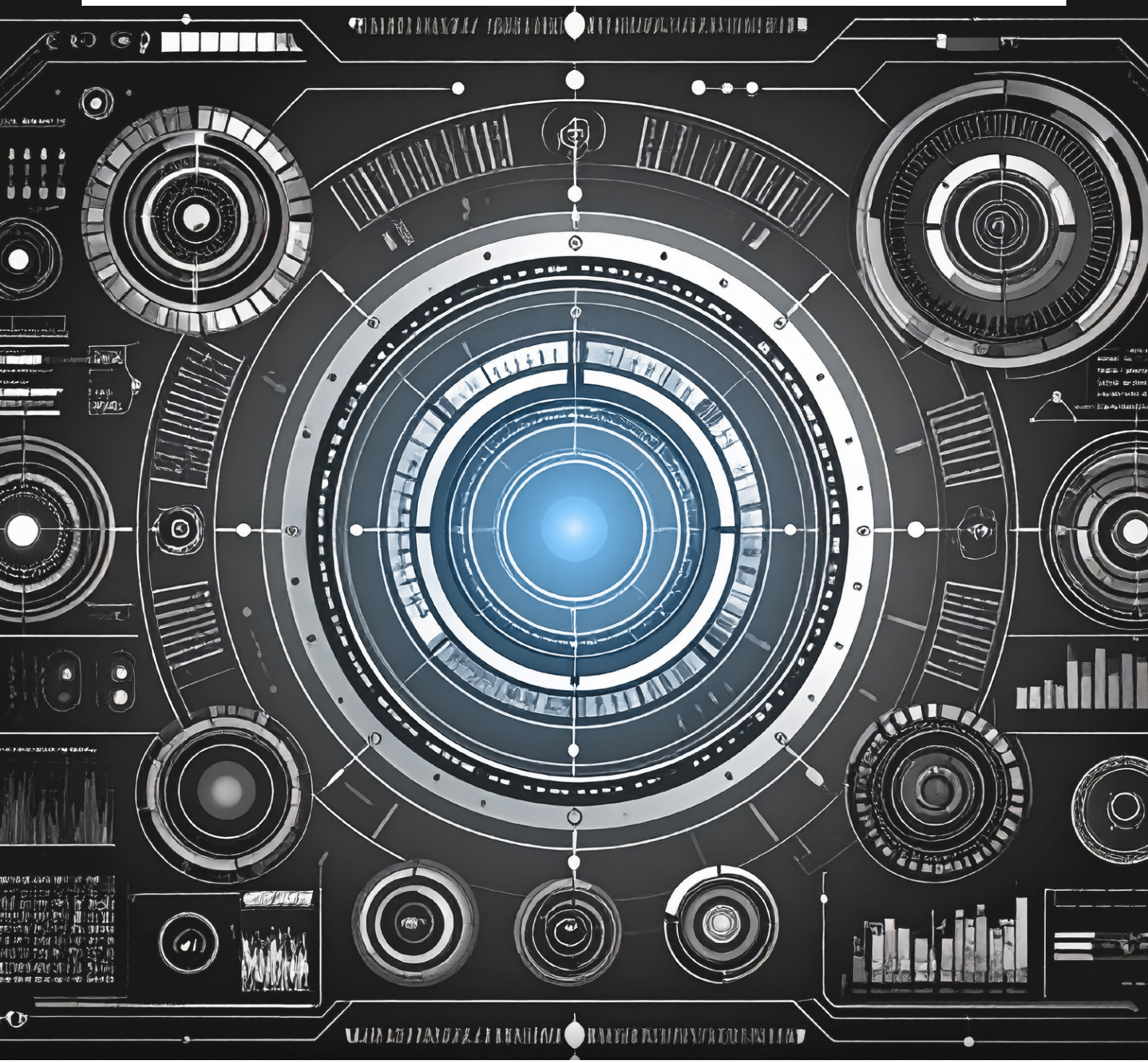
Eine Veröffentlichung des ISACA Germany Chapter e.V.



Security Use-Cases – ein Katalog

Ein Best-Practice-Leitfaden der Fachgruppe Cyber Security zur Erkennung von sicherheitsrelevanten Ereignissen und Prüfung des Umsetzungsstandes

ISACA Germany Chapter

Allianz für Cyber-Sicherheit Multiplikator

dpunkt.verlag

Herausgeber
ISACA Germany Chapter e.V.
Storkower Straße 158
D-10407 Berlin
www.isaca.de
info@isaca.de

Autorenteam
Markus Dreyer
Gerd Dettweiler
Alena Brandenburg
Christian Gerlach
Christian Gresser
Christian Lehrer
Dirk Schugardt
Günther Orth
Sabine Kesberger
Philipp Rieblinger (extern)

Security Use-Cases – ein Katalog

Ein Best-Practice-Leitfaden der Fachgruppe Cyber Security zur Erkennung von sicherheitsrelevanten Ereignissen und Prüfung des Umsetzungsstandes

Allianz für Cyber-Sicherheit

Mit der 2012 gegründeten Allianz für Cyber-Sicherheit (ACS) verfolgt das Bundesamt für Sicherheit in der Informationstechnik (BSI) das Ziel, die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyberangriffen zu stärken. Stand 02. Juli 2025 gehören dieser Initiative 8463 Teilnehmer, 207 Partner und 117 Multiplikatoren an, die so ihren Beitrag für mehr Cybersicherheit am Wirtschaftsstandort Deutschland leisten. ISACA Germany Chapter e.V. ist bereits seit 2019 als Multiplikator an der Allianz für Cyber-Sicherheit gelistet und trägt dazu bei, die Reichweite der ACS zu erhöhen.

Die Fachgruppe Cyber Security des ISACA Germany Chapter e.V. hat bereits mit dem im März 2014 in der ersten Version veröffentlichten Leitfaden Cyber-Sicherheits-Check, mit dessen Überarbeitung in der Version 2 von Februar 2020 und dem Leitfaden Cyber-Sicherheits-Check für operative Technologie (OT) von September 2021 Grundsteine gelegt, wie über die sechsstufigen Vorgehensmodelle das operative Sicherheitsniveau der Büro-IT sowie der Produktions- und Prozessanlagen bestimmt und verbessert werden kann.

Durch die Anwendererfahrungen bei der Verwendung der Leitfäden hat sich die Fachgruppe Cyber Security des ISACA Germany Chapter e.V. dazu entschlossen, ein bislang schwierig zu behandelndes Thema aus den Maßnahmenzielen dieser Leitfäden herauszugreifen und den »Security Use Cases – ein Katalog« zu entwickeln und diesen frei zur Verfügung zu stellen. Der Katalog richtet sich an Verantwortliche und Prüfer, die eine Erkennung von sicherheitsrelevanten Ereignissen umsetzen und die Prüfung des Umsetzungsstandes der Erkennung durchführen wollen.

Quelle der Zahlen:
https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Ueber-uns/Teilnehmer/teilnehmer_node.html

Vorwort

Das ISACA Germany Chapter e.V. ist der deutsche Zweig des weltweit führenden Berufsverbandes der IT-Revisoren, Informationssicherheitsmanager und IT-Governance-Beauftragten. Der Verein wurde 1986 gegründet und ist mit über 4.000 Mitgliedern Teil des internationalen Verbandes ISACA, dem weltweit mehr als 180.000 Know-how-Träger in 188 Ländern mit 225 Chapter angehören. Zweck des Vereins ist es, durch Diskussion und Informationsaustausch zwischen den Mitgliedern und Interessenten das Verständnis der Probleme auf dem Gebiet der IT-Revision, Informationssicherheit, Cyber Security sowie IT-Governance zu fördern und diese Erfahrungen durch Publikationen und Seminare allen Mitgliedern und Interessenten zur Kenntnis zu bringen.

Bereits 2014, im damals frisch veröffentlichten Cyber-Sicherheits-Check [ISACA 2014], wurde ein Thema als wesentlich für die Cyberabwehr in den Maßnahmenzielen aufgenommen [ISACA 2020]: zu erkennen, dass gerade ein Angriff erfolgt, um darauf reagieren zu können. Das war und ist bereits sehr lange ein Thema. Aber auch heute noch, nachdem von uns ausgebildete Cyber Security Practitioner unzählige Cyber-Sicherheits-Checks durchgeführt haben, hat sich nichts Wesentliches an der Situation geändert: Protokolldaten werden zumeist stiefmütterlich behandelt, in der Standardkonfiguration nur kurzzeitig aufbewahrt und nur ausgewertet, wenn schon etwas passiert ist. Wenn überhaupt, dann leisten sich nur größere Unternehmen oder Institutionen (nachfolgend auch Organisationen) ein Security Information and Event Management (SIEM) System und können zeitnah auf Anomalien reagieren.

Doch warum ist das so? Protokolldaten sind Massendaten und eine menschengeführte permanente Kontrolle der Ereignisse ist nicht möglich. Nur ein kleiner Teil der Ereignisse ist auch relevant. Doch auch dieser Teil ist zumeist noch immer zu umfangreich, um von Menschen effektiv und effizient ausgewertet zu werden. Erschwerend kommt hinzu, dass jedes System Daten unterschiedlicher Formate, Inhalte, Strukturen und Relevanz liefert. Zudem ändern sich diese Daten oftmals mit den regelmäßigen System- und Anwendungsupdates. Außerdem gibt es auch proprietäre Formate, besonders im Bereich der operativen Technologie (OT) [ISACA 2021] oder bei eigenentwickelten Lösungen, bei denen eine Auswertung erst mühsam erarbeitet werden muss. Und es kommt immer noch vor, trotz einer rasanten Entwicklung auf dem Gebiet der IT-Sicherheit, dass wichtige Ereignisse erst gar nicht protokolliert werden.

Wie könnte das abgestellt werden? Diese Frage stellte sich 2021 die Fachgruppe Cyber Security und es wurden die folgenden Gründe gefunden:

1. Es gibt keine standardisierte Protokollierung, die zumindest sicherheitsrelevante Ereignisse am besten in Format, Struktur und Inhalt auf gleiche Weise zur Verfügung stellt.
2. Es gibt keine Übersicht, welche Daten sicherheitsrelevante Ereignisse darstellen.
3. Es gibt keine Aufstellung, welche Use-Cases (Anwendungsfälle) als Mindestmaß betrachtet werden sollten.

In der hierzu gegründeten Arbeitsgruppe (AG) SIEM hat man sich mit dem Punkt 1 auseinandergesetzt und geprüft, welche Entwicklungen es hinsichtlich einer standardisierten Protokollierung gibt und was damit erreicht werden kann (siehe auch Positionspapier SIEM – Vorschlag für einen Protokollierungsstandard [ISACA 2022]). Es wurden bereits von namhaften Herstellern wie Microsoft oder Amazon Initiativen gestartet und das OCSF (Open Cybersecurity Schema Framework) sieht aktuell nach einem erfolgversprechenden Format aus.

Hierbei ist aufgefallen, dass es bislang noch keine Aufstellung der Protokollinformationen gibt, die als sicherheitsrelevantes Ereignis aus Sicht der Verteidiger betrachtet werden sollten. Neben anderen Quellen wurde von der AG SIEM insbesondere das MITRE ATT&CK® Framework herangezogen. Als mit dem Use-Case-Katalog begonnen wurde, wurden insgesamt nur wenig Details zur Umsetzung einer Angriffserkennung und zu benötigten Ereignisinformationen vorgefunden.

In der Arbeitsgruppe wurde daraufhin entschieden, einen Use-Case-Katalog aufzubauen, der die wichtigsten Anwendungsfälle für die Erkennung aufzeigt und ihre Umsetzung in einer allgemein verständlichen Form darstellt. Der Katalog soll systemunabhängig für alle System- und Protokolldaten der IT und OT angewendet werden können. Es war erkennbar, dass zusätzlich ein Katalog der relevanten Ereignisse entsteht und hierdurch die effektive Angriffserkennung einen Schritt vorankommt. Da der Use-Case-Katalog insbesondere auch kleine und mittelständische Unternehmen wie auch Institutionen im Fokus hat, ist es wichtig, dass viele der Use-Cases auch mit einfachen Lösungen oder »Bordmitteln« realisierbar sein müssen. Ebenso ist es wichtig, dass für den Aufbau der Angriffserkennung ein Stand dokumentiert werden kann, der wiederum auch zur Umsetzungsverfolgung ge-

nutzt werden kann. Umgekehrt kann hierüber eine Prüfung der umgesetzten Angriffserkennung durchgeführt werden. Um zu wissen, welche Angriffe mit dem Stand der Umsetzung bereits erkannt werden können, war sowohl die Referenz zu ATT&CK als auch zum BSI IT-Grundschutz bedeutsam.

Folgendes steht Ihnen nun mit dem hier vorliegenden Dokument zur Verfügung:

- Eine Sammlung von Use-Cases zur Erkennung von Anomalien, die auf Angriffe hindeuten, und Empfehlungen und Hinweise bzgl. der Reaktion auf diese Anomalien (Use-Case-Katalog)
- Eine abstrakte Regelbeschreibung, welche Ereignisinformationen in welcher Form ausgewertet werden können
- Allgemeine Anwendbarkeit für IT und OT
- Aufbau nach einem Auswertungsniveau basierend auf der Größe der Organisation
- Use-Cases, die bereits ohne Angriffserkennungssysteme auswertbar sind
- Ein Prüfkatalog, mit dem der Stand der Anomalien-Erkennung für die IT-Infrastruktur und -Anwendungen aufgestellt und kontrolliert sowie auch der weitere Ausbau gesteuert werden kann
- Referenzen zu ATT&CK und mindestens ein Use-Case zu jeder Taktik (»Tactic«)
- Referenz zu BSI IT-Grundschutz-Kompendium [BSI 2023], sofern möglich

Uns ist bewusst, dass wir hier Neuland betreten. Das, was hier in nunmehr über zweieinhalb Jahren ehrenamtlich erarbeitet wurde, gibt es in dieser Form noch nicht. Wir konnten uns also auch nicht auf bereits bestehende Ausarbeitungen beziehen. Wir wissen daher, dass wir mit der hier vorliegenden Fassung den ersten Schritt wagen und hierauf weitere Änderungen folgen werden.

An dieser Stelle möchten ich mich im Namen der Fachgruppe Cyber Security bedanken.

Mein Dank geht an

- die Leitung der Arbeitsgruppe und die Hauptautoren Markus Dreyer und Gerd Dettweiler, die unermüdlich das Thema vorangebracht und einen Großteil der Arbeitsleistung getragen haben,
- die Helfer aus der Fachgruppe und die externen Helfer, die sich in dieses doch komplexe Thema eingebracht und viel Arbeit abgenommen haben,
- den Vorstand für die umfangreiche Unterstützung sowie
- die Unterstützer aus staatlichen Institutionen, die uns durch ihre konstruktiven Kritiken geholfen haben, den Use-Case-Katalog auf- und auszubauen und zu verbessern.

Dirk Schugardt
Leiter Fachgruppe Cyber Security
ISACA Germany Chapter e.V.

Inhaltsverzeichnis

1 Zielsetzung 7

1.1 Motivation ... 7
1.2 Definition von Use-Case ... 7
1.3 Definition des Begriffes »Use-Case-Katalog« ... 9
1.4 Vorteile und Nutzen des Use-Case-Katalogs ... 9

2 Grundlagen zur Erkennung von Angriffsszenarien 11

2.1 Protokolle ... 11
2.2 Zentralisierung und Normalisierung ... 12
2.3 Auswertung und Aktualisierung ... 13
2.4 Forensische Analyse ... 13

3 Use-Case-Katalog 15

3.1 Designprinzipien ... 15
3.2 Auswertungsniveaus ... 16
3.3 IT-Landschaftskonzept ... 17
3.4 Übersichten zur Abdeckung ... 19
3.5 Liste der abstrakten Ereignisdefinitionen ... 26
3.6 Hinweise zur Umsetzung ... 27
3.7 Beispiele für die Umsetzung ... 29
3.8 Hinweise zur Nomenklatur der Use-Cases ... 31
3.9 Liste der Use-Cases ... 33
3.9.1 B01 – Löschung von Ereignisprotokollen ... 34
3.9.2 B02 – Änderung von Ereignisprotokollen ... 36
3.9.3 B03 – Änderung der Protokollierungsfunktion ... 38
3.9.4 B04 – Deaktivierung der Protokollierungsfunktion ... 40
3.9.5 B05 – Änderung von sicherheitsrelevanten Konfigurationseinstellungen ... 42
3.9.6 B06 – Deaktivierung von Sicherheitslösungen ... 44
3.9.7 B07 – Verwendung spezieller Benutzerkonten ... 46
3.9.8 B08 – Erkennung von Brute-Force-Angriffen (mehrere Benutzerkonten) ... 48
3.9.9 B09 – Erkennung von Brute-Force-Angriffen (einzelnes Benutzerkonto) ... 50
3.9.10 B10 – Ausfall Zeitsynchronisationsdienst ... 52
3.9.11 B11 – Unautorisierte Änderung der Systemzeit ... 53
3.9.12 B12 – Ungenehmigter Start oder Stopp einer Anwendung oder eines Service ... 55
3.9.13 B13 – Alarmmeldung von Security-Lösung ... 57
3.9.14 B14 – Erkennung von Portscans am Perimeter – horizontal ... 59
3.9.15 B15 – Erkennung von Portscans am Perimeter – vertikal ... 61
3.9.16 B16 – Erkennung von internen Portscans – horizontal ... 63
3.9.17 B17 – Erkennung von internen Portscans – vertikal ... 65
3.9.18 B18 – Keine Daten von Protokollquelle ... 67

3.9.19 B19 – Technisches Konto – Sperrung aufgrund zu vieler fehlgeschlagener Anmeldeversuche 69
3.9.20 B20 – Erfolgreicher Login nach fehlgeschlagenen Anmeldeversuchen 71
3.9.21 B21 – Technisches Konto – fehlgeschlagener interaktiver Anmeldeversuch 73
3.9.22 B22 – Technisches Konto – erfolgreiche interaktive Anmeldung 76
3.9.23 B23 – Benutzer administriert sich selbst 79
3.9.24 B24 – Administration von Benutzerkonten 81
3.9.25 B25 – Administration von Rechten 83
3.9.26 B26 – Änderungen an Regelwerken oder Konfigurationen 85
3.9.27 B27 – Benutzer erhält besondere privilegierte Rechte 87
3.9.28 B28 – Logins zu ungewöhnlichen Zeiten 89
3.9.29 B29 – Mehrfach fehlgeschlagene Anmeldeversuche über längeren Zeitraum 91
3.9.30 B30 – Zugriff auf PAM-verwaltete Systeme ohne PAM 94
3.9.31 B31 – Verwendung kritischer Funktionen 96
3.9.32 B32 – Systemkommunikation in externe Netze 98
3.9.33 B33 – Unzulässige Systemkommunikation erkennen 100
3.9.34 B34 – Unbekanntes Gerät entdeckt 102
3.9.35 B35 – Erkennung unerwünschter Software 104
3.9.36 B36 – Herunterladen bösartiger Inhalte 106
3.9.37 B37 – Datenausleitung 108
3.9.38 B38 – Erkennung bösartiger Zugriffe von externen Systemen auf interne Systeme 110
3.9.39 B39 – Erkennung interner Zugriffe von bekannt bösartigen Hosts 112
3.9.40 B40 – Ungewöhnliche Netzwerkaktivität außerhalb der Geschäftszeiten 114
3.9.41 B41 – Unzulässiger Zugriff auf sensible Daten 116
3.9.42 B42 – Unzulässiger Zugriff auf System- und Konfigurationsdaten 118
3.10 Dokumentation von Use-Cases und Use-Case-Umsetzungen 120

4 Bericht 123

5 Zusammenfassung und Ausblick 126

6 Abbildungs- und Tabellenverzeichnis 127

7 Abkürzungsverzeichnis 128

8 Literaturverzeichnis 129

1 Zielsetzung

1.1 Motivation

Seit Jahren steigt weltweit die Bedrohung der Wirtschaft durch Cyberkriminalität. Gemäß Bitkom [Bitkom 2024] beträgt der finanzielle Schaden von Cyberattacken allein in Deutschland über 178 Milliarden Euro jährlich, Tendenz weiterhin ansteigend. Der Trend zeigt, dass insbesondere die digitalen Angriffe zunehmen, was auch durch kriegerische Auseinandersetzungen verstärkt wird. Zwei Drittel der Unternehmen sehen sich aufgrund von potenziellen Cyberattacken in ihrer Existenz gefährdet.

Auch die Zeitspanne, nach der ein erfolgreicher Angriff von der Organisation erkannt wird, ist erschreckend groß: Statistisch gesehen schwanken die Angaben verschiedener Studien zwischen 10 [Mandiant 2024] und 150 Tagen [IBM 2024].

Es ist jedoch für die IT-Sicherheitshygiene einer Organisation ausgesprochen wichtig, Cyberangriffe möglichst früh zu erkennen – idealerweise noch bevor die Angreifer sich auf Systemen etablieren konnten. Ein probates Mittel dafür ist die Überwachung der IT-Vorgänge mithilfe von im Vorfeld antizipierten Angriffsszenarien, hier als Security Use-Cases oder kurz nur Use-Cases bezeichnet. Die Nutzung von Verfahren zur Angriffserkennung ist mittlerweile eine vielfach geforderte Maßnahme in Standards oder Best-Practices-Leitlinien. So empfiehlt bspw. die ISO 27001:2022 mit Control 8.16 aus Anhang A, Netze, Systeme und Anwendungen auf anormales Verhalten zu überwachen und geeignete Maßnahmen zu ergreifen, um im Verdachtsfall mögliche Vorfälle im Bereich der Informationssicherheit bewerten zu können. Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) steuert zu diesem Thema eine Orientierungshilfe [BSI 2024] bei. Die Betreiber kritischer Infrastrukturen sind in Deutschland durch das aktuelle IT-Sicherheitsgesetz (§8a Abs. 1a BSIG) dazu verpflichtet, Systeme zur Angriffserkennung nach dem geltenden Stand der Technik einzusetzen.

Die Gewährleistung der Informationssicherheit in den Organisationen ist Aufgabe des Managements. Auch wenn die Umsetzung in der Regel an Fachpersonal (wie CISO – Chief Information Security Officer, ISB – Informationssicherheitsbeauftragte oder IT-Leitung) delegiert wird, bleibt die Ergebnisverantwortung dafür stets bei der Geschäftsleitung. Dieser Use-Case-Katalog soll dabei helfen, die Transparenz für das komplexe Thema zu verbessern, auch die Führungsebene mit einzubinden und hier das notwendige Verständnis zu schaffen. Gleichzeitig leistet er einen wichtigen Beitrag für die praktikable und zugleich effiziente Umsetzung der Erkennung von Cyberangriffen für Organisationen aller Größenordnungen.

Die Empfehlungen zur Dokumentation und zum Berichtswesen sollen es den Anwendern des Katalogs erleichtern, die Use-Cases umzusetzen und zu dokumentieren. Zudem erhalten damit externe Prüfer, Revisoren und Aufsichtsbehörden effizient alle erforderlichen Informationen und die Organisationen einen Überblick über die damit verbundenen Aufwände. Beides trägt wesentlich zur Transparenz und Kostenoptimierung in Umsetzung und Prüfwesen bei.

1.2 Definition von Use-Case

Es gab im Internet oder in der Fachliteratur zum Zeitpunkt der Recherche keine klare Festlegung darüber, was unter einem Security Use-Case im Kontext der Informations- und Kommunikationstechnologie (IKT) konkret zu verstehen ist. Die Ausführungen dazu waren recht unterschiedlich und gehen von engen Definitionen, z. B. aus der Softwareentwicklung, bis zu sehr weiten Auffassungen, die nicht nur das Erkennen eines Sicherheitsvorfalls, sondern auch die Reaktion auf ihn einbeziehen.

Gemäß dem Verständnis in der Arbeitsgruppe wurde diesem Leitfaden folgende Definition zugrunde gelegt, die alle wesentlichen Merkmale enthält, ohne unnötig einzuschränken:

»Ein Security Use-Case beschreibt, wie ein Angriffsszenario erkannt werden kann. Dies geschieht in Form einer technischen Sicherheitskontrolle, mit dem Ziel, auf das Angriffsszenario möglichst frühzeitig zu reagieren.«

Derjenige, der den Use-Case erstellt, benötigt Informationen zu potenziellen Sicherheitsrisiken, bspw. IT-Schwachstellen, über deren Ausnutzung er informiert werden möchte. Diese Schwachstellen können organisations- bzw. produktspezifisch sein – z. B. bei einer selbst programmierten Anwendung – oder genereller Natur. Es ist daher wichtig, sich bereits beim Aufbau der Angriffserkennung Gedanken über die Risiken beim Betrieb der IT-Landschaft zu machen, idealerweise in

Form eines Risikomanagements. Das erleichtert die Auswahl der für die Organisation sinnvollen Use-Cases erheblich. Die technische Umsetzung und somit die Implementierung der Elemente eines Use-Case geht stets mit technischen Maßnahmen einher. Sie basiert auf der hier zur Verfügung gestellten Beschreibung eines Use-Case und zusätzlich auf zu ergänzenden spezifischen Use-Cases der jeweiligen Organisation.

Hierzu ein Beispiel als Erläuterung:

Die auf Angreiferseite beliebte Möglichkeit, sich durch Deaktivierung der Protokollierung einer Erkennung zu entziehen, wird im Use-Case-Katalog unter B04 ausführlich beschrieben. Risikobezogen sind hier zumindest die Protokolle wichtiger und zentraler Systeme einzubeziehen, bspw. für die Organisation geschäftskritische Systeme, zentrale Firewall- oder Authentifizierungssysteme. Gerade über zentrale IT-Systeme bzw. IT-Dienste sind Angriffe auf die gesamte Infrastruktur möglich, daher ist deren Schutz von hoher Bedeutung. Eine fehlende Protokollierung macht es unmöglich, forensische Auswertungen der Angriffsvektoren durchzuführen, um im Nachgang die vorliegenden Schwachstellen zu erkennen und zu schließen. Idealerweise sollten daher möglichst alle IT-Systeme berücksichtigt werden.

Um einen Use-Case in den Regelbetrieb einzubeziehen, sind neben der risikobasierten Auswahl noch weitere Parameter zu berücksichtigen. Dies veranschaulicht das Bearbeitungsschema in Abbildung 1. Es müssen ein protokollierbares Ereignis ausgewählt und eine Prüfregel nebst Auslöser (»Trigger«) definiert werden. Dabei dienen ergänzende Listen dazu, sowohl die Überprüfung, ob eine Störung bzw. ein potenzieller Sicherheitsvorfall – ein sogenannter »Security-Incident« oder kurz »Incident« – vorliegt, auszulösen als auch unerwünschte Fehlalarme zu minimieren. Wird gemäß einer Prüfregel ein potenzieller Incident erkannt, erfolgt eine manuelle oder automatisierte Validierung. Fällt diese positiv aus, ist ein Security-Incident erkannt und bestätigt, woraufhin eine Reaktion erfolgt (im Sinne von festgelegten Schritten). Aufgrund der dynamischen Entwicklung der Angriffe sind die Use-Cases auch permanent zu überprüfen und an sich verändernde Szenarien anzupassen (Regeloptimierung)[1]. Sobald ein Use-Case-Ereignis durch manuelle oder automatisierte Überprüfung validiert wird, entsteht daraus entlang der Prozesskette ein Security-Incident, auf den gemäß den durch die Organisation festgelegten Schritten zu reagieren ist.

Der Betrieb und die Pflege eines Use-Case sollten nach den bekannten Mechanismen des PDCA-Zyklus[2] erfolgen. Die Farben in Abbildung 1 zeigen an, welchen Teilschritten des Bearbeitungsschemas welche Phasen des PDCA-Zyklus zuzuordnen sind. Die Elemente innerhalb des grau hinterlegten Kastens wirken zusammen, um einen Use-Case technisch abzubilden, und verdeutlichen nochmals das hier zugrunde gelegte Verständnis.

1 Enthält neben Prüfung auf Überarbeitungsbedarf im Fall von False Positives und False Negatives auch die regelmäßige Kontrolle und Tests, ob die Regeln bspw. nach Updates der überwachten Systeme noch korrekt funktionieren. So könnte sich auch die Protokollierung der Ereignisse geändert haben (Konfiguration oder Inhalte).

