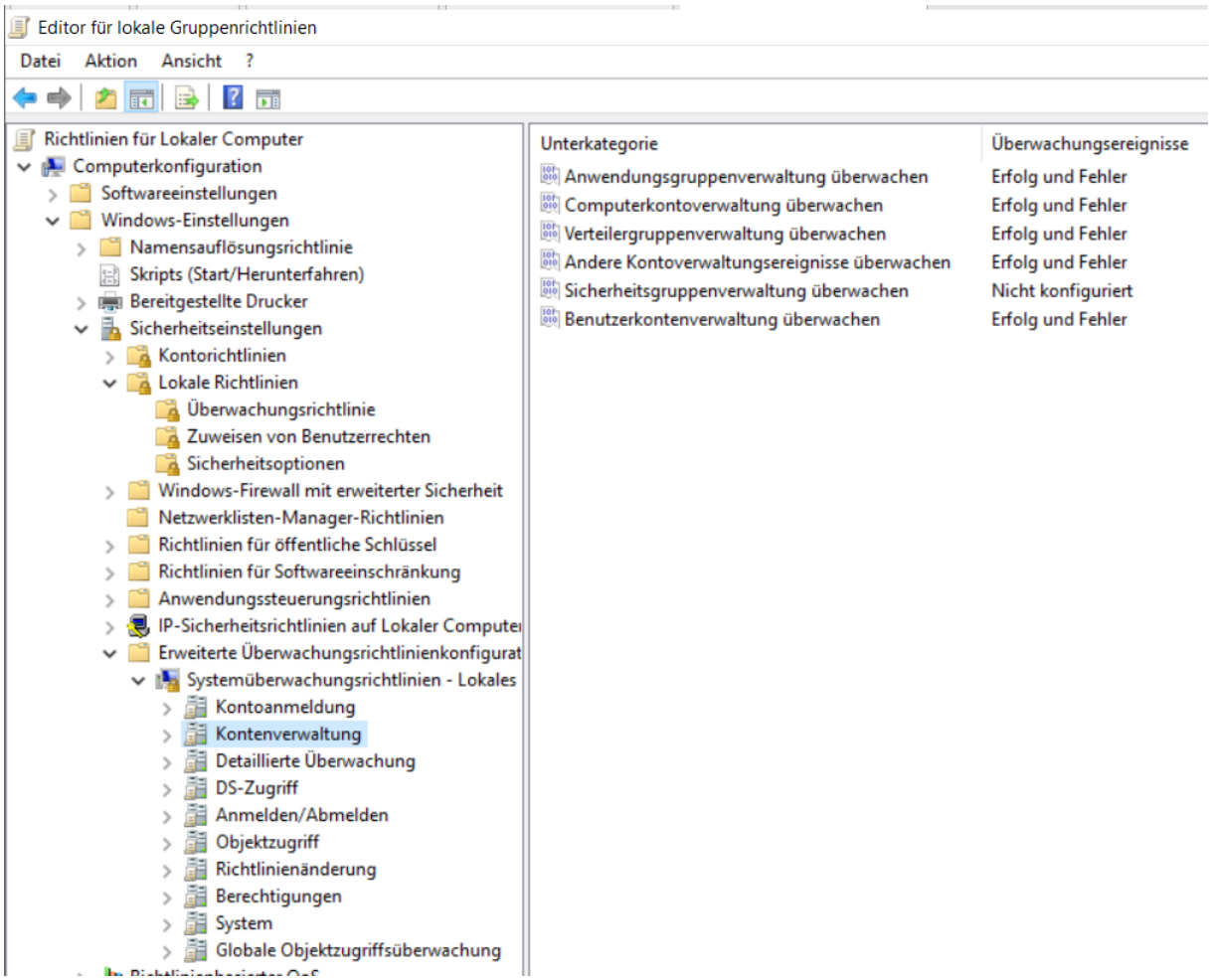


Abbildung 25: Anpassung der Überwachungsrichtlinie (eigene Darstellung)

Damit die Zugriffe auf die Netzwerkfreigabe in die Ereignisanzeige geschrieben werden, muss die Audit-Funktion der Freigabe angepasst werden (siehe Abbildung 26). Hierzu bietet Microsoft die Möglichkeit an, eine Überwachung von Freigaben zu aktivieren. Hierbei können Lese-, Schreibzugriffe, Anzeige der Ordnerinhalte, etc. überwacht und dementsprechend auch ausgewertet werden. Bei einem Ordnerzugriff und einem Lesen oder Manipulieren von Inhalten kann so ein Vorfall einfacher aufgeklärt werden.

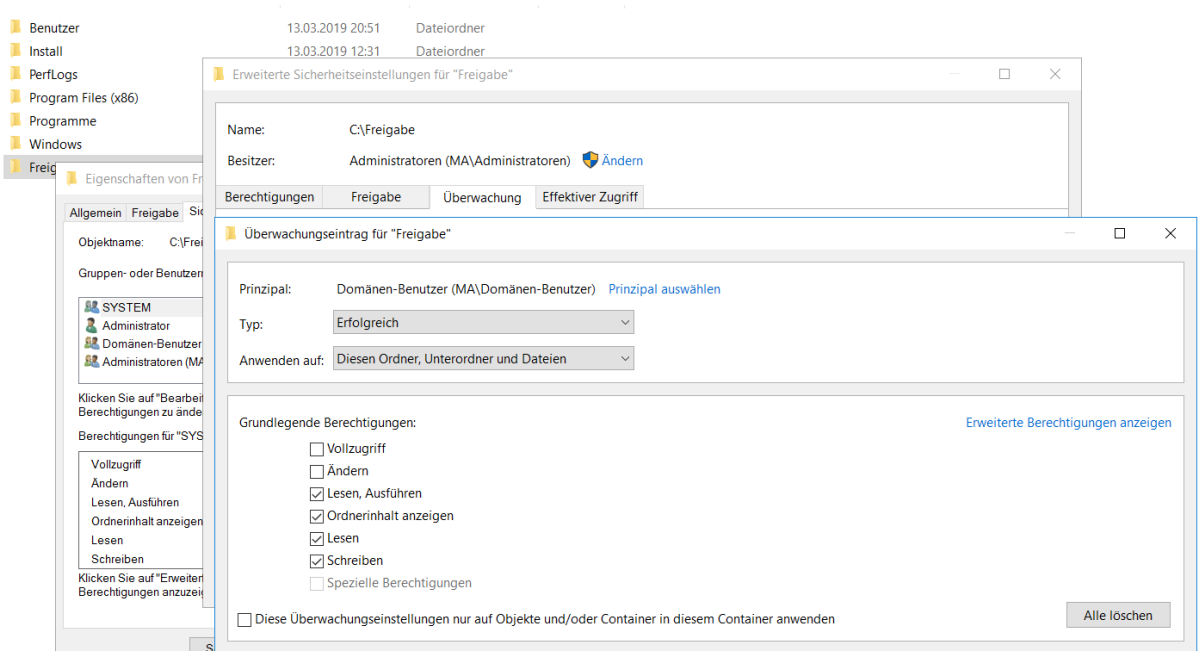


Abbildung 26: Anpassungsmöglichkeit der Audit-Funktion (eigene Darstellung)

Für Windows 2016, Windows 2019 und Windows 10 bietet Microsoft die EventID 6146 an, über die neu installierte Geräte, wie z. B. Wechseldatenträger speziell geloggt werden können.[109]

Nachdem alle relevanten Ereignisse protokolliert werden, muss die Weiterleitung von Ereignissen an das zentrale Logging angepasst werden. Dazu müssen in Auditbeat und Winlogbeat diverse Parameter angepasst werden.

Anpassungen in Winlogbeat und Auditbeat:

```
#------------------------------ Logstash output --------------------------------
output.logstash:
  # The Logstash hosts
  hosts: ["192.168.3.241:5044", "192.168.3.240:5044"]

  # Optional SSL. By default is off.
  # List of root certificates for HTTPS server verifications
  #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]

  # Certificate for SSL client authentication
  #ssl.certificate: "/etc/pki/client/cert.pem"

  # Client Certificate Key
  #ssl.key: "/etc/pki/client/cert.key"
```

Abbildung 27: Anpassung Winlogbeat (eigene Darstellung)

[109] Vgl. https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=6416 (Stand 07.05.2019)

In der Konfigurationsdatei von Auditbeat und Winlogbeat muss festgelegt werden, an welchen Server die Ereignisse geschickt werden sollen. Da ein Vergleich zwischen Security Onion und ELK bzw. dem Elastic-Stack stattfinden soll, werden die Ergebnisse an beide Server geschickt. Über die Konfigurationsdatei ist es ebenso möglich einen Fallback zu hinterlegen. Dieser empfängt nur die Daten, sobald der Hauptserver ausfällt. Je nachdem in welcher Sektion der Host hinterlegt wird, schickt der Forwarder, der die Ereignisse weiterleitet, die Daten an eine andere Schnittstelle. Wird der Host in der Sektion „output.Logstash:“ hinterlegt, werden alle Daten, die der Forwarder bereithält, an Logstash geschickt. Da Daten manipuliert werden sollen, wurde Logstash als Empfänger der Daten gewählt. Die Daten können auch ohne Manipulation an die Datenbank Elasticsearch oder an Kibana, die Weboberfläche, geschickt werden. Logstash bietet die Möglichkeit der Manipulation von Daten. Hierbei können irrelevante Ereignisse gelöscht werden, Daten durch andere Quellen angereichert werden, Daten anonymisiert oder pseudonymisiert werden, etc.

Nach der Anpassung der Konfigurationsdatei für Winlogbeat wurde das Programm als Dienst installiert. Hierbei schlug der erste Versuch wegen einer zu hohen Sicherheitseinstellung fehl (siehe Abbildung 28). Mit der Parameteränderung für die Ausführungsrichtlinie konnte der Dienst anschließend erfolgreich installiert werden (siehe Abbildung 29).

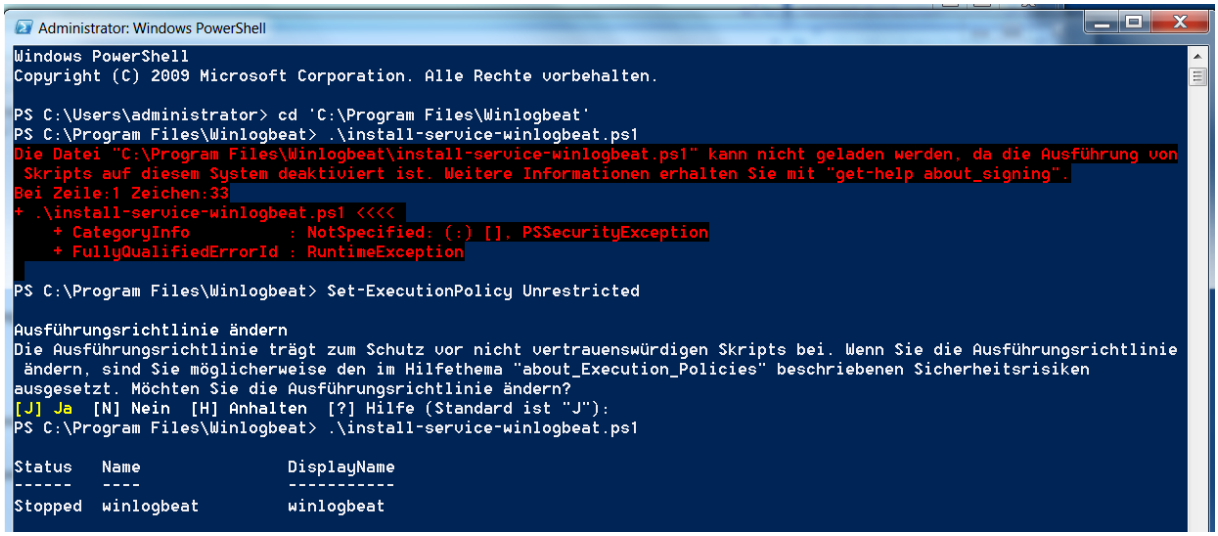


Abbildung 28: Installation Winlogbeat als Dienst (eigene Darstellung)

Der Dienst wurde anschließend in den Windowsdiensten gestartet und geprüft. Da auch die Logdateien erstellt wurden, schien der Dienst fehlerfrei zu laufen. Bei der

weiteren Kontrolle der Logdatei wurde festgestellt, dass eine Verbindung zu Security Onion nicht möglich war.

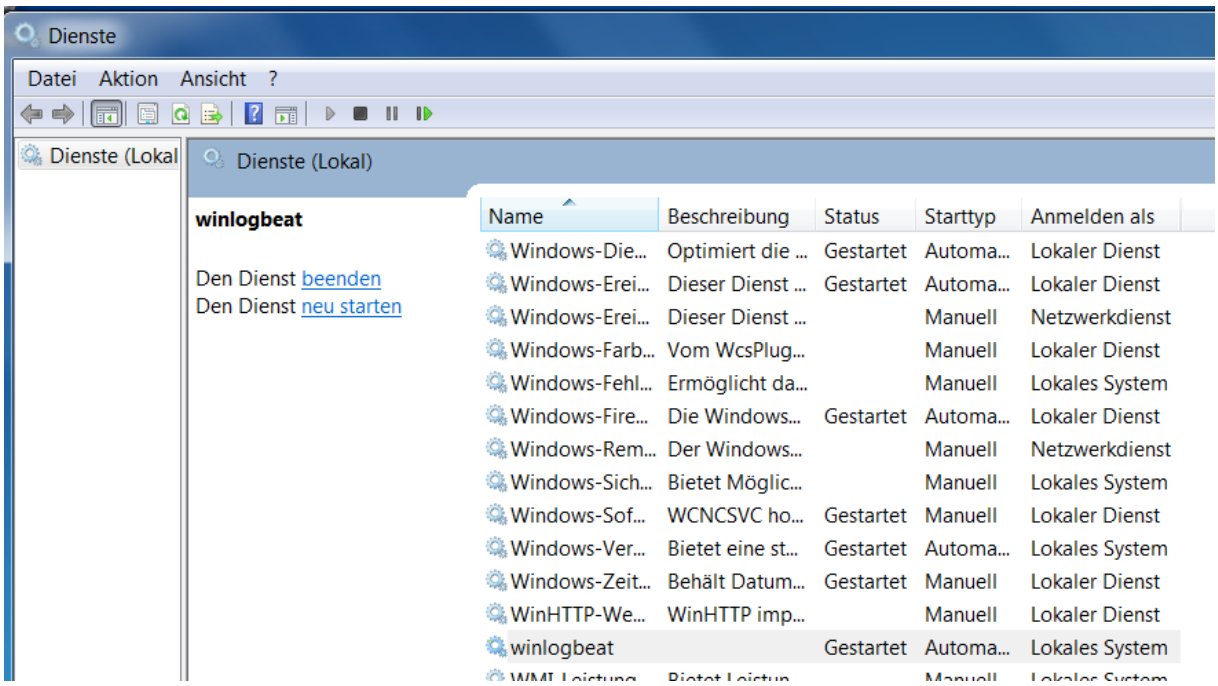


Abbildung 29: Kontrolle des Winlogbeat-Dienstes (eigene Darstellung)

Da die Firewall-Einstellung bei Security Onion etwas anders ist als bei anderen Linux-Systemen, die lediglich die ufw-Firewall[110] einsetzen, liefert der Hersteller eine Möglichkeit die Anpassungen ohne große Konfigurationsänderungen vorzunehmen.

Über den Befehl „sudo so-allow“ kann eine einfache Firewall-Änderung durchgeführt werden, die auch die Anpassungen der IPTables am Docker-Proxy vornimmt. Im Standard akzeptiert Security Onion lediglich Anfragen auf Port 22 (ssh).[111]

Da die Windows Event-IDs über Logstash und/oder Elasticsearch gemeldet werden sollen, musste eine Anpassung erfolgen. Hierzu wurden alle IP-Adressen der Testsysteme hinterlegt, die an Security Onion melden sollen.

[110] Unkomplizierte Firewall (ufw)

[111] Vgl. https://securityonion.readthedocs.io/en/latest/firewall.html (Stand 23.05.2019)

```
File  Edit  View  Search  Terminal  Help
so@so-virtual-machine:~$ sudo so-allow
[sudo] password for so:
This program allows you to add a firewall rule to allow connections from a new IP address.

What kind of device do you want to allow?

[a] - Analyst - ports 22/tcp, 443/tcp, and 7734/tcp
[b] - Logstash Beat - port 5044/tcp
[c] - apt-cacher-ng client - port 3142/tcp
[e] - Elasticsearch REST endpoint - port 9200
[f] - Logstash forwarder - standard - port 6050/tcp
[j] - Logstash forwarder - JSON - port 6051/tcp
[l] - Syslog device - port 514
[n] - Elasticsearch node-to-node communication - port 9300
[o] - OSSEC agent - port 1514
[s] - Security Onion sensor - 22/tcp, 4505/tcp, 4506/tcp, and 7736/tcp

If you need to add any ports other than those listed above,
you can do so using the standard 'ufw' utility.

For more information, please see the Firewall page on our Wiki:
https://github.com/Security-Onion-Solutions/security-onion/wiki/Firewall

Please enter your selection (a - analyst, c - apt-cacher-ng client, l - syslog, o - ossec, or s - Security Onion sensor, etc.):
b
Please enter the IP address of the Logstash - Beat you'd like to allow to connect to port(s) 5044:
192.168.3.222
We're going to allow connections from 192.168.3.222 to port(s) 5044.

Here's the firewall rule we're about to add:
sudo iptables -I DOCKER-USER ! -i docker0 -o docker0 -s 192.168.3.222 -p tcp --dport 5044 -j ACCEPT

To continue and add this rule, press Enter.
Otherwise, press Ctrl-c to exit.

Rule has been added.

Here is the entire firewall ruleset:


================================================================================
UFW Rules
================================================================================

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
9200                       ALLOW       Anywhere
5044                       ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
9200 (v6)                  ALLOW       Anywhere (v6)
5044 (v6)                  ALLOW       Anywhere (v6)


================================================================================
Docker IPTables Rules
================================================================================

To                Action From
--                ------ ----
5044/tcp docker0 ACCEPT !docker0 192.168.3.222
5044/tcp docker0 ACCEPT !docker0 192.168.3.20
5044/tcp docker0 ACCEPT !docker0 so-virtual-machine
9200/tcp docker0 ACCEPT !docker0 so-virtual-machine
9300/tcp docker0 ACCEPT !docker0 192.168.3.240
9200/tcp docker0 ACCEPT !docker0 192.168.3.20
```

Abbildung 30: Anpassung SO-Firewall (eigene Darstellung)

Nachdem die IP-Adressen der Systeme hinzugefügt wurden, wurden auch direkt die ersten Windows-Events an den ELK-Stack übertragen. Bei der Ubuntu-Lösung wurden die Ports 9200 (Elasticsearch) und 5044 (Logstash) über die Befehle „sudo ufw allow 9200“ und „sudo ufw allow 5044“ freigeschaltet (siehe Abbildung 30). Auch hier wurde der Eingang von Events geprüft (siehe Abbildung 31).