2 Definition siehe z. B. [BSI 2018].

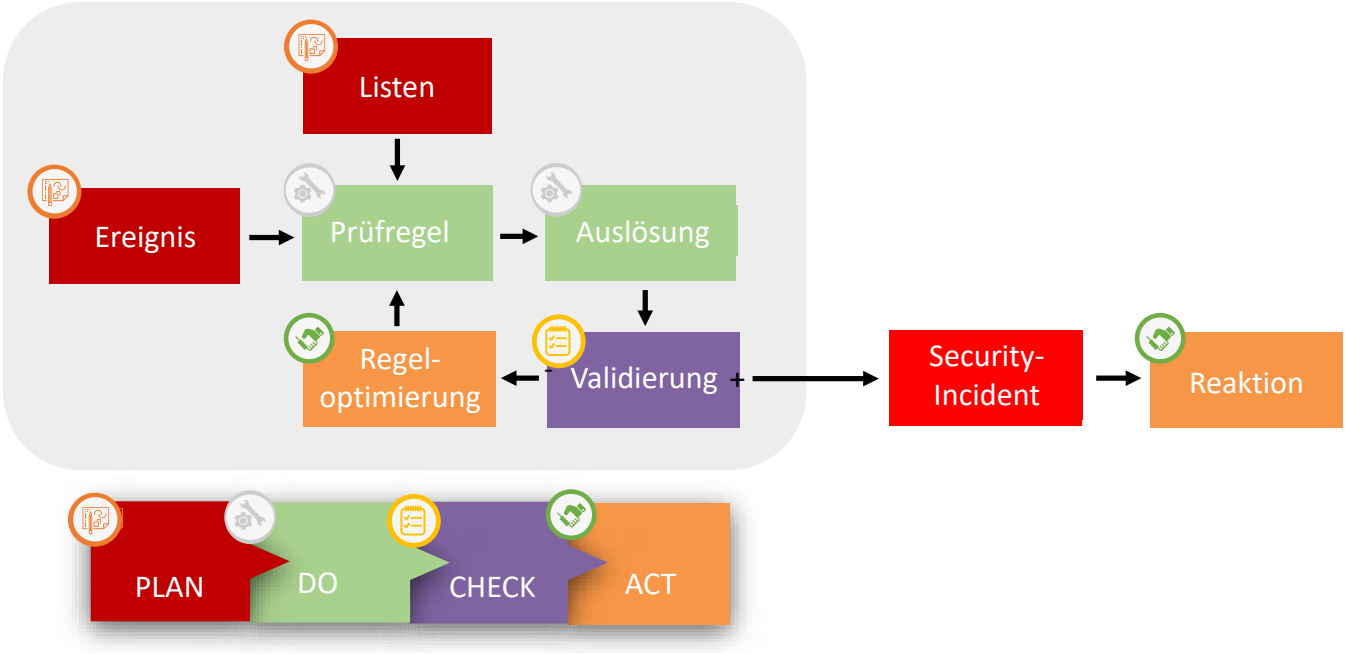


Abbildung 1: Funktionaler Ablauf eines IT-Security Use-Case

Alle den Use-Case betreffenden Elemente aus Abbildung 1 sind in Tabelle 10 »Steckbrief für Use-Cases« (Seite 120) und Tabelle 11 »Steckbrief zur einheitlichen Dokumentation von Use-Case-Umsetzungen« (Seite 121) den jeweiligen Zeilen der Tabellen zugeordnet. Hierdurch lässt sich aufzeigen, welcher der oben genannten Schritte im Use-Case-Katalog umgesetzt wird. Der Anwender des Katalogs kann dies als Hilfestellung zur Orientierung nutzen. Nicht enthalten ist die organisationsspezifisch umzusetzende Tätigkeit der Validierung. Diese kann so unterschiedlich sein, dass ihre Beschreibung im Rahmen dieses Leitfadens nicht möglich ist. Der Schritt »Reaktion« ist im Use-Case-Katalog enthalten und mit den Handlungsempfehlungen versehen, die sich anhand der jahrelangen Erfahrung der Autoren in der Praxis bewährt haben. Auch dies ist als Hilfestellung für den weniger erfahrenen Anwender des Katalogs zu verstehen.

Ein einfaches Beispiel zur Erläuterung:

Das »Ereignis« »Deaktivierung der Protokollierungsfunktion« (Use-Case B04) tritt ein. Die Informationen aus den »Listen«, wie z. B. die Benutzer, die das Ereignis auslösen dürfen, werden entnommen. In der »Prüfregel« wird verglichen, ob die Benutzer, die die Protokollierung deaktiviert haben, in der Liste der berechtigten Benutzer enthalten sind. Ist dies nicht der Fall, wird der Use-Case »ausgelöst«. Die »Validierung« ist üblicherweise die Überprüfung der Auslösung durch einen Analysten. Die »Regeloptimierung« findet bei Bedarf statt, wenn zu viele Ereignisse nicht erkannt oder falsche Auslösungen aufgetreten sind (False Negatives / False Positives). Als Ergebnis erhält man einen validen »Security-Incident«, auf den entsprechend mit Gegenmaßnahmen »reagiert« werden muss.

1.3 Definition des Begriffes »Use-Case-Katalog«

Ein Use-Case-Katalog ist eine Zusammenstellung einer Vielzahl von Use-Cases, die einen Großteil von Angriffen erkennen, die in der Praxis verbreitet sind. Hervorzuheben ist, dass die hier angeführten Use-Cases aufgrund der Erfahrungen der Verfasser schon seit Jahrzehnten als »Evergreens« gelten und auch in Zukunft relevant sein dürften. Es handelt sich dabei um einen Katalog aus Sicht der Verteidiger, der sich durch eine grundlegende Abdeckung von Use-Cases zur Erkennung von Cyberattacken auszeichnet.

Der hier vorliegende Use-Case-Katalog ist über das ISACA Germany Chapter frei verfügbar und bietet eine standardisierte Dokumentation. Da trotz umfangreicher Recherche ein vergleichbarer öffentlich verfügbarer Use-Case-Katalog nicht gefunden werden konnte, wurden alle Use-Cases den Bedrohungen des anerkannten Katalogs für Angriffsszenarien (MITRE ATT&CK®)[3] zugeordnet.

3 Sowohl MITRE ATT&CK® als auch ATT&CK® sind eingetragene Markenzeichen von The MITRE Corporation. Siehe [MITRE 2025a].

Ein allgemeiner Use-Case-Katalog, wie der vorliegende, kann nur grundlegende Szenarien abdecken und ist als Referenz zu verstehen. So kann der Katalog durchaus Use-Case-Vorschläge enthalten, die aus Sicht der Organisation für die Absicherung nicht notwendig sind. Daher müssen die Use-Cases hinsichtlich organisationsspezifischer Konstellationen von den jeweiligen Organisationen bewertet und ggf. um eigene Use-Cases ergänzt, konkretisiert und in den eigenen Katalog mit aufgenommen werden. Die empfohlene Vorgehensweise für die Use-Cases aus dem Katalog ist in Abbildung 2 in ihren Teilschritten veranschaulicht: Die erste Überlegung sollte darin bestehen, welche Referenz-Use-Cases für die Organisation generell als hilfreich erachtet werden. Sodann ist zu entscheiden, wie ein ausgewählter Use-Case auszugestalten ist. Im letzten Schritt sind die Use-Cases an die organisationsspezifischen Gegebenheiten technisch anzupassen.

Die Verwendung dieses Katalogs bietet Organisationen den Vorteil, dass ein Großteil der Use-Case-Entwicklung vereinfacht wird. Aufgrund der Dynamik der Bedrohungsszenarien und der eigenen IT-Landschaft sollte der oben beschriebene Prozess in sinnvollen Zeitabständen wiederholt werden, um die Vollständigkeit des eigenen Use-Case-Katalogs zu überprüfen und entstandene Lücken zu identifizieren.

1.4 Vorteile und Nutzen des Use-Case-Katalogs

Der vorliegende Use-Case-Katalog wurde für das Sicherheitsmonitoring aller Organisationsgrößen erstellt und soll damit eine möglichst große Zielgruppe abdecken. Er soll somit auch Erkennungen bereits ohne zusätzliche Lösungen erlauben.

Derzeit gibt es eine Vielzahl an kommerziellen Angeboten, die eine Früherkennung von Cyberangriffen ermöglichen. Allerdings sind dies meist kostenintensive und komplexe Systeme, wie On-Premises-Appliances, oder Services von Dienstleistern, die z. B. Unterstützung in Form von SOCaaS (Security Operations Center as a Service) bieten. Hier kann der Use-Case-Katalog für eine Vergleichbarkeit der Anbieter und der verwendeten Angriffserkennungen genutzt werden und auch für die Anbieter eine Hilfestellung darstellen.

Ein weiterer Aspekt ist die Größe der Unternehmen bzw. Institutionen: Wie aus Abbildung 3 ersichtlich ist, steht die Mitarbeiterzahl eines Unternehmens im umgekehrten Verhältnis zur Zahl der Unternehmen. In Deutschland zählen laut dem Statistischen Bundesamt über 99 % zu den kleinen und mittleren Unternehmen (KMU), nur knapp 1 % zu den Großunternehmen [D_STATIS 2025]. Allerdings erwirtschaften die Großunternehmen 73 % des Nettoumsatzes der deutschen Wirtschaft. Für die Cyberabwehr ist aus unserer Sicht davon auszugehen, dass auch zukünftig ein Großteil der Angriffe im Bereich KMU zu erwarten ist. Leider ist aber genau diese Gruppe bislang nur wenig vorbereitet.

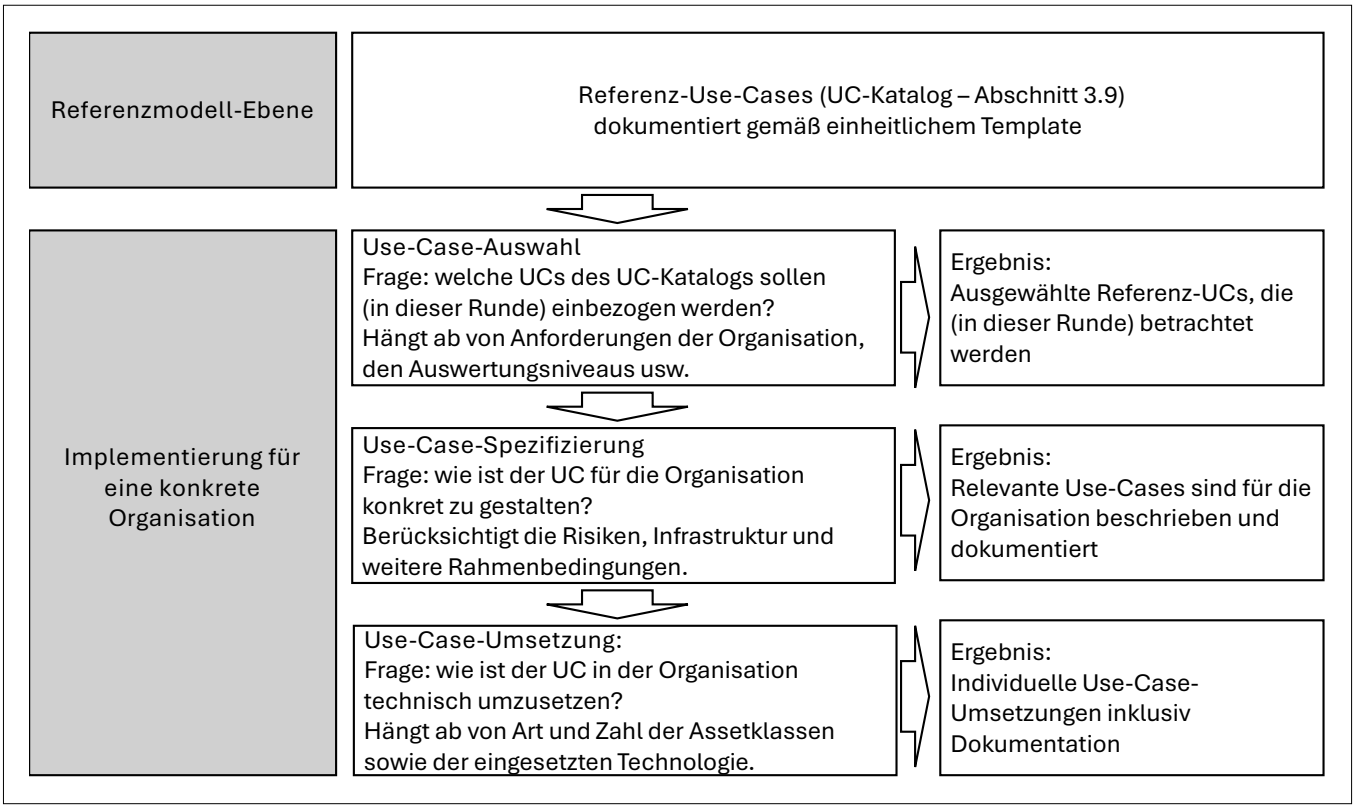


Abbildung 2: Vorgehensschema zur Implementierung von Use-Cases aus dem Katalog

Daher kann der Katalog gerade dieser Zielgruppe einen hohen Mehrwert bieten, indem er als Einstiegshilfe zum Thema Incident-Erkennung genutzt wird.

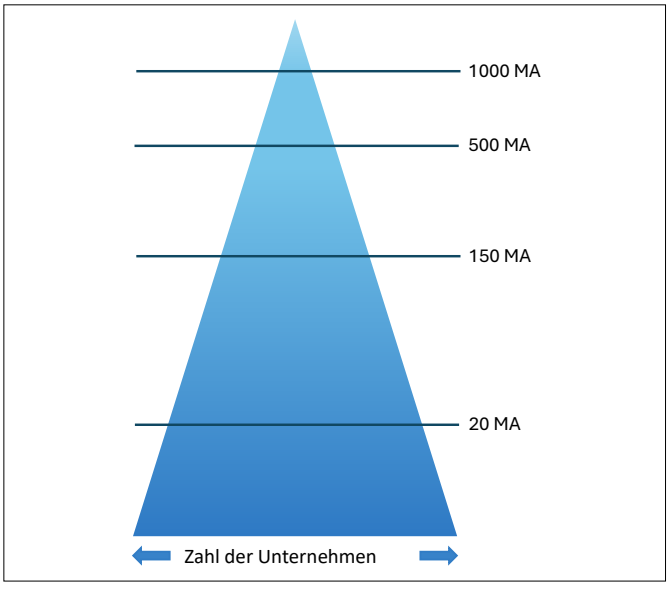


Abbildung 3: Zahl der Unternehmen im Vergleich zur Anzahl der Mitarbeiter – KMU beschäftigen den Großteil der Arbeitnehmerinnen und Arbeitnehmer

Zur Einschätzung der IT-Sicherheitslage einer Organisation hat sich als kostendämpfende Maßnahme eine initiale Bedrohungsanalyse (»Threat Modeling«) bewährt. Diese umfasst die Analyse der eigenen System- und Applikationslandschaft sowie Prozesse und letztendlich deren Verwundbarkeit. Verwendete Komponenten und Datenflüsse werden lokalisiert und mögliche Sicherheitsmängel aufgelistet. Der Use-Case-Katalog hilft, Angriffe zeitnah zu entdecken, wenn die vorher aufgeführten Maßnahmen z. B. aus Gründen mangelnder Erfahrung und/oder Budgets nicht umgesetzt werden können.

Ein weiterer Vorteil dieses Katalogs ist die Transparenz der jeweiligen Use-Cases und die leichte Überprüfbarkeit ihres Umsetzungsgrades. Unterstützt wird dies durch die ergänzenden Empfehlungen zur einheitlichen Dokumentation und zum Berichtswesen. Hierdurch ist es im Rahmen eines Audits sehr einfach aufzuzeigen, welche Use-Cases aus welchem Grund und zu welchem Zweck implementiert wurden und wie wirksam diese sind.

Großunternehmen haben in der Regel bereits entsprechende Erkennungsmaßnahmen implementiert. Allerdings kann hier der Katalog dazu dienen, sich Anregungen zu holen oder die bestehenden Maßnahmen zu überprüfen.

2 Grundlagen zur Erkennung von Angriffsszenarien

Schon 2012 sagte der damalige FBI-Direktor Robert Mueller, dass es nur zwei Arten von Unternehmen gibt: diejenigen, die schon gehackt wurden, und diejenigen, die es noch werden. Und selbst diese verschmelzen zu einer Kategorie: Unternehmen, die gehackt worden sind und wieder gehackt werden. Sicherheitsüberwachung, also »Detektion«, ist somit ein zentrales Thema für Organisationen und stellt den Schwerpunkt dieses Dokuments dar.

Die unvermeidbare Nutzung der Informationstechnik bietet bekanntlich nicht nur Chancen, sondern birgt auch Risiken. Es ist daher notwendig, diese Risiken zu bewerten. In einer entsprechenden Risikoanalyse werden die Eintrittswahrscheinlichkeit oder Eintrittshäufigkeit und der mögliche Schaden bei Eintritt des Risikos beschrieben. Eine Reduzierung des Risikos kann entweder über die Reduzierung der Eintrittswahrscheinlichkeit durch präventive Maßnahmen oder durch präventive oder reaktive Maßnahmen zur Reduzierung des Schadens führen.

Zentrale technische Maßnahmen sind bspw. die Nutzung von Firewallfiltern, Intrusion-Detection-/-Prevention-Systemen und Virenschutz. Auch die Härtung von Systemen wie die Deaktivierung unnötiger Dienste fallen in diese Kategorie.

Die wichtigste reaktive Maßnahme zur Reduzierung des Schadens ist allerdings die möglichst frühzeitige Erkennung der Vorbereitung eines Angriffs, spätestens jedoch des erfolgreichen Angriffs. Erst wenn ein Angriff erkannt wurde, können Gegenmaßnahmen eingeleitet werden, um weitere Versuche zu blockieren, das Ausleiten oder die Verschlüsselung von Daten zu verhindern und kompromittierte Systeme zu separieren, zu bereinigen bzw. wiederherzustellen. Die Notwendigkeit der Angriffserkennung wurde auch vom Gesetzgeber erkannt, bspw. in §8a des BSI-Gesetzes, der NIS-2-Richtlinie oder DORA. Die Umsetzung dieser Anforderungen soll durch dieses Dokument und insbesondere durch die Anwendung des Use-Case-Katalogs unterstützt werden.

In den nachfolgenden Abschnitten wird erläutert, was für eine Sicherheitsüberwachung beachtet werden sollte.

2.1 Protokolle

Alle Betriebssysteme und Sicherheitslösungen sowie die meisten Anwendungen können umfangreiche Protokolle aller Ereignisse erzeugen, die zentral gesammelt werden sollten. Ereignisse sind dabei im weitesten Sinne alles, was Auswirkungen auf die Informationssicherheit haben kann: die Anmeldung eines Benutzers an einem System, der lesende oder schreibende Zugriff auf eine Datei, das Herunterladen von Dateien aus dem Internet, der Start oder Stopp von Programmen und Diensten. Je nachdem, welche Auswertungstiefe benötigt wird, kann praktisch jede Aktion in einem IT-System ein zu protokollierendes Ereignis sein.

Die protokollierten Ereignisse sollten idealerweise in Echtzeit, zumindest jedoch möglichst zeitnah ausgewertet werden. Beispielsweise können mithilfe von Regelwerken oder sogenannten »Indicators of Compromise« (IoC) ungewöhnliches Verhalten von Benutzern oder Systemen, verdächtige Handlungen und Ereignisse identifiziert (Anomalie-Erkennung) und Sicherheitsvorfälle erkannt werden.

Das sehr verbreitete Betriebssystem Windows kann bspw. jede erfolgreiche oder fehlerhafte Anmeldung eines Benutzers protokollieren (siehe Abbildung 4). Alle Ereignisse werden standardmäßig in den Ereignisprotokollen des Betriebssystems gespeichert, die lokal auf dem jeweiligen System mit der Ereignisanzeige geprüft werden können. Dies gilt für eine Office-Umgebung genauso wie für eine mit Windows betriebene Produktionsmaschine.

Fehler beim Anmelden eines Kontos

Antragsteller:
- Sicherheits-ID: SYSTEM
- Kontoname: IMNAIQ$
- Kontodomäne: WORKGROUP
- Anmelde-ID: 0x3E7

Anmeldetyp: 2

Konto, für das die Anmeldung fehlgeschlagen ist:
- Sicherheits-ID: NULL SID
- Kontoname: cgadmin
- Kontodomäne: IMNAIQ

Fehlerinformationen:
- Fehlerursache: Unbekannter Benutzername oder ungültiges Kennwort
- Status: 0xC000006D
- Unterstatus: 0xC000006A

Abbildung 4: Windows Eventlog einer fehlerhaften Anmeldung

Viele Anwendungen, wie z. B. der Apache Webserver, schreiben ihre Protokolle häufig im Textformat in eigene Dateien auf dem lokalen System. Auf einem Linux-System wiederum findet man viele dieser Protokolle im Unterverzeichnis »/var/log«. Insbesondere bei Linux liegen die meisten Protokolle als einfache Textdateien vor, an die sukzessive weitere Einträge angehängt werden.

Die Auswertung der Protokolle kann z. B. durch Skripte direkt auf jedem System erfolgen. Allerdings wird dann für jedes System und jede Anwendung eine eigene Auswertungslogik benötigt. Es ist daher oft sinnvoller, die Protokolle auf speziell dafür eingerichteten zentralen Servern abzulegen. Diese werden meist als zentrale »Logserver« oder »Protokollserver« bezeichnet. Viele Systeme bzw. Geräte, wie Firewalls, Router und Switches, können Protokolle z. B. im Syslog-Format oft direkt an ein zentrales System senden. Diese Server müssen wiederum besonders geschützt werden. Alternativ kann auch ein Cloud-basiertes System oder der Service eines Dienstleisters genutzt werden.

2.2 Zentralisierung und Normalisierung

Sicherheitsvorfälle können oft nicht durch einen einzelnen Protokolleintrag erkannt werden. In vielen Fällen müssen Protokolle von verschiedenen Systemen korreliert, d. h. miteinander in Verbindung gebracht werden. Dies soll mit folgenden Beispielen verdeutlicht werden:

- Wird von einem Virenscanner eine Schadsoftware erkannt und protokolliert, kann es sich direkt um einen möglichen Sicherheitsvorfall handeln.
- Die erfolgreiche Anmeldung eines Benutzers an einem Windows-System hingegen dürfte in den meisten Fällen keinen Sicherheitsvorfall darstellen. Meldet sich ein Benutzer jedoch in der Nacht oder innerhalb weniger Minuten an vielen verschiedenen Systemen oder von verschiedenen Standorten an, könnte ein Sicherheitsvorfall vorliegen, wenn ein Angreifer mit abgefangenen Zugangsdaten die Systeme ausforscht.

Damit Protokolldaten für die Angriffserkennung in Analysen und Prüfregeln sinnvoll verwendet werden können, müssen sie bestimmte Anforderungen erfüllen. Daraus ergeben sich mehrere Empfehlungen:

1. **Zentralisierung:**
   Die Protokolle der verschiedenen Systeme müssen auf einem zentralen System zusammengeführt und in ein einheitliches Format umgewandelt werden (Parsen und Normalisieren), damit die Informationen aus diesen Protokollen zueinander in Verbindung gesetzt werden können.
2. **Synchronität:**
   Um Protokolldaten systemübergreifend und in der richtigen zeitlichen Reihenfolge korrelieren zu können, müssen die Uhren auf allen Systemen auf eine einheitliche Zeit synchronisiert werden (zeitliche Konsistenz). Üblicherweise kommt dafür ein Zeitsynchronisationsprotokoll wie NTP (Network Time Protocol) oder PTP (Precision Time Protocol) zum Einsatz.
3. **Mindestinhalt:**
   Alle zur Erkennung relevanten Informationen sollten protokolliert werden (Vollständigkeit). Dazu gehören das Ereignis selbst, Datum und genaue Uhrzeit, Quell- und Ziel-IP-Adressen (wenn möglich auch die Hostnamen) sowie Kommunikationsdienste der beteiligten Systeme, verwendete und betroffene Benutzerkonten sowie ggf. weitere Informationen wie z. B. Dateinamen, auf die zugegriffen wurde.
4. **Integrität:**
   Die Protokolle müssen vor einer unberechtigten Veränderung geschützt werden. Dies berücksichtigt sowohl die Übertragung zum zentralen Protokollserver als auch der dort abgelegten Protokolle, damit sie nicht manipuliert oder gelöscht werden können[1]. Häufig wird deshalb ein separierter, dedizierter Protokollserver mit eigener Authentifizierung genutzt, um kritische Protokolle auch bei einem Sicherheitsvorfall möglichst effektiv zu schützen.

Mittlerweile handelt es sich bei dem zentralen Protokollserver zunehmend um eine integrierte Sicherheitslösung wie ein Security Information and Event Management System (sog. »SIEM-System«). Bei der Planung derartiger Systeme muss insbesondere beachtet werden, welche Leistungsdaten und welches Lizenzmodell die jeweiligen Hersteller anbieten. Manche Hersteller lizenzieren nach Anzahl der verarbeiteten Ereignisse pro Sekunde oder der verarbeiteten Datenmenge in Gigabytes (GB), wobei über die lizenzierte Anzahl oder Datenmenge hinausgehende Ereignisse ggf. verworfen werden. Dies führt dann dazu, dass Angriffe nicht mehr erkannt werden können. Andere Hersteller wiederum lizenzieren nach der Gesamtmenge gespeicherter Daten, was dazu führen kann, dass eventuell für eine forensische Analyse benötigte Daten nicht mehr vorliegen, da sie inzwischen aus Kostengründen gelöscht wurden.

Wenn Systeme und Anwendungen die Weiterleitung von Protokollen zu einem zentralen System nicht von sich aus unterstützen, ist es oft notwendig, Agenten auf den verschiedenen Quellsystemen zu installieren. Diese Agenten können die Protokolle z. B. aus Textdateien auslesen und an den zentralen Protokollserver weiterleiten.

Um Protokolle zu korrelieren, d. h. Ereignisse zueinander in Verbindung setzen zu können, müssen die enthaltenen Informationen in einem auswertbaren Format vorliegen. Es ist daher notwendig, dass entweder auf dem zentralen Proto-

1 Sowohl »Data-in-Transit« als auch »Data-at-Rest«.

kollserver oder bereits beim Einlesen von Protokollen durch die Agenten die verschiedenen Protokolleinträge durch einen Parser analysiert werden, um die notwendigen Informationen des jeweiligen Systems zu extrahieren und in ein einheitliches internes Format zu übertragen. Ein herstellerübergreifendes Format zur Erstellung oder internen Verarbeitung von Protokolldateieinträgen, mit dem idealerweise alle Systeme kompatibel wären, existiert trotz verschiedener Versuche zur Standardisierung bisher noch nicht.

2.3 Auswertung und Aktualisierung

Wenn eine Sicherheitslösung die gemäß dem vorigen Abschnitt aufbereiteten Protokollinformationen auswertet, können konkrete Sicherheitsvorfälle und Angriffe erkannt werden. In der Praxis kann es jedoch schwierig sein zu entscheiden, welche Ereignisse wichtig sind. Insbesondere auch, da sich IT/OT-Infrastrukturen und die Anwendungslandschaft einer Organisation im Laufe der Zeit ändern. Gleichzeitig entwickeln Angreifer neue Angriffsmethoden, die sogenannten »Tactics, Techniques and Procedures« (TTPs) [MITRE 2025a], und neue Systeme und Anwendungen ermöglichen neue Angriffsvektoren. Daher sind die Use-Cases inklusive der Prüfregeln kontinuierlich anzupassen (Regeloptimierung). Dies gilt auch für die Entscheidungskriterien der Validierung.

Eine erfolgreiche und wirksame Angriffserkennung sollte deshalb mehrere Faktoren berücksichtigen:

1. Jede Organisation muss für die eigenen Systeme, Anwendungen und Daten identifizieren, welche Angriffe zu erwarten sind und wie diese durch geeignete Use-Cases erkannt werden können.
2. Für die jeweiligen Use-Cases muss identifiziert werden, welche Protokolle und Ereignisse für die Erkennung notwendig sind, von welchen Systemen diese erzeugt werden und wie diese von der Sicherheitslösung verarbeitet werden können.
3. Außerdem sollten IoCs, die in konkreten Use-Cases zur Erkennung genutzt werden, regelmäßig auf ihre Aktualität geprüft werden, bspw. mithilfe von Bedrohungsaufklärung (»Threat Intelligence«).

Nur wenn die Organisation aktuelle Bedrohungen ihrer Systemlandschaft (Infrastruktur, Software, IT, OT etc.) durch geeignete Use-Cases zeitnah erkennen kann, reduziert sich das Risiko erfolgreicher Angriffe.

Während einfache Angriffe wie ein SQL-Injection-Befehl im Protokoll des Datenbankservers noch mit einfacher Mustererkennung oder regulären Ausdrücken gefunden werden können, kommen auf modernen Sicherheitssystemen zur Erkennung eines von der Norm abweichenden Verhaltens Verfahren des maschinellen Lernens (»Machine Learning«) und komplexe Heuristiken zum Einsatz. Dadurch können Angriffe nicht nur aufgrund von festen Angriffssignaturen, sondern auch durch ein plötzlich anderes Verhalten identifiziert werden.

Threat-Intelligence-Feeds, die entweder direkt vom Hersteller einer verwendeten Sicherheitslösung wie SIEM oder von Drittanbietern abonniert werden, helfen, neue Angriffsmuster und Methoden schnell zu identifizieren.

2.4 Forensische Analyse

Neben der Erkennung eines gerade aktiv ablaufenden Angriffs helfen gespeicherte Protokolle auch bei der forensischen Analyse und der Nachbereitung des Vorfalls. Beispielsweise kann mithilfe der vorhandenen Protokolle geprüft werden, auf welche Daten der Angreifer tatsächlich Zugriff hatte, um den Schaden abzuschätzen oder um festzustellen, ob bei Zugriff auf bzw. Abfluss von Daten eine Meldepflicht eingehalten werden muss. Außerdem helfen Protokolle auch bei der Nachverfolgung der Angriffswege und somit beim Schließen von den ausgenutzten Sicherheitslücken wie auch abschließend bei einer strafrechtlichen Verfolgung der Täter.

Die wichtigste Aufgabe in der forensischen Analyse ist jedoch, die Ursache für den erfolgreichen Angriff und die folgende Kompromittierung zu identifizieren. Wenn diese Ursache nicht beseitigt wird, bevor wiederhergestellte Systeme wieder verfügbar gemacht werden, besteht das große Risiko, dass die Angreifer über denselben, bereits bekannten Weg, erneut in die Systeme eindringen können.

Die Nachbereitung umfasst neben der Regeloptimierung (siehe Abbildung 1) möglicherweise auch die Frage, ob – im Sinne einer kontinuierlichen Verbesserung – Angriffe auf das Fehlen relevanter Use-Cases hindeuten. Sie können Anlass geben, die Vollständigkeit der bestehenden Sammlung zu überprüfen, um ggf. neue Use-Cases zu entwickeln. Dies trägt dazu bei, die Abwehrmechanismen zu stärken und das System gegenüber zukünftigen Angriffen besser abzusichern.

3 Use-Case-Katalog

In diesem Kapitel wird der von der Fachgruppe Cyber Security mit seinen Bestandteilen entwickelte Use-Case-Katalog im Detail vorgestellt. Dazu gehören die folgenden Aspekte, die in den angegebenen Abschnitten näher ausgeführt werden:

- Darlegung der Designprinzipien (3.1)
- Konzept der Auswertungsniveaus (3.2)
- IT-Landschaftskonzept (3.3)
- Übersichten zur Abdeckung (3.4)
- Liste der abstrakten Ereignisdefinitionen (3.5)
- Hinweise zur Umsetzung (3.6)
- Beispiele für die Umsetzung (3.7)
- Einführung wesentlicher Begriffe und der verwendeten abstrakten Sprache für die Beschreibung der fachlichen Regeln und der Nomenklatur (3.8)
- Liste der Use-Cases (UC), inklusive Details (3.9)

3.1 Designprinzipien

Bei der Erstellung dieses Use-Case-Katalogs wurde eine Vielzahl von **Designprinzipien** zugrunde gelegt, damit dieser Katalog bei einer breiten Masse von Organisationen Anwendung finden kann. Diese sollen Folgendes sicherstellen:

- Der Use-Case-Katalog ist für Organisationen aller Größenklassen geeignet.
- Der Use-Case-Katalog unterstützt ein strukturiertes Vorgehen zur Umsetzung.
- Die Use-Cases sind »grundsätzlich« in dem Sinne, dass sie sowohl bereits seit langer Zeit üblich sind als auch voraussichtlich künftig relevant bleiben.
- Der Use-Case-Katalog deckt möglichst den gesamten Ablauf eines Angriffs ab.
- Der Use-Case-Katalog soll eine breite, grundlegende Basisabsicherung bieten.
- Die Abbildung auf andere Rahmenwerke und Vorgaben wird unterstützt.
- Die Use-Cases sind nicht auf ein bestimmtes Überwachungswerkzeug oder für bestimmte Systemarten bzw. Assetklassen eingeschränkt.
- Die Beschreibung der einzelnen Use-Cases orientiert sich an einem einheitlichen Template. Dieses wird sowohl für ihre Beschreibung im Rahmen des Use-Case-Katalogs verwendet als auch – mit Ergänzungen – für die organisationsspezifische Dokumentation empfohlen, die Gegenstand von Abschnitt 3.10 ist.

Die einheitliche **Umsetzung** dieser zuvor genannten Designprinzipien wird durch das folgende Vorgehen sichergestellt:

- Für jede Taktik (»Tactic«) der ATT&CK Enterprise-Matrix wird mindestens eine Technik (»Technique«) durch einen Use-Case abgedeckt.
- Für jeden Use-Case werden Referenzen zu ATT&CK Tactics und Techniques sowie zu Bausteinen des BSI IT-Grundschutz-Kompendiums 2023 angegeben.
- Es wurde ein IT-Landschaftskonzept entwickelt, das die typischen IT-Systeme von Unternehmen als Orientierungshilfe darlegt. Diese werden in den Use-Cases berücksichtigt (Abschnitt 3.3).
- Die Use-Cases wurden in verschiedene Auswertungsniveaus (AN) eingeteilt, anhand derer ein strukturiertes Vorgehen zur Umsetzung und Erreichung des gewünschten Schutzniveaus ermöglicht wird (Abschnitt 3.2).
- Es werden konkrete Regelwerke und Implementierungshilfen zur Verfügung gestellt, die aufgrund der abstrakten Beschreibungssprache einen leichten Einstieg bieten, und auf unterschiedliche Weise und ohne die Notwendigkeit komplexer oder dedizierter Überwachungssysteme umsetzbar sind.
- Es werden Hilfestellungen zu typischen Ergebnissen wie »Falsch-Positiv-Meldungen« (»False Positives«) und deren Ursachen gegeben.
- Kritikalitäts-, Dringlichkeits- und Reaktionsanforderungen wurden beim Design und der Auswahl der Use-Cases berücksichtigt, sodass bspw. grundsätzlich ähnliche Use-Cases, die sich aber bzgl. dieser Kriterien unterscheiden, separat behandelt werden[1].
- Für jeden Use-Case sind die adressierten Risiken und die Detektionsziele angegeben, was eine Verknüpfung mit Risikomanagementprozessen erleichtert.
- Autoren und Reviewer mit langjähriger Praxiserfahrung in unterschiedlichen Arbeitsfeldern wirkten am Use-Case-Katalog mit. Dazu gehören Prüfer (Auditoren), Berater (Consultants), SOC-Analysten, SIEM-Experten und Experten aus Feldern wie bspw. dem Penetration-Testing.

[1] Beispielsweise ist es beim Portscanning ein Unterschied, ob dies von außerhalb oder innerhalb des eigenen Netzwerks erfolgt.

3.2 Auswertungsniveaus

Eine Liste von Use-Cases (UCs) zur Verfügung zu stellen, ist hilfreich, jedoch ergeben sich schnell Fragen:

- Mit welchen UCs soll angefangen werden?
- Wie viele und welche UCs sind erforderlich, um das gewünschte Schutzniveau für die Organisation zu erreichen?

Um dies zu unterstützen, wurden vier »Auswertungsniveaus« (ANs) entwickelt und festgelegt. Diese beginnen bei AN1 (niedrigstes Niveau) und enden bei AN4 (höchstes Niveau). Dabei enthält jedes Auswertungsniveau die Use-Cases des vorigen, AN2 enthält also neben den eigenen UCs zusätzlich die von AN1, AN3 neben den eigenen UCs zusätzlich die von AN2 und AN1.

Die Auswertungsniveaus gruppieren die UCs und ermöglichen so ein planerisches schrittweises Vorgehen. Kategorisiert und zugeordnet sind sie wie nachfolgend aufgeführt:

- **Auswertungsniveau 1 (AN1):** Elementare Use-Cases. Es werden nur wenige organisationsspezifische Informationen für die Umsetzung benötigt.
- **Auswertungsniveau 2 (AN2):** Erste Informationen zu Netzwerk und Benutzerkontenstrukturen (z. B. Namenskonvention) sowie Sicherheitslösungen werden benötigt.
- **Auswertungsniveau 3 (AN3):** Detaillierte Informationen zu Netzwerk und Benutzerkontenstrukturen (z. B. Namenskonvention) sowie Sicherheitslösungen werden benötigt. Aktuelle Bedrohungsinformationen sind teils erforderlich und die Umsetzung mit einfachen Bordmitteln und ohne spezialisierte Systeme wird komplex.
- **Auswertungsniveau 4 (AN4):** Detaillierte Informationen zu sensiblen und zu schützenden Daten inklusive Zugriffswegen sowie untypischen Arbeitsabläufen werden benötigt. Die Umsetzung ist oftmals herausfordernd.

Die Auswertungsniveaus sollten in aufsteigender Reihenfolge umgesetzt werden, d. h. beginnend mit AN1, danach AN2, dann AN3 und nachfolgend AN4. Dabei ist das gewünschte Zielniveau von der Organisation festzulegen.

Es sollten zudem zunächst alle Use-Cases eines Auswertungsniveaus umgesetzt werden, bevor mit der Implementierung von Use-Cases aus höheren Auswertungsniveaus begonnen wird, da sich diese ergänzen und aufeinander aufbauen.

Teilweise können die Ziele von Use-Cases höherer Auswertungsniveaus durch ein geeignetes Design der Systemlandschaft und der Prozesse erreicht werden. So könnte für eine exemplarische Organisation die Überwachung des Datenzugriffs auf sensible Mitarbeiterdaten mittels des Use-Case B41 (siehe Abschnitt 3.9.41 »B41 – Unzulässiger Zugriff auf sensible Daten«) durchgeführt werden, was sich aber in der Umsetzung für die durchführende Organisation als zu schwierig herausstellt. Alternativ könnte sie die entsprechenden Daten in einem separaten und besonders geschützten System unterbringen, den Zugriff beschränken und diesen gezielt bzgl. der zugelassenen Benutzerkonten und Datenverbindungen überwachen. Stellt sich dies als einfacher heraus, so kann das Risiko möglicherweise auf ein dem Risikoappetit der Organisation entsprechendes Niveau gesenkt werden.

Es ist jedoch stets sinnvoll für eine Organisation zu prüfen, ob einzelne Use-Cases aus den höheren Auswertungsniveaus eine hilfreiche Ergänzung darstellen. Beispielsweise könnten aufgrund von Gesetzen oder aufsichtsrechtlichen Anforderungen eine bestimmte Überwachung erforderlich sein, ein Organisationsrisiko reduziert oder bereits vorhandene Sicherheitssysteme besser genutzt werden.

Auch der umgekehrte Fall kann eintreten: Es ist nicht immer erforderlich, alle in diesem Katalog vorgestellten Use-Cases in der Organisation für jede Assetklasse, also unterschiedliche Arten von Systemen bzw. Software[2], umzusetzen. Vielmehr ist der Katalog als ein Angebot zu betrachten, das bewährte und effektive Use-Cases aufzeigt und beschreibt. Inwieweit ein Use-Case in einer bestimmten Organisation die Erkennung eines Angriffs auf eine Assetklasse verbessern kann, müssen die Verantwortlichen der Organisation bewerten und entscheiden. Dies erfolgt sinnvollerweise über eine Risikoerhebung und -analyse der potenziellen Gefahren, denen ein Asset, also die Instanzen einer Assetklasse, ausgesetzt ist (siehe auch Kapitel 4) sowie durch eine Messung der Effektivität der Maßnahmen. Anhand des daraus abgeleiteten Risikokatalogs kann geprüft werden, welche Use-Cases geeignet sind, um die für ein Asset identifizierten Risiken zu mindern. Dies können sowohl aus diesem Use-Case-Katalog verwendete und auf die Organisation abgestimmte als auch selbst entwickelte Use-Cases sein.

Die folgende Übersicht in Tabelle 1 zeigt die Zuordnung der Use-Cases zu den entsprechenden Auswertungsniveaus.

2 Beispiele für Assetklassen sind Betriebssysteme, Firewalls, Proxy-Systeme, Webserver, Produktionsmaschinen oder Anwendungen. Eine einheitliche Definition von Assetklassen gibt es nicht. Sie werden daher typischerweise je Unternehmen und Kontext festgelegt.

Use-Case	AN1	AN2	AN3	AN4
B01	X	-	-	-
B02	X	-	-	-
B03	X	-	-	-
B04	X	-	-	-
B05	X	-	-	-
B06	X	-	-	-
B07	X	-	-	-
B08	X	-	-	-
B09	X	-	-	-
B10	-	X	-	-
B11	-	X	-	-
B12	-	X	-	-
B13	-	X	-	-
B14	-	X	-	-
B15	-	X	-	-
B16	-	X	-	-
B17	-	X	-	-
B18	-	X	-	-
B19	-	X	-	-
B20	-	X	-	-
B21	-	X	-	-
B22	-	X	-	-
B23	-	X	-	-
B24	-	X	-	-
B25	-	X	-	-
B26	-	-	X	-
B27	-	-	X	-
B28	-	-	X	-
B29	-	-	X	-
B30	-	-	X	-
B31	-	-	X	-
B32	-	-	X	-
B33	-	-	X	-
B34	-	-	X	-
B35	-	-	X	-
B36	-	-	X	-
B37	-	-	X	-
B38	-	-	X	-
B39	-	-	X	-
B40	-	-	-	X
B41	-	-	-	X
B42	-	-	-	X

Tabelle 1: Use-Case-Zuordnung je Auswertungsniveau

3.3 IT-Landschaftskonzept

Mit der Größe einer Organisation wächst und diversifiziert sich typischerweise auch die IT-Landschaft. Es kommen mehr Assetklassen und Assets hinzu.

Tabelle 2 bietet einen Überblick über das im Use-Case-Katalog als Orientierungshilfe aufgestellte und auf Praxiserfahrung basierende IT-Landschaftskonzept und enthält die nachfolgend beschriebenen Spalten:

- **Landschaft-ID:** Die Klassifizierung erfolgt in fünf aufeinander aufbauenden Kategorien von L01 (klein) bis L05 (sehr groß).
- **Assetklasse:** Die aufgeführten verbreiteten Assetklassen dienen als nicht abschließende Beispiele, die typischerweise in der jeweiligen Landschaftskategorie anzutreffen sind. Dabei ist es unerheblich, ob diese selbst oder von Dritten verwaltet werden oder ob sie lokal eingerichtet oder Cloud-basiert sind.
- **Größe:** Die Größe gibt die typische Anzahl der Mitarbeiter einer Organisation der jeweiligen Landschaftskategorie an.
- **Auswertungsniveau:** Das Auswertungsniveau gibt das empfohlene minimale Auswertungsniveau bzw. die Kategorie der dafür empfohlenen Use-Cases an.

Tabelle 2 zeigt die fünf Landschaftsgrößen, wobei jede größere Landschaft die Assetklassen der vorigen Landschaften beinhaltet: So enthält bspw. L02 alle Assetklassen aus L01 plus zusätzliche, L03 die von L02 und L01 plus zusätzliche Assetklassen.

Die Assetklassen und ihre Verteilung selbst können je Organisation variieren. Auch sind die aufgeführten Assetklassen exemplarisch und keineswegs abschließend zu verstehen. So werden bspw. häufig zusätzlich Apple-Clients zusammen mit Windows-Clients eingesetzt. Auch kommt es vor, dass ein kleines Unternehmen mit 15 Mitarbeitern Linux-, AIX- oder IBM i-Server statt Windows-Servern einsetzt, oder dass ein größeres Unternehmen mit 200 Angestellten keine Webserver verwendet. Tabelle 2 erfüllt in diesem Kontext mehrere Funktionen:

- Sie dient als Basis für die Verifikation, dass eine sinnvolle und breite Abdeckung wesentlicher Assetklassen in Organisationen durch die Use-Cases gewährleistet ist.
- Gleichsam soll sie Organisationen eine Orientierungshilfe geben, welches Auswertungsniveau abhängig von der Unternehmensgröße als Minimum angestrebt werden sollte. Abweichungen sind, wie bei den Ausführungen zu den Auswertungsniveaus oben angegeben, immer möglich. Insbesondere bei der Umsetzung eines geringeren Auswertungsniveaus – bspw., wenn ein Unternehmen mit 2.000 Angestellten nur Auswertungsniveau 1 (AN1) statt

Landschaft-ID	Assetklassen (exemplarisch)	Größe bzgl. Mitarbeiter	Auswertungsniveau Empfehlung Minimum
L01	-	bis 20	1
	Windows-Clients		
	Windows-Server		
	Anti-Virus		
	Internet-Router		
	Mailserver		
	Anwendungen		
L02	*L01*	21 bis 150	2
	WebProxy		
	Firewall, basic (bis Layer 3)		
	Non-Windows-Server		
	Webserver		
	Active Directory / LDAP		
	WLAN-Router		
	NTP-Programm / - Server		
	Dienstleister/Cloud-Übergang		
	Remote-Zugang/VPN		
	eigener DNS-Service		
	Netzwerkdrucker		
	Datenbanken		
	Virtualisierung		
	Zentrale Laufwerke (Shares / Fileserver)		
	Weitere Middleware		
L03	*L02*	151 bis 500	2
	FW, advanced (NG und WAF, bis L7)		
	VoIP / Softwarebasierte Telefonanlage		
	Zentrales Logmanagement		
	Sicherheitslösung zur Auswertung wie SIEM		
	Bring Your Own Device		
L04	*L03*	501 bis 1000	3
	PAM-Server		
	Reverse-Proxy		
	NAC		
	IDS/IPS		
	Mobile Device Management (MDM)		
L05	*L04*	ab 1001	3
	PAM-Architektur		
	DLP		

Tabelle 2: IT-Landschaft

Auswertungsniveau 3 (AN3) umsetzt – sollten Abweichungen bewusst entschieden und die Risiken bewertet, begründet und dokumentiert werden.

- Sicherheitsrelevante Infrastruktur wie Antivirus oder Firewalls stellt einen großen Teil der aufgeführten Assetklassen dar. Idealerweise hätte jede Organisation möglichst viele Sicherheitsinfrastrukturen im Einsatz, doch ist dies gerade für sehr kleine Unternehmen in Anbetracht der verfügbaren Ressourcen nicht realistisch. Insofern sollen die oben angegebenen Assetklassen dabei helfen, einzuschätzen, ab wann spätestens der Einsatz der aufgeführten Sicherheitsinfrastrukturen geprüft werden sollte.

Im Lauf der Zeit verändern sich die verwendeten Assetklassen aufgrund technologischer Entwicklungen. Insbesondere durch die zunehmende Verbreitung Cloud-basierter Lösungen werden leistungsfähigere Sicherheitsinfrastrukturen mehr und mehr kleineren Organisationen zur Verfügung stehen. Die jeweiligen Cloud-Anbieter werden für ihren Kundenstamm und ihre Dienstleistungen die entsprechenden Überwachungsfunktionen selbst übernehmen müssen. Dass dies tatsächlich erfolgt, ist jedoch nicht garantiert und sollte daher in die Risikobetrachtung der Dienstleister aufgenommen werden.

3.4 Übersichten zur Abdeckung

Die folgenden Tabellen 3 bis 6 geben einen Überblick über die Use-Cases, die in Abschnitt 3.9 aufgeführt werden. Sie sollen sowohl Unternehmen und Institutionen als auch Prüfern Aufschluss geben über

- die Abdeckung der ATT&CK Tactics durch die Use-Cases,
- welche und wie viele Techniques durch welche Use-Cases wie umgesetzt werden sowie
- das minimale Auswertungsniveau, das für die Adressierung einer bestimmten Tactic-Technique-Kombination erforderlich ist.

Im Zusammenspiel wird so die Prüfung, ob gesetzliche und regulatorische Vorgaben eingehalten sind, erleichtert. Zudem kann eine Organisation effektiv und schnell verifizieren, ob bestimmte Bedrohungen bereits grundsätzlich abgedeckt sind oder ob Handlungsbedarf besteht.

Tactic	Zahl der Use-Cases
Reconnaissance	6
Resource Development	1
Initial Access	13
Execution	4
Persistence	8
Privilege Escalation	10
Defense Evasion	17
Credential Access	7
Discovery	9
Lateral Movement	2
Collection	4
Command and Control	4
Exfiltration	4
Impact	5

Tabelle 3: Zahl der Use-Cases je Tactic

Use-Case	Zahl der Techniques	Use-Case	Zahl der Techniques
B01	1	B22	2
B02	1	B23	2
B03	1	B24	4
B04	1	B25	2
B05	3	B26	1
B06	1	B27	2
B07	1	B28	1
B08	2	B29	2
B09	2	B30	1
B10	1	B31	16
B11	2	B32	21
B12	4	B33	11
B13	1	B34	2
B14	2	B35	6
B15	2	B36	2
B16	2	B37	7
B17	2	B38	5
B18	1	B39	15
B19	3	B40	3
B20	3	B41	3
B21	2	B42	3

Tabelle 4: Zahl der zugeordneten Techniques je Use-Case

Use-Case	Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
B01	-	-	-	-	-	-	X	-	-	-	-	-	-	-
B02	-	-	-	-	-	-	X	-	-	-	-	-	-	-
B03	-	-	-	-	-	-	X	-	-	-	-	-	-	-
B04	-	-	-	-	-	-	X	-	-	-	-	-	-	-
B05	-	-	-	-	X	X	X	-	-	-	-	-	-	-
B06	-	-	-	-	-	-	X	-	-	-	-	-	-	-
B07	-	-	X	-	-	-	X	-	-	-	-	-	-	-
B08	-	-	-	-	-	-	-	X	X	-	-	-	-	-
B09	-	-	-	-	-	-	-	X	X	-	-	-	-	-
B10	X	-	-	-	-	-	-	-	-	-	-	-	-	-
B11	-	-	-	-	-	-	X	-	-	-	-	-	-	-
B12	-	-	-	X	X	X	X	-	-	-	-	-	-	X
B13	X	X	X	X	X	X	X	X	X	X	X	X	X	X
B14	X	-	-	-	-	-	-	-	-	-	-	-	-	-
B15	X	-	-	-	-	-	-	-	-	-	-	-	-	-
B16	X	-	-	-	-	-	-	-	-	-	-	-	-	-
B17	X	-	-	-	-	-	-	-	-	-	-	-	-	-
B18	-	-	-	-	-	-	X	-	-	-	-	-	-	-
B19	-	-	-	-	-	-	-	X	X	-	-	-	-	X
B20	-	-	X	-	X	X	X	-	-	-	-	-	-	-
B21	-	-	-	-	-	-	-	X	X	-	-	-	-	-
B22	-	-	X	-	X	X	X	X	-	-	-	-	-	-
B23	-	-	X	-	X	X	X	-	-	-	-	-	-	-
B24	-	-	X	-	X	X	-	-	-	-	-	-	-	X
B25	-	-	-	-	-	X	-	-	-	-	-	-	-	-
B26	-	-	-	-	-	-	X	-	-	-	-	-	-	-
B27	-	-	-	-	-	X	-	-	-	-	-	-	-	-
B28	-	-	X	-	-	X	-	-	-	-	-	-	-	-
B29	-	-	-	-	-	-	-	X	X	-	-	-	-	-
B30	-	-	X	-	X	-	-	-	-	-	-	-	-	-
B31	-	-	-	-	-	-	X	-	X	-	-	-	-	X
B32	-	-	-	-	-	-	-	-	-	-	-	X	X	-
B33	-	-	-	-	-	-	-	-	X	X	X	-	-	-
B34	-	-	X	-	-	-	X	-	-	-	-	-	-	-
B35	-	-	X	X	-	-	-	-	-	-	-	-	-	-
B36	-	-	X	X	-	-	-	-	-	-	-	-	-	-
B37	-	-	-	-	-	-	-	-	-	-	-	-	X	-
B38	-	-	X	-	-	-	-	-	-	-	-	X	-	-
B39	-	-	-	-	-	-	-	-	-	-	-	X	X	-
B40	-	-	-	-	-	-	-	-	X	-	-	-	-	-
B41	-	-	-	-	-	-	-	-	-	-	X	-	-	-
B42	-	-	-	-	-	-	-	-	-	-	X	-	-	-

Tabelle 5: Use-Case-Zuordnung je Tactic

Tabelle 6 zur Abdeckung der Techniques durch Use-Cases enthält folgende Angaben:

- **– :** Nicht abgedeckt
- **G:** Generelle Abdeckung, d.h., der Use-Case adressiert die Bedrohung allgemein oder indirekt, geht aber nicht direkt bzw. dediziert auf sie ein.
- **D:** Dedizierte Abdeckung, d.h., der Use-Case adressiert die Bedrohung direkt.
- **x:** Genaue Art der Abdeckung kann nicht spezifiziert werden.

Der Unterschied zwischen genereller und dedizierter Abdeckung kann an einem Beispiel verdeutlicht werden: Wird der Datenfluss aus der Organisation in externe Netze überwacht und wird bei verdächtigen Datenmengen, Zeiten oder Zielen gewarnt, so ist es unerheblich, ob dies ein »Exfiltration Over Alternative Protocol« (ATT&CK T1048) oder ein »Exfiltration Over C2 Channel« (ATT&CK T1041) ist – es fällt auf und ist somit generell abgedeckt. Eine dedizierte Abdeckung würde genau den Abfluss über alternative Protokolle (ATT&CK T1048) oder C2-Kanäle (ATT&CK T1041) erkennen.

Eine generelle Abdeckung ist also für die Zielsetzung nicht schlechter als eine dedizierte, sondern lediglich anders. Für bestimmte Szenarien oder Randfälle kann dies einen Unterschied machen, daher wurde die entsprechende Kennzeichnung vorgenommen.

(Sub-) Technique	B01	B02	B03	B04	B05	B06	B07	B08	B09	B10	B11	B12	B13	B14	B15	B16	B17	B18	B19	B20	B21	B22	B23	B24	B25	B26	B27	B28	B29	B30	B31	B32	B33	B34	B35	B36	B37	B38	B39	B40	B41	B42
T1001	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-
T1005	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	D
T1007	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-	-
T1008	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	G	-	-	-
T1011	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	G	-	-	-	-	-
T1018	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	D	-	-	-	-	-	-	G	-	-
T1020	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	D	-	-	-	-	G	-	G	-	-	-
T1021	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-
T1025	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	D
T1029	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	D	-	-	-	-	G	-	G	-	-	-
T1030	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	D	-	-	-	-	-	-	G	-	-	-
T1033	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-	-
T1039	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	D
T1041	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	D	-	-	-	-	G	-	G	-	-	-
T1046	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	D	-	-	-	-	-	-	G	-	-
T1048	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	D	-	-	-	-	G	-	G	-	-	-
T1049	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-	-
T1053	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
T1057	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-	-
T1059	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-
T1068	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
T1070	D	G	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
T1071	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	G	-	-	-
T1072	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	G	-	-	-	-	-	-
T1074.002	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-
T1078	-	-	-	-	-	-	D	-	-	-	-	-	-	-	-	-	-	-	-	D	-	D	G	G	G	-	-	G	-	D	-	-	-	-	-	-	-	G	-	-	-	-
T1080	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-
T1082	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-	-
T1087	-	-	-	-	-	-	-	G	G	-	-	-	-	-	-	-	-	-	G	G	G	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-	-	-	-
T1090	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-
T1095	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	G	-	-	-
T1098	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	D	G	D	-	D	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
T1102	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-
T1104	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-
T1105	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-
T1110	-	-	-	-	-	-	-	D	D	-	-	-	-	-	-	-	-	-	D	D	G	G	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-	-	-	-
T1124	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-	-
T1132	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-
T1133	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	D	-	-	-	-
T1135	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	D	-	-	-	-	-	-	G	-	-
T1136	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	D	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
T1189	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-
T1190	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	D	-	-	-	-
T1200	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	D	-	-	-	-	-	-	-	-	-
T1203	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-
T1204	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	G	-	-	-	-	-	-
T1210	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-
T1219	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-
T1485	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-	-
T1486	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-	-
T1489	-	-	-	-	-	-	-	-	-	-	-	D	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-	-
T1490	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-	-
T1495	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-	-
T1526	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-
T1529	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-	-
T1531	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	D	-	-	-	-	D	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-	-
T1537	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-
T1543	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
T1547	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
T1548	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-	-
T1553	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
T1561	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-	-
T1562	-	-	D	D	D	D	-	-	-	G	G	-	-	-	-	-	-	G	-	-	-	-	-	-	-	D	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
T1565	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-	-
T1567	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	G	-	G	-	-	-
T1568	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	G	-	-	-
T1569	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
T1570	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	D	-	-	-	-	-	-	-	-	-
T1571	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	G	-	-	-
T1572	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	G	-	-	-
T1573	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	G	-	-	-
T1578.002	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	D	-	-	-	-	-	-	-	-	-
T1580	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-	-
T1590	-	-	-	-	-	-	-	-	-	-	-	-	-	G	G	G	G	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
T1595	-	-	-	-	-	-	-	-	-	-	-	-	-	D	D	D	D	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
T1619	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	-	-
T1659	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	G	G	-	-	-
T1665	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	-	-	-	-	-	-	-	G	-	-	-
Txxxx	-	-	-	-	-	-	-	-	-	-	-	-	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Tabelle 6: Abdeckung Techniques durch Use-Cases

Die folgenden Abbildungen 5 bis 9 sind Screenshots des ATT&CK Navigators [MITRE 2024] der Abdeckung hinsichtlich der Tactics und der Techniques durch die Use-Cases je Auswertungsniveau: Weiße Techniques sind nicht abgedeckt, das hellste Grün ist AN1, das dunkelste AN4. Sind Use-Cases unterschiedlicher Auswertungsniveaus der gleichen Tactic und Technique zugeordnet, so wird das geringste Auswertungsniveau angezeigt[4,5].