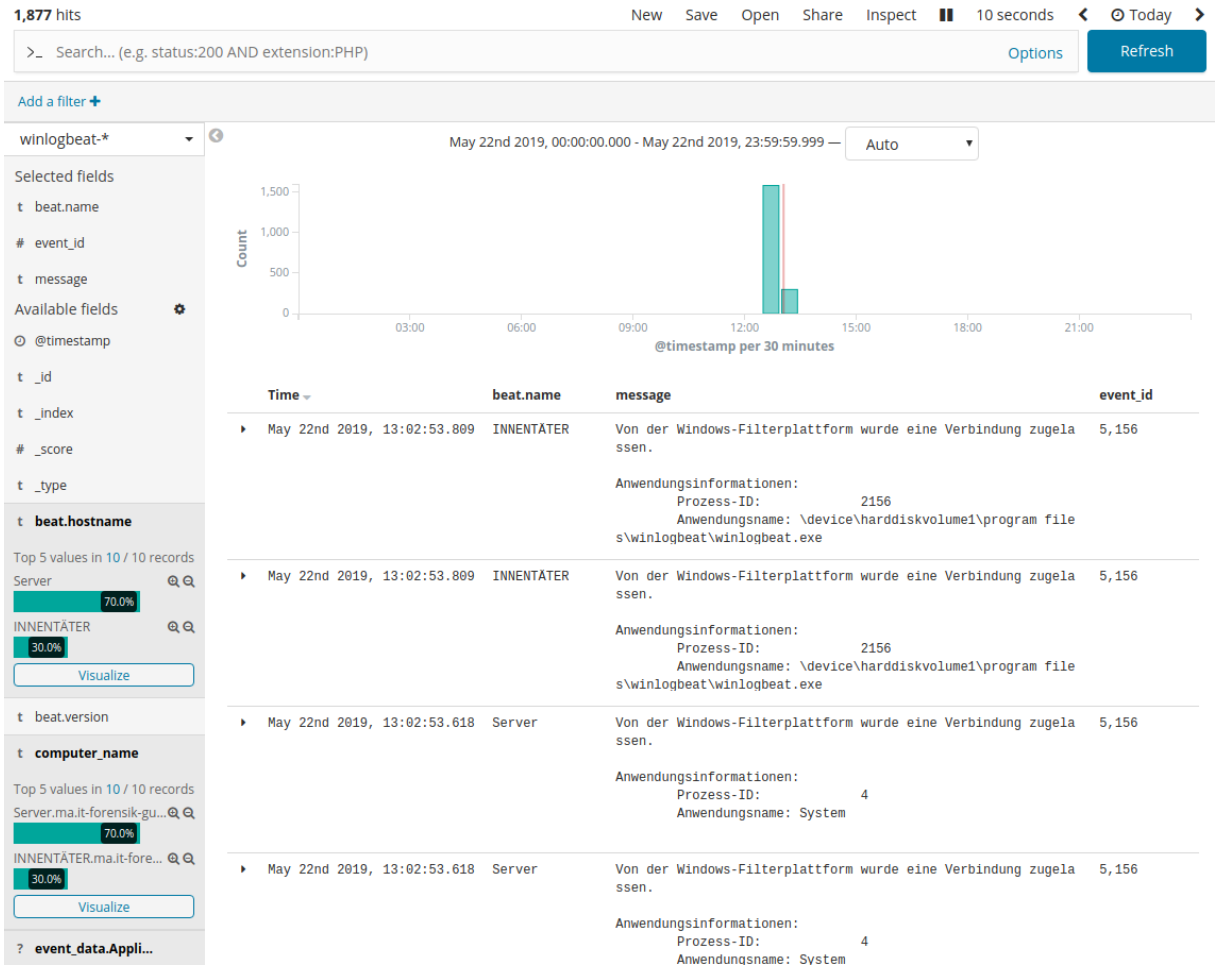


Abbildung 31: Windows Events in Security Onion (eigene Darstellung)

Durch die ankommenden Meldungen ist ersichtlich, dass die Kommunikation durch den Server und durch die Innentäter-VM funktioniert. Der „beat.name“ zeigt den Computernamen des Systems an, das die Daten meldet. Über die „event.id“ ist die Event-ID ersichtlich. Oben links in Abbildung 31 zeigt Kibana direkt die Anzahl der Treffer an, die durch den aktuellen Suchfilter angezeigt werden können. Gerade bei der ersten Verwendung von Kibana ist die Anpassung des Zeitfilters, der oben rechts ist, wichtig. Die Anzeige kann durch ein anklicken des gewünschten Felds erweitert werden. Über die Filterfunktion können Felder, die aktuell nicht gewünscht sind, herausgefiltert werden. Speziell bei der Untersuchung eines Vorfalls ist diese Funktion äußerst hilfreich.

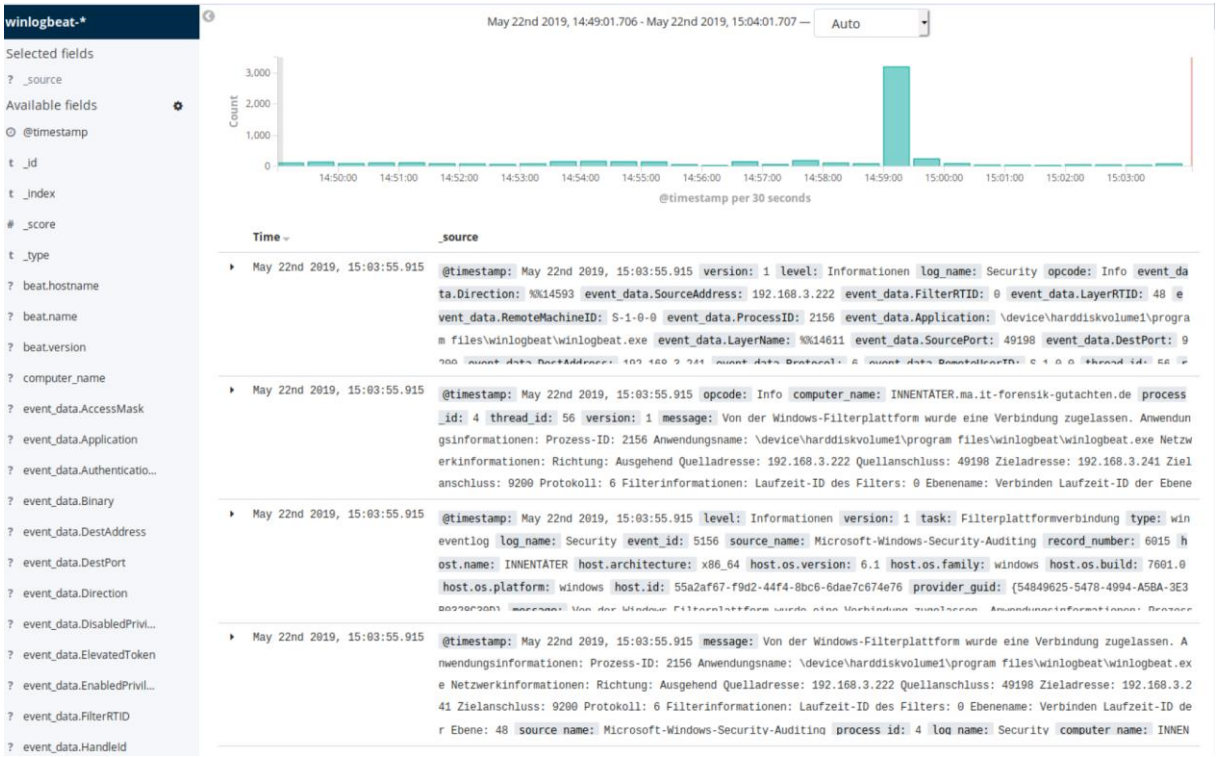


Abbildung 32: Windows Events in Ubuntu (ELK) (eigene Darstellung)

Im Elastic-Stack wurden ebenfalls die Ereignisse des Servers und der Innentäter-VM angezeigt. Lediglich bei der Feldauswahl gab es im Elastic-Stack deutlich mehr Felder zur Auswahl. Bei einer weiteren Untersuchung des Problems, musste lediglich der Datenbankindex neu aufgebaut werden. Da dies bei ELK nur ein paar Klicks sind, war dies ohne Probleme möglich.

5.3 Erfolgskriterien

Nach Umsetzung der durchgeführten Maßnahmen, sollten folgende Aktivitäten ohne eine tiefgehende forensische Analyse sichtbar sein:

- USB-Stick wurde eingesteckt
- Dateien wurden vom Server auf den USB-Stick kopiert
- Remote-Access-Tool wurde gestartet
- Dateien wurden über den Remote-Zugangs kopiert.

Hierzu wurde auf beiden Systemen jeweils ein Dashboard gebaut, in dem die Informationen übersichtlich dargestellt werden. Über die Informationen aus den Windows Event-IDs können so Ereignisse, die keinen Mehrwert liefern herausgefiltert werden.

Beispielsweise sind in der Übersicht viele Meldungen zu Kerberos-Tickets enthalten, die für Password-Spray-Attacken hilfreich sein können, enthalten. Dementsprechend

müssen die Dashboards pro Anwendungsfall angepasst werden. Ein Dashboard, das direkt alle Sicherheitslücken und Gefahren aufdeckt ist unwahrscheinlich.

Meldungen müssen oftmals im Zusammenhang angeschaut werden, da nicht jedes Ereignis ein Vorfall ist. Um eine Klassifizierung vorzunehmen, müssen weitere Schritte, die in anderen Kapiteln nachzulesen sind, durchgeführt werden.

Wird ein Vorfall erkannt, kann über die Dashboards schnell geprüft werden, ob diese Ereignisse auch auf anderen Systemen auftreten.

5.4 Ergebnisse der Erfolgsprüfung

Zur Erfolgsprüfung (siehe Tabelle 11) wurde der Versuch auf dem Innentäter-System erst ohne Anpassung der erweiterten Audit-Funktion durchgeführt und anschließend forensisch in einer Post-Mortem-Analyse analysiert (PMA 1). Nachdem die Anpassungen vorgenommen wurden, (siehe 5.1 Umsetzung der Maßnahmen) wurde der Versuch wiederholt. Die virtuelle Maschine wurde anschließend – wie auch im ersten Versuch – forensisch gesichert und ausgewertet (PMA 2). Die forensische Sicherung wurde mit dem FTK-Imager durchgeführt. Da die Sicherung auch eventuell gelöschte Dateien und Spuren beinhalten sollte, wurde die physische Sicherung gewählt. Da Winlogbeat und Auditbeat aktiviert waren und Windows alle relevanten Event-IDs in die Ereignisanzeige schrieb, konnte in der PMA 2 nachgewiesen werden, dass ein USB-Stick eingesteckt wurde, und dass auf den Server zugegriffen wurde. Bei Manipulationen und Lesezugriffen kann bei PMA 1 und PMA 2 nachgewiesen werden, dass der Editor (Notepad.exe) gestartet wurde und die Dateien auf der Freigabe geöffnet wurden. Der Kopiervorgang der „Kopieren.txt“ konnte jedoch erst nach einer Aktivierung der Freigabenüberwachung erkannt werden. Beim Kopieren der Dateien über den Remotezugang (Fastviewer) konnte dasselbe Verhalten erkannt werden.

Tabelle 11: Erfolgsprüfung

Tätigkeit	**PMA 1**	**PMA 2**	**Elastic-Stack**	**Security Onion**
USB-Stick wurde eingesteckt	✓	✓	✓	✓
Dateien wurden vom Server auf den USB-Stick kopiert			✓	✓
Remote-Access-Tool wurde gestartet	✓	✓	✓	✓
Dateien wurden über den Remote-Zugang kopiert			✓	✓

Nach einer Anbindung des Servers und des Clients an den Elastic-Stack und an Security Onion konnten Kopiervorgänge der „Kopieren.txt“ auch nachgewiesen werden. Das Löschen von Dateien wurde ebenso sofort erkannt und in den beiden Lösungen gemeldet. Da der Elastic-Stack seit Version 7 mit einem integrierten SIEM (das noch in der Betaphase ist) ausgestattet ist, konnte aufgrund der Korrelation ein möglicher Datenabfluss gleich erkannt werden.

6. Bewertung der erarbeiteten Lösung

Durch die Implementierung und Anpassung der Windows-Richtlinien wurden die Ereignisse, die zum Aufklären eines Vorfalls generiert werden müssen, in der Windows-Ereignisanzeige generiert. Die Ereignisse werden anschließend durch Winlogbeat und Auditbeat direkt an Security Onion und den Elastic-Stack weitergeleitet. Dort wurden die Informationen aller Logquellen zusammengeführt, was eine Korrelation der Daten ermöglichte (siehe Abbildung 33).

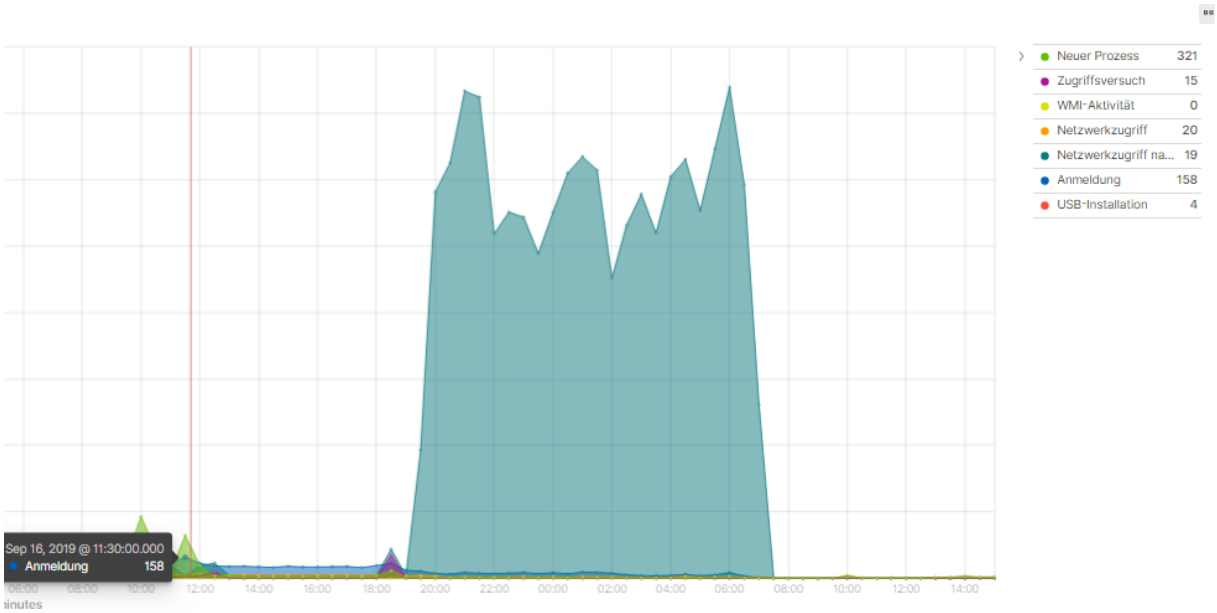


Abbildung 33: Analyse-Dashboard (eigene Darstellung)

Bei dem selbstentwickelten Analyse-Dashboard wurden die relevanten Event-IDs herausgefiltert. Durch die Korrelation können neue Prozesse, Zugriffsversuche, WMI-Aktivitäten, Netzwerkzugriffe, Anmeldungen und USB-Installationen auf einen Blick erkannt werden. Abbildung 33 zeigt, dass 4 USB-Installationen erfolgten und anschließend die Netzwerkzugriffe stark zunahmen. Dies kann für einen Analysten ein abweichendes Verhalten sein und einen Vorfall auslösen. Abbildung 34 zeigt einen neuen Prozess „FastRemoteService.exe“. Durch einen Klick auf das Ereignis werden im unteren Bereich weitere Informationen angezeigt. Mit einem Blick ist ersichtlich, von welchen Client das Programm ausgeführt wird und in welchem Verzeichnis die ausführbare Datei liegt. Programme, die der Analyst bereits kennt, können herausgefiltert werden, was die Analyse deutlich erleichtert.

Abbildung 34: Analyse-Dashboard (eigene Darstellung)

In Abbildung 35 wird gezeigt, wie eine einfache Analyse der „Lesen.txt“ möglich ist.

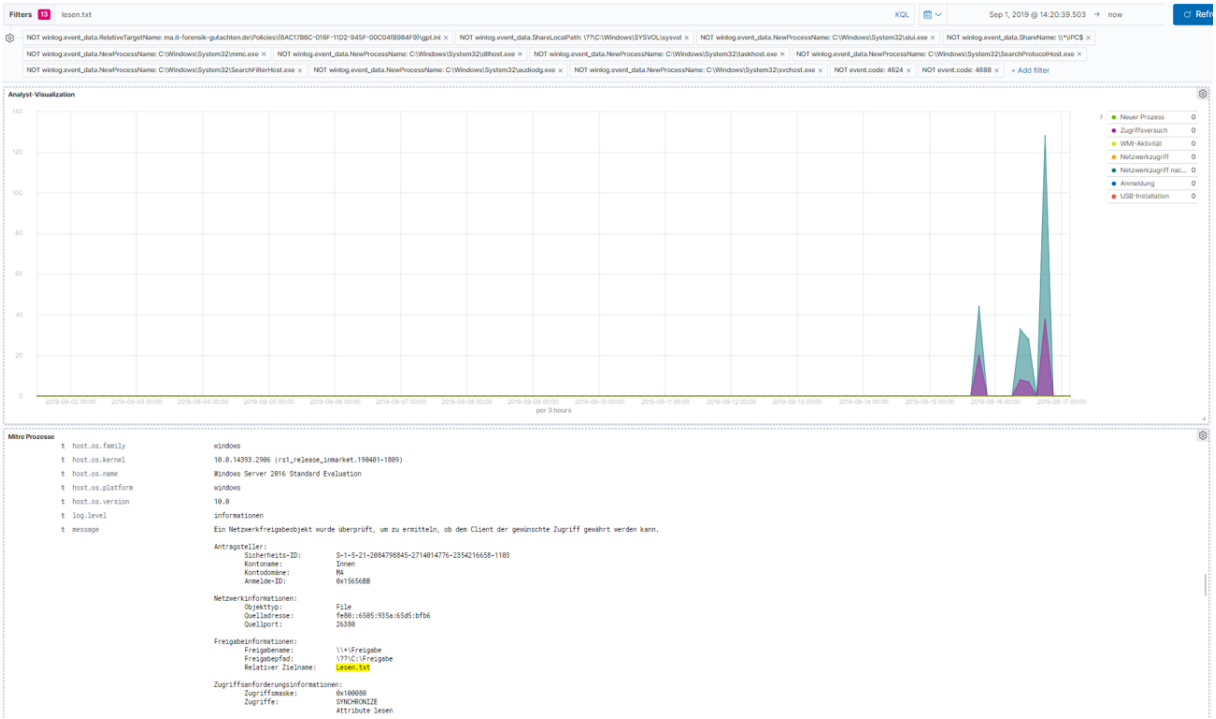


Abbildung 35: Analyse Lesezugriff auf "Lesen.txt" (eigene Darstellung)

Da durch die Event-IDs auch gestartete Prozesse angezeigt werden, kann hier darauf geachtet werden, wenn ungewöhnliche Programme (siehe Abbildung 36) gestartet werden und anschließend die Netzwerkzugriffe zunehmen.

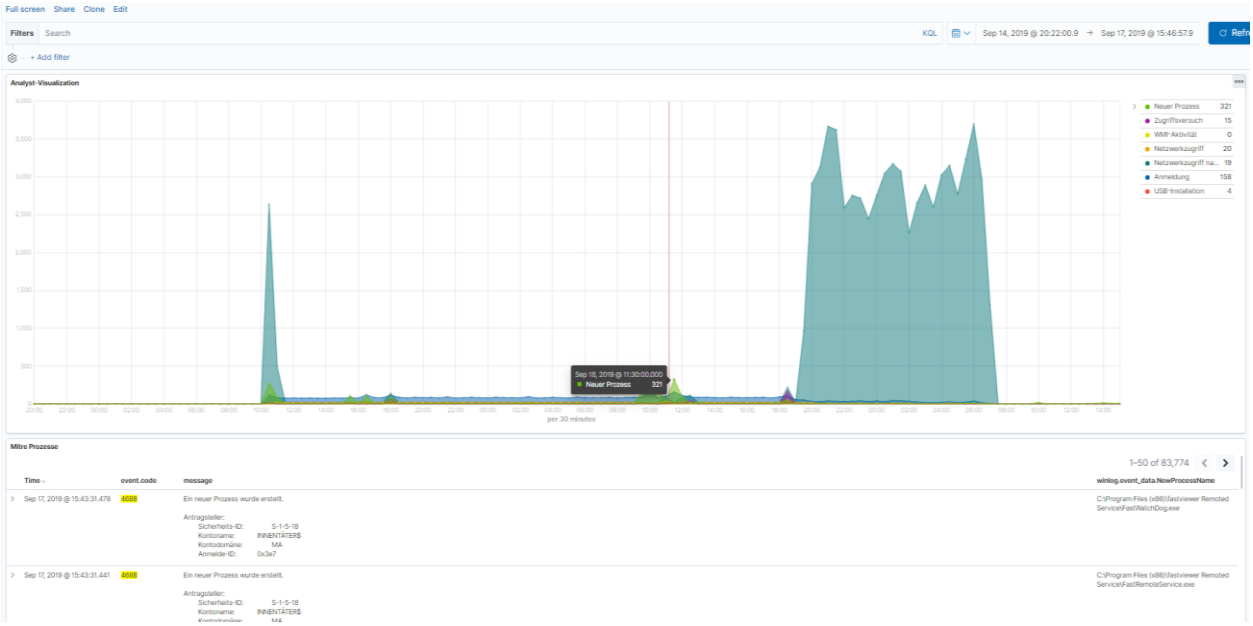


Abbildung 36: Start eines Remote Access Tools und anschließender Anstieg der Netzwerkzugriffe (eigene Darstellung)

Bei einer Installation eines Wechseldatenträgers wird diese sofort angezeigt und ermöglicht einen sofortigen Zugriff bei dolosen Handlungen (siehe Abbildung 37).