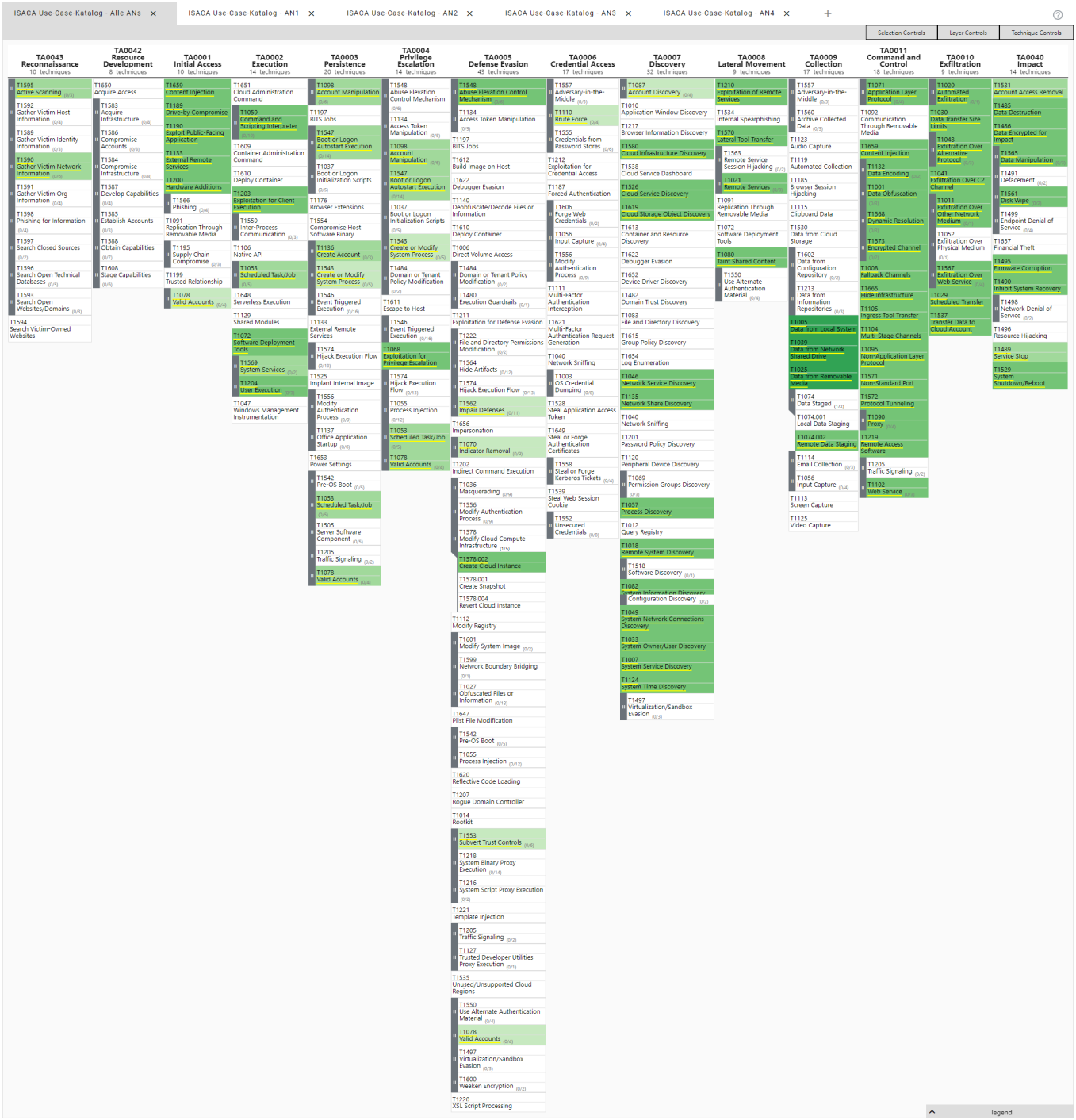


Abbildung 5: Screenshot ATT&CK Navigator: Abdeckung kombiniert AN1-AN4

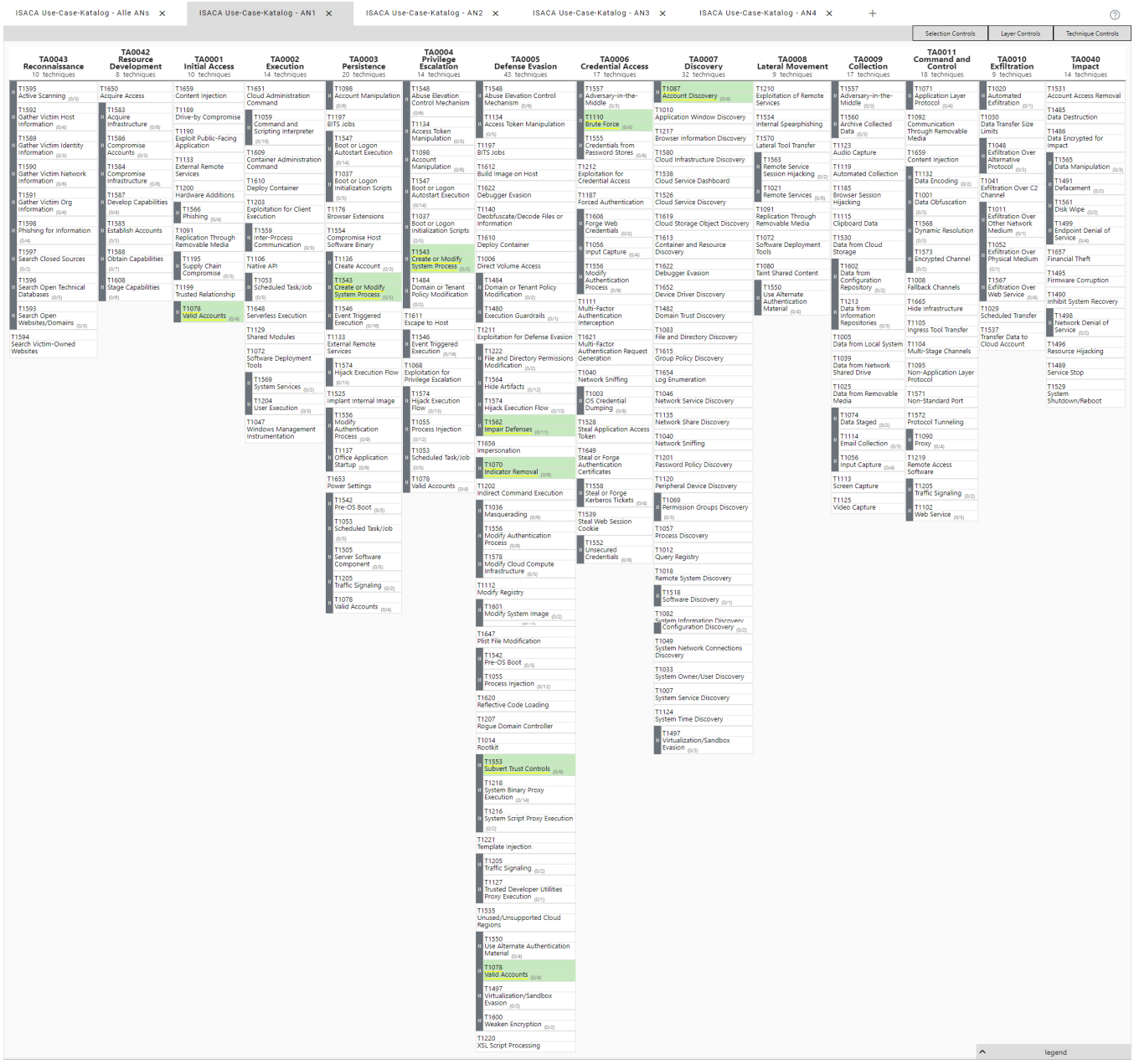


Abbildung 6: Screenshot ATT&CK Navigator: Abdeckung AN1

3 Die Konfigurationsdatei für den ATT&CK Navigator wird separat zur Verfügung gestellt. Im Navigator selbst sind die dargestellten Informationen besser ersichtlich. Aufgrund der Größe der Darstellung ist im Dokumentenformat eine effektive Darstellung schwierig und soll hier nur einen groben optischen Überblick geben.

4 Unter den Techniques ist auch eine mit Txxxx. Diese steht stellvertretend für unterschiedliche Techniques, die aufgrund der Art des Use-Cases und seiner Abstraktion nicht zugeordnet werden können. Entsprechend kann sie im ATT&CK Navigator nicht dargestellt werden, was sich bspw. auf die visuelle Abdeckung der Tactic »Resource Development« auswirkt.

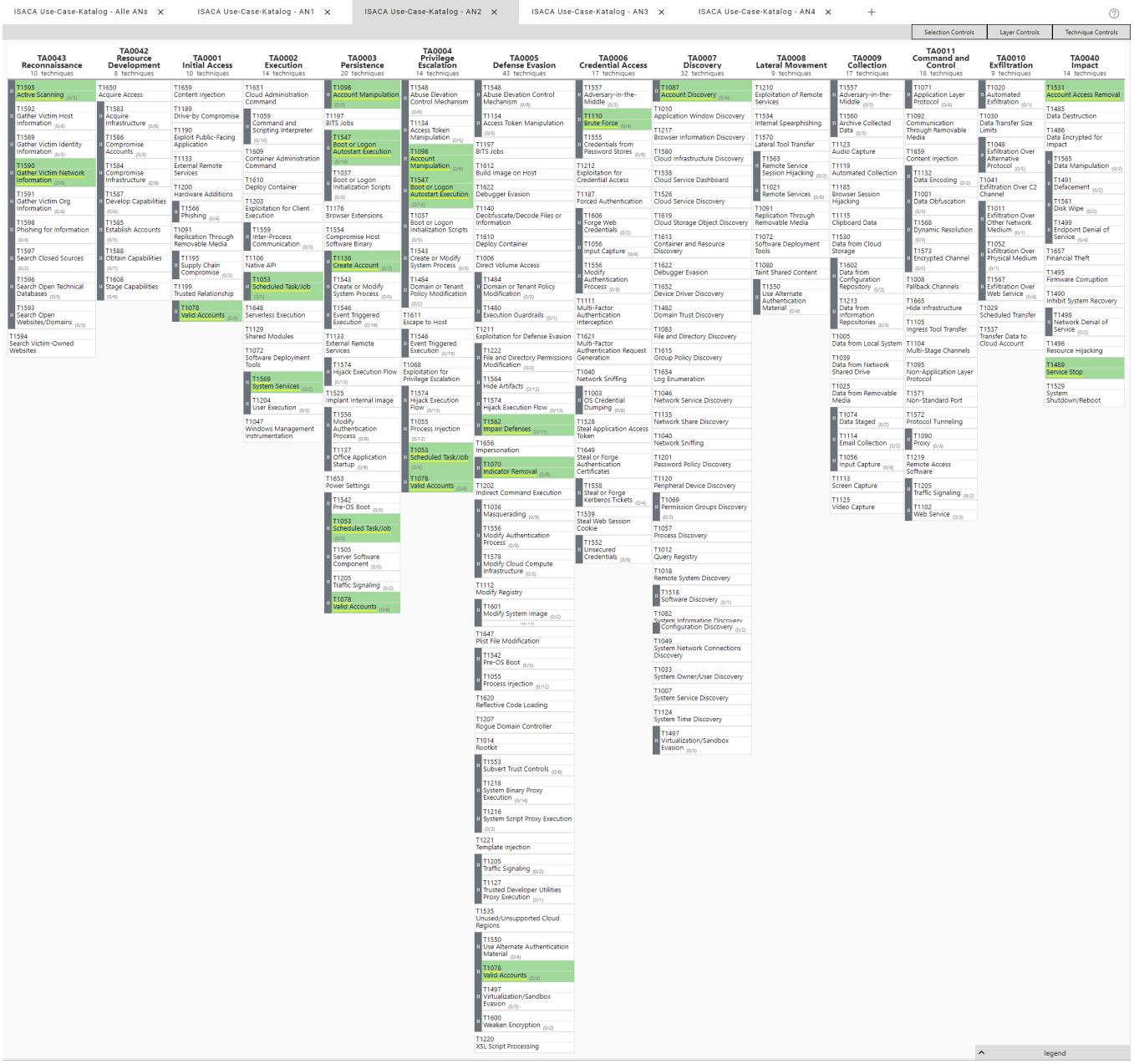


Abbildung 7: Screenshot ATT&CK Navigator: Abdeckung AN2

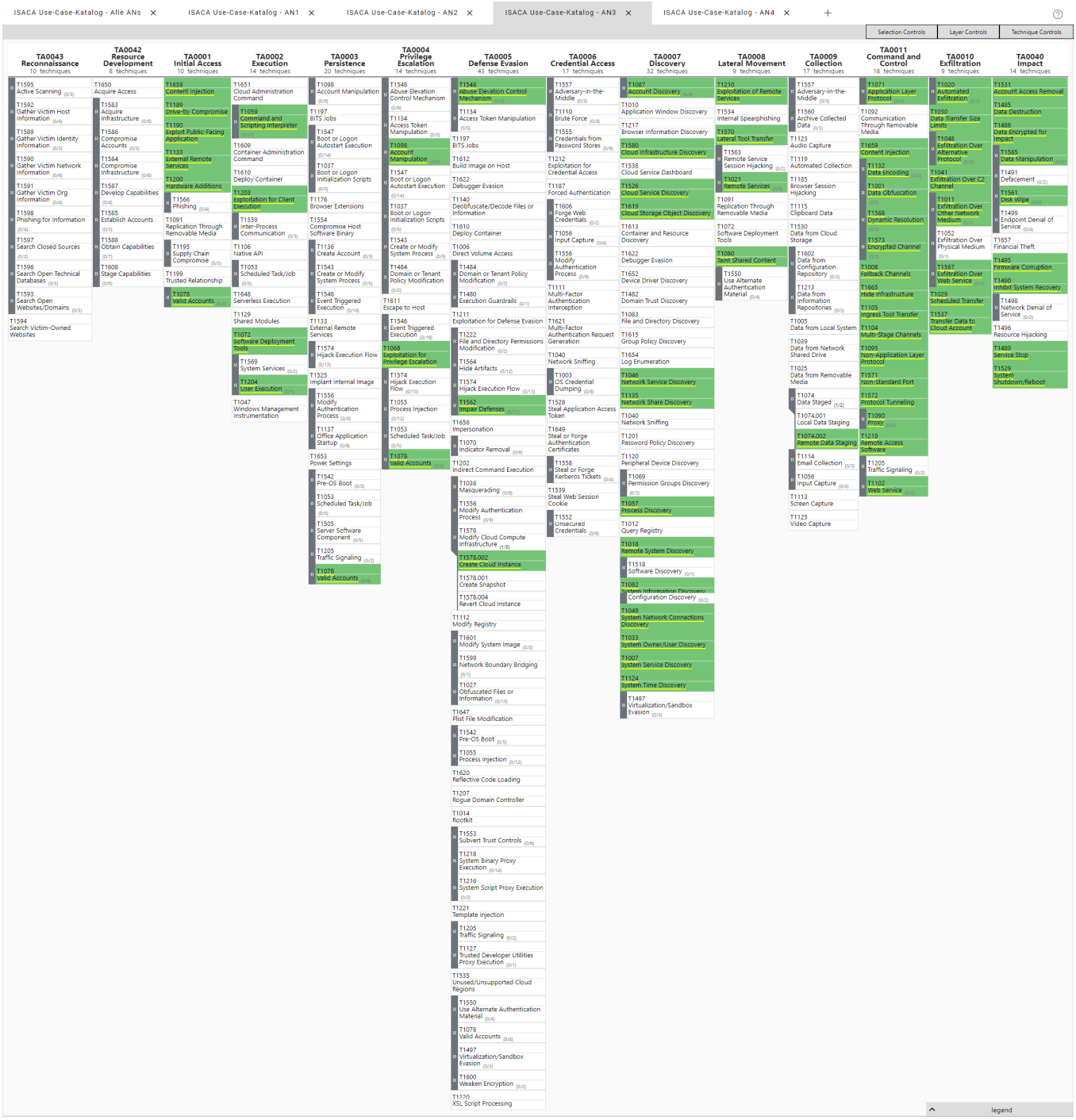


Abbildung 8: Screenshot ATT&CK Navigator: Abdeckung AN3

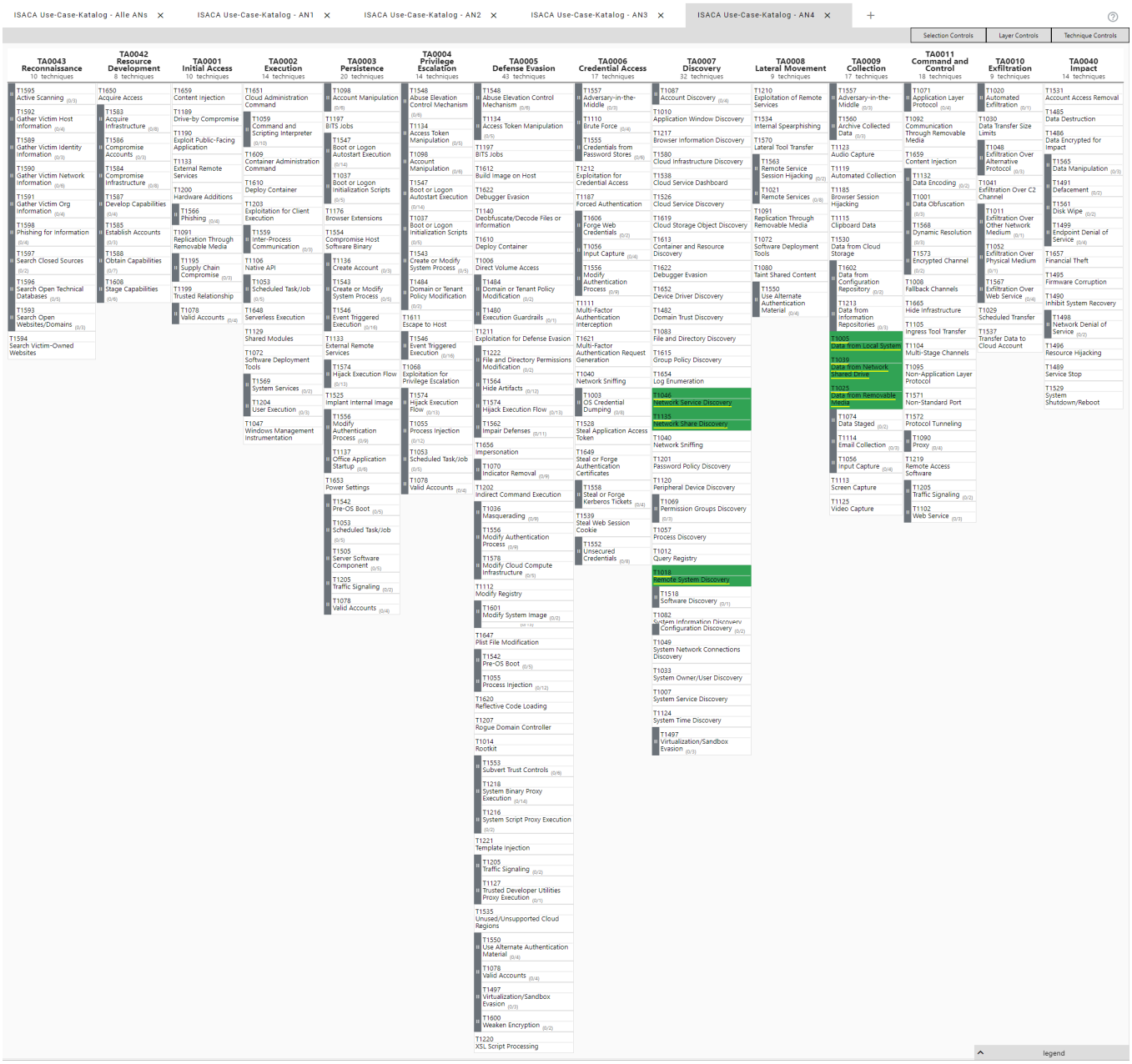


Abbildung 9: Screenshot ATT&CK Navigator: Abdeckung AN4

3.5 Liste der abstrakten Ereignisdefinitionen

Protokolle unterscheiden sich üblicherweise sehr in Struktur und Inhalt. Beispielsweise verwendet Windows für Anmeldeereignisse Ereigniscodes wie 4624, SAP-Systeme wiederum Ereigniscodes wie AU1 und AU5. Es unterscheiden sich aber nicht nur die Protokolle von unterschiedlichen Systemen wie bspw. Datenbanksystemen zu denen von Webservern, sondern auch vergleichbare Software erzeugt unterschiedliche Einträge. So unterscheiden sich z.B. die Protokolle von Oracle-Datenbanksystemen und Microsoft SQL-Servern, Cisco Firepower IDS und Checkpoint SmartDefense.

Um bei den hier vorgestellten Use-Cases eine einheitliche und systemunabhängige Vorgabe geben zu können, wurden daher für diesen Leitfaden abstrakte Ereigniscodes definiert und verwendet (siehe Tabelle 7), insofern sich diese als nötig erwiesen haben.

So steht »AUTH01« für Anmeldungen mittels eines Benutzerkontos. Bezogen auf die genannten Beispiele würde AUTH01 also für Windows-Systeme den Ereigniscode 4624 (und ggf. weitere) in der Umsetzung bedeuten, und für SAP-Systeme AU1 und AU5.

Ereigniscode	Bedeutung
ACCT01	Berechtigungsänderung an einem Benutzerkonto (bspw. Zuweisung einer anderen Rolle)
ACCT02	Berechtigungsänderungen an einer Rolle, Gruppe oder Vergleichbarem (inhaltlich, nicht Mitglieder)
ACCT03	Änderungen am Objekt eines Benutzerkontos (Beschreibungen, User Record, ...) oder einer Gruppe (Zuweisung Mitglieder, ...)
ACCT04	Anlage eines Benutzerkontos oder einer Gruppe
ACCT05	Löschung eines Benutzerkontos oder einer Gruppe
ALERT01	Warnmeldung eines Sicherheitssystems, bspw. Virenfund durch ein Antivirus-System, Warnmeldung eines IDS/IPS-Systems usw.
APP01	Ein System, eine Applikation oder Ähnliches wird gestartet
APP02	Ein System, eine Applikation oder Ähnliches wird gestoppt
APP03	Ein System, eine Applikation oder Ähnliches ist erreichbar
AUTH01	Anmeldung (»Login«) mit einem Benutzerkonto
AUTH02	Abmeldung (»Logout«) von einem Benutzerkonto
CONFIG01	Konfiguration (nicht Protokollierung) wird geändert
CONFIG02	Sicherheitsrelevante Konfiguration (nicht Protokollierung) wird geändert
CONFIG03	Konfigurationen von Regelwerken oder Inhalten (»Content«)
DATA01	Lesender Datenzugriff
DATA02	Schreibender Datenzugriff
DET01	Ein Gerät oder System wurde erkannt, typischerweise im Rahmen einer Service Discovery via Netzwerkscan
HB01	Ereignis, das anzeigt, dass noch Protokolldaten von einem Quellsystem ankommen (»Heartbeat« für die Protokollquelle)
LOCK01	Sperrung eines Benutzerkontos aufgrund fehlerhafter Anmeldung
LOCK02	Manuelle Sperrung eines Benutzerkontos
LOG01	Löschung von Protokollen
LOG02	Veränderung von Protokollen
LOG03	Konfiguration der Protokollierungsfunktion
LOG04	Deaktivierung der Protokollierungsfunktion
NET01	Ereignis im Netflow (nach RFC 3954) oder Netzwerkereignis, bspw. FW-Ereignis über Kontaktaufnahme/-ablehnung, Router-Traffic, Endpunkt-Ereignis wie Windows-Anmelde-Ereignis, entscheidend ist, dass es Netzwerkinformationen wie Quell- und Ziel-IPs/Hostnamen, Portinformationen und Ähnliches enthält
NET02	Portscan wurde erkannt
PSTART01	Programm/Prozess wurde gestartet/ausgeführt
PSTART02	Funktion in einem Programm/Prozess wurde gestartet/ausgeführt
TIME01	Änderung der Systemzeit

Tabelle 7: Liste der abstrakten Ereignisdefinitionen

In den Regeldefinitionen der Use-Cases werden zudem teilweise folgende Suffixe zum Ereigniscode hinzugefügt:

- **.succ:** Die Aktion war erfolgreich.
- **.fail:** Die Aktion war nicht erfolgreich.
- *ohne* oder .*: Die Aktion war erfolgreich oder nicht erfolgreich.

Ein angegebener Ereigniscode »AUTH01.succ« steht also für eine erfolgreiche Anmeldung, »AUTH01.fail« für eine fehlgeschlagene und »AUTH01« oder »AUTH01.*« für erfolgreiche und/oder erfolglose Anmeldeversuche.

3.6 Hinweise zur Umsetzung

Oben wurde auf die unterschiedlichen Auswertungsniveaus eingegangen und dass sie der Reihe nach umgesetzt werden sollten. Ebenso ist es wichtig, die Auswertungsniveaus bzw. Use-Cases auf allen Softwarestackebenen umzusetzen. Es gibt unterschiedliche Schnitte, in denen zur Illustration für den Zweck dieses Dokuments folgende Aufteilung vorgenommen wird (von der untersten Ebene zur höchsten):

1. Virtualisierung (falls vorhanden)
2. Betriebssystem
3. Netzwerk

4. Datenhaltungssysteme wie Datenbanksysteme
5. Middleware wie Webserver, Applikationsserver oder Ähnliches
6. Anwendungssysteme

Außer für den Fall, dass es gesonderte Anforderungen oder Risiken gibt, sollte stets systematisch von der untersten Stackebene zur obersten umgesetzt werden. Zudem sollten die Auswertungsniveaus (ANx) nicht zu sehr auseinander gehen. So ist es im Allgemeinen nicht sinnvoll, für Betriebssysteme AN3 umzusetzen, für die anderen Auswertungsniveaus aber keine Use-Cases zu implementieren. Oder AN1 für Betriebssysteme, AN2 ganz auszulassen und dann nur noch für die Datenbanken AN3 umzusetzen.

Meist ist es zielführender, systematisch eine einheitliche Mindestabdeckung sicherzustellen, anstatt einen Teilbereich besonders stark auszubauen und dies nicht für den Rest zu berücksichtigen, z. B.:

- AN1 für alle Softwarestackebenen
- AN2 für Betriebssysteme und AN1 für alle anderen Systeme

Generell wird der volle Nutzen des Use-Case-Katalogs erst erreicht, wenn alle Softwarestackebenen und Assetklassen geschützt sind. Risikoanalysen und ein daraus abgeleitetes risikoorientiertes Vorgehen helfen, eine wirtschaftliche und effektive Überwachung sicherzustellen. So kann es bspw. für eine Organisation sinnvoll sein, dieses Vorgehen zunächst mit wenigen besonders kritischen Systemen umzusetzen und risikoabhängig sukzessive auszubauen. Dagegen könnte für eine andere Organisation wiederum der Ansatz sinnvoller sein, für alle Systeme mit der Betriebssystemebene anzufangen.

Innerhalb einer Softwarestackebene sollte die Organisation grundsätzlich die Sicherheit aller vorhandenen Infrastrukturkomponenten per Use-Case überwachen. Das sollte durchgängig von den Endgeräten (z. B. PCs, Notebooks, Smartphones und Drucker) über die Netzwerkgeräte (z. B. Router und Switches), die Sicherheitskomponenten (z. B. Firewalls und Proxys) bis hin zu den Übergabepunkten zwischen Netzen (z. B. Internet oder OT-Netzen) erfolgen. Es reicht also normalerweise nicht aus, einen Use-Case nur im Netzwerk zu implementieren. Vielmehr sollte versucht werden, grundsätzlich alle vorhandenen Softwarestackebenen abzudecken. Im Gegensatz dazu ist es gängige Praxis, bei Anwendungen nur diejenigen zu überwachen, die besonders kritisch sind oder für das Kerngeschäft eine hohe Relevanz haben. Allerdings sollten für die Umsetzung des Use-Case-Katalogs alle entsprechenden Anwendungen berücksichtigt und die Herleitung für die Einordnung, ob relevant oder nicht, dokumentiert werden. Es sollte dabei beachtet werden, dass Angriffe auch über die als nicht relevant bewerteten Systeme auf die kritische Infrastruktur erfolgen können.

Eine mögliche Folge einer solchen Analyse kann die Erkenntnis sein, dass eine bestimmte Software zwar Risiken in einem zu überwachenden Szenario hat, dieses Szenario aber nicht in der Organisation bzw. der IT/OT-Landschaft besteht. Somit wäre es nicht nötig, diesen Use-Case umzusetzen.

Aus diesen Erläuterungen geht implizit hervor, dass eine Grundvoraussetzung für die Auswahl von Use-Cases das Vorhandensein einer (möglichst vollständigen) Liste aller vorhandenen Assets (»Assetregister«) ist.

Die konkrete Umsetzung eines Use-Case verläuft stets nach einem einfachen Muster, wie es in Abbildung 10 zusammen mit einem Beispiel (hellblau) dargestellt ist.

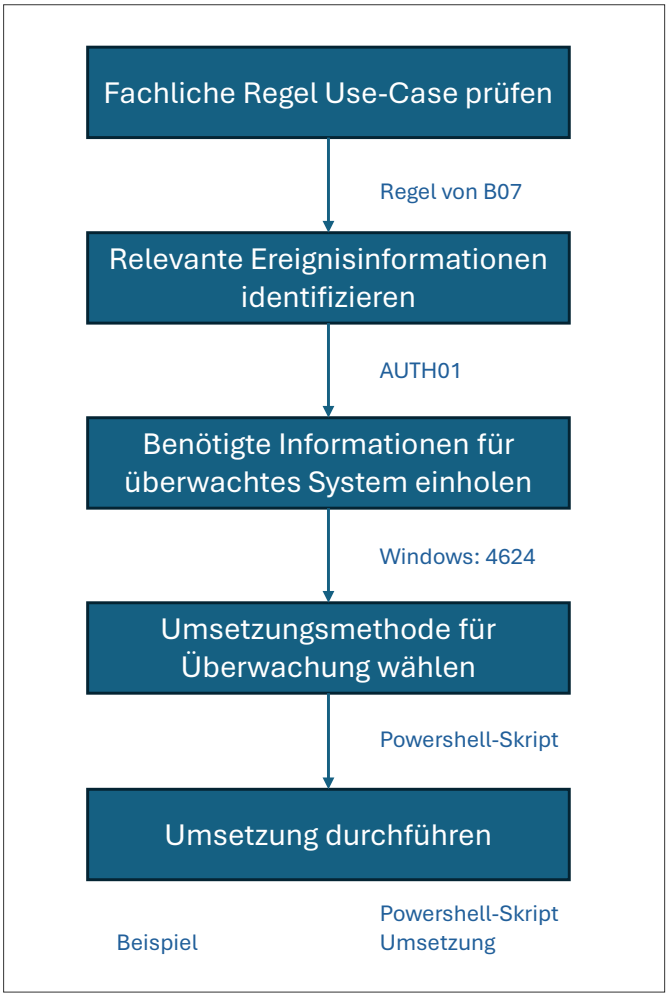


Abbildung 10: Typischer prozessualer Ablauf einer Use-Case-Umsetzung

Das Beispiel in Abbildung 10 zeigt die Umsetzung der Benutzeranmeldung (AUTH01) für Windows:

1. Umzusetzenden Use-Case auswählen: B07
2. Welche Ereignisinformationen und insbesondere welche Ereigniscodes werden benötigt: AUTH01. Anschließend wird in Informationsquellen nachgeschla-

gen, wie Anmeldeinformationen identifizierbar sind. Dies ergibt, dass für Windows mehrere Ereigniscodes relevant sind, darunter 4624 und 4625. Die Ereigniscodes 4634, 4647, 4648 und 4779 werden zunächst zurückgestellt, da sie für Spezialfälle wie Terminal-Services verwendet werden, die in diesem Beispiel nicht relevant sind.
3. Umsetzungsvarianten prüfen: Entscheidung für PowerShell-Skript, das regelmäßig ausgeführt und geprüft wird
4. Umsetzung durchführen

Die sinnvollste Art der Umsetzung wird von den Besonderheiten einer Organisation und ihrer Situation beeinflusst und hängt u.a. von folgenden Aspekten ab:

- **Zahl der Assets:**
  Ein einzelner Server lässt sich mit wenigen und einfacheren Mitteln überwachen als eine Vielzahl von Servern.
- **Erforderliches Auswertungsniveau bzw. erforderliche Use-Cases und deren Komplexität:**
  Je mehr und je komplexere Use-Cases verwendet werden, umso schwieriger wird es, diese mit Bordmitteln oder einfachen Werkzeugen umzusetzen.
- **Integrationsanforderungen:**
  Gerade eine Integration unterschiedlicher Datenströme oder multipler Quell- und Zielsysteme im Prozessablauf hat Auswirkungen auf die Umsetzungen. Hinweise hierauf geben Fragestellungen wie:
  - Sollen die Ergebnisse in Ticketing-Tools oder Vergleichbares integriert werden?
  - Werden Informationen aus unterschiedlichen Systemen oder sogar externen Informationssystemen (»Threat Intelligence«) integriert?
- **Wissen und Fertigkeiten in der Organisation:**
  Komplexe Systeme einzuführen, für die erforderliche Fertigkeiten fehlen oder Personen für einen sinnvollen dauerhaften Betrieb nicht vorhanden sind, ist nicht zielführend. Hier sind einfache Lösungen typischerweise effektiver, die dafür verstanden, betrieben und weiterentwickelt werden können.

Um das oben angegebene Beispiel AUTH01 für Windows gemäß B07 auszuwerten, könnten bspw. folgende Varianten als Alternativen umgesetzt werden:

- Variante 1: Programm »Ereignisanzeige« unter Windows nutzen
- Variante 2: Auswertung per Programm oder Skript
- Variante 3: Verwendung eines zentralen SIEM-Systems zur Auswertung

Im folgenden Abschnitt wird dies konkretisiert.

3.7 Beispiele für die Umsetzung

Für das Beispiel der Umsetzung von Use-Case B07 mit Ereignis AUHT01 ist im Folgenden die Auswertung mittels verschiedener Umsetzungsvarianten dargestellt. Als speziell zu überwachende Benutzerkonten wurden exemplarisch »SYSTEM« und »Netzwerkdienst« verwendet.

Variante 1: Nutzen der »Ereignisanzeige«

Hierfür wird das entsprechende Windows-Systemprogramm genutzt. Es erlaubt das Laden, Ansehen und Filtern der Protokolle, allerdings kann es keine Logik abbilden und keine automatischen Auswertungen vornehmen.

Variante 2: Auswertung per Skript

Eine Umsetzung z.B. mittels eines PowerShell-Skripts könnte wie in Variante 2a aussehen.

Wird dieses ausgeführt, so liefert es Daten in der in Variante 2b dargestellten Form.

Eine solche Implementierung integriert Auswertungslogik und kann über Systemmittel regelmäßig automatisch oder manuell aufgerufen werden. Zudem lässt sie sich ausbauen und so bspw. auch befähigen, Remote-Abfragen anderer Systeme von einem zentralen System aus durchzuführen.

Grundsätzlich ist eine solche Lösung bereits für viele kleine Organisationen mit überschaubaren Systemlandschaften geeignet. Allerdings kann es herausfordernd werden,

- dies für unterschiedliche Assetklassen wie Firewalls, Router/Switche oder Anwendungen zu implementieren (das wird insbesondere dann schwieriger, wenn die Assets nicht das Abholen oder gezielte Abfragen der Protokolle erlauben, sondern diese nur an andere Zielsysteme z.B. über das Syslog-Protokoll übertragen können),
- die Auswertung über Kombination und Korrelation der Protokolle verschiedener Assetklassen durchzuführen,
- die Ergebnisse für eine größere Zahl von Systemen effizient auszuwerten,
- Nachweise über durchgeführte Überprüfungen so zu dokumentieren, dass sie potenziellen Prüfungen (»Audits«) genügen,
- Programm- bzw. Skriptlösungen zu warten sowie
- alle relevanten Fehlerszenarien wie bspw. eine temporäre Nichterreichbarkeit von Systemen bei der Protokollabfrage und -auswertung zu berücksichtigen.

```
$GL_SPEZIELLENUTZER_01 = @(„SYSTEM“,“Netzwerkdienst“)
$NL_ZUGELASSENENUTZER_01 = @()
$NL_ZUGELASSENESYSTEME_01 = @()
$logins    =    Get-EventLog    -LogName    Security    -InstanceId    4624,4625    |
    ForEach-Object {
     [PSCustomObject]@{
     Timestamp   = $_.TimeGenerated
     Workstation = $_.ReplacementStrings[11]
     Domain      = $_.ReplacementStrings[6]
     User        = $_.ReplacementStrings[5]
     ProcessName = $_.ReplacementStrings[17]
     LoginType   = $_.ReplacementStrings[8]
     SourceIP    = $_.ReplacementStrings[18]
     }
   }
$logins | Where-Object { $GL_SPEZIELLENUTZER_01.Contains($_.User) -and -not
$NL_ZUGELASSENENUTZER_01.Contains($_.User) -and -not $NL_ZUGELASSENESYSTEME_
01.Contains($_.Workstation) }
```

Variante 2a Powershell Script

```
...
Timestamp   : 18.04.2024 22:35:43
Workstation : -
Domain      : NT-AUTORITÄT
User        : SYSTEM
ProcessName : C:\Windows\System32\services.exe
LoginType   : 5
SourceIP    : -

Timestamp   : 18.04.2024 22:35:43
Workstation : -
Domain      : NT-AUTORITÄT
User        : SYSTEM
ProcessName : C:\Windows\System32\services.exe
LoginType   : 5
SourceIP    : -
...
```

Variante 2b Beispiel einer Ereignisausgabe

Variante 3: Sicherheitssystem, wie z.B. ein SIEM-System, zur Auswertung verwenden

Ist die Nutzung von Bordmitteln oder das Erstellen von einfachen Lösungen mittels Programmierung nicht ausreichend, bietet es sich an, spezialisierte Sicherheitslösungen einzusetzen.

Derartige Lösungen ähneln sich stets im Grundsatz:

- Sie sammeln Protokolldaten und ggf. weitere Metriken.
- Sie bieten Funktionen zur Normalisierung und Anreicherung der Daten.
- Sie bieten Funktionen zur Auswertung, üblicherweise über unterschiedliche Protokolle von unterschiedlichen Assetklassen.
- Sie bieten oftmals auch die Möglichkeit der Hinterlegung von Logiken in Form eines Regelwerks inklusive der regelmäßigen automatisierten Auswertung und konfigurierbarer Reaktionen.

Im Detail unterscheiden sich die Lösungen unter anderem in Bezug auf Kosten, Funktionalitäten, Ansprüche an Fähigkeiten der Mitarbeiter und Systemvoraussetzungen, Verbreitung, unterstützte Protokolle von Assetklassen sowie verfügbaren Support. Entsprechend sollte eine Organisation sorgsam auswählen, was zu ihr passt.

Zunächst werden Agenten auf den zu überwachenden Systemen installiert, die die Protokolldaten an das SIEM-System senden.
Anschließend wird im SIEM-System Folgendes eingestellt:

- Anlage Liste `GL_SPEZIELLENUTZER_01` mit Einträgen
  - „SYSTEM"
  - „Netzwerkdienst"
- Anlage Liste `NL_ZUGELASSENENUTZER_01` ohne Einträge
- Anlage Liste `NL_ZUGELASSENESYSTEME_01` ohne Einträge
- Erstellung der Regel:
  `((e.rv40=4624 OR e.rv40=4625) AND (e.dun inlist GL_SPEZIELLENUTZER_01)) AND (NOT (e.dun inlist NL_ZUGELASSENENUTZER_01)) AND (NOT (e.dun inlist NL_ZUGELASSENESYSTEME_01))`

Variante 3 Festlegung eines Sicherheitssystems

Würde bspw. ein SIEM-System gewählt werden, so könnte die Umsetzung des B07 wie in Variante 3 aussehen.

Auch wenn sich die Details wie die konkrete Regelsprache zwischen unterschiedlichen SIEM-Systemen unterscheiden, so dürfte es so ähnlich wie oben dargestellt aussehen. Hierbei gilt grundsätzlich, dass die Protokolleinträge analysiert werden. Häufig werden sie vor oder während der Auswertung in Felder aufgeteilt, in denen wesentliche Teile der Protokolle gezielter ausgewertet werden können. Im oben aufgeführten Beispiel würden die Ereignis-IDs 4624 oder 4625 im Feld *rv40* des aktuellen Ereignisses *e* abgespeichert sein, und *dun* das für den Anmeldeversuch verwendete Benutzerkonto enthalten. Falls die Bedingungen in der Regel erfüllt werden, wird die hinterlegte Aktion wie bspw. die Erstellung eines Tickets mit einer Warnmeldung ausgeführt.

SIEM-Systeme können große Datenmengen verarbeiten und zentralisieren und unterstützen die Auswertung. Sie sind jedoch auch aufwendiger und komplexer im Betrieb und können auch Entwicklungsbedarf erfordern, z. B. wenn die Protokolle einer zu überwachenden Anwendung nicht unterstützt werden oder sich durch Softwareupdates verändern.

Die in den Use-Cases dieses Dokuments verwendete Regelsprache sollte sich für die meisten regelbasierten Sicherheitssysteme wie SIEM mit geringem Aufwand adaptieren lassen, was eine Umsetzung mit derartigen Systemen erleichtern dürfte.

3.8 Hinweise zur Nomenklatur der Use-Cases

Die in Abschnitt 3.9 aufgeführten Use-Cases werden in einer einheitlichen Struktur beschrieben. Diese ist in Tabelle 8 dargestellt, die aus zwei Blöcken besteht:
Die Elemente des Zuordnungsblocks (linker Block) ordnen die Begrifflichkeiten des PDCA-Zyklus, eingeführt in Abbildung 1, den Bezeichnungen der Use-Case-Steckbriefe im Beschreibungsblock (rechter Block) zu.
Hierzu werden nachfolgend in Tabelle 9 einige Begriffe ausführlicher beschrieben.

Zuordnung zu den Elementen in **Abbildung 1**	**Bezeichnung**	**Inhalte**
	ID	im Unternehmen vergebene ID für diesen Use-Case
	Name	Bezeichnung des Use-Cases
	Kurzbeschreibung mit Detektionsziel	Beschreibung, was detektiert werden soll
	Adressierte Risiken	Beschreibung, welche Risiken adressiert werden
Ereignis Listen	Erforderliche Informationen	erforderliche Informationen bzw. Daten
Ereignis Listen	Benötigte Positiv- und Negativlisten	Listenaufstellung mit Inhalten, soweit erforderlich
Ereignis Listen	Empfohlener Reaktionstyp	Warnmeldung, Bericht, andere ...
Ereignis Listen	Kritikalität	normal (1), hoch (2), sehr hoch (3)
Ereignis Listen	Dringlichkeit	normal (1), schnell (2), unverzüglich (3)
Regel-optimierung	Typische True-Positives (kritisch)	Auflistung der Arten von True-Positives, also Fälle korrekter Detektionen
Regel-optimierung	Typische True-Negatives (unkritisch)	Auflistung der Arten von True-Negatives, also in welchen Fällen gewollt nicht detektieren soll
Regel-optimierung	Typische False-Positives (unkritisch)	Auflistung der Arten von False-Positives, also in welchen Fällen detektiert werden könnte, obwohl das grundsätzlich nicht erwünscht ist
Regel-optimierung	Typische False-Negatives (kritisch)	Auflistung der Arten von False-Negatives, also wenn tatsächliche Fälle nicht detektiert werden könnten
Prüfregel, Auslösung	Fachliche Beschreibung Regel	Fachliche Beschreibung, wie der Use-Case funktioniert
Prüfregel, Auslösung	Gruppierung	Nach was werden die detektierten Ereignisse bzw. erstellten Warnmeldungen gruppiert
Prüfregel, Auslösung	Optionen und Anmerkungen	Ergänzungen, bspw. Sonderverhalten, Spezialfälle, besondere Art der Durchführung, Abhängigkeiten oder ähnliches
Reaktion	Reaktion	Welche typischen Reaktionen hier durchgeführt werden. Dies kann abstrakt ("allgemeine Detail- und Umfeldanalyse") oder konkret ("Überprüfung, ob betroffenes Benutzerkonto jünger als 1 Tag ist, falls ja Aktivität ... durchführen")
	Referenz ATT&CK Techniques	Referenz ATT&CK Techniques und Subtechniques, siehe hier: https://attack.mitre.org/tactics/enterprise/
	Referenz BSI	Referenz BSI IT-Grundschutz wenn möglich
	Referenz ATT&CK Tactics	Die Zuordnung zu den entsprechenden ATT&CK Tactics, siehe hier: https://attack.mitre.org/tactics/enterprise/

Tabelle 8: Format der im Folgenden beschriebenen Use-Cases

Begriff	Beschreibung
Positivliste	Eine Positivliste ist eine Liste, deren Elemente in einem Use-Case zu einer Warnmeldung führen (False Positive, True Positive). **Beispiel:** Ein Benutzer X darf sich nicht an einem System anmelden. Er muss bei einem Use-Case, der dies überwacht, auf eine entsprechend zugehörige Positivliste gesetzt werden, damit Warnmeldungen ausgelöst werden können. **Format:** <PL_NAME_ID>
Negativliste	Eine Negativliste ist eine Liste, deren Elemente in einem Use-Case zur Vermeidung einer Warnmeldung führen (False Negative, True Negative). **Beispiel:** Ein automatischer Housekeeping-Vorgang, der alte Protokolle löscht, sollte auf die Negativliste gesetzt werden, um nicht täglich falsche Warnmeldungen (False Positives) auszulösen. **Format:** <NL_NAME_ID>
Generelle Liste	Teil von »erforderliche Informationen«: Allgemeine Liste, die selbst nicht zwingend zu einer Warnmeldung oder der Vermeidung einer Warnmeldung führt. **Format:** <GL_NAME_ID>
Schutzbedarf (SBF)	Es wird bei manchen Use-Cases für die Gruppierung auf den »Schutzbedarf« verwiesen. Hier wird die Definition nach BSI verwendet; normal (1), hoch (2), sehr hoch (3)
ATT&CK Tactics	Die Zuordnung zu den entsprechenden ATT&CK Tactics, siehe: https://attack.mitre.org/tactics/enterprise/
ATT&CK Techniques	Abdeckungsbeschreibung hinsichtlich Techniques und Subtechniques im Format Tx [G/D] (TECHNIQUE), ... Wenn keine Techniques direkt zugeordnet werden können, wird Txxxx (Various) angegeben. TECHNIQUE = Name der Technique/Subtechnique G = Generelle Abdeckung D = Dedizierte/Direkte Abdeckung
Referenz BSI	Die Referenz zu passenden Bausteinen des BSI IT-Grundschutz-Kompendiums 2023. Wenn keine existieren, dann folgt die Angabe »Keine Entsprechung«.

Tabelle 9: Wichtige Begriffe des Use-Case-Steckbriefes

Es wird eine abstrakte Regelsprache zur fachlichen Beschreibung der Regel verwendet. Diese ist deskriptiv in natürlicher Sprache gehalten. Grundsätzlich haben Einrückungen den gleichen Effekt wie Klammerungen, sie erhöhen aber die Übersichtlichkeit. Daher sind die beiden Einträge[5] im folgenden Beispiel logisch gesehen identisch:

- ```
  WENN
     das Ereignis LOG01.*
     für System Z
     mit Benutzer U
  EINTRITT,
  UND
     (U,Z) oder (U,*) ist nicht enthal-
     ten in <NL_ZUGELASSENENUTZER_01>
     ODER
     (U,Z) oder (U,*) ist enthalten in
     <PL_SENSIBLENUTZER_01>

  DANN
    löse aus
  ```

- ```
  WENN (das Ereignis LOG01.* für Sys-
  tem Z mit Benutzer U) EINTRITT, UND
  (((U,Z) oder (U,*) ist nicht ent-
  halten in <NL_ZUGELASSENENUTZER_01>)
  ODER ((U,Z) oder (U,*) ist enthalten
  in <PL_SENSIBLENUTZER_01>))) DANN
  (löse aus)
  ```

Die Regel operiert immer auf einem aktuellen Protokollereignis, das die im Use-Case spezifizierten erforderlichen Daten enthält. Es wird davon ausgegangen, dass stets neben denen im Use-Case spezifizierten und in der Regel verwendeten Daten mindestens ein Datum- und Zeitstempel enthalten ist und dass die Ereignisse in der Reihenfolge ihres zeitlichen Auftretens ausgewertet werden.

Das Regelbeispiel verwendet Listen. Diese werden in den Use-Cases vielfach genutzt. Grundsätzlich ginge es auch ohne sie, indem die entsprechenden Inhalte fest in den Regeltext übernommen werden. Bei der Erstellung der Use-Cases wurde abgewogen, ob die Informationen häufigen Anpassungen unterliegen oder sich je Implementierung, bspw. je Assetklasse, unterscheiden. In letzterem Fall wurden Listen verwendet, eine derartige Umsetzung wird aufgrund leichterer Wartbarkeit auch empfohlen.

Grundsätzlich gilt bei Listen die folgende Hierarchie (von niedrigster zu höchster Stufe):

1. Generelle Listen
2. Negativlisten
3. Positivlisten

Negativlisten können also die Effekte von generellen Listen überschreiben, aber nicht die von Positivlisten, die wiederum alle anderen übertrumpfen.

Bezüglich des Regeltexts sind noch folgende Notationen wesentlich:

- `<X>`: Liste von Inhalten, ein- oder mehrdimensional
- `(x1,x2,...)`: Tupel, also Kombination von Werten. Wird typischerweise verwendet, um die Prüfung auf Elemente einer Liste darzustellen.
  Bspw.: `<X>=<System,Port>`, dann bedeutet `»(SysA,443) enthalten in <X>«` die Prüfung auf `System=SysA` und `Port=443`.

  Hinweis: Zur Abkürzung kann anstelle von `(x1)` auch `x1` geschrieben werden (1-dimensionales Tupel).
- `»y enthalten in <X>«`: Element bzw. Tupel `y` ist enthalten in der Liste `X`. Es kann auch ein `'*'` angegeben werden, wenn jeder Wert dieser Listendimension zulässig ist.

  Beispiele:
  - Ein Benutzer `B1` und ein System `S1` sind enthalten in `(B1,S1)` sowie in `(B1,*)` oder `(*,S1)`. `»(*,S1) enthalten in <P1>«` ist für `<P1>=<Benutzer,System>` also für alle Benutzer wahr, solange das System `S1` enthalten ist.
  - `»'*' enthalten in <X>«` ist immer wahr, außer `<X>` ist leer (enthält keine Einträge).
- Es werden folgende mathematische Operatoren benutzt: `gleich` (=), `größer als` (>), `kleiner als` (<), `größer oder gleich` (>=), `kleiner oder gleich` (<=), `ungleich` (!=)

Für weitere Informationen zur Dokumentation von Use-Cases und deren Umsetzung wird auf das Abschnitt 3.10 verwiesen.

3.9 Liste der Use-Cases

In diesem Abschnitt werden die einzelnen Use-Cases in der Reihenfolge nach ihren Auswertungsniveaus aufgeführt:

Auswertungsniveau	Use-Cases
AN1	B01 bis B09
AN2	B10 bis B25
AN3	B26 bis B39
AN4	B40 bis B42

5 Regel entstammt Use-Case B01.

3.9.1 B01 – Löschung von Ereignisprotokollen

ID	B01
Name	Löschung von Ereignisprotokollen
Kurzbeschreibung mit Detektionsziel	Es soll erkannt werden, wenn Ereignisprotokolle gelöscht werden.
Adressierte Risiken	Werden Ereignisprotokolle gelöscht, so ist die Nachvollziehbarkeit der Aktivitäten nicht mehr gewährleistet. Darauf basierende Use-Cases funktionieren nicht mehr.
Erforderliche Informationen	◗ Ereignis: – Ereigniscode LOG01 für Löschung von Logs – Benutzer U, der die Aktivität durchführt – Zielsystem Z, auf dem die Aktivität durchgeführt wird ◗ Benutzer je System oder global, die Ereignisprotokolle löschen dürfen
Benötigte Positiv- und Negativlisten	◗ Negativliste <NL_ZUGELASSENENUTZER_01>: Benutzer je System oder global, die Ereignisprotokolle auf dem entsprechenden System ohne Warnmeldung löschen dürfen ◗ Positivliste <PL_SENSIBLENUTZER_01>: Benutzer, die auf dieser Liste stehen, führen immer zu einer Warnmeldung, auch wenn sie in <NL_ZUGELASSENENUTZER_01> enthalten sind (Vorrangigkeit).
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	3 (sehr hoch)
Dringlichkeit	3 (unverzüglich)
Typische True Positives (kritisch)	◗ Angreifer löschen die Ereignisprotokolle, um ihre Spuren zu verwischen.
Typische True Negatives (unkritisch)	◗ Ein genehmigter automatisierter Bereinigungsvorgang löscht alte bzw. nicht mehr benötigte Ereignisprotokolle gemäß Vorgabe, und der hierzu verwendete Benutzer steht auf der Negativliste für das System.
Typische False Positives (unkritisch)	◗ Ein genehmigter manueller Eingriff war erforderlich, da eine automatisierte erforderliche Bereinigung nicht stattfinden konnte und der Speicher volllief. ◗ Der verwendete Benutzer steht nicht auf der Negativliste, obwohl dies korrekt wäre.
Typische False Negatives (kritisch)	◗ Der verwendete Benutzer steht auf der Negativliste für das System, obwohl dies nicht korrekt ist. Beispielsweise für ein falsches System oder pauschal eingetragen, oder der Benutzer sollte nicht mehr für die Löschung eingesetzt werden, wurde jedoch nicht in der Negativliste ausgetragen.
Fachliche Beschreibung der Regel	WENN das Ereignis LOG01.* für System Z mit Benutzer U EINTRITT, UND (U,Z) oder (U,*) ist nicht enthalten in <NL_ZUGELASSENENUTZER_01> ODER (U,Z) oder (U,*) ist enthalten in <PL_SENSIBLENUTZER_01> DANN löse aus
Gruppierung	**Empfehlung:** Gruppierung nach System Z **Begründung:** Mehrfache Löschungen von Ereignisprotokollen werden nach betroffenem System zusammengefasst.