Abbildung 37: Analyse einer USB-Installation (eigene Darstellung)

Der Elastic-Stack bietet dank dem integrierten SIEM auch eine bereits vorgefertigte Analysefunktion, die diese Aktionen ebenso anzeigt. Da jedoch die SIEM-Funktion erst ab Version 7.x implementiert ist, konnte diese Funktion bei Security Onion nicht

genutzt werden. Die Dashboards, die im Rahmen dieser Masterthesis gebaut wurden, jedoch schon.

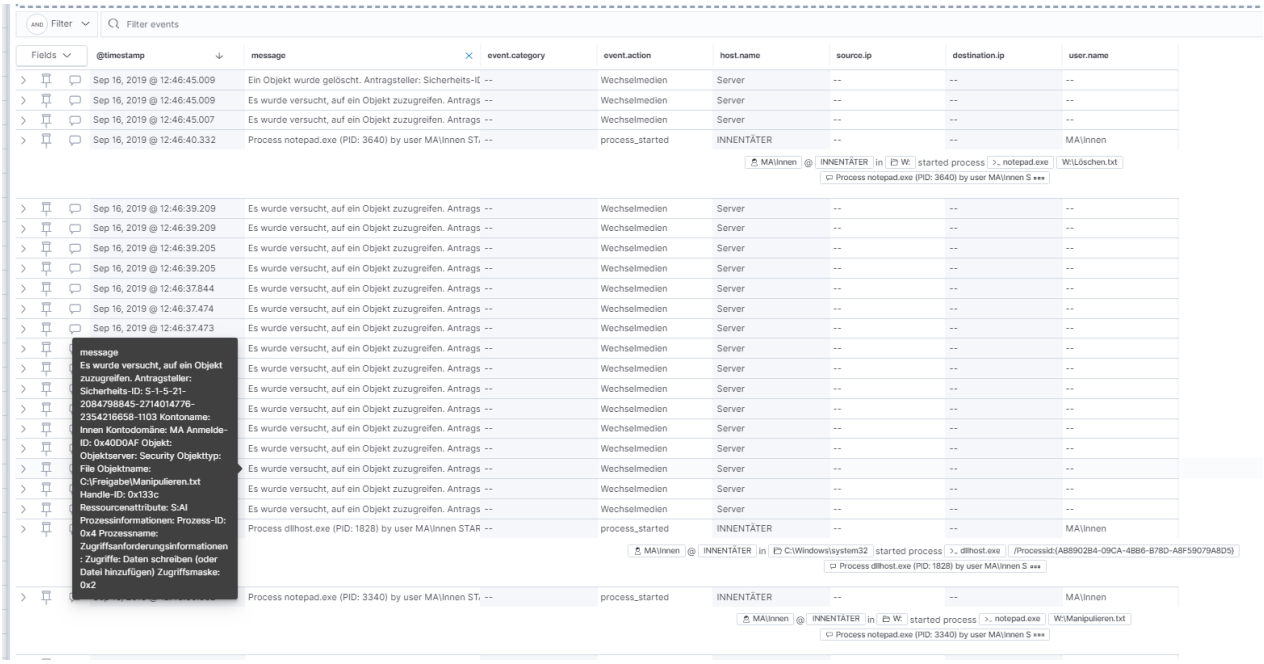


Abbildung 38: Elastic SIEM beim Nachweis von Manipulationen (eigene Darstellung)

Da die Dashboards alle Sachverhalte schnell anzeigen und aus der Menge an Daten eine sinnvolle Analyse erfolgen kann, stellt ein zentrales Log-Management mit einem SIEM (siehe Abbildung 38) oder entsprechender Dashboards eine Verbesserung für die Post-Mortem-Analyse dar, da teilweise ganz auf eine forensische Post-Mortem-Analyse verzichtet werden kann. Installationen, Anmeldungen, Zugriffe und Prozesse werden sofort dargestellt und werden sicher in der Elasticsearch-Datenbank abgespeichert.

7. Vergleich ELK-Stack und Security Onion

In diesem Kapitel wird ein Vergleich des reinen Elastic-/ELK-Stack und Security Onion durchgeführt.

7.1 ELK-Stack

Der ELK-Stack ist ein Verbund aus Elasticsearch, Logstash und Kibana. In Kombination bilden diese drei Werkzeuge eine leistungsfähige Suchmaschine, die dem Benutzer hilft, Protokolle und Daten verschiedenster Systeme in kürzester Zeit zu analysieren.

Elasticsearch ist hierbei die zentrale Datenbank, die von Logstash mit Daten beliefert wird und von Kibana, dem Webinterface ausgelesen werden kann. Da Elasticsearch alle Daten automatisch indexiert, kann über Kibana eine Volltextsuche über alle Datenfelder stattfinden.

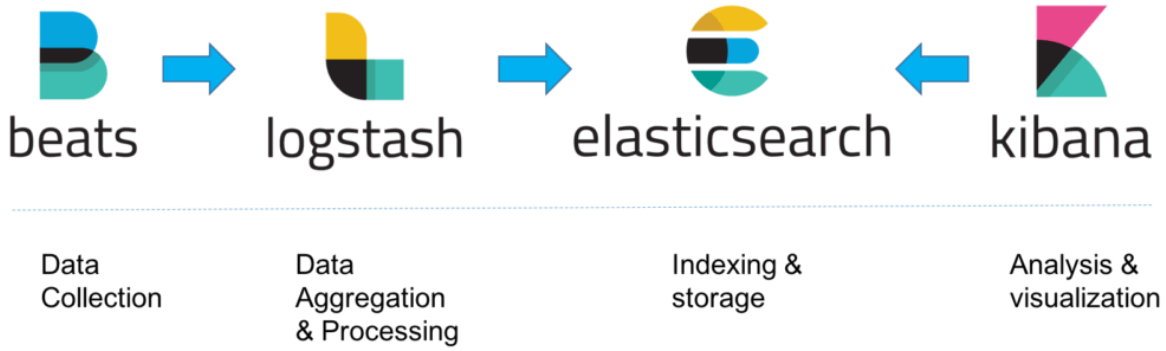


Abbildung 39: Zusammenspiel ELK-Stack (Quelle: https://logz.io/learn/complete-guide-elk-stack/)

7.1.1 Elasticsearch

Elasticsearch dient zum Speichern, Analysieren und Durchsuchen von Daten. Dabei verfolgt Elasticsearch den noSQL-Ansatz, bei dem Daten nicht in einer relationalen Datenbank, sondern Dokumentenbasiert abgespeichert werden. Dadurch entfallen die typischen Tabellen einer Datenbank.[112] Durch die RESTful API, einer Programmierschnittstelle, können Daten über http angefragt werden um über GET, PUT, POST oder DELETE Daten zu bearbeiten oder zu speichern.[113]

[112] Vgl. https://www.elastic.co/de/products/elasticsearch (Stand 29.04.2019)

[113] Vgl. https://www.computerweekly.com/de/definition/RESTful-API (Stand 29.04.2019)

Daten werden für die spätere Suche als JSON-Dokument an Elasticsearch übergeben und gespeichert. Diese werden direkt in Indizes abgelegt. In dem Index, welcher nur ein logischer Namensraum ist, können beliebig viele Dokumente unterschiedlichen Typs abgespeichert werden. Um eine Lastverteilung zu ermöglichen und eine Ausfallsicherheit zu erreichen, wird die physische Speicherung in mehrere „Primary Shards“ Lucene-Instanzen aufgeteilt. Durch das integrierte Master-Slave-Konzept können weitere Cluster im Netzwerk installiert werden.[114]

Die Elasticsearch-Knoten synchronisieren sich untereinander und können eingehende Suchanfragen selbstständig verteilen.[115]

7.1.2 Logstash

Um Daten vor der Speicherung in Elasticsearch zu manipulieren, können diese an Logstash weitergeleitet werden, das die Daten manipuliert und normalisiert. Hierbei kann Logstash von unterschiedlichsten Quellen beliefert werden.[116]

Über die Filterfunktion können unnötige Felder herausgefiltert werden, Werte ersetzt werden oder Daten angereichert werden. Dabei kann durch diverse Plugins beispielsweise zu der Quell- oder Ziel-IP die Geolokation ermittelt und in Elasticsearch gespeichert werden. Nach erfolgter Manipulation durch Logstash werden die Daten an Elasticsearch weitergeleitet, sofern diese nicht verworfen wurden (siehe Abbildung 40).

[114] Vgl. https://www.heise.de/developer/artikel/Volltextsuche-mit-ElasticSearch-1920454.html?seite=all (Stand 29.04.2019)

[115] Vgl. https://www.linux-magazin.de/ausgaben/2016/02/elk-stack/ (Stand 29.04.2019)

[116] Vgl. https://www.linux-magazin.de/ausgaben/2016/02/elk-stack/2/ (Stand 29.04.2019)

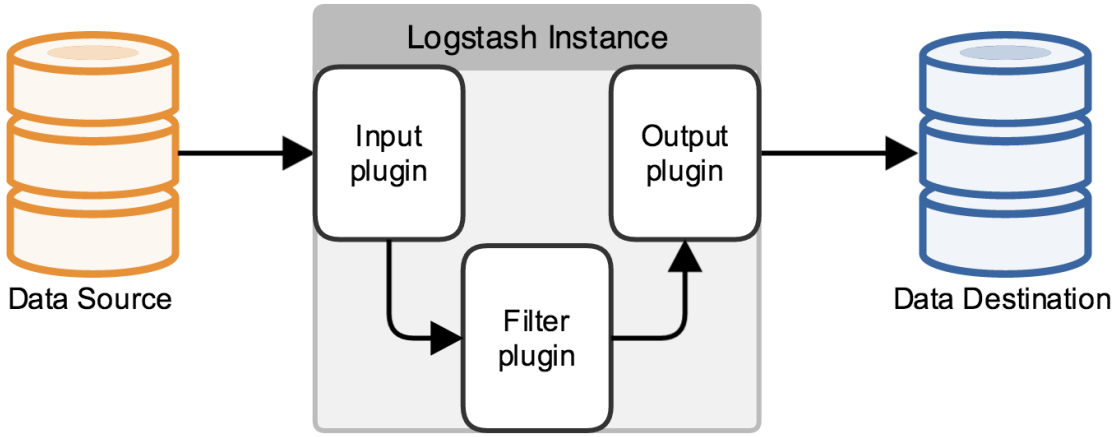


Abbildung 40: Übersicht Logstash[117]

7.1.3 Kibana

Kibana ist das Webinterface, mit dem Daten aus Elasticsearch angezeigt und ausgewertet werden können. Abfragen werden dank der bereits durch Elasticsearch indizierten Daten sofort angezeigt.

Abbildung 41: Beispieldashboard in Kibana[118]

[117] https://www.elastic.co/guide/en/logstash/2.3/advanced-pipeline.html (Stand 03.08.2019)

[118] (Quelle: https://www.linux-magazin.de/ausgaben/2016/02/elk-stack/5/) (Stand 03.08.2019)

Durch flexible Suchalgorithmen können komplexe Abfragen erstellt werden. Diese können als Suchabfragen oder Dashboards abgespeichert werden. In dem Bereich Visualisierung können Statistiken, Zeitverläufe, Datenfelder, etc. erstellt werden, die anschließend für die Dashboards bereitstehen. In den Dashboards können mehrere Abfragen und Visualisierungen dargestellt werden (siehe Abbildung 41).[119]

7.1.4 Elastic SIEM

Mit der aktuellen Version 7.2 bietet Elastic Sicherheitsanalysen durch das integrierte SIEM an, das Threat Hunting entscheidend vorantreiben soll.

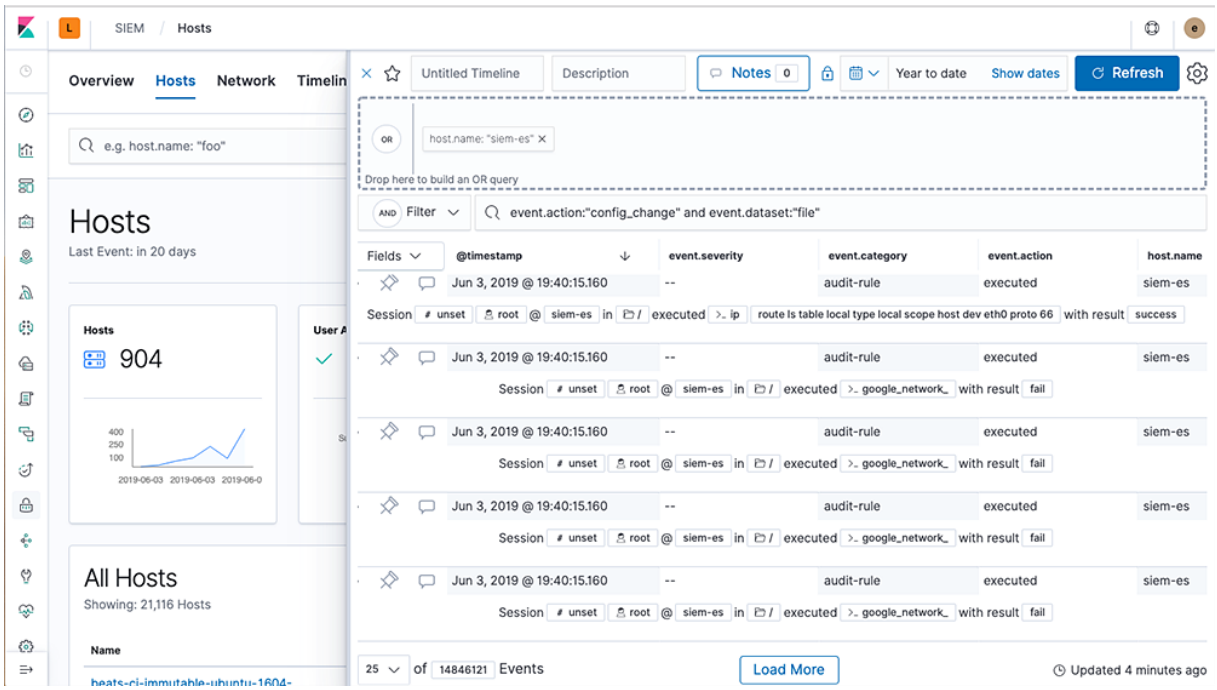


Abbildung 42: SIEM bei Elastic 7.2[120]

Durch diese Neuerung können Unternehmen die eigenen Untersuchungen von Sicherheitsvorfällen im Vergleich zur Vorversion ohne SIEM deutlich verbessern.

7.1.5 Beats

Damit Logstash Daten empfangen kann, müssen Systeme Daten über Beats an Logstash senden. Diese stehen in diversen Ausprägungen auf der Herstellerseite zur Verfügung. Dabei stehen Beats wie Filebeat (für Log-Dateien), Winlogbeat (spezielle

---

[119] Vgl. https://www.linux-magazin.de/ausgaben/2016/02/elk-stack/5/ (Stand 29.04.2019)

[120] (Quelle: https://static-www.elastic.co/v3/assets/bltefdd0b53724fa2ce/bltf1fec946608941d0/5d02862f210698013c6f2b0b/screenshot-siem-timeline-with-authentications-background.png)

für Windows-Ereignis-Logs), Auditbeat (für Audit-Daten), Packetbeat (speziell für Netzwerkdaten), und viele weitere zur Verfügung. Je nach Anwendungsfall können hier auf einem System mehrere Beats installiert werden.[121]

7.2 Security Onion

Security Onion ist eine Linux-Distribution für Intrusion Detection, Enterprise Security Monitoring und Log-Management.

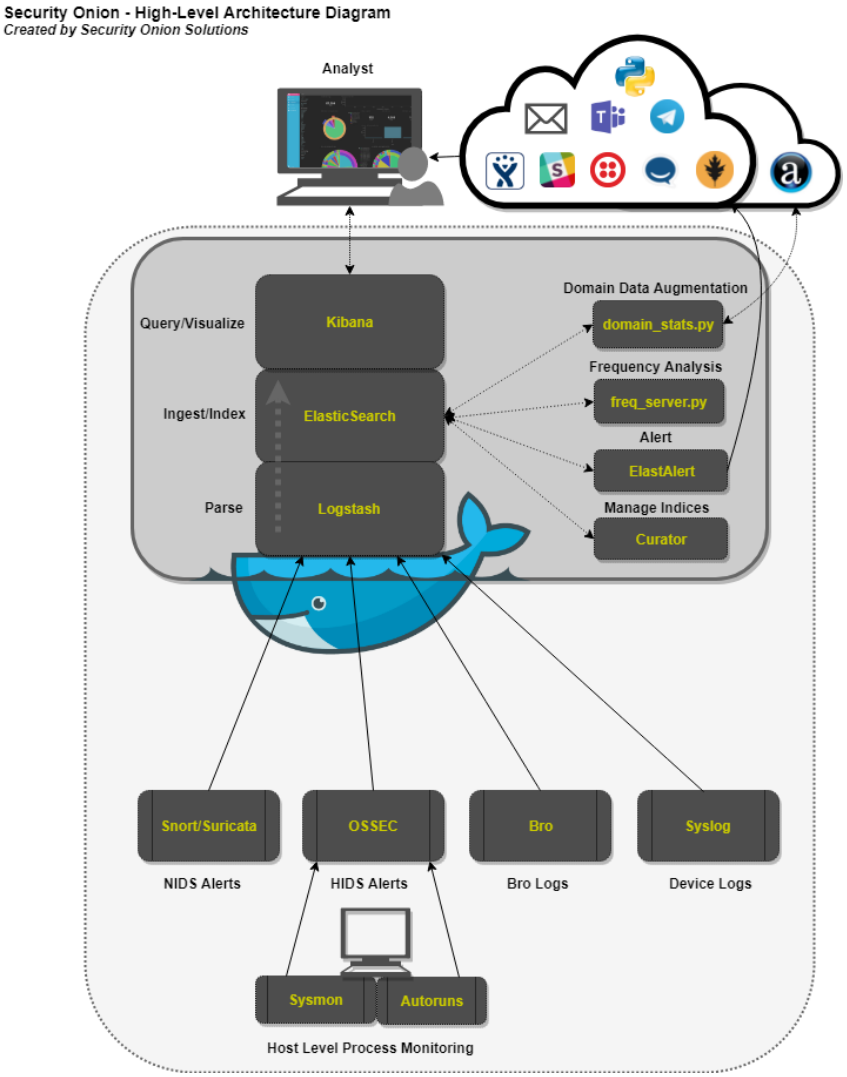


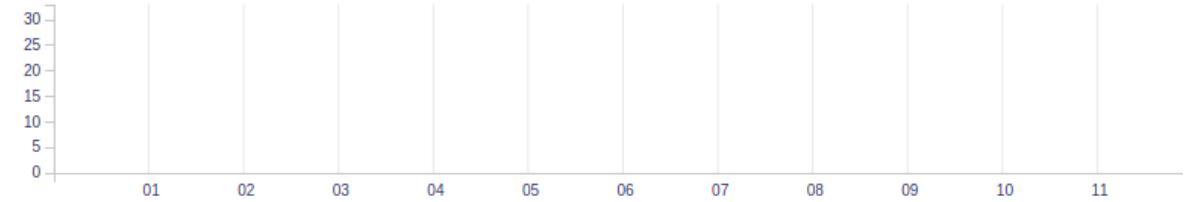
Abbildung 43: Überblick Security Onion-Komponenten[122]

[121] Vgl. https://www.elastic.co/de/products/beats (Stand 29.04.2019)

[122] *https://user-images.githubusercontent.com/16829864/38870831-025d1ae2-421d-11e8-9b68-ac1d7d8113a6.png) (Stand 06.05.2019)*

Es beinhaltet Elasticsearch, Logstash, Kibana, Snort, Suricata, Bro, Wazuh, Squil, Squert, CyberChef, NetworkMiner und viele weitere Sicherheitstools (siehe Abbildung 43).