→

Optionen und Anmerkungen	◗ Dies ist ein sehr elementarer Use-Case, da ohne ihn die meisten anderen Use-Cases bzw. Regeln nicht funktionieren. ◗ Es wird empfohlen und angenommen, dass der Use-Case für alle Systeme gelten soll. Soll er jedoch nur für eine eingeschränkte Menge angewandt werden, so werden Informationen entweder zu den zu überwachenden oder zu den nicht zu überwachenden Systemen benötigt. ◗ Weitere Einschränkungen wie Uhrzeiten, Quellsysteme des Zugriffs o. Ä. sind ebenfalls denkbar.
Empfohlene Reaktion	Ohne Ereignisprotokolle ist eine Überprüfung von Aktivitäten nicht mehr möglich. Grundsätzlich ist daher anzuraten, Ereignislogs so zeitnah an einen zentralen, durch die üblichen Administratoren nicht zugänglichen Ort zu übertragen, dass ein Löschen von Ereignisprotokollen auf dem System Z nicht die Spuren verwischen kann. Sollten die Daten so vorliegen, so kann auf dieser Basis weiter ermittelt werden. Im Fall des Eintritts ist dann eine unverzügliche Prüfung des Vorgangs und möglicher Ursachen erforderlich. Hier ist auch immer zu bedenken, dass andere Use-Cases ab dem Zeitpunkt der Löschung, falls es tatsächlich aktuelle Logs sind, nicht mehr greifen. Sind nur ältere Ereignisprotokolle betroffen, so ist zumindest die nachträgliche Überprüfbarkeit nicht mehr möglich.
Referenz ATT&CK Techniques	T1070 [D] (Indicator Removal)
Referenz BSI	CON.6 Löschen und Vernichten OPS.1.1.5 Protokollierung
Referenz ATT&CK Tactics	Defense Evasion

3.9.2 B02 – Änderung von Ereignisprotokollen

ID	B02
Name	Änderung von Ereignisprotokollen
Kurzbeschreibung mit Detektionsziel	Erkennen, ob Veränderungen von Ereignisprotokollen stattfanden.
Adressierte Risiken	Ein Angreifer kann Logs verändern, um seine Spuren zu verwischen, Aktivitäten jemand anderem zuzuordnen oder nie stattgefundene Handlungen vorzugeben.
Erforderliche Informationen	◗ Ereignis: – Ereigniscode LOG02 für Änderung von Logs – Benutzer U, der die Aktivität durchführt – Zielsystem Z, auf dem die Aktivität durchgeführt wird ◗ Benutzer je System oder global, die Ereignisprotokolle verändern dürfen
Benötigte Positiv- und Negativlisten	◗ Negativliste <NL_ZUGELASSENENUTZER_01>: Benutzer je System oder global, die Ereignisprotokolle auf dem entsprechenden System ohne Warnmeldung verändern dürfen ◗ Positivliste <PL_SENSIBLENUTZER_01>: Benutzer, die auf dieser Liste stehen, führen immer zu einer Warnmeldung, auch wenn sie in <NL_ZUGELASSENENUTZER_01> enthalten sind (Vorrangigkeit).
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	3 (sehr hoch)
Dringlichkeit	3 (unverzüglich)
Typische True Positives (kritisch)	◗ Angreifer verändern die Ereignisprotokolle, um ihre Spuren zu verwischen oder die Logs aus anderen Gründen zu modifizieren.
Typische True Negatives (unkritisch)	◗ Ein genehmigter automatisierter Bereinigungsvorgang löscht nicht erforderliche Anteile in Logs, bspw. zum Sparen von Speicherplatz, oder anonymisiert Daten darin. Der hierzu verwendete Benutzer steht auf der Negativliste für das System.
Typische False Positives (unkritisch)	◗ Ein genehmigter manueller Eingriff war erforderlich, da eine automatisierte erforderliche Modifikation nicht stattfinden konnte und der Vorgang manuell nachträglich durchgeführt werden muss. ◗ Der verwendete Benutzer steht nicht auf der Negativliste, obwohl dies korrekt wäre.
Typische False Negatives (kritisch)	◗ Der verwendete Benutzer steht auf der Negativliste für das System, obwohl dies nicht korrekt ist. Beispielsweise für ein falsches System oder pauschal eingetragen, oder der Benutzer sollte nicht mehr für die Modifikation eingesetzt werden, wurde jedoch nicht in der Negativliste ausgetragen.
Fachliche Beschreibung der Regel	WENN das Ereignis LOG02.* für System Z mit Benutzer U EINTRITT, UND (U,Z) oder (U,*) ist nicht enthalten in <NL_ZUGELASSENENUTZER_01> ODER (U,Z) oder (U,*) ist enthalten in <PL_SENSIBLENUTZER_01> DANN löse aus
Gruppierung	**Empfehlung:** Gruppierung nach System Z **Begründung:** Mehrfache Änderungen an Ereignisprotokollen werden nach betroffenem System zusammengefasst.

→

Optionen und Anmerkungen	◗ Dies ist ein sehr elementarer Use-Case, da ohne ihn die meisten anderen Use-Cases bzw. Regeln nicht verlässlich funktionieren ◗ Es wird empfohlen und angenommen, dass der Use-Case für alle Systeme gelten soll. Soll er jedoch nur für eine eingeschränkte Menge angewendet werden, so werden Informationen entweder zu den zu überwachenden oder zu den nicht zu überwachenden Systemen benötigt. ◗ Weitere Einschränkungen wie Uhrzeiten, Quellsysteme des Zugriffs o. Ä. sind ebenfalls denkbar.
Empfohlene Reaktion	Ohne korrekte Ereignisprotokolle ist eine Überprüfung von Aktivitäten nicht mehr möglich. Grundsätzlich ist daher anzuraten, Ereignislogs so zeitnah an einen zentralen, durch die üblichen Administratoren nicht zugänglichen Ort zu übertragen, dass eine Modifikation der Ereignisprotokolle auf dem System Z Spuren nicht verfälschen oder löschen kann. Sollten die Daten so vorliegen, dann kann auf dieser Basis weiter ermittelt werden. Im Fall des Eintritts ist eine unverzügliche Prüfung des Vorgangs und möglicher Ursachen erforderlich. Hier ist auch immer zu bedenken, dass andere Use-Cases ab dem Zeitpunkt der Modifikation, falls es tatsächlich aktuelle Logs sind, nicht mehr greifen oder fälschlicherweise aufgrund eingefügter Daten eine Warnmeldung auslösen. Sind nur ältere Ereignisprotokolle betroffen, so ist mindestens die nachträgliche Überprüfbarkeit nicht mehr möglich.
Referenz ATT&CK Techniques	T1070 [G] (Indicator Removal)
Referenz BSI	OPS.1.1.5 Protokollierung
Referenz ATT&CK Tactics	Defense Evasion

3.9.3 B03 – Änderung der Protokollierungsfunktion

ID	B03
Name	Änderung der Protokollierungsfunktion
Kurzbeschreibung mit Detektionsziel	Erkennen, ob eine Änderung der Protokollierungsfunktion, also bspw. der Logumfang, stattgefunden hat.
Adressierte Risiken	Ein Angreifer kann verändern, was in Logs erfasst wird, wie groß sie sind oder Ähnliches. Auf diese Weise werden seine Tätigkeiten nicht erfasst oder zeitnah überschrieben und können entsprechend auch nicht (zuverlässig) überwacht werden.
Erforderliche Informationen	◗ Ereignis: – Ereigniscode LOG03 für Änderung der Protokollierungsfunktion – Benutzer U, der die Aktivität durchführt – Zielsystem Z, auf dem die Aktivität durchgeführt wird ◗ Benutzer je System oder global, die Ereignisprotokolle verändern dürfen
Benötigte Positiv- und Negativlisten	◗ Negativliste <NL_ZUGELASSENENUTZER_01>: Benutzer je System oder global, die die Protokollierungsfunktion auf dem entsprechenden System ohne Warnmeldung verändern dürfen ◗ Positivliste <PL_SENSIBLENUTZER_01>: Benutzer, die auf dieser Liste stehen, führen immer zu einer Warnmeldung, auch wenn sie in <NL_ZUGELASSENENUTZER_01> enthalten sind (Vorrangigkeit).
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	3 (sehr hoch)
Dringlichkeit	3 (unverzüglich)
Typische True Positives (kritisch)	◗ Angreifer verändern die Protokollierungsfunktion, um die Aufzeichnung ihrer Tätigkeiten zu verhindern oder zeitnah überschreiben zu lassen.
Typische True Negatives (unkritisch)	◗ Ein Benutzer, der auf der Negativliste steht, konfiguriert die Protokollierungsfunktion.
Typische False Positives (unkritisch)	◗ Ein genehmigter manueller Eingriff wird durchgeführt, da eine Veränderung der Protokollierungsfunktion erforderlich ist. ◗ Der verwendete Benutzer steht nicht auf der Negativliste, obwohl dies korrekt wäre.
Typische False Negatives (kritisch)	◗ Der verwendete Benutzer steht auf der Negativliste für das System, obwohl dies nicht korrekt ist. Beispielsweise für ein falsches System oder pauschal eingetragen, oder der Benutzer sollte nicht mehr für die Modifikation eingesetzt werden, wurde jedoch nicht in der Negativliste ausgetragen.
Fachliche Beschreibung der Regel	WENN das Ereignis LOG03.* für System Z mit Benutzer U EINTRITT, UND (U,Z) oder (U,*) ist nicht enthalten in <NL_ZUGELASSENENUTZER_01> ODER (U,Z) oder (U,*) ist enthalten in <PL_SENSIBLENUTZER_01> DANN löse aus
Gruppierung	**Empfehlung:** Gruppierung nach System Z **Begründung:** Mehrfache Änderungen an der Protokollierungsfunktion werden nach betroffenem System zusammengefasst.

→

Optionen und Anmerkungen	◗ Dies ist ein sehr elementarer Use-Case, da ohne ihn die meisten anderen Use-Cases bzw. Regeln nicht verlässlich funktionieren. ◗ Es wird empfohlen und angenommen, dass der Use-Case für alle Systeme gelten soll. Soll er jedoch nur für eine eingeschränkte Menge angewendet werden, so werden Informationen entweder zu den zu überwachenden oder zu den nicht zu überwachenden Systemen benötigt. ◗ Weitere Einschränkungen wie Uhrzeiten, Quellsysteme des Zugriffs o. Ä. sind ebenfalls denkbar.
Empfohlene Reaktion	Ohne vollständige Ereignisprotokolle ist eine Überprüfung von Aktivitäten nicht mehr möglich. Grundsätzlich ist daher anzuraten, die Konfiguration der Protokollierungsfunktion regelmäßig dahingehend zu überprüfen, ob das IST dem SOLL entspricht. Im Fall des Eintritts ist eine unverzügliche Prüfung des Vorgangs und möglicher Ursachen erforderlich. Hier ist auch immer zu bedenken, dass andere Use-Cases ab dem Zeitpunkt der Änderung der Protokollierungsfunktion möglicherweise nicht mehr greifen.
Referenz ATT&CK Techniques	T1562 [D] (Impair Defenses)
Referenz BSI	OPS.1.1.5 Protokollierung
Referenz ATT&CK Tactics	Defense Evasion

3.9.4 B04 – Deaktivierung der Protokollierungsfunktion

ID	B04
Name	Deaktivierung der Protokollierungsfunktion
Kurzbeschreibung mit Detektionsziel	Erkennung, ob die Protokollierung deaktiviert wurde.
Adressierte Risiken	Ein Angreifer kann die Aufzeichnung von Logs deaktivieren. Auf diese Weise werden seine Tätigkeiten nicht erfasst und können entsprechend auch nicht (zuverlässig) überwacht werden.
Erforderliche Informationen	◗ Ereignis: – Ereigniscode LOG04 für Deaktivierung der Protokollierungsfunktion – Benutzer U, der die Aktivität durchführt – Zielsystem Z, auf dem die Aktivität durchgeführt wird ◗ Benutzer je System oder global, die Ereignisprotokolle verändern dürfen
Benötigte Positiv- und Negativlisten	◗ Negativliste <NL_ZUGELASSENENUTZER_01>: Benutzer je System oder global, die die Protokollierungsfunktion auf dem entsprechenden System ohne Warnmeldung deaktivieren dürfen ◗ Positivliste <PL_SENSIBLENUTZER_01>: Benutzer, die auf dieser Liste stehen, führen immer zu einer Warnmeldung, auch wenn sie in <NL_ZUGELASSENENUTZER_01> enthalten sind (Vorrangigkeit).
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	3 (sehr hoch)
Dringlichkeit	3 (unverzüglich)
Typische True Positives (kritisch)	◗ Angreifer deaktivieren die Protokollierungsfunktion, um die Aufzeichnung ihrer Tätigkeiten zu verhindern.
Typische True Negatives (unkritisch)	◗ Ein Benutzer, der auf der Negativliste steht, deaktiviert die Protokollierungsfunktion auf einem System, für die die Erfassung der Logs nicht erforderlich ist.
Typische False Positives (unkritisch)	◗ Eine genehmigte manuelle Deaktivierung der Protokollierungsfunktion wird durchgeführt für ein System. ◗ Der verwendete Benutzer steht nicht auf der Negativliste, obwohl dies korrekt wäre.
Typische False Negatives (kritisch)	◗ Der verwendete Benutzer steht auf der Negativliste für das System, obwohl dies nicht korrekt ist. Beispielsweise für ein falsches System oder pauschal eingetragen, oder der Benutzer sollte nicht (mehr) für die Konfiguration eingesetzt werden, wurde jedoch nicht in der Negativliste ausgetragen.
Fachliche Beschreibung der Regel	WENN das Ereignis LOG04.* für System Z mit Benutzer U EINTRITT, UND (U,Z) oder (U,*) ist nicht enthalten in <NL_ZUGELASSENENUTZER_01> ODER (U,Z) oder (U,*) ist enthalten in <PL_SENSIBLENUTZER_01> DANN löse aus
Gruppierung	**Empfehlung:** Gruppierung nach System Z **Begründung:** Wiederholte Deaktivierungen der Protokollierungsfunktion werden nach betroffenem System zusammengefasst.

→

Optionen und Anmerkungen	◗ Dies ist ein sehr elementarer Use-Case, da ohne ihn die meisten anderen Use-Cases bzw. Regeln nicht verlässlich funktionieren. ◗ Es wird empfohlen und angenommen, dass der Use-Case für alle Systeme gelten soll. Soll er jedoch nur für eine eingeschränkte Menge angewandt werden, so werden Informationen entweder zu den zu überwachenden oder zu den nicht zu überwachenden Systemen benötigt. ◗ Weitere Einschränkungen wie Uhrzeiten, Quellsysteme des Zugriffs o. Ä. sind ebenfalls denkbar.
Empfohlene Reaktion	Ohne Ereignisprotokolle ist eine Überprüfung von Aktivitäten nicht möglich. Grundsätzlich ist daher anzuraten, die Konfiguration der Protokollierungsfunktion regelmäßig dahingehend zu überprüfen, ob das IST dem SOLL entspricht. Im Fall des Eintritts ist dann eine unverzügliche Prüfung des Vorgangs und möglicher Ursachen erforderlich. Hier ist auch immer zu bedenken, dass andere Use-Cases ab dem Zeitpunkt der Deaktivierung der Protokollierungsfunktion möglicherweise nicht mehr greifen.
Referenz ATT&CK Techniques	T1562 [D] (Impair Defenses)
Referenz BSI	OPS.1.1.5 Protokollierung
Referenz ATT&CK Tactics	Defense Evasion

3.9.5 B05 – Änderung von sicherheitsrelevanten Konfigurationseinstellungen

ID	B05
Name	Änderung von sicherheitsrelevanten Konfigurationseinstellungen
Kurzbeschreibung mit Detektionsziel	Konfigurationen, die die Sicherheit von Systemen regeln, bspw. Passwortlängen, ob Passwortanmeldungen zulässig sind oder überhaupt benötigt werden, welche SSL/TLS-Anmeldeverfahren zulässig sind usw., werden verändert.
Adressierte Risiken	Veränderungen der Sicherheitskonfigurationen sind ein potenzielles Risiko: Die damit einhergehenden Abweichungen von der Sollkonfiguration können den Geschäftsbetrieb einschränken oder gefährden. Zum einen können versierte Angreifer dadurch unbefugt das gewünschte Sicherheitsniveau herabsetzen. Im Erfolgsfall bleiben im Nachgang die schädlichen Aktivitäten der Angreifer unerkannt. Zum anderen können unbeabsichtigte Veränderungen der Sicherheitskonfigurationen auch nach Updates oder Patches von softwarebasierten Sicherheitslösungen auftreten. Daher ist es erforderlich, nach entsprechender Umsetzung neben der Funktionalität auch die Sicherheitseinstellungen daraufhin zu überprüfen, ob die definierten Standardeinstellungen weiterhin korrekt konfiguriert sind.
Erforderliche Informationen	◗ Ereigniscode CONFIG02 für die zu überwachenden Konfigurationen ◗ Z: Betroffenes Sicherheitssystem ◗ Q: Quellsystem des Zugriffs ◗ Liste der zu überwachenden Sicherheitssysteme (IPs oder Hostnamen), auf denen sicherheitsrelevante Konfigurationen verwaltet werden ◗ Liste der Quellen (IPs oder Hostnamen), die auf die zu überwachenden Geräte zugreifen dürfen (optional)
Benötigte Positiv- und Negativlisten	◗ Negativliste <NL_SICHERHEITSSYSTEME_01>: Diese Liste enthält Sicherheitssysteme (IPs oder Hostnamen), die temporär von der Überwachung ausgenommen werden sollen. Dies kann bei genehmigten Aktualisierungen der Konfiguration oder vor der Liveschaltung neuer Systeme erforderlich sein.
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	2 (hoch)
Dringlichkeit	2 (schnell)
Typische True Positives (kritisch)	◗ Es wurden sicherheitsrelevante Konfigurationen durch nicht autorisierte Personen oder Systeme verändert.
Typische True Negatives (unkritisch)	◗ Es wurden durch autorisierte Personen oder Systeme genehmigte Konfigurationsänderungen auf zu überwachenden Systemen durchgeführt.
Typische False Positives (unkritisch)	◗ Es wurden Konfigurationsänderungen auf Systemen erkannt, die versehentlich nicht in die Negativliste <NL_SICHERHEITSSYSTEME_01> aufgenommen wurden. Obwohl diese Systeme von der Überwachung auszunehmen sind, werden sie fälschlicherweise geprüft und es kommt bei Änderungen zu Fehlalarmen.
Typische False Negatives (kritisch)	◗ Sicherheitsrelevante Konfigurationsänderungen erzeugen nicht das Ereignis CONFIG02. Sie werden daher nicht erkannt. ◗ Z ist fälschlicherweise in <NL_SICHERHEITSSYSTEME_01> aufgenommen.
Fachliche Beschreibung der Regel	WENN Ereignis CONFIG02 für System Z (von Quelle Q) - optional EINTRITT, UND Z ist nicht enthalten in <NL_SICHERHEITSSYSTEME_01> DANN löse aus
Gruppierung	**Empfehlung:** Gruppierung nach Zielsystem Z **Begründung:** Mehrfache Änderungen je System werden zusammengefasst.

→

Optionen und Anmerkungen	◗ In kleineren Umgebungen sollte der Use-Case generell für alle Konfigurationsereignisse eingerichtet werden. In größeren Umgebungen ist es aufgrund der Fülle der zu erwartenden Meldungen sinnvoll, die Zugriffe, die von legitimen Quellen (z. B. dedizierte Managementsysteme) erfolgen, als Ausnahme zu definieren und nicht zu überwachen (siehe optionale Liste). ◗ Am Markt sind dedizierte Security-Management-Systeme verfügbar. Die Einsatzmöglichkeiten derartiger Software ergänzen diesen Use-Case.
Empfohlene Reaktion	Zeitnahe Prüfung, ob die festgestellte Änderung erwünscht und legitim ist. Gegebenenfalls geht mit ihr eine Sicherheitslücke oder eine Einschränkung des gewünschten Datenverkehrs einher.
Referenz ATT&CK Techniques	T1562 [D] (Impair Defenses), T1553 [G] (Subvert Trust Controls), T1543 [G] (Create or Modify System Process)
Referenz BSI	OPS.1.1.3 Patch- und Änderungsmanagement
Referenz ATT&CK Tactics	Persistence, Privilege Escalation, Defense Evasion

3.9.6 B06 – Deaktivierung von Sicherheitslösungen

ID	B06
Name	Deaktivierung von Sicherheitslösungen
Kurzbeschreibung mit Detektionsziel	Werden Sicherheitslösungen wie Antivirussoftware, Application Firewalls, IDS-Systeme oder Ähnliches deaktiviert, so wird zum einen der Erkennung die Grundlage zur Forensik entzogen, zum anderen aber auch der Schutz des Netzes deutlich reduziert. Hinweise auf diesen Use-Case sind dringend zu überprüfen.
Adressierte Risiken	Die Deaktivierung von Sicherheitslösungen kann bedeuten, dass ein Sicherheitsvorfall vorliegt. Dabei versuchen Angreifer ihre Aktivitäten zu verschleiern, indem sie zur Vorbereitung einer Attacke die Sicherheitssysteme außer Funktion setzen.
Erforderliche Informationen	◗ Benutzer B ◗ Ereigniscode APP02 ◗ IDS-Logs, AV-Logs, Firewall-Logs, Systemlogs und Ähnliches; dazu Prozessname der entsprechenden Sicherheitskomponente (bspw. On-Demand-Virusscanner-Agent) ◗ Liste <GL_SICHERHEITSKOMPONENTE_01>: Prozessnamen P der zu überwachenden Sicherheitslösungen, ggf. mit System Z
Benötigte Positiv- und Negativlisten	◗ Negativliste <NL_NUTZER_01> der Benutzer, die die entsprechenden Prozesse deaktivieren dürfen (bspw. bei Shutdowns Systemprozesse und Ähnliches)
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	3 (sehr hoch)
Dringlichkeit	3 (unverzüglich)
Typische True Positives (kritisch)	◗ Eine zu überwachende Sicherheitslösung wurde auf dem System unberechtigterweise deaktiviert.
Typische True Negatives (unkritisch)	◗ Ein Prozess wird beendet, der keine Sicherheitslösung ist und entsprechend auch nicht auf der Liste der Sicherheitslösungen steht. ◗ Eine Sicherheitslösung wurde gestoppt, aber durch einen dazu befugten Benutzer.
Typische False Positives (unkritisch)	◗ Eine zu überwachende Sicherheitslösung ist auf dem Quellsystem ausgefallen. Die Ursache war ein technisch bedingter Systemfehler, der nicht mit böser Absicht zur Verschleierung durchgeführt wurde.
Typische False Negatives (kritisch)	◗ Es wurde vergessen, Prozesse von Sicherheitslösungen in die Liste aufzunehmen, die eigentlich überwacht werden sollen. Eine ungewollte Deaktivierung löst daher keine Warnmeldung aus.
Fachliche Beschreibung der Regel	WENN Ereignis APP02.* mit Benutzer B EINTRITT, UND P ist enthalten in Liste <GL_SICHERHEITSKOMPONENTE_01> UND B ist nicht enthalten in <NL_NUTZER_01> DANN löse aus
Gruppierung	**Empfehlung:** Gruppierung nach Prozessnamen P der Sicherheitslösung **Begründung:** Sicherheitslösungen könnten aufgrund eines Fehlers oder eines Angreifers deaktiviert worden sein. Dies kann, bspw. im Fall von Agenten, bei Fehlern schnell auf vielen Systemen gleichzeitig geschehen. Nach der Sicherheitslösung zu gruppieren, verhindert eine Flut von Warnmeldungen und zeigt gleichzeitig auf, wenn mehrere Sicherheitslösungen betroffen sind.

→

Optionen und Anmerkungen	Alltägliche Problemfälle sollten bedacht und berücksichtigt werden. ◗ Beispiel Problemfall: Neustart von System, Warnung bzw. Probleme auf Clients/Servern Zur Lösung dieser Fälle empfiehlt sich die Nutzung einer weiteren Wartungsliste (= Negativliste): Je nach gewünschter Granularität der Überwachung können hierbei in einem gegebenen Zeitfenster bestimmte Prozesse auf allen Logquellen deaktiviert werden (flächendeckender Rollout/Update) oder die Überwachung bestimmter Prozesse wird nur für dedizierte Logquellen (z. B. am AV-Management bei Update der AV-Scanner-Software) deaktiviert. ◗ Bei einer bestimmten Sicherheitslösung kann ein Prozess nicht direkt überwacht werden, sondern nur der Heartbeat (Übertragung von Ereignissen im erwarteten Turnus). Dann ist diesen Meldungen besondere Gewichtung zu geben, wenn sie ausbleiben. ◗ Es gibt Fälle, in denen kein Prozessstopp stattfindet, sondern nur die Konfiguration entsprechend verändert wird. Dies ist für die einzelnen eingesetzten Lösungen zu prüfen.
Empfohlene Reaktion	Beim Auftreten einer validierten Warnmeldung sollte die Ursache möglichst unverzüglich untersucht werden. Es könnte Gefahr im Verzug sein.
Referenz ATT&CK Techniques	T1562 [D] (Impair Defenses)
Referenz BSI	OPS.1.1.1 Allgemeiner IT-Betrieb OPS.1.1.7 Systemmanagement
Referenz ATT&CK Tactics	Defense Evasion

3.9.7 B07 – Verwendung spezieller Benutzerkonten

ID	B07
Name	Verwendung spezieller Benutzerkonten
Kurzbeschreibung mit Detektionsziel	Spezielle Benutzerkonten, z. B. Notfallkonten oder fest eingebaute Benutzerkonten, in Applikationen oder Systemen, die sonst nicht verwendet werden dürfen, werden plötzlich verwendet (bspw. SAP* in SAP). Dies ist ein typisches Angriffsmuster, gerade für existierende Benutzerkonten.
Adressierte Risiken	Spezielle Benutzerkonten können für Angriffe genutzt werden. Zudem sind sie oft nicht deaktivierbar, sodass Versuche der Nutzung schnell erkannt werden müssen.
Erforderliche Informationen	◗ Ereignis: – Ereigniscode für Logins, erfolgreich AUTH01.succ und fehlgeschlagen AUTH01.fail – Benutzer B, der die Aktivität durchführt – Zielsystem Z, auf dem die Aktivität durchgeführt wird ◗ Liste <GL_SPEZIELLENUTZER_01>: spezielle Benutzerkonten, bei deren Login auf einem spezifischen System oder global hingewiesen werden soll
Benötigte Positiv- und Negativlisten	◗ Negativliste <NL_ZUGELASSENENUTZER_01>: Benutzerkonten je System oder global, bei denen dieses Verhalten zugelassen wird (bspw. wegen Nutzung durch andere Fremdsysteme zur Integration) ◗ Negativliste <NL_ZUGELASSENESYSTEME_01>: Systeme, bei denen dieses Verhalten zugelassen wird (bspw. wegen bekannten technischen Fehlimplementierungen oder aufgrund ihrer Netzexponiertheit)
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	Entspricht SBF
Dringlichkeit	2 (schnell)
Typische True Positives (kritisch)	◗ Angreifer probieren verschiedene Passwörter für ein Benutzerkonto und schaffen es, Zugang zu erhalten. ◗ Angreifer haben das Passwort für einen Notfallbenutzer erfahren und nutzen die hohen Privilegien für ihre Aktivitäten.
Typische True Negatives (unkritisch)	◗ Ein eingebautes Benutzerkonto wird auf einem System, für das die Nutzung zulässig ist, verwendet. ◗ Ein anderes Benutzerkonto als solche, die auf der Positivliste stehen, wird verwendet.
Typische False Positives (unkritisch)	◗ Ein automatisierter und für diesen Zweck autorisierter Prozess versucht sich an einem System anzumelden, jedoch ist das eingestellte Passwort falsch. ◗ Ein Benutzerkonto auf der Positivliste wird im Rahmen einer befugten Tätigkeit irrtümlich verwendet, weil ein Benutzer dieses in einer im Internet verfügbaren Dokumentation gelesen hat und nicht wusste oder übersah, dass für die internen Zwecke ein eigenes spezifisches Benutzerkonto angelegt wurde.
Typische False Negatives (kritisch)	◗ Benutzerkonten/Systeme stehen auf Negativlisten, obwohl dies inkorrekt ist. ◗ Nicht alle speziellen Benutzerkonten sind in der Positivliste erfasst, z. B. weil neu eingebaute Benutzerkonten unbemerkt bei einem Update hinzugekommen sind.
Fachliche Beschreibung der Regel	WENN das Ereignis AUTH01.* für System Z mit Benutzer B EINTRITT, UND (B,Z) oder (B,*) sind enthalten in <GL_SPEZIELLENUTZER_01> UND (B,Z) oder (B,*) ist nicht enthalten in <NL_ZUGELASSENENUTZER_01> UND Z ist nicht enthalten in <NL_ZUGELASSENESYSTEME_01> DANN löse aus
Gruppierung	**Empfehlung:** Gruppierung nach Kombination Benutzer und System (B,Z) **Begründung:** So ist eine Identifikation der betroffenen Benutzer mit einzelnen Systemen möglich.

→

Optionen und Anmerkungen	◗ Die Wahl der Ereignisse, die die Systeme für AUTH01.succ und AUTH01.fail verwenden und die in der technischen Implementierung des Use-Case berücksichtigt werden, müssen sorgfältig gewählt und insbesondere bei Systemupdates regelmäßig überprüft werden. Beispielsweise könnten durch ein Update andere oder neue Ereignisse für spezifische Situationen geschrieben werden, die dann nicht berücksichtigt werden. ◗ Gegebenenfalls lohnt es sich zudem, das Quellsystem Q zu berücksichtigen: Anstelle der Kombination <B,Z> könnte <B,Q,Z> verwendet werden. Dies kann False-Positive-Befunde wie die Benutzung einiger weniger spezieller Benutzerkonten durch mehrere Personen reduzieren, jedoch auch bei Angriffen von mehreren Quellen gleichzeitig eine rechtzeitige Erkennung verhindern. Auch hier empfiehlt sich eine differenzierte Betrachtung. ◗ Die Liste der vorhandenen eingebauten Benutzerkonten muss regelmäßig geprüft werden, insbesondere nach Updates der entsprechenden Software bzw. des Systems.
Empfohlene Reaktion	Die typischen False-Positive-Szenarien sollten schnell geprüft werden, da bei einem tatsächlichen Angriff ein Angreifer sich bereits erfolgreich Zugang verschafft hat.
Referenz ATT&CK Techniques	T1078 [D] (Valid Accounts)
Referenz BSI	ORP.4 Identitäts- und Berechtigungsmanagement
Referenz ATT&CK Tactics	Initial Access, Defense Evasion

3.9.8 B08 – Erkennung von Brute-Force-Angriffen (mehrere Benutzerkonten)

ID	B08
Name	Erkennung von Brute-Force-Angriffen (mehrere Benutzerkonten)
Kurzbeschreibung mit Detektionsziel	Erkennung von versuchten Anmeldungen mit vielen unterschiedlichen Benutzern innerhalb kurzer Zeit (hohe Zahlen wie > 100 in einer Minute von den gleichen oder von wenigen Quellen)
Adressierte Risiken	Brute-Force-Angriffe dienen dem Zweck, Passwörter zu Zugängen zu erraten. Dies geschieht automatisiert bspw. mithilfe von Hackertools unter Verwendung von im Vorfeld extrahierten Benutzern oder teilweise sogar Benutzerlisten in Kombination mit gängigen Passwortlisten. Die Idee dieses Use-Case geht davon aus, dass die Hackertools auf wenigen gekaperten Geräten installiert werden (Quellen) und von dort die Angriffe ins interne Netz erfolgen. Oft werden dann die Benutzerlisten passwortweise abgearbeitet. Dadurch können auf einem Ziel minütlich Hunderte von Anfragen eingehen. Ohne entsprechende Erkennungs- und Behandlungsmaßnahmen besteht das Risiko, dass wichtige Benutzerkonten kompromittiert werden.
Erforderliche Informationen	◗ Ereignis: – Ereigniscode AUTH01.fail für abgelehnte Anmeldung – Benutzer B1 bis Bn, für die eine Anmeldung durchzuführen versucht wird – Zielsystem Z, auf dem die Aktivität durchgeführt wird – Schwellenwert thr_Login für die Anzahl der versuchten Anmeldungen pro Zeiteinheit, z. B. > 100/min – Schwellenwert thr_Benutzer für die Anzahl von verschiedenen Benutzern, die sich pro Zeiteinheit anzumelden versuchen, z. B. > 5/min – Quellsystem Q, von dem aus die Aktivität durchgeführt wird
Benötigte Positiv- und Negativlisten	◗ Negativliste <NL_SYSTEME_01>: IP-Adressen oder Hostnamen der Systeme, deren Logins mit diesem Use-Case nicht zu überwachen sind
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	2 (hoch)
Dringlichkeit	1 (normal) für Benutzerkonten 2 (schnell) für privilegierte Konten 3 (unverzüglich) für besonders privilegierte Konten wie bspw. Domänenadministratoren
Typische True Positives (kritisch)	◗ Es gelingt dem Angreifer, sich an einem Zielsystem aus der Positivliste erfolgreich anzumelden, das führt zu einer erwünschten Warnmeldung.
Typische True Negatives (unkritisch)	◗ Es gelingt dem Angreifer, sich an einem Zielsystem erfolgreich anzumelden, das nicht in der Positivliste steht und auch nicht überwacht werden muss.
Typische False Positives (unkritisch)	◗ Es gelingt dem Angreifer, sich an einem Zielsystem erfolgreich anzumelden, das führt zu einer Warnmeldung. Das System muss nicht überwacht werden, wurde aber versehentlich in die Positivliste eingetragen.
Typische False Negatives (kritisch)	◗ Es gelingt dem Angreifer, sich an einem zu überwachenden Zielsystem erfolgreich anzumelden. Versehentlich wurde das betreffende Zielsystem nicht in die Positivliste aufgenommen, daher erfolgt keine Warnmeldung.

→

Fachliche Beschreibung der Regel	WENN das Ereignis AUTH01.fail für Benutzer (B1,...,Bn) auf Zielsystem Z EINTRITT, UND Z ist nicht enthalten in <NL_SYSTEME_01> UND Auftreten > thr_Login UND n > Schwellenwert thr_Benutzer DANN löse aus Empfohlene Schwellenwerte: thr_Login = 100/min, thr_Benutzer = 5
Gruppierung	**Empfehlung:** Gruppierung nach der Kombination Quellsystem und Zielsystem (Q,Z) **Begründung:** Da mehrere Benutzer je System ausprobiert werden, eignet sich eine Gruppierung nach Benutzer nicht. Über die Kombination Quell- und Zielsystem lassen sich sinnvolle Gruppen bilden.
Optionen und Anmerkungen	◗ Um Brute-Force-Angriffe zu erschweren, werden flankierende Maßnahmen als Teil des Sicherheitskonzepts empfohlen. So kann bspw. die Anzahl der zulässigen Eingabeversuche reglementiert werden. Bei fehlerhaften Logins ist ebenfalls denkbar, weitere Eingaben für einen bestimmten Zeitraum zu verweigern. ◗ Sinnvolle Schwellenwerte sind stark abhängig von der Quellhardware, die die Angreifer ausgewählt haben, und dem Angriffsaufbau. Die angegebenen Werte sollten aber für eine Erkennung ausreichend empfindlich sein.
Empfohlene Reaktion	Bei Brute-Force-Angriffen kann eine Vielzahl an Warnmeldungen eintreffen. Diese sollten entsprechend der Kritikalität der kompromittierten Zielsysteme bearbeitet werden.
Referenz ATT&CK Techniques	T1110 [D] (Brute Force), T1087 [G] (Account Discovery)
Referenz BSI	ORP.4 Identitäts- und Berechtigungsmanagement
Referenz ATT&CK Tactics	Credential Access, Discovery

3.9.9 B09 – Erkennung von Brute-Force-Angriffen (einzelnes Benutzerkonto)

ID	B09
Name	Erkennung von Brute-Force-Angriffen (einzelnes Benutzerkonto)
Kurzbeschreibung mit Detektionsziel	Erkennung zahlreicher versuchter Anmeldungen mit einem Benutzer innerhalb kurzer Zeit (sehr hohe Zahlen wie > 1.000 pro Stunde)
Adressierte Risiken	Brute-Force-Angriffe dienen dem Zweck, Passwörter zu Zugängen zu erraten. Dies geschieht automatisiert bspw. mithilfe von Hackertools unter Verwendung von einem im Vorfeld extrahierten Benutzerkonto in Kombination mit gängigen Passwortlisten. Die Idee dieses Use-Case geht davon aus, dass dem Angreifer ein Benutzername bereits bekannt ist. Es wird dann automatisiert versucht, sich mit diesem Account unter Verwendung von Passwortlisten oder per zufälligen Zeichenkombinationen an möglichst vielen Geräten anzumelden. Dadurch können stündlich 5-stellige Anmeldeversuche auftreten. Dieses Verhalten wird zur Erkennung derartiger Angriffe genutzt. Ohne entsprechende Erkennungs- und Behandlungsmaßnahmen besteht das Risiko, dass auch wichtige Benutzerkonten kompromittiert werden.
Erforderliche Informationen	◗ Ereignis: – Ereigniscode AUTH01.fail für abgelehnte Anmeldung – Benutzer B, für den eine Anmeldung durchzuführen versucht wird – Zielsystem Z, auf dem die Aktivität durchgeführt wird – Schwellenwert thr_Login für die Anzahl der versuchten Anmeldungen pro Zeiteinheit, z. B. > 500/Stunde – Optional: Quellsystem Q, von dem aus die Aktivität durchgeführt wird
Benötigte Positiv- und Negativlisten	◗ Negativliste <NL_SYSTEME_01>: IP-Adressen oder Hostnamen der Systeme, deren Logins nicht mit diesem Use-Case zu überwachen sind
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	2 (hoch)
Dringlichkeit	1 (normal) für Benutzerkonten 2 (schnell) für privilegierte Konten 3 (unverzüglich) für besonders privilegierte Konten wie bspw. Domänenadministratoren
Typische True Positives (kritisch)	◗ Es gelingt dem Angreifer, sich an einem Zielsystem aus der Positivliste erfolgreich anzumelden, das führt zu einer erwünschten Warnmeldung.
Typische True Negatives (unkritisch)	◗ Es gelingt dem Angreifer, sich an einem Zielsystem erfolgreich anzumelden, das nicht in der Positivliste steht und auch nicht überwacht werden muss.
Typische False Positives (unkritisch)	◗ Es gelingt dem Angreifer, sich an einem Zielsystem erfolgreich anzumelden, das führt zu einer Warnmeldung. Das System muss nicht überwacht werden, wurde aber versehentlich in die Positivliste eingetragen.
Typische False Negatives (kritisch)	◗ Es gelingt dem Angreifer, sich an einem zu überwachenden Zielsystem erfolgreich anzumelden. Versehentlich wurde das betreffende Zielsystem nicht in die Positivliste aufgenommen, daher erfolgt keine Warnmeldung.

→

Fachliche Beschreibung der Regel	WENN das Ereignis AUTH01.fail für Benutzer B auf Zielsystem Z EINTRITT, UND Auftreten > thr_Login UND Z ist nicht enthalten in <NL_SYSTEME_01> DANN löse aus Empfohlener Schwellenwert: thr_Login = 1.000/Stunde
Gruppierung	**Empfehlung:** Gruppierung nach der Kombination Benutzer und System (B,Z) **Begründung:** So lassen sich die betroffenen Benutzer und Systeme schnell identifizieren.
Optionen und Anmerkungen	◗ Um Brute-Force-Angriffe zu erschweren, werden flankierende Maßnahmen als Teil des Sicherheitskonzepts empfohlen. So kann bspw. die Anzahl der zulässigen Eingabeversuche reglementiert werden. Bei fehlerhaften Logins ist ebenfalls denkbar, weitere Eingaben für einen bestimmten Zeitraum zu verweigern. ◗ Sinnvolle Schwellenwerte sind stark abhängig von der Quellhardware, die die Angreifer ausgewählt haben, und dem Angriffsaufbau. Der angegebene Wert sollte aber für eine Erkennung ausreichend empfindlich sein. ◗ Das Loggen des Quellsystems ist für die Anwendung der fachlichen Regel nicht erforderlich. Diese Daten erleichtern aber die forensische Arbeit, wenn im Nachhinein der Angriffsvektor untersucht werden soll (daher optional).
Empfohlene Reaktion	Bei Brute-Force-Angriffen kann eine Vielzahl an Warnmeldungen eintreffen. Diese sollten entsprechend der Kritikalität der kompromittierten Zielsysteme bearbeitet werden.
Referenz ATT&CK Techniques	T1110 [D] (Brute Force), T1087 [G] (Account Discovery)
Referenz BSI	ORP.4 Identitäts- und Berechtigungsmanagement
Referenz ATT&CK Tactics	Credential Access, Discovery

3.9.10 B10 – Ausfall Zeitsynchronisationsdienst

ID	B10
Name	Ausfall Zeitsynchronisationsdienst
Kurzbeschreibung mit Detektionsziel	Der Ausfall der automatischen Zeitsynchronisation wird gemeldet und/oder erkannt.
Adressierte Risiken	Zeitsynchronisation ist notwendig, um Logfiles verschiedener Geräte zusammenführen und korrelieren zu können. Zeitsynchronisation ist außerdem für zeitabhängige Authentifizierungsinformationen, z. B. Kerberos-Tickets oder TOTP, erforderlich. Ein Ausfall des Zeitsynchronisationsdienstes kann zu fehlerhaften Logfiles bzw. Fehlern bei der Authentifizierung führen.
Erforderliche Informationen	Informationen, ob der Zeitsynchronisationsdienst läuft. Dies kann aktiv, z. B. durch ein Monitoring-System, das an das SIEM meldet, oder passiv, z. B. durch das Betriebssystem selbst, geprüft werden. ◗ Ereigniscode APP03 ◗ Zeitdienst D ◗ Zielsystem Z, auf dem die Aktivität durchgeführt wird Der Zeitdienst D kann bspw. ein NTP- oder PTP-Daemon sein mit Einträgen bspw. wie folgt: Logfile: time sync service failure, monitoring: alert time sync service not active
Benötigte Positiv- und Negativlisten	◗ Negativliste <NL_OHNEZEITSYNCHRONISIERUNG_01>: IP-Adressen oder Hostnamen, auf denen kein Zeitsynchronisationsdienst läuft
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	2 (hoch)
Dringlichkeit	1 (normal)
Typische True Positives (kritisch)	◗ Der Zeitsynchronisationsdienst ist ausgefallen. ◗ Der Zeitsynchronisationsdienst kann seine Zeitserver nicht mehr erreichen und sich deshalb nicht mehr synchronisieren. ◗ Der Zeitsynchronisationsdienst hat eine ungültige/korrupte Konfiguration und funktioniert deshalb nicht mehr wie erwartet.
Typische True Negatives (unkritisch)	◗ Auf einem System läuft kein Zeitsynchronisationsdienst und das System steht auf der Negativliste <NL_OHNEZEITSYNCHRONISIERUNG_01>.
Typische False Positives (unkritisch)	◗ Ein System ohne Zeitsynchronisationsdienst steht nicht auf der Negativliste <NL_OHNEZEITSYNCHRONISIERUNG_01>. ◗ Das Monitoring kann einen Zeitsynchronisationsdienst z. B. aufgrund eines Netzfehlers nicht mehr erreichen/abfragen, obwohl der Zeitsynchronisationsdienst normal läuft.
Typische False Negatives (kritisch)	◗ Ein System steht auf der Negativliste <NL_OHNEZEITSYNCHRONISIERUNG_01>, obwohl ein Zeitsynchronisationsdienst läuft und dieser Dienst überwacht werden sollte.
Fachliche Beschreibung der Regel	WENN das Ereignis APP03.fail für Dienst D für System Z EINTRITT, UND System Z ist nicht enthalten in <NL_OHNEZEITSYNCHRONISIERUNG_01> DANN löse aus
Gruppierung	**Empfehlung:** Gruppierung nach System Z **Begründung:** Wiederholte Ausfälle des Zeitsynchronisationsdienstes werden zusammengefasst.
Optionen und Anmerkungen	◗ Logfiles können entweder vom Betriebssystem bzw. Zeitsynchronisationsdienst selbst oder von einer Monitoring-Instanz erzeugt werden, die z. B. die Erreichbarkeit eines Zeitservers prüft.
Empfohlene Reaktion	Sofern eine Fehlerursache erkennbar ist, muss diese beseitigt werden. Anschließend muss der Dienst neu gestartet werden.
Referenz ATT&CK Techniques	T1562 [G] (Impair Defenses)
Referenz BSI	OPS.1.2.6 NTP-Zeitsynchronisation
Referenz ATT&CK Tactics	Reconnaissance

3.9.11 B11 – Unautorisierte Änderung der Systemzeit

ID	B11
Name	Unautorisierte Änderung der Systemzeit
Kurzbeschreibung mit Detektionsziel	Die Systemzeit wird durch einen nicht freigegebenen Benutzer verändert, sodass möglicherweise auch Logs nicht mehr mit richtigem Zeitstempel versehen und von einem SIEM korrekt ausgewertet werden können. Ausnahmefälle sind Änderungen durch Zeitservice-Aktualisierungen und freigegebene Sonderfälle (bspw. Störungsbeseitigung oder initiales Setup).
Adressierte Risiken	Durch eine vorsätzliche Veränderung der Systemzeit kann ein Angreifer Logs stören, aber auch zeitabhängige Authentisierungsdaten wie Kerberos-Tickets, Session Cookies oder TOTP missbrauchen, um sich unerlaubten Zugriff auf ein System zu verschaffen.
Erforderliche Informationen	◗ Ereigniscode TIME01 mit Zeitänderung (Delta) DELTA: Informationen über Abweichungen zur gültigen Systemzeit, z. B. Sprünge der Systemzeit zurück oder nach vorne ◗ Benutzer B, der die Zeitänderung durchführt ◗ Zielsystem Z, auf dem die Aktivität durchgeführt wird ◗ Maximaler Schwellenwert MAX_D der Zeitveränderung
Benötigte Positiv- und Negativlisten	◗ Negativliste <NL_OHNEZEITSYNCHRONISIERUNG_01>: IP-Adressen oder Hostnamen, auf denen kein Zeitsynchronisationsdienst konfiguriert ist oder konfiguriert werden kann ◗ Negativliste <NL_ZUGELASSENENUTZER_01>: Benutzer, die die Zeit verändern dürfen. Hierzu sollte typischerweise der Benutzer des Zeitsynchronisationsdienstes gehören.
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	2 (hoch)
Dringlichkeit	2 (schnell)
Typische True Positives (kritisch)	◗ Ein Angreifer verändert vorsätzlich die Systemzeit, typischerweise auf eine frühere Zeit.
Typische True Negatives (unkritisch)	◗ Ein System, das auf der Negativliste <NL_OHNEZEITSYNCHRONISIERUNG_01> steht, wird manuell auf die richtige Zeit konfiguriert. ◗ Ein System wird durch einen dafür befugten Benutzer verändert.
Typische False Positives (unkritisch)	◗ Ein System ohne Zeitsynchronisationsdienst steht nicht auf der Negativliste <NL_OHNEZEITSYNCHRONISIERUNG_01>. ◗ Ein System, das neu startet, wird erstmalig mit einem Zeitsynchronisationsdienst synchronisiert und springt deshalb um einen großen Wert, z. B. vom 01.01.1970 auf die aktuelle Zeit. Der durchführende Benutzer bzw. das System selbst steht auf keiner Negativliste. ◗ Ein berechtigter Administrator setzt manuell die Zeit auf einen anderen bzw. den richtigen Wert. Das kann notwendig sein, wenn die Abweichung zum NTP-Server für eine automatische Anpassung zu groß ist.
Typische False Negatives (kritisch)	◗ Ein System steht fälschlicherweise auf der Negativliste <NL_OHNEZEITSYNCHRONISIERUNG_01>. ◗ Ein Benutzer steht fälschlicherweise auf der Negativliste <NL_ZUGELASSENENUTZER_01>.

→

Fachliche Beschreibung der Regel	WENN Ereignis TIME01 mit dem Benutzer B für System Z EINTRITT, UND DELTA < -MAX_D ODER DELTA > MAX_D UND System Z ist nicht enthalten in <NL_OHNEZEITSYNCHRONISIERUNG_01> UND Benutzer B ist nicht enthalten in <NL_ZUGELASSENENUTZER_01> DANN löse aus Empfohlener Schwellenwert: MAX_D = 1 Sekunde
Gruppierung	**Empfehlung:** Gruppierung nach Z **Begründung:** Mehrfache Änderungen der Systemzeit werden je betroffenem System zusammengefasst.
Optionen und Anmerkungen	◗ Die Regel berücksichtigt nur die Systemzeit als UTC, die sich auch bei Wechsel von Sommer- und Winterzeit nicht ändert. Wenn nur eine Abfrage der relativen Systemzeit möglich ist, müssen Sommer- und Winterzeitwechsel ggf. berücksichtigt werden. Dies kann bspw. über die Aufnahme der entsprechenden vom System verwendeten Benutzer in die Negativliste abgebildet werden. ◗ Zum Teil sind Systeme nicht in der Lage, Zeitwechsel mit dem Wert der Zeitänderung zu protokollieren. In einem solchen Fall kann die Implementierung schwierig sein. Dies kann gelöst werden, indem der Delta-Vergleich ausgelassen wird und jegliche Zeitveränderung, die nicht über Negativlisten ausgeschlossen ist, eine Warnmeldung auslöst (effektiv MAX_D = 0). **Hinweis:** Die Regel erkennt nicht, wenn die Zeit schleichend unterhalb des Schwellenwerts angepasst wird, z. B. immer nur eine Zehntelsekunde pro Minute.
Empfohlene Reaktion	Da viele Dienste von einer korrekten Systemzeit abhängen, sollte auf ein Ereignis sofort reagiert werden, um die Ursache zu ermitteln.
Referenz ATT&CK Techniques	T1562 [G] (Impair Defenses), T1070 [G] (Indicator Removal)
Referenz BSI	OPS.1.2.6 NTP-Zeitsynchronisation
Referenz ATT&CK Tactics	Defense Evasion

3.9.12 B12 – Ungenehmigter Start oder Stopp einer Anwendung oder eines Service

ID	B12
Name	Ungenehmigter Start oder Stopp einer Anwendung oder eines Service
Kurzbeschreibung mit Detektionsziel	Es soll erkannt werden, wenn eine Anwendung oder ein Service auf ungewöhnliche Weise oder zu unüblichen Zeitfenstern gestartet oder gestoppt wird.
Adressierte Risiken	Angreifer können großen Schaden anrichten, indem sie elementar wichtige Systeme oder Services stoppen, bspw. Backup-Systeme, oder Konfigurationen ändern und anschließend neu starten.
Erforderliche Informationen	◗ Ereigniscodes APP01 bzw. APP02 ◗ System bzw. Service oder Prozess APP ◗ Zeitfenster für Start und Stopp je APP ◗ System Z, auf dem der Service oder Prozess gestartet oder gestoppt wird ◗ Liste an Benutzern, die auch außerhalb der Zeitfenster oder grundsätzlich APP starten bzw. stoppen dürfen ◗ Liste der zulässigen Zeitfenster je APP ◗ Liste an zu überwachenden APPs
Benötigte Positiv- und Negativlisten	Da typischerweise nur bestimmte Systeme und Services bei Start bzw. Stopp alarmiert werden sollen, muss eine Auswahl getroffen werden: ◗ <GL_APPS>: Liste mit zu überwachenden APPs, global oder je System Z in Form (APP,Z) Die Ereignisse APP01 und APP02 sollen für diese grundsätzlich eine Warnmeldung ausgeben, sofern sie nicht wie folgt ausgenommen sind: ◗ Negativliste <NL_ZUGELASSENENUTZER_01>: Benutzer, die global, je System oder in speziellen Verbindungen die APP starten oder stoppen dürfen. Inhalt sind die Kombinationen (E,APP,B,Z) mit – E: Ereignis APP01 oder APP02 – APP: Service bzw. Prozess – B: Benutzer-ID – Z: Zielsystem oder '*' (für global), für das die Benutzer-ID als unkritisch gilt **Beispiel:** ("APP01","exampleapp.exe","backup","hostabc") ◗ Positivliste <PL_VERBOTENENUTZER_01>: Benutzer, die global, je System oder in speziellen Verbindungen, die APP nie starten oder stoppen dürfen. Inhalt sind die Kombinationen (E,APP,B,Z) mit – E: Ereignis APP01 oder APP02 – APP: Service bzw. Prozess – B: Benutzer-ID – Z: Zielsystem oder '*' (für global), für das die Benutzer-ID als kritisch gilt **Beispiel:** ("APP02","exampleapp.exe","backup","hostabc") ◗ Negativliste <NL_ZUGELASSENEZEITFENSTER_01>: Zeitfenster, in denen global, je System oder in speziellen Verbindungen die APP gestartet oder gestoppt werden darf. Inhalt sind die Kombination (E,APP,ZFS,ZFE,Z) mit – E: Ereignis APP01 oder APP02 – APP: Service bzw. Prozess – ZFS: Zeitfenster-Start – ZFE: Zeitfenster-Ende – Z: Zielsystem oder '*' (für global), für das das Zeitfenster zulässig ist **Beispiel:** ("APP01","exampleapp.exe","22:00:00","22:10:00","hostabc“) ◗ Positivliste <PL_VERBOTENEZEITFENSTER_01>: Zeitfenster, in denen global, je System oder in speziellen Verbindungen die APP nie gestartet oder gestoppt werden darf. Inhalt sind die Kombinationen (E,APP,ZFS,ZFE,Z) mit – E: Ereignis APP01 oder APP02 – APP: Service bzw. Prozess – ZFS: Zeitfenster-Start – ZFE: Zeitfenster-Ende – Z: Zielsystem oder '*' (für global), für das das Zeitfenster unzulässig ist **Beispiel:** ("APP02","exampleapp.exe","22:10:01","21:59:59","hostabc") **Hinweis:** Im Fall von '*' ist jeder Wert enthalten, es gilt also: ein Benutzer B1 und ein System S1 sind enthalten in (B1,S1) sowie in (B1,*) oder (*,S1).
Empfohlener Reaktionstyp	Warnmeldung

→

Kritikalität	3 (sehr hoch)
Dringlichkeit	3 (unverzüglich)
Typische True Positives (kritisch)	◗ Ein bösartiger Akteur stoppt einen wichtigen Service wie z. B. die Datensicherung (Backup) oder Antivirus. ◗ Das Konfigurationsprogramm zur Änderung und insbesondere Löschung einer Datensicherung wird jenseits der üblichen Zeitfenster oder mit falschem Benutzer aufgerufen. ◗ In einem System werden Konfigurationsänderungen an einer Datei oder in einer Datenbank vorgenommen, die erst bei einem Neustart greifen.
Typische True Negatives (unkritisch)	◗ Ein Service mit Zeitfenster oder Benutzer steht korrekterweise auf der Negativliste. ◗ Ein Service, der nicht überwacht werden soll oder muss, steht auf der Negativliste oder nicht auf der Liste der zu überwachenden Services.
Typische False Positives (unkritisch)	◗ Aufgrund eines Fehlers bei einem Service muss genehmigt eingegriffen werden. ◗ Für das Starten oder Stoppen autorisierte Benutzer stehen nicht auf der Negativliste. ◗ Services stehen fälschlicherweise auf der Liste der zu überwachenden Services. ◗ Die Zeitfenster sind in den Listen oder auf dem System falsch eingestellt.
Typische False Negatives (kritisch)	◗ APPs stehen nicht auf der Liste der zu überwachenden Services. ◗ APPs stehen fälschlicherweise auf einer Negativliste.
Fachliche Beschreibung der Regel	WENN das Ereignis E = APP01 oder APP02 für System Z mit Benutzer B für Service APP zu Uhrzeit T EINTRITT, UND APP ist enthalten in <GL_APPS> UND (E,APP,B,Z) ist enthalten in <PL_VERBOTENENUTZER_01> ODER (E,APP,T) ist enthalten in <PL_VERBOTENEZEITFENSTER_01> mit T zwischen ZFS und ZFE ODER (E,APP,B,Z) ist nicht enthalten in <NL_ZUGELASSENENUTZER_01> ODER (E,APP,T) ist nicht enthalten in <NL_ZUGELASSENEZEITFENSTER_01> mit T zwischen ZFS und ZFE DANN löse aus
Gruppierung	**Empfehlung:** Gruppierung nach Kombination von Service und Zielsystem (APP,Z) **Begründung:** Mehrere Starts und Stopps einer Applikation werden je Zielsystem gruppiert und sind so leichter analysierbar.
Optionen und Anmerkungen	Die Zahl möglicherweise zu überwachender Services bzw. Prozesse kann sehr lang sein. Zudem kann es sein, dass für reguläre Neustarts diese individuell ausgenommen werden müssen. Daher sollte anfangs die Priorität auf die essenziellsten Services für das Funktionieren und die Resilienz der Organisation gesetzt werden. Hierzu wird empfohlen, mit ◗ Sicherheitssystemen wie Antivirus, SIEM-Agenten (falls vorhanden), Firewallsystemen, ◗ Sicherungssystemen wie Backup-Systemen und -Diensten, inklusive Managementsystemen, ◗ essenziellen IT-Services wie E-Mail, Telefonie und VPN, ◗ kritischen Geschäftsprozessen zu beginnen, um die Abdeckung der IT-Landschaft nach und nach zu verfeinern bzw. auszubauen.
Empfohlene Reaktion	Überprüfung und Untersuchung
Referenz ATT&CK Techniques	T1489 [D] (Service Stop), T1569 [G] (System Services), T1547 [G] (Boot or Logon Autostart Execution), T1053 [G] (Scheduled Task/Job)
Referenz BSI	Keine Entsprechung
Referenz ATT&CK Tactics	Impact, Defense Evasion, Execution, Persistence, Privilege Escalation