Ähnlich wie bei dem reinen ELK-Stack arbeitet der Analyst mit Kibana und wertet die dort eingehenden Daten aus. Es stehen deutlich mehr Daten für den Analysten zur Verfügung, da die vorinstallierten Tools bereits angebunden sind und schon vor dem ersten Einspeisen von Beats-Daten Daten empfangen und speichern. Aufgrund diverser Netzwerksniffer kann bereits ohne Client-Anbindung ein Angriff im Netzwerk erkannt werden (siehe Abbildung 44).



QUEUE		SC	DC	ACTIVITY	LAST EVENT	SIGNATURE
49	7	1	1		16:36:31	[OSSEC] Integrity checksum changed.
40		1	2		15:40:24	ET POLICY DNS Update From External net
10	7	1	1		17:45:38	[OSSEC] Listened ports status (netstat) changed (new port opened or closed).
8		1	1		15:09:51	ET SCAN NMAP OS Detection Probe
4		1	1		15:07:05	ET SCAN Potential VNC Scan 5800-5820
3	5	1	1		15:58:54	[OSSEC] File added to the system.
3		1	1		15:06:23	ET SCAN Potential VNC Scan 5900-5920
2		1	1		15:09:14	ET SCAN Suspicious inbound to mSQL port 4333
2		1	1		15:05:09	ET SCAN Suspicious inbound to Oracle SQL port 1521
2		1	1		15:03:57	ET SCAN Suspicious inbound to MSSQL port 1433
2		1	1		15:00:28	ET SCAN Suspicious inbound to PostgreSQL port 5432
2		1	1		14:45:11	ET SCAN Suspicious inbound to mySQL port 3306

Abbildung 44: Auszug aus Squert nach NMAP-Scan (eigene Darstellung)

Ein Portscan, der verwendet wurde, um die offenen Ports in Security Onion zu prüfen schlug in Squert, das über Kibana erreicht werden kann, sofort Alarm und meldete verdächtige Aktivitäten im Netzwerk. Squert nutzt die Squil-Datenbank, die Daten des IDS speichert, um diese visuell darzustellen, zu gewichten und in logische Gruppen zu

unterteilen. In Squert können Daten aus NIDS, HIDS, Asset-Daten und die von Bro bereitgestellten http-Logs dargestellt werden.[123]

Bro bzw. Zeek ist ein Netzwerkanalyse-Framework, das hauptsächlich als Intrusion-Detection-System (IDS) dient (siehe Abbildung 45).[124]

Die vorgefertigten Dashboards zeigen dem Analysten direkt die wichtigsten Inforationen. So wurden direkt während des Portscans schon angezeigt, dass im Augenblick ein Portscan von 192.168.3.20 (Server) nach 192.168.3.241 (Security Onion) durchgeführt wird.

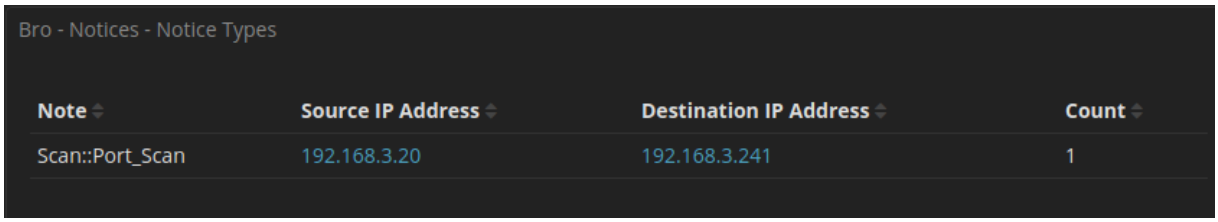


Abbildung 45: Bro-Meldung des Portscans (eigene Darstellung)

Das NIDS zeigt weitere hilfreiche Informationen an und klassifiziert diese direkt.

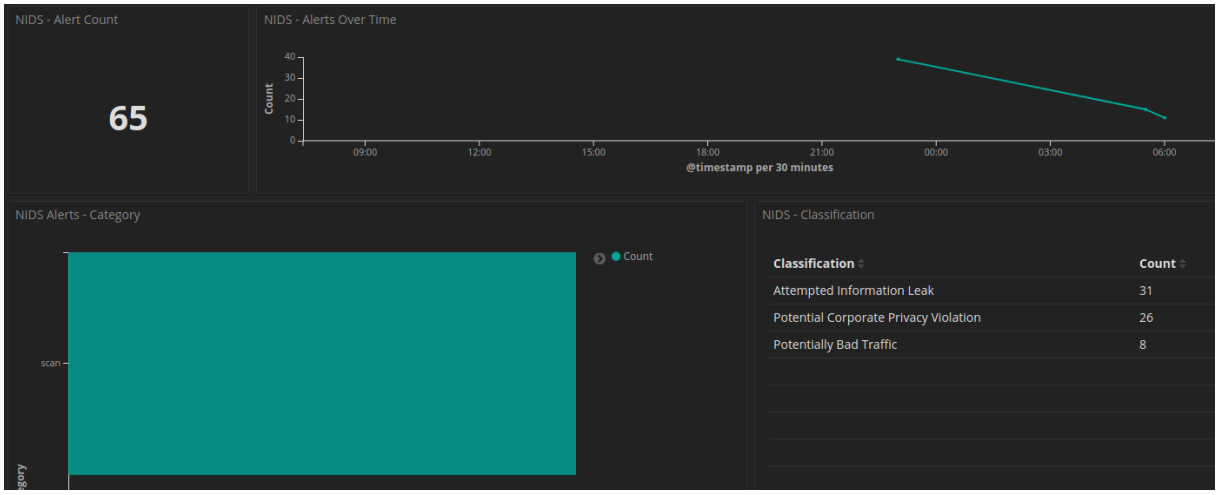


Abbildung 46: NIDS-Meldung nach Portscan (eigene Darstellung)

Die erkannten Meldungen und Angriffe können über das Plugin Elastalert direkt an den Analysten oder weitere Instanzen (Datenschutzbeauftragter, Informationssicherheitsbeauftragter, …) per E-Mail geschickt werden. Diese

[123] Vgl. https://github.com/Security-Onion-Solutions/security-onion/wiki/Squert (Stand 01.05.2019)

[124] Vgl. http://www.admin-magazine.com/Archive/2014/24/Network-analysis-with-the-Bro-Network-Security-Monitor (Stand 01.05.2019)

Möglichkeit kann auch zum automatisierten Erstellen von Tickets in einem Incident-Response-Tool genutzt werden (siehe Abbildung 47).

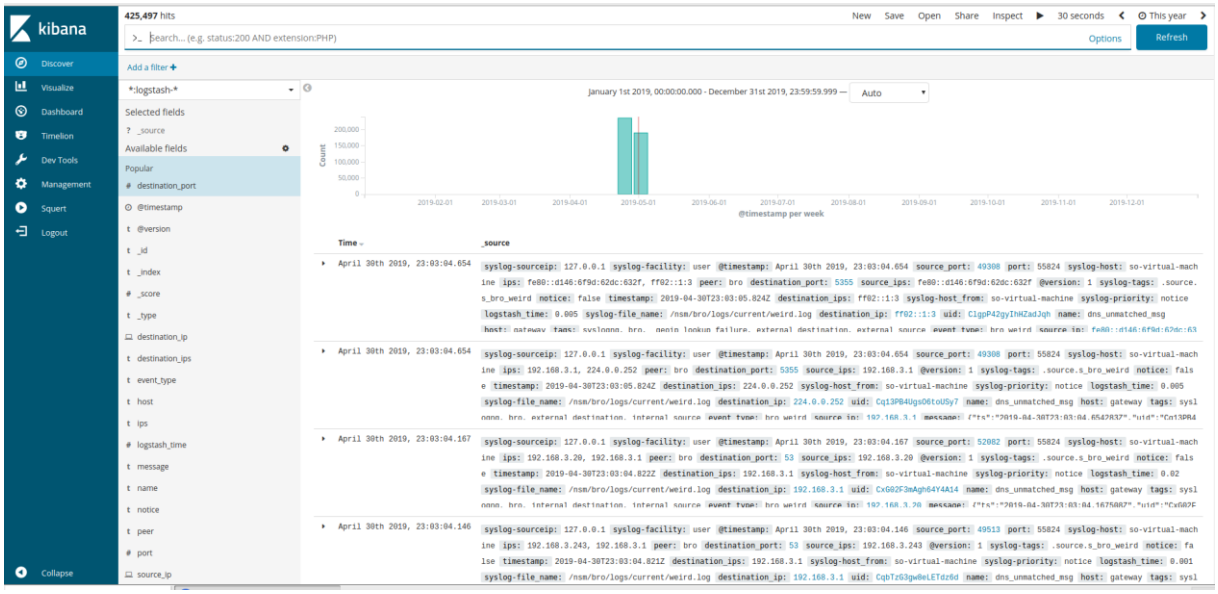


Abbildung 47: Kibana-Weboberfläche des Analysten (eigene Darstellung)

Snort ist ein Network-Intrusion-Detection-System (NIDS), das verdächtige Pakete, Aktivitäten und Verbindungen erkennt Dabei kann ein flexibler Regelsatz erstellt werden, der zum Beispiel Portscans, Angriffe auf Server und Schwachstellen Scans abwehren kann. Über diverse Plugins können Subsysteme zur Angriffserkennung und zum Logging erweitert werden.[125]

Suricata ist eine Echtzeit-Angriffserkennung für IDS, IPS, NSM und offline PCAP-Dateien. Bei der Analyse des Verkehrs werden Regeln und Signaturen angewendet, um daraus auch komplexe Bedrohungen ableiten zu können.[126]

Cyberchef kann Texte entschlüsseln, Archive entpacken, Programmcode hervorheben, Schadcode analysieren.[127] Ebenso hilft es bei der Encodierung von XOR oder Base64, berechnet Hashwerte und Checksummen und unterstützt komplexe Verschlüsselungen wie AES, DES und Blowfish.[128]

---

[125] Vgl. https://www.heise.de/download/product/snort-6004 (Stand 01.05.2019)

[126] Vgl. https://suricata-ids.org/ (Stand 01.05.2019)

[127] Vgl. https://www.heise.de/ratgeber/Schnelle-Rezepte-zum-Kombinieren-von-Datenoperationen-4334220.html (Stand 01.05.2019)

[128] Vgl. https://github.com/gchq/CyberChef (Stand 01.05.2019)

Wazuh kann Bedrohungen erkennen und automatische Reaktionen darauf bieten und unterstützt bei folgenden Aufgaben:

- Log- und Ereignissammlung
- Monitoring der Datei- und Registryintegrität
- Inventarisierung von Prozessen und installierten Anwendungen
- Monitoring offener Ports und Netzwerkkonfigurationen
- Erkennung von Rootkits und Malwareartefakten
- Ausführung aktiver Antworten auf Angriffe.[129]

Der NetworkMiner kann als passiver Netzwerkscanner oder zum Speichern von PCAC-Dateien genutzt werden, die später forensisch analysiert werden können.[130]

Elastalert ist ein Plugin, das eine Erstellung von Alarmmeldungsregeln direkt über die Kibana-Oberfläche ermöglicht. Derzeit sind folgende Regeln in Elastalert enthalten:

- Frequenz: X Events in Y Zeit
- Spitze: Melde, wenn die Rate von X über- oder unterschritten wird
- Black-/Whitelist: Melde, sobald ein Feld einen Wert enthält.
- Beliebiger Wert: Melde, sobald Wert X in einem Feld steht
- Änderung: Melde, sobald in Zeit X Unterschiedliche Werte gemeldet werden.[131]

7.3 Vergleich

Bei einem direkten Vergleich der Module fällt auf, dass Security Onion von Haus aus mit diversen Features ausgestattet ist, die einen schnellen Einsatz eines Network Security Monitoring (NSM) erlauben. Hiermit sind durch die integrierten Paketfilter und Paketanalysen direkt nach der Installation von Security Onion Daten im Netzwerk lesbar. Da der Elastic-Stack auf einem eigenen Betriebssystem installiert werden muss, müssen Elasticsearch, Kibana und Logstash einzeln installiert und konfiguriert werden. Bei Security Onion sind auch diese Programme bereits in der Standardinstallation enthalten. Da jedoch die Entwickler neue Programmversionen des Elastic-Stacks erst testen und anschließend implementieren müssen, ist in der

[129] Vgl. https://wazuh.com/product/ (01.05.2019)

[130] Vgl. https://www.netresec.com/?page=Networkminer (Stand 01.05.2019)

[131] Vgl. https://buildmedia.readthedocs.org/media/pdf/elastalert/latest/elastalert.pdf (Stand 06.09.2019)

Security Onion-Installation meist eine etwas ältere Version des Elastic-Stacks enthalten. So wurde während der ersten Tests die Version 7.3 mit einem integrierten SIEM herausgegeben. Trotz eines Updates in Security Onion, konnte diese Version nicht installiert werden, lediglich ein Update der Version 6.8. Dementsprechend ist in der aktuellen Version von Security Onion auch noch kein Elastic Commom Schema (ECS) implementiert, das die Analyse unterschiedlicher Quellen durch eine Vereinheitlichung von Datenfeldern durchführt. In Tabellen 12 sind weitere Features beschrieben, die bei dem Elastic-Stack nicht implementiert sind.

Tabelle 12: Vergleich Elastic-Stack und Security Onion (eigene Darstellung)

Features	Elastic-Stack	Security Onion	Hinweis
Eigenes OS	Nein	Ja	ELK ist flexibel
Elasticsearch	Ja	Ja	
Kibana	Ja	Ja	
Logstash	Ja	Ja	
Beats	Ja	Ja	
Firewall	Nein	Ja	Anbindung möglich
Snort	Nein	Ja	Anbindung möglich
Suricata	Nein	Ja	Anbindung möglich
Bro	Nein	Ja	Anbindung möglich
Wazuh	Nein	Ja	Anbindung möglich
Squert	Nein	Ja	Anbindung möglich
CyberChef	Nein	Ja	Anbindung möglich
NetworkMiner	Nein	Ja	Anbindung möglich

Während bei Security Onion Programme wie Snort, Bro und Suricata bereits implementiert sind, und automatisch Daten an Elasticsearch weiterleiten, kann bei einer Elastic-Stack-Installation jedes Tool zusätzlich installiert werden, muss aber dafür selbst konfiguriert werden.

Insgesamt lässt sich sagen, dass Security Onion eine vollständige Lösung zum Network Security Monitoring ist und sich perfekt als Zusatz zu einer aktuellen Elastic-

Stack-Installation eignet. Wenn beide Installationen den Netzwerkverkehr und die Logquellen analysieren, können Vorfälle schnell erkannt und gelöst werden.

8. Zusammenfassung und Ausblick

Die Aufdeckung von Aktivitäten, die durch Innentäter verursacht werden, sind schwierig herauszufinden, da Innentäter bereits über legitime Zugriffe verfügen, sich im Netzwerk auskennen und Windows in der Standardkonfiguration zu wenig mitprotokolliert. Werden diese Auditmechanismen aktiviert und angepasst und an eine zentrale Stelle zur Auswertung weitergeleitet, kann eine Korrelation von Ereignissen stattfinden und kann mehr Details liefern, als bei einer forensischen Auswertung eines Notebooks. Da der Server über die Audit-Mechanismen der Netzwerkfreigabe die Zugriffe protokolliert, kann festgestellt werden, auf welche Datei wann zugegriffen wird. Somit konnten Kopiervorgänge, Löschvorgänge, Lesezugriffe und eine Manipulation ohne eine forensische Post-Mortem-Analyse nachgewiesen werden. Da Installationen von Wechseldatenträgern, neue Prozesse, An- und Abmeldungen, Netzwerkzugriffe, etc. auch auf dem Dashboard gemeldet werden, kann ein Analyst bei beiden Lösungen die Daten mit den Zugriffen korrelieren und so die Aktivitäten schnell aufdecken.

Dies war mit der Security Onion-Lösung nur mit den selbstentwickelten Dashboards, jedoch nicht mit der SIEM-Lösung abbildbar. Security Onion bietet viele hilfreiche Programme zum Aufdecken des Netzwerkverkehrs, hat aber dank der fehlenden SIEM-Integration keine praktische Möglichkeit zur Korrelation. Die Security Onion-Lösung nutzt die derzeit verfügbare Elastic Common Schema noch nicht, deshalb müssen Daten der Netzwerktools durch Logstash erneut geparst werden und können dann erst in den Dashboards sinnvoll angezeigt werden. Eine Kombination beider Lösungen kann für Unternehmen einen großen Mehrwert liefern. Wenn die Daten des Netzwerkverkehrs von Security Onion an den Elastic-Stack mit SIEM weitergeleitet werden, kann eine Korrelation des gesamten Netzwerkverkehrs vorgenommen werden.

Bei einem Angriff durch einen Innen- oder Außentäter können Verbindungsversuche durch eine Firewall blockiert werden. Wird diese überwunden, kann das IPS den Datenstrom unterbinden. Dringt der Angreifer trotzdem ein, schützt das Antivirenprogramm oder ein Whitelisting vor Schadsoftware. Gelingt der Angreifer bis zu den Daten, auf die er es abgesehen hat, kann das DLP vor einer Exfiltration

schützen. Schlägt auch diese fehl, kann ein DRM das Lesen der Daten unterbinden. Eine Verschlüsselung über EFS bietet die Möglichkeit, dass nur Nutzer, die das Zertifikat haben, auf die Daten zugreifen können. Die Daten werden dabei mit dem öffentlichen Schlüssel verschlüsselt und können nur mit dem privaten Schlüssel verschlüsselt werden. Über Bitlocker können Festplatten von DV-Systemen verschlüsselt werden, damit ein Innentäter ohne gültiges Kennwort nicht offline auf die Daten zugreifen kann. Somit ist auch der Ausbau einer Festplatte für den Innentäter sinnlos, da nur ein verschlüsseltes Laufwerk vorliegt. Mit einem adäquaten Kennwort ist ein guter Schutz gewährleistet.

Werden diese Maßnahmen mit der Security Onion- und der Elastic-Stack-Lösung kombiniert, können Vorfälle, egal ob von Innen- oder Außentäter weitestgehend aufgedeckt werden. Damit ist die Lösung eine Möglichkeit zur Erweiterung der Post-Mortem-Analyse. Da sich Logdaten und deren enthaltenen Informationen teilweise von Update zu Update ändern, ist eine entsprechende Anpassung inkl. Normalisierung regelmäßig durchzuführen. Die Installation dieser Lösung stellt demnach eine einmalige Angelegenheit dar, sondern ist in einem regelmäßigen Zyklus durchzuführen.

Abkürzungsverzeichnis

AES	Advanced Encryption Standard
BAFIN	Bundesanstalt für Finanzdienstleistungsaufsicht
BSI	Bundesamt für Sicherheit in der Informationstechnik
DES	Data Encryption Standard
DLP	Data Leak Prevention
EFS	Encrypting File System
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
KI	Künstliche Intelligenz
NIDS	Network Intrusion Detection System
NSM	Network Security Monitoring
PCAP	Packet Capture
SCADA	Supervisory Control And Data Acquisition
SIEM	Security Information and Event Management

Literatur- und Quellenverzeichnis

Elasticsearch B.V. (02. 06 2019). *Elasticsearch*. Von https://www.elastic.co/de/products/elasticsearch abgerufen

al, K. H. (2016). *IT-Management nach ISO27001.* Wiesbaden: Springer Verlag.

Bartsch, M. (2018). *Cybersecurity Best Practices.* Wiesbaden: Springer Verlag.

Bejtlich, R. (2005). *The tao of network security monitoring: beyond intrusion detection.* Boston: Pearson Education Inc.

Bibliographisches Institut GmbH. (03. 09 2019). *Duden*. Von https://www.duden.de/rechtschreibung/entwenden abgerufen

Bibliographisches Institut GmbH. (03. 09 2019). *Duden*. Von Stehlen: https://www.duden.de/rechtschreibung/stehlen abgerufen

Brüss, M. (05. 09 2019). *Versicherungsjournal*. Von Wirtschaftskriminalität: GDV warnt vor Tabuthema Mitarbeiter: https://www.versicherungsjournal.de/markt-und-politik/wirtschaftskriminalitaet-gdv-warnt-vor-tabuthema-mitarbeiter-136521.php abgerufen

BSI. (2008). *BSI-Standard 100-1. Managementsysteme für Informationssicherheit (ISMS).* Bonn: Bundesamt für Sicherheit in der Informationstechnik.

BSI. (02 2019). IT-Grundschutz-Kompendium 2019. Wiesbaden, Deutschland.

Bundesamt für Sicherheit in der Informationstechnik. (20. 05 2019). *IT-Grundschutzkatalog*. Von https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b05/b05022.html?nn=6610630 abgerufen

Bundeskriminalamt, F. u. (2015). *Täter im Bereich Cybercrime.* Wiesbaden: Bundeskriminalamt. Von https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&cad=rja&uact=8&ved=2ahUKEwjYtJz4i4fgAhVPqaQKHVaLCh0QFjAEegQIBhAC&url=https%3A%2F%2Fcdn.netzpolitik.org%2Fwp-upload%2FBKA-Studie_Taeter-im-Bereich-Cybercrime_Eine-Literaturanalyse.pdf&usg=AOvV abgerufen

Bundesministerium der Justiz und für Verbraucherschutz . (04. 09 2019). *Gesetze-im-Internet.de*. Von https://www.gesetze-im-internet.de/bsig_2009/__8a.html abgerufen

Center for Internet Security®. (07. 08 2019). *CIS-Controls*. Von https://www.cisecurity.org/controls/cis-controls-list/ abgerufen

Channelpartner. (05. 09 2019). *Channelpartner*. Von Kriminelle Mitarbeiter verursachen mehr Schaden als externe Täter: https://www.channelpartner.de/a/kriminelle-mitarbeiter-verursachen-mehr-schaden-als-externe-taeter,3606122 abgerufen

Computec Media GmbH . (01. 02 2016). *Linux-Magazin.de*. Von Elasticsearch, Logstash & Kibana: https://www.linux-magazin.de/ausgaben/2016/02/elk-stack/ abgerufen

Dörsam, A. (2017). *Den Tätern auf der Spur.* Wiesbaden: Springer Verlag.

Elasticsearch B.V. (02. 07 2019). *Advanced Pipeline*. Von https://www.elastic.co/guide/en/logstash/2.3/advanced-pipeline.html abgerufen

Elasticsearch B.V. (06. 07 2019). *Beats*. Von https://www.elastic.co/de/products/beats abgerufen

Elasticsearch B.V. (07. 08 2019). *File Integrity Module*. Von https://www.elastic.co/guide/en/beats/auditbeat/master/auditbeat-module-file_integrity.html abgerufen

Forum Wirtschaftskriminalität. (01. 05 2019). *Dolose Handlungen*. Von http://www.forum-wirtschaftskriminalitaet.org/einfuehrung/begriffe/dolose-handlungen.html abgerufen

Gabler. (03. 09 2019). *Wirtschaftslexikon*. Von https://wirtschaftslexikon.gabler.de/definition/aggregation-30653 abgerufen

Gabler Verlag. (19. 02 2018). *Wirtschaftslexikon*. Von https://wirtschaftslexikon.gabler.de/definition/besitz-27446 abgerufen

Geschonneck, A. (2014). *Computer-Forensik.* Berlin: dpunkt.verlag.

Geschonneck, A. (kein Datum). *www.computer-forensik.org*. Abgerufen am 24. 01 2019 von https://www.computer-forensik.org/blog/2008/01/29/studie-zu-angriffen-von-innentatern/

Greve, H. (12 2009). Kritische Infrastrukturen. *DuD • Datenschutz und Datensicherheit* , S. 756f.

Handelskammerjournal. (30. 10 2018). *Handelskammerjournal*. Abgerufen am 01. 12 2019 von https://www.handelskammerjournal.ch/innentaeter-ein-unterschaetztes-risiko

Heise Medien GmbH & Co. KG. (28. 08 2019). *Snort 2.9.7.3*. Von https://www.heise.de/download/product/snort-6004 abgerufen

Heise Verlag. (26. 07 2013). *Volltextsuche mit ElasticSearch* . Von https://www.heise.de/developer/artikel/Volltextsuche-mit-ElasticSearch-1920454.html?seite=all abgerufen

Inc., W. (08. 08 2019). *A comprehensive open source security platform*. Von Wazuh agent: https://wazuh.com/product/ abgerufen

Informationstechnik, B. f. (2017). *Informationssicherheit und IT-Grundschutz.* Köln: Bundesanzeiger Verlag GmbH.

Intersoft Consultin. (04. 09 2019). *dsgvo-gesetz.de*. Von https://dsgvo-gesetz.de/bdsg/76-bdsg/ abgerufen

Justiz, B. f. (09. 09 20). *gesetze-im-internet.de*. Von Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG): https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html abgerufen

Klapproth, U. (2017). *Tax Fraud & Forensic Accounting - Umgang mit Wirtschaftskriminalität.* München: Springer Fachmedien Wiesbaden.

Kral, P. (05. 12 2011). *SANS-Institute.* Von Incident Handler's Handbook: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901 abgerufen

Kuhlee, L. (2012). *Computer Forensik Hacks.* Köln: O'Reilly Verlag GmbH & Co. KG.

Logz.io. (01. 07 2019). *Complete Guide ELk-Stack*. Von https://logz.io/learn/complete-guide-elk-stack/ abgerufen

Luber, S. (06. 11 2018). *Was ist ein SIEM?* Von https://www.security-insider.de/was-ist-ein-siem-a-772821/ abgerufen

Luber, S. (28. 05 2019). *Security-Insider*. Von https://www.security-insider.de/was-ist-ein-intrusion-detection-system-ids-a-612870/ abgerufen

Malware Archaeology LLC. (05. 06 2019). *Malware Archaeology*. Von Cheat Sheets: https://www.malwarearchaeology.com/cheat-sheets abgerufen

McCarty, R. (09. 02 2014). *Admin-Magazine.de*. Von Network analysis with the Bro Network Security Monitor: http://www.admin-magazine.com/Archive/2014/24/Network-analysis-with-the-Bro-Network-Security-Monitor abgerufen

Menges, F., Böhm, F., Vielberth, M., Puchta, A., Taubmann, B., Rakotondravony, N., & Latzo, T. (2018). *Introducing DINGfest: An architecture for next generation SIEM systems*. Abgerufen am 27. 6 2019 von https://epub.uni-regensburg.de/37266

Microsoft. (13. 08 2019). *Microsoft Technet*. Von Grundsätzliche Informationen zum Security Event Logging / Auditing: https://blogs.technet.microsoft.com/deds/2008/07/22/grundstzliche-informationen-zum-security-event-logging-auditing/ abgerufen

Microsoft Corporation. (31. 05 2017). *Empfehlungen zu Überwachungsrichtlinien*. Von https://docs.microsoft.com/de-de/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations abgerufen

Mittelstaedt, A. (19. 02 2018). *Gabler Wirtschaftslexikon*. Von Gabler Wirtschaftslexikon: https://wirtschaftslexikon.gabler.de/definition/geistiges-eigentum-53871/version-276933 abgerufen

Mühlich, R. (02. 07 2019). *Computerwoche*. Von Zutritt, Zugang oder Zugriff?: https://www.computerwoche.de/a/zutritt-zugang-oder-zugriff,3096937 abgerufen

National Institute for Standards of Technology. (18. 05 2019). *Guide to Computer Security Log Management*. Von https://csrc.nist.gov/publications/detail/sp/800-92/final abgerufen

NETRESEC AB. (07. 08 2019). *NetworkMiner*. Von https://www.netresec.com/?page=Networkminer abgerufen

Newman, R. (2007). *Computer forensics: evidence collection and management.* Boca Raton, Florida: Taylor & Francis Group, LLC.

Open Information Security Foundation. (05. 08 2019). *Sucicata-IDS*. Von https://suricata-ids.org/ abgerufen

Pranav Shukla, S. K. (2017). *Learning Elastic Stack 6.0: A beginner's guide to distributed search, analytics, and visualization using Elasticsearch, Logstash and Kibana (English Edition).* Packt.

Randy Smith. (09. 04 2019). *Windows Security Log Event ID 6416*. Von https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=6416 abgerufen

Riegel, D. (20. 09 2019). *to.com*. Von Log Management vs. SIEM: Gemeinsamkeiten und Unterschiede: https://blog.to.com/log-management-vs-siem-gemeinsamkeiten-und-unterschiede abgerufen

Rouse, M. (01. 07 2015). *RESTful API*. Von https://www.computerweekly.com/de/definition/RESTful-API abgerufen

Rouse, M. (05. 08 2019). *Computerweekly.com*. Von https://www.computerweekly.com/de/definition/Vorfallreaktionsplan-Incident-Response-Plan-IRP abgerufen

Rowlingson, R. (2004). A Ten Step Process for Forensic Readiness. New Yoek, USA.

Sanders, C., & Smith, J. (2016). *Hacking mit Security Onion: Sicherheit im Netzwerk überwachen: Daten sammeln, analysieren und Angriffe rechtzeitig erkennen.* Franzis.

Schlede, F.-M. (10. 09 2012). *TecChannel*. Von https://www.tecchannel.de/a/workshop-log-dateien-auf-windows-systemen-auswerten,2032597,5 abgerufen

Schneider, P. D. (05. 09 2019). *GDV.de*. Von Wirtschaftskriminalität: Tabuthema Innentäter: https://www.gdv.de/resource/blob/50540/5a143d772962c2ddf43432f3a47fc1f7/download-verlaufsmodell-data.pdf abgerufen

Schonscheck, O. (03. 10 2017). *www.security-insider.de*. Abgerufen am 24. 01 2019 von https://www.security-insider.de/warum-insider-attacken-so-gefaehrlich-sind-a-588534/

Secupedia. (01. 09 2019). *Die Plattform für Sicherheits-Informationen*. Von https://www.secupedia.info/wiki/SIEM abgerufen

Security Onion Solutions, LLC. (16. 05 2019). Von https://user-images.githubusercontent.com/16829864/38870831-025d1ae2-421d-11e8-9b68-ac1d7d8113a6.png abgerufen

Security Onion Solutions, LLC. (03. 08 2019). *Firewall*. Von https://securityonion.readthedocs.io/en/latest/firewall.html abgerufen

Security Onion Solutions, LLC. (07. 06 2019). *Squert*. Von https://github.com/Security-Onion-Solutions/security-onion/wiki/Squert abgerufen

Sprotte, U. (23. 03 2012). *Security Information- und Event-Management automatisieren*. Von SIEM-Systeme richtig konfigurieren und einsetzen: https://www.security-insider.de/siem-systeme-richtig-konfigurieren-und-einsetzen-a-357534/index5.html abgerufen

Statista GmbH. (03. 09 2019). *Statistik-Lexikon: Definition Korrelation* . Von https://de.statista.com/statistik/lexikon/definition/77/korrelation/ abgerufen

Sule, D. (2014). *ISACA Journal*. Von Importance of Forensic Readiness : https://www.isaca.org/Journal/archives/2014/Volume-1/Pages/JOnline-Importance-of-Forensic-Readiness.aspx?utm_referrer= abgerufen

Tanriverdi, T. (21. 12 2018). *Süddeutsche Zeitung GmbH* . Abgerufen am 14. 01 2019 von https://www.sueddeutsche.de/digital/it-sicherheit-innentaeter-hacker-1.4260798

Tietz, A. M. (kein Datum). *Data Leakage Prevention". In: Patrick Horster, Peter Schartner (Hrsg.): "D.A.CH Security 2009 – Bestandsaufnahme, Konzepte, Anwendungen, Perspektiven.* Abgerufen am 26. 6 2019

T-Systems Austria GesmbH. (08. 11 2017). *Zentrales Log-Management vs. SIEM*. Von https://www.t-systems.com/at/de/newsroom/blog/security/securityservices/zentrales-log-management-vs--siem-766564 abgerufen

Van Randen, H. (2016). *Einführung in UML.* Wiesbaden: Springer Fachmedien.

Verfassungsschutz. (2017). *www.verfassungsschutz.de*. (Verfassungsschutz) Abgerufen am 24. 01 2019 von https://www.verfassungsschutz.de/de/aktuelles/schlaglicht/schlaglicht-2015-06-asw-tagung-innentaeter

Verlag, H. (19. 03 2019). *CyberChef: Mit wenigen Klicks Datenoperationen kombinieren* . Von https://www.heise.de/ratgeber/Schnelle-Rezepte-zum-Kombinieren-von-Datenoperationen-4334220.html abgerufen

Walter, J. (18. 06 2019). *der-windows-papst.de*. Von https://www.der-windows-papst.de/wp-content/uploads/2018/01/Windows-EFS-Verschl%C3%BCsselung.pdf abgerufen

Willer, C. (2012). *PC-Forensik - Daten suchen und wiederherstellen.* Böblingen: C&L Computer und LIteraturverlag.

Wyllie, D. (28. 10 2009). *Computerwoche*. Von https://www.computerwoche.de/a/mysql-ist-guenstig-sicher-und-stabil,1906974,4 abgerufen

Abbildungsverzeichnis

Tabellenverzeichnis

Anlagen

Anlage I

```
C:\Users\Administrator>auditpol.exe /get /category:*
Systemüberwachungsrichtlinie
Kategorie/Unterkategorie                    Einstellung
System
  Sicherheitssystemerweiterung              Keine Überwachung
  Systemintegrität                          Erfolg und Fehler
  IPSEC-Treiber                             Keine Überwachung
  Andere Systemereignisse                   Erfolg und Fehler
  Sicherheitsstatusänderung                 Erfolg
An-/Abmeldung
  Anmelden                                  Erfolg und Fehler
  Abmelden                                  Erfolg
  Kontosperrung                             Erfolg
  IPsec-Hauptmodus                          Keine Überwachung
  IPsec-Schnellmodus                        Keine Überwachung
  IPsec-Erweiterungsmodus                   Keine Überwachung
  Spezielle Anmeldung                       Erfolg
  Andere Anmelde-/Abmeldeereignisse         Keine Überwachung
  Netzwerkrichtlinienserver                 Erfolg und Fehler
  Benutzer-/Geräteansprüche                 Keine Überwachung
  Gruppenmitgliedschaft                     Keine Überwachung
Objektzugriff
  Dateisystem                               Keine Überwachung
  Registrierung                             Keine Überwachung
  Kernelobjekt                              Keine Überwachung
  SAM                                       Keine Überwachung
  Zertifizierungsdienste                    Keine Überwachung
  Anwendung wurde generiert.                Keine Überwachung
  Handleänderung                            Keine Überwachung
  Dateifreigabe                             Keine Überwachung
  Filterplattform: Verworfene Pakete        Keine Überwachung
  Filterplattformverbindung                 Keine Überwachung
  Andere Objektzugriffsereignisse           Keine Überwachung
  Detaillierte Dateifreigabe                Keine Überwachung
  Wechselmedien                             Keine Überwachung
  Staging zentraler Richtlinien             Keine Überwachung
Berechtigungen
  Nicht sensible Verwendung von Rechten     Keine Überwachung
  Andere Rechteverwendungsereignisse        Keine Überwachung
  Sensible Verwendung von Rechten           Keine Überwachung
Detaillierte Nachverfolgung
  Prozesserstellung                         Keine Überwachung
  Prozessbeendigung                         Keine Überwachung
  DPAPI-Aktivität                           Keine Überwachung
  RPC-Ereignisse                            Keine Überwachung
  Plug & Play-Ereignisse                    Keine Überwachung
  Token Right Adjusted Events               Keine Überwachung
```

Abbildung 48: Auszug der überwachten Logereignisse Teil 1 (eigene Darstellung)

```
C:\Users\Administrator>auditpol.exe /get /category:*
Systemüberwachungsrichtlinie
Kategorie/Unterkategorie                    Einstellung
System
  Sicherheitssystemerweiterung              Keine Überwachung
  Systemintegrität                          Erfolg und Fehler
  IPSEC-Treiber                             Keine Überwachung
  Andere Systemereignisse                   Erfolg und Fehler
  Sicherheitsstatusänderung                 Erfolg
An-/Abmeldung
  Anmelden                                  Erfolg und Fehler
  Abmelden                                  Erfolg
  Kontosperrung                             Erfolg
  IPsec-Hauptmodus                          Keine Überwachung
  IPsec-Schnellmodus                        Keine Überwachung
  IPsec-Erweiterungsmodus                   Keine Überwachung
  Spezielle Anmeldung                       Erfolg
  Andere Anmelde-/Abmeldeereignisse         Keine Überwachung
  Netzwerkrichtlinienserver                 Erfolg und Fehler
  Benutzer-/Geräteansprüche                 Keine Überwachung
  Gruppenmitgliedschaft                     Keine Überwachung
Objektzugriff
  Dateisystem                               Keine Überwachung
  Registrierung                             Keine Überwachung
  Kernelobjekt                              Keine Überwachung
  SAM                                       Keine Überwachung
  Zertifizierungsdienste                    Keine Überwachung
  Anwendung wurde generiert.                Keine Überwachung
  Handleänderung                            Keine Überwachung
  Dateifreigabe                             Keine Überwachung
  Filterplattform: Verworfene Pakete        Keine Überwachung
  Filterplattformverbindung                 Keine Überwachung
  Andere Objektzugriffsereignisse           Keine Überwachung
  Detaillierte Dateifreigabe                Keine Überwachung
  Wechselmedien                             Keine Überwachung
  Staging zentraler Richtlinien             Keine Überwachung
Berechtigungen
  Nicht sensible Verwendung von Rechten     Keine Überwachung
  Andere Rechteverwendungsereignisse        Keine Überwachung
  Sensible Verwendung von Rechten           Keine Überwachung
Detaillierte Nachverfolgung
  Prozesserstellung                         Keine Überwachung
  Prozessbeendigung                         Keine Überwachung
  DPAPI-Aktivität                           Keine Überwachung
  RPC-Ereignisse                            Keine Überwachung
  Plug & Play-Ereignisse                    Keine Überwachung
  Token Right Adjusted Events               Keine Überwachung
```

Abbildung 49: Auditpol-Ausgabe nach Anpassung (eigene Darstellung)

Anlage II: Überwachungsrichtlinie

Table 1: Empfehlungen zur Audit-Richtlinie[132]

WindowsServer 2016, Windows Server 2012 R2, WindowsServer 2012, Windows Server 2008 R2 und Windows Server 2008 Audit Settings Empfehlungen			
Audit Policy-Kategorie oder Unterkategorie	**Windows -Standard**	**Baseline-Empfehlung**	**Eine stärkere Empfehlung**
	Erfolg Fehler	**Erfolg Fehler**	**Erfolg Fehler**
Kontoanmeldung			
Überprüfen der Anmeldeinformationen überwachen	Nein, nein	Ja, ja	Ja, ja
Kerberos-Authentifizierungsdienst überwachen			Ja, ja
Ticketvorgänge des Kerberos-Diensts überwachen			Ja, ja
Andere Kontoanmeldungsereignisse überwachen			Ja, ja
Kontoverwaltung			
Anwendungsgruppenverwaltung überwachen			
Computerkontoverwaltung überwachen		Ja DC	Ja, ja
Verteilergruppenverwaltung überwachen			
Andere Kontoverwaltungsereignisse überwachen		Ja, ja	Ja, ja
Sicherheitsgruppenverwaltung überwachen		Ja, ja	Ja, ja
Benutzerkontenverwaltung überwachen	Ja Nein	Ja, ja	Ja, ja
Detaillierte nachverfolgung			
DPAPI-Aktivität überwachen			Ja, ja
Prozesserstellung überwachen		Ja Nein	Ja, ja
Prozessbeendung überwachen			
RPC-Ereignisse überwachen			
DS-Zugriff			
Detaillierte Verzeichnisdienstreplikation überwachen			
Verzeichnisdienstzugriff überwachen		DC DC	DC DC
Verzeichnisdienständerungen überwachen		DC DC	DC DC

[132] Quelle: https://docs.microsoft.com/de-de/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations (Stand 07.05.2019)

Verzeichnisdienstreplikation überwachen			
An- und Abmeldung			
Kontosperrung überwachen	Ja Nein		Ja Nein
Benutzer-/Geräteansprüche überwachen			
IPsec-Erweiterungsmodus überwachen			
IPsec-Hauptmodus überwachen			IF IF
IPsec-Schnellmodus überwachen			
Abmelden überwachen	Ja Nein	Ja Nein	Ja Nein
Anmelden überwachen	Ja, ja	Ja, ja	Ja, ja
Netzwerkrichtlinienserver überwachen	Ja, ja		
Andere Anmelde-/Abmeldeereignisse überwachen			Ja, ja
Spezielle Anmeldung überwachen	Ja Nein	Ja Nein	Ja, ja
Zugriff auf Objekte			
Anwendung generiert überwachen			
Zertifizierungsdienste überwachen			
Detaillierte Dateifreigabe überwachen			
Dateifreigabe überwachen			
Dateisystem überwachen			
Filterplattformverbindung überwachen			
Filterplattform: Verworfene Pakete überwachen			
Handleänderung überwachen			
Kernelobjekt überwachen			
Andere Objektzugriffsereignisse überwachen			
Registrierung überwachen			
Wechselmedien überwachen			
SAM überwachen			
Staging zentraler Zugriffsrichtlinien überwachen			
Änderung der Richtlinie			
Überwachungsrichtlinienänderung überwachen	Ja Nein	Ja, ja	Ja, ja
Authentifizierungsrichtlinienänderung überwachen	Ja Nein	Ja Nein	Ja, ja
Autorisierungsrichtlinienänderung überwachen			
Filterplattform-Richtlinienänderung überwachen			
MPSSVC-Richtlinienänderung auf Regelebene überwachen			Ja

Andere Richtlinienänderungsereignisse überwachen			
Rechteverwendung			
Nicht sensible Verwendung von Rechten überwachen			
Andere Rechteverwendungsereignisse überwachen			
Sensible Verwendung von Rechten überwachen			
System			
IPsec-Treiber überwachen		Ja, ja	Ja, ja
Andere Systemereignisse überwachen	Ja, ja		
Sicherheitsstatusänderung überwachen	Ja Nein	Ja, ja	Ja, ja
Sicherheitssystemerweiterung überwachen		Ja, ja	Ja, ja
Systemintegrität überwachen	Ja, ja	Ja, ja	Ja, ja
Globale Überprüfung			
IPsec-Treiber überwachen			
Andere Systemereignisse überwachen			
Sicherheitsstatusänderung überwachen			
Sicherheitssystemerweiterung überwachen			
Systemintegrität überwachen			

Anlage III

Table 2 Zu überwachende Ereignisse:[133]

Aktuelle Windows-Ereignis-ID	**Ältere Windows-Ereignis-ID**	**Potenzielle Gefährlichkeit**	**Ereigniszusammenfassung**
4618	Nicht zutreffend	Hoch	Ein überwachtes Sicherheitsmuster ist aufgetreten.
4649	Nicht zutreffend	Hoch	Ein Replay-Angriff wurde erkannt. Möglicherweise ein harmloser falsch positives Ergebnis aufgrund einer fehlerhaften Konfiguration-Fehler auf.
4719	612	Hoch	Die Systemüberwachungsrichtlinie wurde geändert.
4765	Nicht zutreffend	Hoch	Der SID-Verlauf eines Kontos wurde hinzugefügt.
4766	Nicht zutreffend	Hoch	Fehler beim Versuch, den SID-Verlauf einem Konto hinzuzufügen.
4794	Nicht zutreffend	Hoch	Es wurde versucht, den Verzeichnisdienst-Wiederherstellungsmodus einzustellen.
4897	801	Hoch	Rollentrennung ist aktiviert:
4964	Nicht zutreffend	Hoch	Sondergruppen wurden einer neuen Anmeldung zugewiesen.
5124	Nicht zutreffend	Hoch	Eine Sicherheitseinstellung wurde auf der OCSP-Responder-Dienst aktualisiert.
Nicht zutreffend	550	Mittel bis hoch	Möglichen Denial-of-Service (DoS) Angriffe
1102	517	Mittel bis hoch	Das Überwachungsprotokoll wurde gelöscht.
4621	Nicht zutreffend	Mittel	Der Administrator hat das System nach einem CrashOnAuditFail wiederhergestellt. Benutzer ohne Administratorrechte können sich jetzt anmelden. Einige überwachbare Aktivitäten wurden möglicherweise nicht aufgezeichnet.
4675	Nicht zutreffend	Mittel	SIDs wurden gefiltert.
4692	Nicht zutreffend	Mittel	Es wurde versucht, den Datenschutz-Hauptschlüssel zu sichern.
4693	Nicht zutreffend	Mittel	Es wurde versucht, den Datenschutz-Hauptschlüssel wiederherzustellen.

[133] https://docs.microsoft.com/de-de/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor (Stand 14.09.2019)

4706	610	Mittel	Eine neue Vertrauensstellung zu einer Domäne wurde erstellt.
4713	617	Mittel	Die Kerberos-Richtlinie wurde geändert.
4714	618	Mittel	Die Wiederherstellungsrichtlinie für verschlüsselte Daten wurde geändert.
4715	Nicht zutreffend	Mittel	Die Überwachungsrichtlinie (SACL) für ein Objekt wurde geändert.
4716	620	Mittel	Die Informationen bei einer vertrauenswürdigen Domäne wurden geändert.
4724	628	Mittel	Es wurde versucht, das Kennwort eines Kontos zurückzusetzen.
4727	631	Mittel	Eine sicherheitsaktivierte globale Gruppe wurde erstellt.
4735	639	Mittel	Eine sicherheitsaktivierte lokale Gruppe wurde geändert.
4737	641	Mittel	Eine sicherheitsaktivierte globale Gruppe wurde geändert.
4739	643	Mittel	Die Domänenrichtlinie wurde geändert.
4754	658	Mittel	Eine sicherheitsaktivierte universelle Gruppe wurde erstellt.
4755	659	Mittel	Eine sicherheitsaktivierte universelle Gruppe wurde geändert.
4764	667	Mittel	Eine Gruppe mit deaktivierter Sicherheit wurde gelöscht.
4764	668	Mittel	Der Typ einer Gruppe wurde geändert.
4780	684	Mittel	Die ACL wurde für Konten festgelegt, die Mitglieder der Gruppe „Administratoren“ sind.
4816	Nicht zutreffend	Mittel	Der Remoteprozeduraufruf (RPC) hat bei der Entschlüsselung einer eingehenden Nachricht eine Integritätsverletzung festgestellt.
4865	Nicht zutreffend	Mittel	Ein Informationseintrag für eine vertrauenswürdige Gesamtstruktur wurde hinzugefügt.
4866	Nicht zutreffend	Mittel	Ein Informationseintrag für eine vertrauenswürdige Gesamtstruktur wurde entfernt.
4867	Nicht zutreffend	Mittel	Ein Informationseintrag für eine vertrauenswürdige Gesamtstruktur wurde geändert.
4868	772	Mittel	Die Zertifikatverwaltung hat eine anstehende Zertifikatanforderung abgelehnt.

4870	774	Mittel	Die Zertifikatdienste haben ein Zertifikat gesperrt.
4882	786	Mittel	Die Sicherheitsberechtigungen für die Zertifikatdienste wurden geändert.
4885	789	Mittel	Der Überwachungsfilter für die Zertifikatdienste wurde geändert.
4890	794	Mittel	Die Zertifikatverwaltungseinstellungen für die Zertifikatdienste wurden geändert.
4892	796	Mittel	Es wurde eine Eigenschaft der Zertifikatdienste geändert.
4896	800	Mittel	Eine oder mehrere Zeilen wurden aus der Zertifikatdatenbank gelöscht.
4906	Nicht zutreffend	Mittel	Der CrashOnAuditFail-Wert wurde geändert.
4907	Nicht zutreffend	Mittel	Die Überwachungseinstellungen für das Objekt wurden geändert.
4908	Nicht zutreffend	Mittel	Eine Anmeldetabelle für Sondergruppen wurde geändert.
4912	807	Mittel	Eine Benutzerüberwachungsrichtlinie wurde geändert.
4960	Nicht zutreffend	Mittel	IPsec hat ein eingehendes Paket verworfen, das eine Integritätsüberprüfung nicht bestanden hat Wenn dieses Problem weiterhin besteht, kann dies darauf hinweisen, dass ein Netzwerkproblem vorliegt oder Pakete während der Übertragung an diesen Computer geändert werden. Vergewissern Sie sich, dass die vom Remotecomputer gesendeten Pakete mit den von diesem Computer empfangenen Paketen identisch sind. Dieser Fehler kann auch auf Interoperabilitätsprobleme mit anderen IPsec-Implementierungen hinweisen.
4961	Nicht zutreffend	Mittel	IPsec hat ein eingehendes Paket verworfen, das eine Rahmenprüfung nicht bestanden hat. Wenn dieses Problem weiterhin besteht, kann dies auf einen Replay-Angriff auf diesen Computer hinweisen.
4962	Nicht zutreffend	Mittel	IPsec hat ein eingehendes Paket verworfen, das eine Rahmenprüfung nicht bestanden hat. Die Sequenznummer des eingehenden Pakets war zu niedrig, um zu gewährleisten, dass es sich nicht um einen Replay-Angriff handelt.

4963	Nicht zutreffend	Mittel	IPsec hat ein eingehendes Klartextpaket verworfen, das geschützt hätte sein sollen. Dies ist normalerweise darauf zurückzuführen, dass der Remotecomputer seine IPsec-Richtlinie ändert, ohne diesen Computer zu informieren. Es kann auch auf einen versuchten Spoofingangriff hinweisen.
4965	Nicht zutreffend	Mittel	IPsec hat von einem Remotecomputer ein Paket mit einem falschen Sicherheitsparameterindex (SPI) empfangen. Dies ist normalerweise auf eine fehlerhafte Hardware zurückzuführen, die Pakete beschädigt. Vergewissern Sie sich, dass die vom Remotecomputer gesendeten Pakete mit den von diesem Computer empfangenen Paketen identisch sind, wenn diese Fehler weiterhin auftreten. Dieser Fehler kann auch auf Interoperabilitätsprobleme mit anderen IPsec-Implementierungen hinweisen. In diesem Fall können diese Ereignisse ignoriert werden, sofern die Konnektivität nicht beeinträchtigt ist.
4976	Nicht zutreffend	Mittel	Während der Hauptmodusverhandlung hat IPsec ein ungültiges Verhandlungspaket empfangen. Wenn dieses Problem weiterhin besteht, kann dies darauf hinweisen, dass ein Netzwerkproblem vorliegt oder versucht wird, diese Verhandlung zu ändern oder durch einen Replay-Angriff zu manipulieren.
4977	Nicht zutreffend	Mittel	Während der Schnellmodusverhandlung hat IPsec ein ungültiges Verhandlungspaket empfangen. Wenn dieses Problem weiterhin besteht, kann dies darauf hinweisen, dass ein Netzwerkproblem vorliegt oder versucht wird, diese Verhandlung zu ändern oder durch einen Replay-Angriff zu manipulieren.
4978	Nicht zutreffend	Mittel	Während der Erweiterungsmodusverhandlung hat IPsec ein ungültiges Verhandlungspaket empfangen. Wenn dieses Problem weiterhin besteht, kann dies darauf hinweisen, dass ein Netzwerkproblem vorliegt oder versucht wird, diese Verhandlung zu ändern oder durch einen Replay-Angriff zu manipulieren.

4983	Nicht zutreffend	Mittel	Fehler bei der Verhandlung des IPsec-Erweiterungsmodus. Die entsprechende Sicherheitszuordnung des Hauptmodus wurde gelöscht.
4984	Nicht zutreffend	Mittel	Fehler bei der Verhandlung des IPsec-Erweiterungsmodus. Die entsprechende Sicherheitszuordnung des Hauptmodus wurde gelöscht.
5027	Nicht zutreffend	Mittel	Der Windows-Firewalldienst konnte die Sicherheitsrichtlinie nicht aus dem lokalen Speicher abrufen. Der Dienst wendet weiterhin die aktuelle Richtlinie an.
5028	Nicht zutreffend	Mittel	Der Windows-Firewalldienst konnte die neue Sicherheitsrichtlinie nicht analysieren. Der Dienst wendet weiterhin die aktuelle Richtlinie an.
5029	Nicht zutreffend	Mittel	Der Windows-Firewalldienst konnte den Treiber nicht initialisieren. Der Dienst wendet weiterhin die aktuelle Richtlinie an.
5030	Nicht zutreffend	Mittel	Der Windows-Firewalldienst konnte nicht gestartet werden.
5035	Nicht zutreffend	Mittel	Der Windows-Firewalltreiber konnte nicht gestartet werden.
5037	Nicht zutreffend	Mittel	Der Windows-Firewalltreiber hat einen kritischen Laufzeitfehler erkannt. Der Treiber wird beendet.
5038	Nicht zutreffend	Mittel	Die Codeintegrität hat festgestellt, dass der Abbildhash einer Datei nicht gültig ist. Die Datei wurde möglicherweise durch eine nicht autorisierte Änderung beschädigt. Dieses Problem kann auch auf einen potenziellen Fehler des Datenträgergeräts hinweisen.
5120	Nicht zutreffend	Mittel	OCSP-Responder-Dienst wurde gestartet
5121	Nicht zutreffend	Mittel	OCSP-Responder-Dienst wurde beendet
5122	Nicht zutreffend	Mittel	Ein Konfigurationseintrag in OCSP-Responder-Dienst geändert
5123	Nicht zutreffend	Mittel	Ein Konfigurationseintrag in OCSP-Responder-Dienst geändert
5376	Nicht zutreffend	Mittel	Anmeldeinformationen der Anmeldeinformationsverwaltung wurden gesichert.
5377	Nicht zutreffend	Mittel	Anmeldeinformationen der Anmeldeinformationsverwaltung wurden von einer Sicherung wiederhergestellt.

5453	Nicht zutreffend	Mittel	Eine IPsec-Aushandlung mit einem Remotecomputer war nicht erfolgreich, da der IKE- und AuthIP IPsec-Schlüsselerstellungsmodul-Dienst (IKEEXT) nicht gestartet wurde.
5480	Nicht zutreffend	Mittel	Die IPsec-Dienste konnten die vollständige Liste von Netzwerkschnittstellen auf dem Computer nicht abrufen. Dies stellt ein potenzielles Sicherheitsrisiko dar, da einige Netzwerkschnittstellen möglicherweise nicht durch die angewendeten IPsec-Filter geschützt werden. Verwenden Sie das Snap-In „IP-Sicherheitsmonitor“, um das Problem zu diagnostizieren.
5483	Nicht zutreffend	Mittel	Die IPsec-Dienste konnten den RPC-Server nicht initialisieren. Die IPsec-Dienste konnten nicht gestartet werden.
5484	Nicht zutreffend	Mittel	In den IPsec-Diensten ist ein kritischer Fehler aufgetreten, und die Dienste wurden beendet. Das Beenden der IPsec-Dienste kann das Risiko von Netzwerkangriffen auf den Computer und potenzielle Sicherheitsrisiken erhöhen.
5485	Nicht zutreffend	Mittel	Die IPsec-Dienste konnten einige IPsec-Filter für ein Plug-and-Play-Ereignis für Netzwerkschnittstellen nicht verarbeiten. Dies stellt ein potenzielles Sicherheitsrisiko dar, da einige Netzwerkschnittstellen möglicherweise nicht durch die angewendeten IPsec-Filter geschützt werden. Verwenden Sie das Snap-In „IP-Sicherheitsmonitor“, um das Problem zu diagnostizieren.
6145	Nicht zutreffend	Mittel	Bei der Verarbeitung von Sicherheitsrichtlinien in Group Policy Objects, ist mindestens ein Fehler aufgetreten.
6273	Nicht zutreffend	Mittel	Der Netzwerkrichtlinienserver verweigerte einem Benutzer den Zugriff.
6274	Nicht zutreffend	Mittel	Der Netzwerkrichtlinienserver hat die Anforderung für einen Benutzer verworfen.
6275	Nicht zutreffend	Mittel	Der Netzwerkrichtlinienserver hat die Kontoführungsanforderung für einen Benutzer verworfen.
6276	Nicht zutreffend	Mittel	Der Netzwerkrichtlinienserver hat einen Benutzer unter Quarantäne gestellt.
6277	Nicht zutreffend	Mittel	Der Netzwerkrichtlinienserver hat einem Benutzer den Zugriff gewährt, ihn aber auf

			Probe gesetzt, da der Host die definierten Integritätsrichtlinien nicht erfüllt.
6278	Nicht zutreffend	Mittel	Der Netzwerkrichtlinienserver hat einem Benutzer Vollzugriff erteilt, da der Host die Integritätsrichtlinien erfüllt.
6279	Nicht zutreffend	Mittel	Der Netzwerkrichtlinienserver hat das Benutzerkonto aufgrund mehrerer erfolgloser Authentifizierungsversuche gesperrt.
6280	Nicht zutreffend	Mittel	Der Netzwerkrichtlinienserver hat die Sperre des Benutzerkontos aufgehoben.
-	640	Mittel	Allgemeine Kontodatenbank geändert
-	619	Mittel	QoS-Speicherrichtlinie geändert
24586	Nicht zutreffend	Mittel	Konvertieren von Volume ist ein Fehler aufgetreten
24592	Nicht zutreffend	Mittel	Fehler beim Konvertierung auf dem Volume %2 automatisch neu gestartet.
24593	Nicht zutreffend	Mittel	Schreiben von Metadaten: Volume %2 Zurückgeben von Fehlern beim Versuch, Metadaten zu ändern. Wenn der Fehler weiterhin auftritt, entschlüsseln Sie volume
24594	Nicht zutreffend	Mittel	Metadaten neu erstellen: Beim Schreiben einer Kopie der Metadaten auf dem Volume %2 konnte nicht und möglicherweise als datenträgerbeschädigung angezeigt. Wenn der Fehler weiterhin auftritt, entschlüsseln Sie Volumes an.
4608	512	Niedrig	Windows wird gestartet.
4609	513	Niedrig	Windows wird heruntergefahren.
4610	514	Niedrig	Ein Authentifizierungspaket wurde durch die lokale Sicherheitsinstanz geladen.
4611	515	Niedrig	Ein vertrauenswürdiger Anmeldeprozess wurde bei der lokalen Sicherheitsautorität registriert.
4612	516	Niedrig	Die für die Überwachung reservierten internen Ressourcen sind ausgelastet. Dies wird zu einem Verlust von Überwachungsereignissen führen.
4614	518	Niedrig	Die Sicherheitskontenverwaltung hat ein Benachrichtigungspaket geladen.
4615	519	Niedrig	Unzulässige Verwendung des LPC-Ports.
4616	520	Niedrig	Die Systemzeit wurde geändert.
4622	Nicht zutreffend	Niedrig	Die LSA (Local Security Authority) hat ein Sicherheitspaket geladen.
4624	528,540	Niedrig	Ein Konto wurde erfolgreich angemeldet.

4625	529-537,539	Niedrig	Fehler beim Anmelden eines Kontos.
4634	538	Niedrig	Ein Konto wurde abgemeldet.
4646	Nicht zutreffend	Niedrig	IKE DoS-Schutzmodus wurde gestartet.
4647	551	Niedrig	Benutzerinitiierte Abmeldung.
4648	552	Niedrig	Anmeldeversuch mit expliziten Anmeldeinformationen.
4650	Nicht zutreffend	Niedrig	Eine Sicherheitszuordnung des IPsec-Hauptmodus wurde eingerichtet. Der Erweiterungsmodus wurde nicht aktiviert. Zertifikatauthentifizierung wurde nicht verwendet.
4651	Nicht zutreffend	Niedrig	Eine Sicherheitszuordnung des IPsec-Hauptmodus wurde eingerichtet. Der Erweiterungsmodus wurde nicht aktiviert. Zertifikatauthentifizierung wurde verwendet.
4652	Nicht zutreffend	Niedrig	Fehler bei einer IPsec-Hauptmodusverhandlung.
4653	Nicht zutreffend	Niedrig	Fehler bei einer IPsec-Hauptmodusverhandlung.
4654	Nicht zutreffend	Niedrig	Fehler bei der eine Schnellmodus-IPsec-Aushandlung.
4655	Nicht zutreffend	Niedrig	Beendigung einer IPsec-Hauptmodusverhandlung.
4656	560	Niedrig	Ein Handle zu einem Objekt wurde angefordert.
4657	567	Niedrig	Ein Registrierungswert wurde geändert.
4658	562	Niedrig	Ein Handle zu einem Objekt wurde geschlossen.
4659	Nicht zutreffend	Niedrig	Ein Handle zu einem Objekt wurde angefordert mit der Absicht, es zu löschen.
4660	564	Niedrig	Ein Objekt wurde gelöscht.
4661	565	Niedrig	Ein Handle zu einem Objekt wurde angefordert.
4662	566	Niedrig	Für ein Objekt wurde ein Vorgang ausgeführt.
4663	567	Niedrig	Es wurde versucht, auf ein Objekt zuzugreifen.
4664	Nicht zutreffend	Niedrig	Es wurde versucht, eine feste Verknüpfung herzustellen.
4665	Nicht zutreffend	Niedrig	Es wurde versucht, einen Anwendungsclientkontext zu erstellen.
4666	Nicht zutreffend	Niedrig	Eine Anwendung hat einen Vorgang versucht:

4667	Nicht zutreffend	Niedrig	Löschung des Anwendungsclientkontexts.
4668	Nicht zutreffend	Niedrig	Initialisierung einer Anwendung.
4670	Nicht zutreffend	Niedrig	Berechtigungen für ein Objekt wurden geändert.
4671	Nicht zutreffend	Niedrig	Eine Anwendung hat versucht, über den TBS-Dienst auf eine blockierte Ordnungszahl zuzugreifen.
4672	576	Niedrig	Einer neuen Anmeldung wurden besondere Rechte zugewiesen.
4673	577	Niedrig	Ein privilegierter Dienst wurde aufgerufen.
4674	578	Niedrig	Es wurde versucht, einen Vorgang für ein privilegiertes Objekt auszuführen.
4688	592	Niedrig	Ein neuer Prozess wurde erstellt.
4689	593	Niedrig	Ein Prozess wurde beendet.
4690	594	Niedrig	Es wurde versucht, ein Handle zu einem Objekt zu duplizieren.
4691	595	Niedrig	Der indirekte Zugriff auf ein Objekt wurde angefordert.
4694	Nicht zutreffend	Niedrig	Es wurde versucht, überwachbare geschützte Daten zu schützen.
4695	Nicht zutreffend	Niedrig	Es wurde versucht, den Schutz überwachbarer geschützter Daten aufzuheben.
4696	600	Niedrig	Ein primäres Token wurde zugewiesen, verarbeitet.
4697	601	Niedrig	Versucht, einen Dienst zu installieren
4698	602	Niedrig	Eine geplante Aufgabe wurde erstellt.
4699	602	Niedrig	Eine geplante Aufgabe wurde gelöscht.
4700	602	Niedrig	Eine geplante Aufgabe wurde aktiviert.
4701	602	Niedrig	Eine geplante Aufgabe wurde deaktiviert.
4702	602	Niedrig	Eine geplante Aufgabe wurde aktualisiert.
4704	608	Niedrig	Eine Benutzerberechtigung wurde zugewiesen.
4705	609	Niedrig	Eine Benutzerberechtigung wurde entfernt.
4707	611	Niedrig	Eine Vertrauensstellung zu einer Domäne wurde entfernt.
4709	Nicht zutreffend	Niedrig	Die IPsec-Dienste wurden gestartet.
4710	Nicht zutreffend	Niedrig	Die IPsec-Dienste wurden deaktiviert.
4711	Nicht zutreffend	Niedrig	Kann eines der folgenden Elemente enthalten: Das PAStore-Modul hat eine

			lokal zwischengespeicherte Kopie der Active Directory-Speicher-IPsec-Richtlinie auf dem Computer angewendet. Das PAStore-Modul hat eine Active Directory-Speicher-IPsec-Richtlinie auf dem Computer angewendet. Das PAStore-Modul hat eine Speicher-IPsec-Richtlinie der lokalen Registrierung auf dem Computer angewendet. Das PAStore-Modul konnte die lokal zwischengespeicherte Kopie der Active Directory-Speicher-IPsec-Richtlinie nicht auf dem Computer anwenden. Das PAStore-Modul konnte die Active Directory-Speicher-IPsec-Richtlinie nicht auf dem Computer anwenden. Das PAStore-Modul konnte die Speicher-IPsec-Richtlinie der lokalen Registrierung nicht auf dem Computer anwenden. Das PAStore-Modul konnte einige Regeln der aktiven IPsec-Richtlinie nicht auf dem Computer anwenden. Das PAStore-Modul konnte die Verzeichnisspeicher-IPsec-Richtlinie nicht auf dem Computer laden. Das PAStore-Modul hat die Verzeichnisspeicher-IPsec-Richtlinie auf dem Computer geladen. Das PAStore-Modul konnte die lokale Speicher-IPsec-Richtlinie nicht auf dem Computer laden. PAStore-Modul geladen, lokalen Speicher IPsec-Richtlinie auf dem Computer. PAStore-Modul für Änderungen an die aktive IPsec-Richtlinie abgerufen und keine Änderungen erkannt.
4712	Nicht zutreffend	Niedrig	Schwerwiegender Fehler beim IPsec-Dienst.
4717	621	Niedrig	Einem Konto wurde der Zugriff auf die Systemsicherheit gewährt.
4718	622	Niedrig	Der Zugriff auf die Systemsicherheit wurde von einem Konto entfernt.
4720	624	Niedrig	Ein Benutzerkonto wurde erstellt.
4722	626	Niedrig	Ein Benutzerkonto wurde aktiviert.
4723	627	Niedrig	Es wurde versucht, das Kennwort eines Kontos zu ändern.
4725	629	Niedrig	Ein Benutzerkonto wurde deaktiviert.
4726	630	Niedrig	Ein Benutzerkonto wurde gelöscht.
4728	632	Niedrig	Ein Mitglied einer sicherheitsaktivierten globalen Gruppe wurde hinzugefügt.
4729	633	Niedrig	Ein Mitglied einer sicherheitsaktivierten globalen Gruppe wurde entfernt.

4730	634	Niedrig	Eine sicherheitsaktivierte globale Gruppe wurde gelöscht.
4731	635	Niedrig	Eine sicherheitsaktivierte lokale Gruppe wurde erstellt.
4732	636	Niedrig	Ein Mitglied einer sicherheitsaktivierten lokalen Gruppe wurde hinzugefügt.
4733	637	Niedrig	Ein Mitglied einer sicherheitsaktivierten lokalen Gruppe wurde entfernt.
4734	638	Niedrig	Eine sicherheitsaktivierte lokale Gruppe wurde gelöscht.
4738	642	Niedrig	Ein Benutzerkonto wurde geändert.
4740	644	Niedrig	Ein Benutzerkonto wurde gesperrt.
4741	645	Niedrig	Ein Computerkonto wurde geändert.
4742	646	Niedrig	Ein Computerkonto wurde geändert.
4743	647	Niedrig	Ein Computerkonto wurde gelöscht.
4744	648	Niedrig	Eine sicherheitsdeaktivierte lokale Gruppe wurde erstellt.
4745	649	Niedrig	Eine sicherheitsdeaktivierte lokale Gruppe wurde geändert.
4746	650	Niedrig	Ein Mitglied einer sicherheitsdeaktivierten lokalen Gruppe wurde hinzugefügt.
4747	651	Niedrig	Ein Mitglied einer sicherheitsdeaktivierten lokalen Gruppe wurde entfernt.
4748	652	Niedrig	Eine sicherheitsdeaktivierte lokale Gruppe wurde gelöscht.
4749	653	Niedrig	Eine sicherheitsdeaktivierte globale Gruppe wurde erstellt.
4750	654	Niedrig	Eine sicherheitsdeaktivierte globale Gruppe wurde geändert.
4751	655	Niedrig	Ein Mitglied einer sicherheitsdeaktivierten globalen Gruppe wurde hinzugefügt.
4752	656	Niedrig	Ein Mitglied einer sicherheitsdeaktivierten globalen Gruppe wurde entfernt.
4753	657	Niedrig	Eine sicherheitsdeaktivierte globale Gruppe wurde gelöscht.
4756	660	Niedrig	Ein Mitglied einer sicherheitsaktivierten universellen Gruppe wurde hinzugefügt.
4757	661	Niedrig	Ein Mitglied einer sicherheitsaktivierten universellen Gruppe wurde entfernt.
4758	662	Niedrig	Eine sicherheitsaktivierte universelle Gruppe wurde gelöscht.
4759	663	Niedrig	Eine sicherheitsdeaktivierte universelle Gruppe wurde erstellt.

4760	664	Niedrig	Eine sicherheitsdeaktivierte universelle Gruppe wurde geändert.
4761	665	Niedrig	Ein Mitglied einer sicherheitsdeaktivierten universellen Gruppe wurde hinzugefügt.
4762	666	Niedrig	Ein Mitglied einer sicherheitsdeaktivierten universellen Gruppe wurde entfernt.
4767	671	Niedrig	Die Sperrung eines Benutzerkontos wurde aufgehoben.
4768	672,676	Niedrig	Ein Kerberos-Authentifizierungsticket (TGT) wurde angefordert.
4769	673	Niedrig	Ein Kerberos-Dienstticket wurde angefordert.
4770	674	Niedrig	Ein Kerberos-Dienstticket wurde erneuert.
4771	675	Niedrig	Fehler bei der Kerberos-Vorauthentifizierung.
4772	672	Niedrig	Fehler bei einer Kerberos-Authentifizierungsticketanforderung.
4774	678	Niedrig	Ein Konto wurde für die Anmeldung zugeordnet.
4775	679	Niedrig	Es konnte kein Konto für die Anmeldung zugeordnet werden.
4776	680,681	Niedrig	Der Domänencontroller hat versucht, die Anmeldeinformationen für ein Konto zu bestätigen.
4777	Nicht zutreffend	Niedrig	Der Domänencontroller konnte die Anmeldeinformationen für ein Konto nicht bestätigen.
4778	682	Niedrig	Eine Sitzung wurde erneut mit einer Arbeitsstation verbunden.
4779	683	Niedrig	Eine Sitzung wurde von einer Arbeitsstation getrennt.
4781	685	Niedrig	Der Name eines Kontos wurde geändert:
4782	Nicht zutreffend	Niedrig	Der Kennworthash eines Kontos wurde zugegriffen.
4783	667	Niedrig	Eine Basisanwendungsgruppe wurde erstellt.
4784	Nicht zutreffend	Niedrig	Eine Basisanwendungsgruppe wurde geändert.
4785	689	Niedrig	Einer Basisanwendungsgruppe wurde ein Mitglied hinzugefügt.
4786	690	Niedrig	Ein Mitglied einer Basisanwendungsgruppe wurde entfernt.
4787	691	Niedrig	Eine nicht-Member wurde eine einfache Anwendung-Gruppe hinzugefügt.

4788	692	Niedrig	Eine nicht-Member wurde von einer basisanwendung-Gruppe entfernt.
4789	693	Niedrig	Eine Basisanwendungsgruppe wurde gelöscht.
4790	694	Niedrig	Eine LDAP-Abfragegruppe wurde erstellt.
4793	Nicht zutreffend	Niedrig	Die Kennwortrichtlinienprüfungs-API wurde aufgerufen.
4800	Nicht zutreffend	Niedrig	Die Arbeitsstation wurde gesperrt.
4801	Nicht zutreffend	Niedrig	Die Arbeitsstation wurde entsperrt.
4802	Nicht zutreffend	Niedrig	Der Bildschirmschoner wurde aktiviert.
4803	Nicht zutreffend	Niedrig	Der Bildschirmschoner wurde deaktiviert.
4864	Nicht zutreffend	Niedrig	Ein Namespacekonflikt wurde erkannt.
4869	773	Niedrig	Die Zertifikatdienste haben eine erneut eingereichte Zertifikatanforderung erhalten.
4871	775	Niedrig	Die Zertifikatdienste haben eine Anforderung zum Veröffentlichen der Zertifikatssperrliste erhalten.
4872	776	Niedrig	Die Zertifikatdienste haben die Zertifikatsperrliste veröffentlicht.
4873	777	Niedrig	Eine Zertifikatanforderungserweiterung wurde geändert.
4874	778	Niedrig	Ein oder mehrere Zertifikatanforderungsattribute wurden geändert.
4875	779	Niedrig	Die Zertifikatdienste haben eine Anforderung zum Herunterfahren erhalten.
4876	780	Niedrig	Die Sicherung der Zertifikatdienste wurde gestartet.
4877	781	Niedrig	Die Sicherung der Zertifikatdienste wurde abgeschlossen.
4878	782	Niedrig	Die Wiederherstellung der Zertifikatdienste wurde gestartet.
4879	783	Niedrig	Die Wiederherstellung der Zertifikatdienste wurde beendet.
4880	784	Niedrig	Die Zertifikatdienste wurden gestartet.
4881	785	Niedrig	Die Zertifikatdienste wurden beendet.
4883	787	Niedrig	Die Zertifikatdienste haben einen archivierten Schlüssel abgerufen.

4884	788	Niedrig	Die Zertifikatdienste haben ein Zertifikat in ihre Datenbank importiert.
4886	790	Niedrig	Die Zertifikatdienste haben eine Zertifikatanforderung empfangen.
4887	791	Niedrig	Die Zertifikatdienste haben eine Zertifikatanforderung genehmigt und ein Zertifikat ausgestellt.
4888	792	Niedrig	Die Zertifikatdienste haben eine Zertifikatanforderung abgelehnt.
4889	793	Niedrig	Die Zertifikatdienste haben den Status einer Zertifikatanforderung als "anstehend" festgelegt.
4891	795	Niedrig	Es wurde ein Konfigurationseintrag in den Zertifikatdiensten geändert.
4893	797	Niedrig	Zertifikatdienste haben einen Schlüssel archiviert.
4894	798	Niedrig	Zertifikatdienste haben einen Schlüssel importiert und archiviert.
4895	799	Niedrig	Die Zertifikatdienste haben das Zertifizierungsstellenzertifikat bei den Active Directory-Domänendiensten veröffentlicht.
4898	802	Niedrig	Die Zertifikatdienste haben eine Vorlage geladen.
4902	Nicht zutreffend	Niedrig	Eine Benutzerrichtlinien-Überwachungstabelle wurde erstellt.
4904	Nicht zutreffend	Niedrig	Es wurde versucht, eine Sicherheitsereignisquelle zu registrieren
4905	Nicht zutreffend	Niedrig	Es wurde versucht, die Registrierung einer Sicherheitsereignisquelle aufzuheben.
4909	Nicht zutreffend	Niedrig	Die lokalen Richtlinieneinstellungen für den TBS-Dienst wurden geändert.
4910	Nicht zutreffend	Niedrig	Die gruppenrichtlinieneinstellungen für die TB wurden geändert.
4928	Nicht zutreffend	Niedrig	Ein Namenskontext für Active Directory-Replikatquellen wurde eingerichtet.
4929	Nicht zutreffend	Niedrig	Ein Namenskontext für Active Directory-Replikatquellen wurde entfernt.
4930	Nicht zutreffend	Niedrig	Ein Namenskontext für Active Directory-Replikatquellen wurde geändert.
4931	Nicht zutreffend	Niedrig	Ein Namenskontext für Active Directory-Replikatziele wurde eingerichtet.
4932	Nicht zutreffend	Niedrig	Die Synchronisierung eines Replikats eines Active Directory-Namenskontextes wurde gestartet.

4933	Nicht zutreffend	Niedrig	Die Synchronisierung eines Replikats eines Active Directory-Namenskontextes wurde beendet.
4934	Nicht zutreffend	Niedrig	Die Attribute eines Active Directory-Objekts wurden repliziert.
4935	Nicht zutreffend	Niedrig	Beginn des Replikationsfehlers.
4936	Nicht zutreffend	Niedrig	Ende des Replikationsfehlers.
4937	Nicht zutreffend	Niedrig	Ein veraltetes Objekt wurde aus einem Replikat entfernt.
4944	Nicht zutreffend	Niedrig	Die folgende Richtlinie war beim Start der Windows-Firewall aktiv.
4945	Nicht zutreffend	Niedrig	Beim Start der Windows-Firewall wurde eine Regel aufgelistet.
4946	Nicht zutreffend	Niedrig	Die Ausnahmeliste der Windows-Firewall wurde geändert. Eine Regel wurde hinzugefügt.
4947	Nicht zutreffend	Niedrig	Die Ausnahmeliste der Windows-Firewall wurde geändert. Eine Regel wurde geändert.
4948	Nicht zutreffend	Niedrig	Die Ausnahmeliste der Windows-Firewall wurde geändert. Eine Regel wurde gelöscht.
4949	Nicht zutreffend	Niedrig	Die Einstellungen der Windows-Firewall wurden auf die Standardwerte zurückgesetzt.
4950	Nicht zutreffend	Niedrig	Eine Windows-Firewalleinstellung wurde geändert.
4951	Nicht zutreffend	Niedrig	Eine Regel wurde ignoriert, da ihre Hauptversionsnummer nicht von der Windows-Firewall erkannt wurde.
4952	Nicht zutreffend	Niedrig	Eine Regel wurde teilweise ignoriert, da ihre Nebenversionsnummer nicht von der Windows-Firewall erkannt wurde. Die anderen Teile der Regel werden angewendet.
4953	Nicht zutreffend	Niedrig	Eine Regel wurde von der Windows-Firewall ignoriert, da die Regel nicht analysiert werden konnte.
4954	Nicht zutreffend	Niedrig	Die Windows-Firewall-Gruppenrichtlinieneinstellungen wurden geändert. Die neuen Einstellungen wurden angewendet.
4956	Nicht zutreffend	Niedrig	Die Windows-Firewall hat das aktive Profil geändert.

4957	Nicht zutreffend	Niedrig	Die Windows-Firewall hat die folgende Regel nicht angewendet:
4958	Nicht zutreffend	Niedrig	Die Windows-Firewall hat die folgende Regel nicht angewendet, da die Regel auf Elemente verweist, die auf diesem Computer nicht konfiguriert sind:
4979	Nicht zutreffend	Niedrig	Sicherheitszuordnungen für den IPsec-Hauptmodus und -Erweiterungsmodus wurden eingerichtet.
4980	Nicht zutreffend	Niedrig	Sicherheitszuordnungen für den IPsec-Hauptmodus und -Erweiterungsmodus wurden eingerichtet.
4981	Nicht zutreffend	Niedrig	Sicherheitszuordnungen für den IPsec-Hauptmodus und -Erweiterungsmodus wurden eingerichtet.
4982	Nicht zutreffend	Niedrig	Sicherheitszuordnungen für den IPsec-Hauptmodus und -Erweiterungsmodus wurden eingerichtet.
4985	Nicht zutreffend	Niedrig	Der Status einer Transaktion wurde geändert.
5024	Nicht zutreffend	Niedrig	Der Windows-Firewalldienst wurde erfolgreich gestartet.
5025	Nicht zutreffend	Niedrig	Der Windows-Firewalldienst wurde beendet.
5031	Nicht zutreffend	Niedrig	Der Windows-Firewalldienst hat eine Anwendung blockiert, sodass sie keine eingehenden Verbindungen im Netzwerk annehmen kann
5032	Nicht zutreffend	Niedrig	Der Windows-Firewalldienst konnte den Benutzer nicht darüber benachrichtigen, dass eine Anwendung blockiert wurde und keine eingehenden Verbindungen im Netzwerk annehmen kann.
5033	Nicht zutreffend	Niedrig	Der Windows-Firewalltreiber wurde erfolgreich gestartet.
5034	Nicht zutreffend	Niedrig	Der Windows-Firewalltreiber wurde beendet.
5039	Nicht zutreffend	Niedrig	Ein Registrierungsschlüssel wurde virtualisiert.
5040	Nicht zutreffend	Niedrig	Die IPSec-Einstellungen wurden geändert. Ein Authentifizierungssatz wurde hinzugefügt.
5041	Nicht zutreffend	Niedrig	Die IPSec-Einstellungen wurden geändert. Ein Authentifizierungssatz wurde geändert.
5042	Nicht zutreffend	Niedrig	Die IPSec-Einstellungen wurden geändert. Ein Authentifizierungssatz wurde gelöscht.

5043	Nicht zutreffend	Niedrig	Die IPSec-Einstellungen wurden geändert. Eine Verbindungssicherheitsregel wurde hinzugefügt.
5044	Nicht zutreffend	Niedrig	Die IPSec-Einstellungen wurden geändert. Eine Verbindungssicherheitsregel wurde geändert.
5045	Nicht zutreffend	Niedrig	Die IPSec-Einstellungen wurden geändert. Eine Verbindungssicherheitsregel wurde gelöscht.
5046	Nicht zutreffend	Niedrig	Die IPSec-Einstellungen wurden geändert. Ein Kryptografiesatz wurde hinzugefügt.
5047	Nicht zutreffend	Niedrig	Die IPSec-Einstellungen wurden geändert. Ein Kryptografiesatz wurde geändert.
5048	Nicht zutreffend	Niedrig	Die IPSec-Einstellungen wurden geändert. Ein Kryptografiesatz wurde gelöscht.
5050	Nicht zutreffend	Niedrig	Versuch, die Windows-Firewall, die über einen Aufruf an InetFwProfile.FirewallEnabled(False) programmgesteuert deaktivieren
5051	Nicht zutreffend	Niedrig	Eine Datei wurde virtualisiert.
5056	Nicht zutreffend	Niedrig	Es wurde ein kryptografischer Selbsttest ausgeführt.
5057	Nicht zutreffend	Niedrig	Fehler bei einem einfachen kryptografischen Vorgang.
5058	Nicht zutreffend	Niedrig	Schlüsseldateivorgang.
5059	Nicht zutreffend	Niedrig	Schlüsselmigrationsvorgang.
5060	Nicht zutreffend	Niedrig	Fehler bei der Überprüfung der Kryptografiesignatur.
5061	Nicht zutreffend	Niedrig	Kryptografievorgang.
5062	Nicht zutreffend	Niedrig	Es wurde ein Selbsttest kryptografische Kernelmodus ausgeführt.
5063	Nicht zutreffend	Niedrig	Es wurde versucht, einen Kryptografieanbietervorgang auszuführen.
5064	Nicht zutreffend	Niedrig	Es wurde versucht, einen Kryptografiekontextvorgang auszuführen.
5065	Nicht zutreffend	Niedrig	Es wurde versucht, einen Kryptografiekontext zu ändern.
5066	Nicht zutreffend	Niedrig	Es wurde versucht, einen Kryptografiefunktionsvorgang auszuführen.
5067	Nicht zutreffend	Niedrig	Es wurde versucht, eine Kryptografiefunktion zu ändern.

5068	Nicht zutreffend	Niedrig	Es wurde versucht, einen Vorgang für einen Kryptografiefunktionsanbieter auszuführen.
5069	Nicht zutreffend	Niedrig	Es wurde versucht, einen Vorgang für eine Kryptografiefunktionseigenschaft auszuführen.
5070	Nicht zutreffend	Niedrig	Es wurde versucht, eine Kryptografiefunktionseigenschaft zu ändern.
5125	Nicht zutreffend	Niedrig	Eine Anforderung wurde an der OCSP-Responder-Dienst übermittelt.
5126	Nicht zutreffend	Niedrig	Signaturzertifikat wurde von der OCSP-Responder-Dienst automatisch aktualisiert.
5127	Nicht zutreffend	Niedrig	Die Sperrungsinformationen aktualisiert der OCSP-Sperranbieter erfolgreich
5136	566	Niedrig	Ein Verzeichnisdienstobjekt wurde geändert
5137	566	Niedrig	Ein Verzeichnisdienstobjekt wurde erstellt.
5138	Nicht zutreffend	Niedrig	Ein Verzeichnisdienstobjekt wurde wiederhergestellt.
5139	Nicht zutreffend	Niedrig	Ein Verzeichnisdienstobjekt wurde verschoben.
5140	Nicht zutreffend	Niedrig	Es wurde auf ein Netzwerkfreigabeobjekt zugegriffen.
5141	Nicht zutreffend	Niedrig	Ein Verzeichnisdienstobjekt wurde gelöscht.
5152	Nicht zutreffend	Niedrig	Die Windows-Filterplattform hat ein Paket blockiert.
5153	Nicht zutreffend	Niedrig	Ein stärker einschränkender Windows-Filterplattformfilter hat ein Paket blockiert.
5154	Nicht zutreffend	Niedrig	Die Windows-Filterplattform hat es einer Anwendung oder einem Dienst gestattet, einen Port auf eingehende Verbindungen abzuhören.
5155	Nicht zutreffend	Niedrig	Die Windows-Filterplattform hat eine Anwendung oder einen Dienst daran gehindert, einen Port auf eingehende Verbindungen abzuhören.
5156	Nicht zutreffend	Niedrig	Die Windows-Filterplattform hat eine Verbindung zugelassen.
5157	Nicht zutreffend	Niedrig	Die Windows-Filterplattform hat eine Verbindung blockiert.
5158	Nicht zutreffend	Niedrig	Die Windows-Filterplattform hat eine Bindung an einen lokalen Port zugelassen.
5159	Nicht zutreffend	Niedrig	Die Windows-Filterplattform hat eine Bindung an einen lokalen Port blockiert.

5378	Nicht zutreffend	Niedrig	Die angeforderte Delegierung von Anmeldeinformationen wurde von einer Richtlinie nicht zugelassen.
5440	Nicht zutreffend	Niedrig	Beim Start des Basisfiltermoduls der Windows-Filterplattform war der folgende Callout vorhanden.
5441	Nicht zutreffend	Niedrig	Beim Start des Basisfiltermoduls der Windows-Filterplattform war der folgende Filter vorhanden.
5442	Nicht zutreffend	Niedrig	Beim Start des Basisfiltermoduls der Windows-Filterplattform war der folgende Anbieter vorhanden.
5443	Nicht zutreffend	Niedrig	Beim Start des Basisfiltermoduls der Windows-Filterplattform war der folgende Anbieterkontext vorhanden
5444	Nicht zutreffend	Niedrig	Die folgende Unterebene war vorhanden, wenn die Windows Filtering Platform Basisfiltermodul gestartet.
5446	Nicht zutreffend	Niedrig	Ein Callout der Windows-Filterplattform wurde geändert.
5447	Nicht zutreffend	Niedrig	Ein Filter der Windows-Filterplattform wurde geändert.
5448	Nicht zutreffend	Niedrig	Ein Anbieter der Windows-Filterplattform wurde geändert.
5449	Nicht zutreffend	Niedrig	Ein Anbieterkontext der Windows-Filterplattform wurde geändert.
5450	Nicht zutreffend	Niedrig	Eine Windows-Filterplattform Unterebene wurde geändert.
5451	Nicht zutreffend	Niedrig	Eine IPsec-Schnellmodus-Sicherheitszuordnung wurde eingerichtet.
5452	Nicht zutreffend	Niedrig	Eine IPsec-Schnellmodus-Sicherheitszuordnung wurde beendet.
5456	Nicht zutreffend	Niedrig	Das PAStore-Modul hat eine Active Directory-Speicher-IPsec-Richtlinie auf dem Computer angewendet.
5457	Nicht zutreffend	Niedrig	Das PAStore-Modul konnte die Active Directory-Speicher-IPsec-Richtlinie nicht auf dem Computer anwenden.
5458	Nicht zutreffend	Niedrig	Das PAStore-Modul hat eine lokal zwischengespeicherte Kopie der Active Directory-Speicher-IPsec-Richtlinie auf dem Computer angewendet.
5459	Nicht zutreffend	Niedrig	Das PAStore-Modul konnte die lokal zwischengespeicherte Kopie der Active Directory-Speicher-IPsec-Richtlinie nicht auf dem Computer anwenden.

5460	Nicht zutreffend	Niedrig	Das PAStore-Modul hat eine Speicher-IPsec-Richtlinie der lokalen Registrierung auf dem Computer angewendet.
5461	Nicht zutreffend	Niedrig	Das PAStore-Modul konnte die Speicher-IPsec-Richtlinie der lokalen Registrierung nicht auf dem Computer anwenden.
5462	Nicht zutreffend	Niedrig	Das PAStore-Modul konnte einige Regeln der aktiven IPsec-Richtlinie nicht auf dem Computer anwenden. Verwenden Sie das Snap-In „IP-Sicherheitsmonitor“, um das Problem zu diagnostizieren.
5463	Nicht zutreffend	Niedrig	Das PAStore-Modul hat die aktive IPSec-Richtlinie auf Änderungen überprüft und keine Änderungen ermittelt.
5464	Nicht zutreffend	Niedrig	Das PAStore-Modul hat beim Abfragen von Änderungen für die aktive IPsec-Richtlinie Änderungen erkannt und diese auf die IPsec-Dienste angewendet.
5465	Nicht zutreffend	Niedrig	Das PAStore-Modul hat eine Steuerung, die das erneute Laden der IPSec-Richtlinie erzwingt, ermittelt, und hat die Steuerung erfolgreich verarbeitet.
5466	Nicht zutreffend	Niedrig	Das PAStore-Modul hat beim Abfragen von Änderungen für die Active Directory-IPsec-Richtlinie festgestellt, dass Active Directory nicht erreichbar ist. Stattdessen wird die zwischengespeicherte Kopie der Active Directory-IPsec-Richtlinie verwendet. Alle seit der letzten Abfrage an der Active Directory-IPsec-Richtlinie vorgenommenen Änderungen konnten nicht angewendet werden.
5467	Nicht zutreffend	Niedrig	Das PAStore-Modul hat beim Abfragen von Änderungen für die Active Directory-IPsec-Richtlinie festgestellt, dass Active Directory erreichbar ist und keine Änderungen der Richtlinie vorliegen. Die zwischengespeicherte Kopie der Active Directory-IPsec-Richtlinie wird nicht mehr verwendet.
5468	Nicht zutreffend	Niedrig	Das PAStore-Modul hat beim Abfragen von Änderungen für die Active Directory-IPsec-Richtlinie festgestellt, dass Active Directory erreichbar ist und Änderungen der Richtlinie vorliegen. Die gefundenen Änderungen wurden angewendet. Die zwischengespeicherte Kopie der Active

			Directory-IPsec-Richtlinie wird nicht mehr verwendet.
5471	Nicht zutreffend	Niedrig	Das PAStore-Modul hat die lokale Speicher-IPsec-Richtlinie auf dem Computer geladen.
5472	Nicht zutreffend	Niedrig	Das PAStore-Modul konnte die lokale Speicher-IPsec-Richtlinie nicht auf dem Computer laden.
5473	Nicht zutreffend	Niedrig	Das PAStore-Modul hat die Verzeichnisspeicher-IPsec-Richtlinie auf dem Computer geladen.
5474	Nicht zutreffend	Niedrig	Das PAStore-Modul konnte die Verzeichnisspeicher-IPsec-Richtlinie nicht auf dem Computer laden.
5477	Nicht zutreffend	Niedrig	Das PAStore-Modul konnte den Schnellmodusfilter nicht laden.
5479	Nicht zutreffend	Niedrig	Die IPsec-Dienste wurden erfolgreich beendet. Das Beenden der IPsec-Dienste kann das Risiko von Netzwerkangriffen auf den Computer und potenzielle Sicherheitsrisiken erhöhen.
5632	Nicht zutreffend	Niedrig	Die Authentifizierung bei einem Drahtlosnetzwerk wurde angefordert.
5633	Nicht zutreffend	Niedrig	Die Authentifizierung bei einem verkabelten Netzwerk wurde angefordert.
5712	Nicht zutreffend	Niedrig	Es wurde versucht, einen Remoteprozeduraufruf (RPC) auszuführen.
5888	Nicht zutreffend	Niedrig	Ein Objekt im COM+-Katalog wurde geändert.
5889	Nicht zutreffend	Niedrig	Ein Objekt wurde aus dem COM+-Katalog gelöscht.
5890	Nicht zutreffend	Niedrig	Dem COM+-Katalog wurde ein Objekt hinzugefügt.
6008	Nicht zutreffend	Niedrig	Das vorherige System wurde unerwartet heruntergefahren
6144	Nicht zutreffend	Niedrig	Die Sicherheitsrichtlinien in Group Policy Objects wurde erfolgreich angewendet.
6272	Nicht zutreffend	Niedrig	Der Netzwerkrichtlinienserver hat einem Benutzer den Zugriff gewährt.
Nicht zutreffend	561	Niedrig	Ein Handle zu einem Objekt wurde angefordert.
Nicht zutreffend	563	Niedrig	Objekt kann für das Löschen
Nicht zutreffend	625	Niedrig	Art des Benutzerkontos geändert

Nicht zutreffend	613	Niedrig	IPSec-Richtlinien-Agent gestartet
Nicht zutreffend	614	Niedrig	IPSec-Richtlinien-Agent deaktiviert
Nicht zutreffend	615	Niedrig	IPSec-Richtlinien-agent
Nicht zutreffend	616	Niedrig	IPSec-Richtlinien-Agent hat einen möglichen schwerwiegenden Fehler festgestellt.
24577	Nicht zutreffend	Niedrig	Verschlüsselung von Volume gestartet
24578	Nicht zutreffend	Niedrig	Verschlüsselung des Datenträgers wurde beendet
24579	Nicht zutreffend	Niedrig	Verschlüsselung von Volumes abgeschlossen.
24580	Nicht zutreffend	Niedrig	Entschlüsselung des Volume gestartet
24581	Nicht zutreffend	Niedrig	Entschlüsselung des Volumes, die beendet
24582	Nicht zutreffend	Niedrig	Entschlüsselung des Volumes abgeschlossen.
24583	Nicht zutreffend	Niedrig	Konvertierung der Arbeitsthread für Volume gestartet
24584	Nicht zutreffend	Niedrig	Konvertierung der Arbeitsthread für Volume wurde vorübergehend angehalten.
24588	Nicht zutreffend	Niedrig	Der Konvertierungsvorgang auf dem Volume %2 hat einen schlechten Sektoren-Fehler festgestellt. Überprüfen Sie die Daten auf diesem volume
24595	Nicht zutreffend	Niedrig	Volume %2 enthält ungültige-Cluster. Diese Cluster werden während der Konvertierung übersprungen.
24621	Nicht zutreffend	Niedrig	Überprüfung der anfängliche Zustand: Parallele Transaktion für Volume-Konvertierung auf %2 '.
5049	Nicht zutreffend	Niedrig	Eine IPSec-Sicherheitszuordnung wurde gelöscht.
5478	Nicht zutreffend	Niedrig	Die IPSec-Dienste wurden erfolgreich gestartet.

Anlage IV

Einschränkung von Wechseldatenträgern:

Removable Storage Access

Removable storage such as CD, DVD, and USB drives support a wide variety of scenarios, including data backup, software installation (especially when network access is not available), and easy access to multimedia training materials.

Possible values:

- Enabled
- Disabled
- Not configured

Vulnerability

Removable storage devices such as read-only and read-write CD and DVD drives, USB drives, and tape drives can pose security concerns such as the risk of introducing malware onto network computers, the installation of unapproved software, and data theft.

Countermeasure

An administrator can apply Group Policy settings to control whether users can read from or write to any device with removable media. These policy settings can be used to help prevent sensitive or confidential material from being written to removable media.

You can apply these policy settings at the computer level so they affect every user who logs on to the computer. You can also apply them at the user level and limit enforcement to specific user accounts.

Important

These removable storage access policies do not affect software that runs in the System account context, such as the ReadyBoost® technology in Windows. However, any software that runs under the security context of the current user might be affected by these restrictions. For example, if the **Removable Disks: Deny write access** policy setting is in effect for a user, even if that user is an administrator, then the BitLocker™ setup program cannot write its startup key to a USB drive. You might want to consider applying the restrictions to only users and groups other than the local Administrators group.

The **Removable Storage Access** policy settings also include a setting to allow an administrator to force a restart. If a device is in use when a restricting policy is applied, the policy might not be enforced until the computer is restarted. Use the policy setting to force a restart if you do not want to wait until the next time the user restarts the

computer. If the restricting policies can be enforced without restarting the computer, then the restart option is ignored.

The policy settings can be found in two locations. The policy settings found in **Computer Configuration\Administrative Templates\System\Removable Storage Access** affect a computer and every user who logs on to it. The policy settings found in **User Configuration\Administrative Templates\System\Removable Storage Access** affect only the users to whom the policy setting is applied, including groups if Group Policy is applied by using Active Directory Domain Services.

The following Group Policy settings enable you to control Read or Write access to removable storage drives. Each device category supports two policies: one to deny Read access and one to deny Write access.

Anlage V

Table 3: Möglichkeiten zum Umgang mit Wechseldatenträgern[134]

Policy settings	Description
Time (in seconds) to force reboot	This policy setting sets the amount of time (in seconds) that the system will wait to restart to enforce a change in access rights to removable storage devices. The restart is only forced if the restricting policies cannot be applied without it. **Note** If the policy change affects multiple devices, the change is enforced immediately on all devices that are not currently in use. If any of the affected devices are in use so that the change cannot be immediately enforced, then this policy to restart the computer will be enforced, if it was enabled by the administrator.
CD and DVD: Deny execute access	This policy setting allows you to deny Read or Write access to devices in the CD and DVD removable storage class, including USB connected devices. Important Some non-Microsoft CD and DVD burner software interacts with the hardware in a way that is not prevented by this policy setting. If you want to prevent all writing to CD or DVD burners, you might want to consider applying Group Policy to prevent the installation of that software.
CD and DVD: Deny read access	This policy setting allows you to deny Read access to devices in the CD and DVD removable storage class, including USB connected devices.
CD and DVD: Deny write access	This policy setting allows you to deny Write access to devices in the CD and DVD removable storage class, including USB connected devices. Important Some non-Microsoft CD and DVD burner software interacts with the hardware in a way that is not prevented by the policy.

134 https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/hh125922%28v%3dws.10%29#removable-storage-access (Stand 14.09.2019)

Policy settings	Description
	If you want to prevent all writing to CD or DVD burners, you might want to consider applying a Group Policy setting to prevent the installation of that software.
Custom Classes: Deny read access	This policy setting allows you to deny Read access to any device with a Device Setup Class GUID that is found in the lists you provide.
Custom Classes: Deny write access	This policy setting denies Write access to custom removable storage classes that you specify.
Floppy Drives: Deny execute access	This policy setting allows you to deny Execute access to devices in the Floppy Drive class, including USB connected devices.
Floppy Drives: Deny read access	This policy setting allows you to deny Read access to devices in the Floppy Drive class, including USB connected devices.
Floppy Drives: Deny write access	This policy setting allows you to deny Write access to devices in the Floppy Drive class, including USB connected devices.
Removable Disks: Deny execute access	This policy setting allows you to deny Execute access to removable devices that are emulate hard disks, such as USB memory drives or external USB hard disk drives.
Removable Disks: Deny read access	This policy setting allows you to deny Read access to removable devices that are emulate hard disks, such as USB memory drives or external USB hard disk drives.
Removable Disks: Deny write access	This policy setting allows you to deny Write access to removable devices that emulate hard disks, such as USB memory drives or external USB hard disk drives.
Tape Drives: Deny execute access	This policy setting allows you to deny Execute access to tape drives, including USB connected devices.
Tape Drives: Deny read access	This policy setting allows you to deny Read access to tape drives, including USB connected devices.
Tape Drives: Deny write access	This policy setting allows you to deny Write access to tape drives, including USB connected devices.
WPD Devices: Deny read access	This policy setting allows you to deny Read access to devices in the Windows Portable Device class, such as media players, mobile phones, and Windows CE devices.
WPD Devices: Deny write access	This policy setting allows you to deny Write access to devices in the Windows Portable Device class, such as media players, mobile phones, and Windows CE devices.
All Removable Storage classes: Deny all access	This policy setting takes precedence over any of the policy settings in this list, and if enabled, it denies Execute, Read, and Write access to any device that is identified as using a removable storage device.
All Removable Storage: Allow direct access in remote sessions	This policy setting grants users direct access to removable storage devices in remote sessions.

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die hier vorliegende Arbeit selbstständig, ohne unerlaubte fremde Hilfe und nur unter Verwendung der in der Arbeit aufgeführten Hilfsmittel angefertigt habe.

Heubach, 27.09.2019

Ort, Datum (Unterschrift)

Thesen

- Unternehmen können durch eine vorzeitige Planung die Zeit zum entdecken eines Vorfalls deutlich verringern.
- Ein Log-Management kombiniert mit einem SIEM kann Vorfälle besser aufdecken, als eine Post-Mortem-Analyse eines einzelnen Clients.
- Die Forensic Readiness ist in jedem Unternehmen sinnvoll.
- Verschlüsselung von kritischen Unternehmensdaten ist durchaus sinnvoll.
- Anstatt einer Auswertung der einzelnen Logdateien macht eine Korrelation aller Logdateien in einem Dashboard Sinn und erspart Zeit beim Bearbeiten von Vorfällen.
- Durch eine sinnvolle Erweiterung der Logdaten der Computer und Server, durch die der Firewall und des Proxys können auch Hackerangriffe besser erkannt werden.