3.9.13 B13 – Alarmmeldung von Security-Lösung

ID	B13
Name	Alarmmeldung von Security-Lösung
Kurzbeschreibung mit Detektionsziel	Die Warnmeldung eines Sicherheitssystems wie ein Antivirus-System oder ein Intrusion-Detection-/-Protection-System (IDS/IPS) soll überwacht werden.
Adressierte Risiken	Es gibt zahlreiche Arten von Sicherheitssystemen, die Gefahren detektieren. Dazu gehören Antivirus-Systeme (AV), Intrusion-Detection-/-Prevention-Systeme (IDS/IPS), Threat-Intelligence-Systeme (TI) und viele mehr. Deren Warnmeldungen sollten zentral ausgewertet und überwacht werden.
Erforderliche Informationen	◗ Benutzer B, der die Warnmeldung ggf. verursacht ◗ Zielsystem Z ◗ Quellsystem Q ◗ Ereigniscode ALERT01 für Warnmeldung des entsprechenden Sicherheitssystems, z. B. »Virus gefunden« bei AV ◗ Gegebenenfalls Detailinformationen D aus den Sicherheitssystemen ◗ Negativ- und Positivlisten Die Sicherheitssysteme unterscheiden sich in ihren Informationen sehr, sodass verschiedene Listen je Sicherheitssystemtyp meist die sinnvollste Variante sind. **Beispiele:** ◗ Antivirus-Systeme: typischerweise Benutzer, Zielsystem, Art der Meldung (Virus erkannt, Heuristik, unerwünschtes, aber nicht schädliches Programm gefunden, ...) ◗ IDS/IPS: Quelle, Zielsystem, Signatur ◗ TI: Verdächte Quell-IP, Web-URL, Zertifikate usw. Es werden zwei Varianten vorgeschlagen: ◗ Variante 1: Alle Erkennungen erzeugen direkt eine Warnmeldung. Dies ist am einfachsten zu implementieren und benötigt wenige Informationen im Regelwerk, erzeugt aber schnell False Positives und erfordert Anpassungen in den zuliefernden Sicherheitssystemen, wenn Warnmeldungen nicht mehr auftreten sollen. ◗ Variante 2: Je Sicherheitssystem umzusetzendes und anzupassendes Regelwerk mit eigenen Positiv- und Negativlisten in der folgenden Form: Sie müssen entsprechende Informationen D enthalten, die insbesondere für das Rausfiltern von Warnmeldungen relevant sind. Positivlisten sind <PL_X_mm> und Negativlisten <NL_X_nn>, wobei X für das entsprechende Sicherheitssystem steht und mm bzw. nn eine Zahl zwischen 1 und m für die Positivlisten und 1 und n für die Negativlisten ist.
Benötigte Positiv- und Negativlisten	◗ Für Variante 2: Positivlisten <PL_X_mm> und Negativlisten <NL_X_nn>, die je Sicherheitssystem entsprechende Ausnahmen (Negativlisten) setzen oder Ausnahmen überschreiben (Positivlisten).
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	Variante 1: 2 (hoch) Variante 2: Je nach Sicherheitssystem, bei IDS und TI kommt es eher zu False Positives als bei AV.
Dringlichkeit	Variante 1: 2 (schnell) Variante 2: Je nach Sicherheitssystem, bei IDS und TI kommt es eher zu False Positives als bei AV.
Typische True Positives (kritisch)	◗ Ein Virus (AV) oder eine bekannt bösartige Signatur (IDS/IPS) wurde gefunden. ◗ Die IP-Adresse eines bekannt bösartigen Akteurs (TI) wurde erkannt, oder ein System im Unternehmensnetz versucht, auf eine bekannt bösartige Adresse oder Webseite (TI) zuzugreifen. ◗ Weitere aus Sicherheitssystemen stammende Warnungen
Typische True Negatives (unkritisch)	◗ Es wurde kein verdächtiges Verhalten durch ein Warnsystem erkannt. ◗ Eine Ausnahme, bspw. zu oft False Positives verursachende IDS/IPS-Signaturen, wurde auf eine Negativliste gesetzt.
Typische False Positives (unkritisch)	◗ Warnmeldungen aus den Sicherheitssystemen sind falsch oder diese sind zu empfindlich eingestellt. ◗ Negativlisten sind nicht korrekt befüllt bzw. werden durch Positivlisten überschrieben.
Typische False Negatives (kritisch)	◗ Die zuliefernden Sicherheitssysteme sind nicht auf aktuellem Stand bzw. eine neue, durch sie nicht erkannte Bedrohung tritt ein. ◗ Die entsprechenden Warnmeldungen aus den Sicherheitssystemen sind durch Einträge auf den Negativlisten ausgenommen.

→

Fachliche Beschreibung der Regel	Variante 1: WENN das Ereignis ALERT01 EINTRITT, DANN löse aus Variante 2: WENN das Ereignis ALERT01 vom Sicherheitssystem X für Benutzer B für System Z von System Q aus mit Detailinformation D EINTRITT, UND für alle nn in [1..n]: (D,B,Z,Q) ist nicht enthalten in <NL_X_nn> ODER (D,B,Z,Q) ist enthalten in <PL_X_mm> für mindestens ein mm in [1..m] DANN löse aus
Gruppierung	**Empfehlung:** Gruppierung nach Sicherheitssystem und Zielsystem: (X, Z) **Begründung:** Von einem Sicherheitssystem kommen inhaltlich ähnliche Meldungen. Diese zusammenzufassen und mit betroffenen Zielsystemen zu gruppieren, erleichtert die Auswertung.
Optionen und Anmerkungen	◗ Die Vielzahl von Sicherheitssystemen und ihre unterschiedliche Aussagekraft erfordert eine individuelle Bewertung durch die Organisation. Für den Anfang ist ein Start mit Variante 1 empfohlen. Sollten hier zu viele False Positives auftreten, so kann eine kontinuierliche Migration einzelner Sicherheitssystemmeldungen in Variante 2 Abhilfe schaffen. ◗ Selbst wenn es für die einzelnen Sicherheitssysteme bereits dedizierte Teams zur Überwachung gibt, so wird empfohlen, sie zentral dennoch aufzunehmen und zu überwachen. Hier kann dann allerdings der Fokus mehr auf Zusammenhänge gelegt werden, also bspw. nicht mehr auf einzelne Antivirus-Warnmeldungen einzugehen, sondern diese im Rahmen von Umfeldanalysen auszuwerten oder wenn sie zusammen mit Warnmeldungen anderer Systeme eintreten, bspw. Warnmeldung sowohl durch AV als auch IDS/IPS für System Z.
Empfohlene Reaktion	Prüfung der Warnmeldung und Umfeldanalyse, je nachdem, welche Art von Warnmeldung eingetreten ist – eine Meldung durch AV »Virus erkannt« ist zuverlässiger als eine Heuristikmeldung »Möglicherweise verdächtiges Verhalten«.
Referenz ATT&CK Techniques	Txxxx [x] (Various)
Referenz BSI	DER.1 Detektion von sicherheitsrelevanten Ereignissen
Referenz ATT&CK Tactics	Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact

3.9.14 B14 – Erkennung von Portscans am Perimeter – horizontal

ID	B14
Name	Erkennung von horizontalen Portscans am Perimeter
Kurzbeschreibung mit Detektionsziel	Externe Scans sind üblich, sollten aber zur Trendentwicklung beobachtet werden, typischerweise als regelmäßiger Report.
Adressierte Risiken	Portscans können Angreifern dazu dienen, sich ein Bild vom Netzwerk zu machen und einen Angriffsplan vorzubereiten (Host Discovery). Sie identifizieren damit im Netzwerk erreichbare IP-Adressen und deren offene Ports als potenzielle Angriffsziele. Offene Ports stellen Risiken dar, wenn die darauf laufenden Dienste schlecht konfiguriert sind, Sicherheitslücken enthalten oder nicht gepatcht sind. Bei horizontalen Scans wird ein bestimmter Port, z. B. Port 80 oder 443, an mehreren Netzwerkadressen getestet. Die hier betrachteten Scans werden am Perimeter detektiert, in der Regel handelt es sich dabei um die externe Firewall. Es sind somit üblicherweise externe Scans aus dem Internet.
Erforderliche Informationen	◗ Ereigniscodes NET01 oder NET02 ◗ Quell-IP, von dieser Adresse wird der Scan durchgeführt ◗ Ziel-IP, auf dieser Adresse oder in diesem Netz/Subnetz wird der Scan durchgeführt ◗ Ziel-Port ◗ Optional: Portscan_Arten zur automatischen Erkennung der Portscan-Arten ◗ Schwellenwert_IP_Anzahl als Schwellenwert für die Anzahl der gescannten IPs pro Zeiteinheit, z. B. 50 IPs/Sekunde
Benötigte Positiv- und Negativlisten	◗ Negativliste <NL_ZUGELASSENEZIELSYSTEME_01>: Systeme/Services, auf denen externe Portscans zugelassen sind (z. B. Webserver oder Systeme, die notwendigerweise exponiert im Internet stehen müssen) ◗ Negativliste <NL_ZUGELASSENEQUELLSYSTEME_01>: Quell-IPs, die Portscans durchführen dürfen (z. B. beauftragte Pentester) ◗ Positivliste <PL_VERBOTENEZIELSYSTEME_01>: Systeme/Services, auf denen Portscans auf keinen Fall durchgeführt werden dürfen ◗ Positivliste <PL_VERBOTENEQUELLSYSTEME_01>: Quell-IPs, die Portscans nicht ausführen dürfen
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	1 (normal)
Dringlichkeit	1 (normal)
Typische True Positives (kritisch)	◗ Ein horizontaler Scan wurde an einem nicht erlaubten Zielsystem aus <PL_VERBOTENEZIELSYSTEME_01> festgestellt, oder die Quell-IP ist in <PL_VERBOTENEQUELLSYSTEME_01> enthalten und daher nicht berechtigt, Scans durchzuführen.
Typische True Negatives (unkritisch)	◗ Ein horizontaler Scan wurde durchgeführt an einem System, das gescannt werden darf oder aber auf einer der Negativlisten steht.
Typische False Positives (unkritisch)	◗ Schwachstellenscan oder Penetrationstest, der nicht vorher angekündigt wurde (z. B. im Rahmen einer Sicherheitsüberprüfung)
Typische False Negatives (kritisch)	◗ Ein horizontaler Scan wurde festgestellt unter Beteiligung eines Systems, das fälschlicherweise in einer der Negativlisten aufgeführt ist, oder die Mengengerüste für das Auslösen des UC wurden nicht erfüllt.

→

Fachliche Beschreibung der Regel	WENN Ereignis NET01 ODER NET02 EINTRITT, UND Auftreten >= Schwellenwert_IP_Anzahl UND Quell-IP ist konstant UND Quell-IP ist nicht enthalten in <NL_ZUGELASSENEQUELLSYSTEME_01> ODER Quell-IP ist enthalten in <PL_VERBOTENEQUELLSYSTEME_01> UND Ziel-IP ist unterschiedlich UND Ziel-Port ist konstant UND Ziel-IP ist nicht enthalten in <NL_ZUGELASSENEZIELSYSTEME_01> ODER Ziel-IP ist enthalten in <PL_VERBOTENEZIELSYSTEME_01> DANN löse aus Empfohlener Wert: Schwellenwert_IP_Anzahl = 50 IPs/Sekunde
Gruppierung	**Empfehlung:** Gruppierung nach Quelle, falls möglich auch eine Gruppierung z. B. nach Systemen, Zonen, Schutzbedarf **Begründung:** Quellen von Portscans und somit potenziell unterschiedliche Akteure werden zusammengefasst.
Optionen und Anmerkungen	Dies ist ein grundlegender Use-Case. Es wird angenommen, dass die unterschiedlichen Arten von Portscans von den Quellsystemen automatisch erkannt werden, wie bspw. (Auflistung nur als Beispiel und nicht abschließend): • Ping-Sweep-Scan, ICMP-Echo-Requests • TCP-Connect, Vanilla-Scan, normaler Scan • TCP-SYN-Scan, TCP-half-open-Scan, halber Scan • Strobe-Scan, Scan von nur wenigen Top 10, Top 20 oder Top 100 Ports • UDP-Scan • FTP-Bounce-Scan, über einen FTP-Server geleitete Scans • Xmas-Scans, Manipulation von PSH-, URG- und FIN-Flags der TCP-Header • FIN-Scan, nur FIN-Flag gesetzt • NULL-Scan, keine Flags gesetzt • RST-Scan, nur RST-Flag gesetzt • Stealth-Scans, verschiedene Techniken zur Verschleierung von Scans Der Use-Case kann weiter verfeinert werden für Angriffsszenarien, bei denen die Angreifer zur Verschleierung horizontale Scans von mehreren Quell-IPs ausführen und die Scanraten herabsetzen. Dazu entfällt die Prüfung auf konstante Quell-IP und der Schwellenwert muss nach oben angepasst werden. **Beachte:** SYN-Scans sind Verbindungsanfragen, die nach Bestätigung sofort wieder resetet werden. Da damit keine Verbindung zustande kommt, werden solche Anfragen nicht protokolliert und können nur über ein Netzwerkmonitoring (z. B. mit Netflow) erkannt werden.
Empfohlene Reaktion	Ein Portscan ist nicht zwangsläufig ein Angriff. Trends und Häufigkeiten sollten im Blick behalten werden. Situations- und organisationsabhängige Rahmenbedingungen sind ebenfalls zu berücksichtigen. Zur Erkennung von Fehlkonfigurationen empfehlen sich gelegentliche Portscans über alle zu überprüfende Systeme (Blindtests).
Referenz ATT&CK Techniques	T1595 [D] (Active Scanning), T1590 [G] (Gather Victim Network Information)
Referenz BSI	Keine Entsprechung
Referenz ATT&CK Tactics	Reconnaissance

3.9.15 B15 – Erkennung von Portscans am Perimeter – vertikal

ID	B15
Name	Erkennung von vertikalen Portscans am Perimeter
Kurzbeschreibung mit Detektionsziel	Externe Scans sind üblich, sollten aber für eine Trendentwicklung identifiziert werden, typischerweise als Report.
Adressierte Risiken	Portscans können Angreifern dazu dienen, sich ein Bild vom Netzwerk zu machen und einen Angriffsplan vorzubereiten. Sie identifizieren damit offene Ports als potenzielle Angriffswege. Diese offenen Ports stellen Risiken dar, wenn die darauf laufenden Dienste schlecht konfiguriert sind, Sicherheitslücken enthalten oder nicht gepatcht sind. Einige Ports sind nur intern gedacht, wie z. B. SMB für interne Datei- und Druckfreigaben. Der vertikale Scan untersucht ein einzelnes System auf erreichbare TCP-/UDP-Ports. Die hier betrachteten Scans werden am Perimeter detektiert, in der Regel handelt es sich dabei um die externe Firewall. Es sind somit üblicherweise externe Scans aus dem Internet.
Erforderliche Informationen	◗ Ereigniscodes NET01 oder NET02 ◗ Quell-IP, von dieser Adresse wird der Scan durchgeführt ◗ Ziel-IP, auf dieser Adresse oder in diesem Netz/Subnetz wird der Scan durchgeführt ◗ Ziel-Port(s) = Portrange, mit dem der Scan ausgeführt wird ◗ Optional: Portscan_Arten zur automatischen Erkennung der Portscan-Arten ◗ Schwellenwert_Port_Anzahl als Schwellenwert für die Anzahl der geprüften Ports pro Zeiteinheit, z. B. 100 Ports/Sekunde
Benötigte Positiv- und Negativlisten	◗ Negativliste <NL_ZUGELASSENEZIELSYSTEME_01>: Systeme/Services, auf denen Portscans zugelassen sind ◗ Negativliste <NL_ZUGELASSENEQUELLSYSTEME_01>: Quell-IPs, die Portscans durchführen dürfen ◗ Positivliste <PL_VERBOTENEZIELSYSTEME_01>: Systeme/Services, auf denen Portscans auf keinen Fall durchgeführt werden dürfen ◗ Positivliste <PL_VERBOTENEQUELLSYSTEME_01>: Quell-IPs, die Portscans nicht ausführen dürfen
Empfohlener Reaktionstyp	Warnmeldung oder via Mail
Kritikalität	1 (normal)
Dringlichkeit	1 (normal)
Typische True Positives (kritisch)	◗ Ein vertikaler Scan wurde an einem nicht erlaubten Zielsystem aus <PL_VERBOTENEZIELSYSTEME_01> festgestellt oder die Quell-IP ist in <PL_VERBOTENEQUELLSYSTEME_01> enthalten und daher nicht berechtigt, Scans durchzuführen.
Typische True Negatives (unkritisch)	◗ Ein vertikaler Scan wurde durchgeführt an einem System, das gescannt werden darf oder aber auf einer der Negativlisten steht.
Typische False Positives (unkritisch)	◗ Erwünschter Schwachstellenscan oder Penetrationstest, der nicht vorher angekündigt wurde (z. B. im Rahmen einer Sicherheitsüberprüfung)
Typische False Negatives (kritisch)	◗ Ein vertikaler Scan wurde festgestellt unter Beteiligung eines Systems, das fälschlicherweise in einer der Negativlisten aufgeführt ist, oder die Mengengerüste für das Auslösen des UC wurden nicht erfüllt.

→

Fachliche Beschreibung der Regel	WENN Ereignis NET01 ODER NET02 EINTRITT, UND Auftreten >= Schwellenwert_Port_Anzahl UND Quell-IP ist nicht enthalten in <NL_ZUGELASSENEQUELLSYSTEME_01> ODER Quell-IP ist enthalten in <PL_VERBOTENEQUELLSYSTEME_01> UND Ziel-IP ist konstant UND Ziel-Port ist unterschiedlich UND Ziel-IP ist nicht enthalten in <NL_ZUGELASSENEZIELSYSTEME_01> ODER Ziel-IP ist enthalten in <PL_VERBOTENEZIELSYSTEME_01> DANN löse aus Empfohlener Schwellenwert: Schwellenwert_Port_Anzahl = 100 Portanfragen/Sekunde
Gruppierung	**Empfehlung:** Gruppierung nach Quelle, falls möglich auch eine Gruppierung z. B. nach Systemen, Zonen, Schutzbedarf **Begründung:** Quellen von Portscans und somit potenziell unterschiedliche Akteure werden zusammengefasst.
Optionen und Anmerkungen	Es ist ein grundlegender Use-Case. Es wird angenommen, dass die unterschiedlichen Arten von Portscans automatisch erkannt werden, wie bspw. (Auflistung nur als Beispiel und nicht abschließend): ◗ Ping-Sweep-Scan, ICMP-Echo-Requests ◗ TCP-Connect, Vanilla-Scan, normaler Scan ◗ TCP-SYN-Scan, TCP-half-open Scan, halber Scan ◗ Strobe-Scan, Scan von nur wenigen Top 10, Top 20 oder Top 100 Ports ◗ UDP-Scan ◗ FTP-Bounce-Scan, über einen FTP-Server geleitete Scans ◗ Xmas-Scans, Manipulation von PSH-, URG- und FIN-Flags der TCP-Header ◗ FIN-Scan, nur FIN-Flag gesetzt ◗ NULL-Scan, keine Flags gesetzt ◗ RST-Scan, nur RST-Flag gesetzt ◗ Stealth-Scans, verschiedene Techniken zur Verschleierung von Scans
Empfohlene Reaktion	Ein Portscan ist nicht sofort ein Angriff. Trends und Häufigkeiten sollten im Blick behalten werden. Situations- und organisationsabhängige Rahmenbedingungen sind ebenfalls zu berücksichtigen.
Referenz ATT&CK Techniques	T1595 [D] (Active Scanning), T1590 [G] (Gather Victim Network Information)
Referenz BSI	NET.3.2 Firewall
Referenz ATT&CK Tactics	Reconnaissance

3.9.16 B16 – Erkennung von internen Portscans – horizontal

ID	B16
Name	Erkennung von internen Portscans – horizontal
Kurzbeschreibung mit Detektionsziel	Scans von internen IP-Adressen sollten nicht üblich sein und vor Ausführung angemeldet und freigegeben werden. Alle nicht autorisierten Scans sind daher typischerweise mit einem Alarm zu belegen.
Adressierte Risiken	Portscans können Angreifern dazu dienen, sich ein Bild vom Netzwerk zu machen und einen Angriffsplan vorzubereiten (Host Discovery). Sie identifizieren damit im Netzwerk erreichbare IP-Adressen und deren offene Ports als potenzielle Angriffsziele. Offene Ports stellen Risiken dar, wenn die darauf laufenden Dienste schlecht konfiguriert sind, Sicherheitslücken enthalten oder nicht gepatcht sind. Einige Ports sind nur intern gedacht, wie z. B. SMB für interne Datei- und Druckfreigaben. Bei horizontalen Scans wird ein bestimmter Port, z. B. Port 445 für SMB-Freigaben, an mehreren Netzwerkadressen getestet.
Erforderliche Informationen	◗ Ereigniscodes NET01 oder NET02 ◗ Quell-IP, von dieser Adresse wird der Scan durchgeführt ◗ Ziel-IP, auf diese Adresse oder in diesem Netz/Subnetz wird der Scan durchgeführt ◗ Ziel-Port ◗ Optional: Portscan_Arten zur automatischen Erkennung der Portscan-Arten ◗ Schwellenwert_IP_Anzahl als Schwellenwert für die Anzahl der gescannten IPs pro Zeiteinheit, z. B. 50 IPs/Sekunde
Benötigte Positiv- und Negativlisten	◗ Negativliste <NL_ZUGELASSENEZIELSYSTEME_01>: Systeme/Services, auf denen interne Portscans zugelassen sind ◗ Negativliste <NL_ZUGELASSENEQUELLSYSTEME_01>: Quell-IPs, die Portscans durchführen dürfen ◗ Positivliste <PL_VERBOTENEZIELSYSTEME_01>: Systeme/Services, auf denen Portscans auf keinen Fall durchgeführt werden dürfen. ◗ Positivliste <PL_VERBOTENEQUELLSYSTEME_01>: Quell-IPs, die Portscans nicht ausführen dürfen.
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	2 (hoch)
Dringlichkeit	2 (schnell)
Typische True Positives (kritisch)	◗ Ein horizontaler Scan wurde an einem nicht erlaubten Zielsystem aus <PL_VERBOTENEZIELSYSTEME_01> festgestellt oder die Quell-IP ist in <PL_VERBOTENEQUELLSYSTEME-01> enthalten und daher nicht berechtigt, Scans durchzuführen.
Typische True Negatives (unkritisch)	◗ Ein horizontaler Scan wurde durchgeführt an einem System, das gescannt werden darf oder aber auf einer der Negativlisten steht.
Typische False Positives (unkritisch)	◗ Ein Schwachstellenscan oder Penetrationstest, der zwar gewünscht ist, aber nicht vorher angekündigt wurde (z. B. im Rahmen einer internen Sicherheitsüberprüfung).
Typische False Negatives (kritisch)	◗ Ein horizontaler Scan wurde festgestellt unter Beteiligung eines Systems, das fälschlicherweise in einer der Negativlisten aufgeführt ist, oder die Mengengerüste für das Auslösen des UC wurden nicht erfüllt.

→

Fachliche Beschreibung der Regel	WENN Ereignis NET01 ODER Ereignis NET02 EINTRITT, UND Auftreten >= Schwellenwert_IP_Anzahl UND Quell-IP ist konstant UND Quell-IP ist nicht enthalten in <NL_ZUGELASSENEQUELLSYSTEME_01> ODER Quell-IP ist enthalten in <PL_VERBOTENEQUELLSYSTEME_01> UND Ziel-IP ist unterschiedlich UND Ziel-Port ist konstant UND Ziel-IP ist nicht enthalten in <NL_ZUGELASSENEZIELSYSTEME_01> ODER Ziel-IP ist enthalten in <PL_VERBOTENEZIELSYSTEME_01> DANN löse aus Empfohlener Schwellenwert: Schwellenwert_IP_Anzahl = 50 IPs/Sekunde
Gruppierung	**Empfehlung:** Gruppierung nach Quelle, falls möglich auch eine Gruppierung z. B. nach Systemen, Zonen, Schutzbedarf **Begründung:** Quellen von Portscans und somit potenziell unterschiedliche Akteure werden zusammengefasst.
Optionen und Anmerkungen	Dies ist ein grundlegender Use-Case. Es wird angenommen, dass die unterschiedlichen Arten von Portscans von den Quellsystemen automatisch erkannt werden, wie bspw. (Auflistung nur als Beispiel und nicht abschließend): - Ping-Sweep-Scan, ICMP-Echo-Requests - TCP-Connect, Vanilla-Scan, normaler Scan - TCP-SYN-Scan, TCP-half-open-Scan, halber Scan - Strobe-Scan, Scan von nur wenigen Top 10, Top 20 oder Top 100 Ports - UDP-Scan - FTP-Bounce-Scan, über einen FTP-Server geleitete Scans - Xmas-Scans, Manipulation von PSH-, URG- und FIN-Flags der TCP-Header - FIN-Scan, nur FIN-Flag gesetzt - NULL-Scan, keine Flags gesetzt - RST-Scan, nur RST-Flag gesetzt - Stealth-Scans, verschiedene Techniken zur Verschleierung von Scans Der Use-Case kann weiter verfeinert werden für Angriffsszenarien, bei denen die Angreifer zur Verschleierung horizontale Scans von mehreren Quell-IPs ausführen und die Scanraten herabsetzen. Dazu entfällt die Prüfung auf konstante Quell-IP und der Schwellenwert muss nach oben angepasst werden. Denkbar ist auch eine Zusammenfassung der vertikalen und horizontalen Scans in einem einzigen Use-Case. **Beachte:** SYN-Scans sind Verbindungsanfragen, die nach Bestätigung sofort wieder resetet werden. Da damit keine Verbindung zustande kommt, werden solche Anfragen am Perimeter nicht protokolliert und können nur über ein Netzwerkmonitoring (z. B. mit Netflow) erkannt werden.
Empfohlene Reaktion	Ein Portscan ist nicht zwangsläufig ein Angriff. Trends und Häufigkeiten sollten im Blick behalten werden. Situations- und organisationsabhängige Rahmenbedingungen sind ebenfalls zu berücksichtigen. Zur Erkennung von Fehlkonfigurationen empfehlen sich gelegentliche Portscans über alle zu überprüfenden Systeme (Blindtests).
Referenz ATT&CK Techniques	T1595 [D] (Active Scanning), T1590 [G] (Gather Victim Network Information)
Referenz BSI	NET.3.2 Firewall NET.3.4 Network Access Control
Referenz ATT&CK Tactics	Reconnaissance

3.9.17 B17 – Erkennung von internen Portscans – vertikal

ID	B17
Name	Erkennung von internen Portscans – vertikal
Kurzbeschreibung mit Detektionsziel	Scans von internen IP-Adressen sollten nicht üblich sein und vor Ausführung angemeldet und freigegeben werden. Alle nicht autorisierten Scans sind daher typischerweise mit einem Alarm zu belegen.
Adressierte Risiken	Portscans können Angreifern dazu dienen, sich ein Bild vom Netzwerk zu machen und einen Angriffsplan vorzubereiten. Sie identifizieren damit offene Ports als potenzielle Angriffswege. Diese offenen Ports stellen Risiken dar, wenn die darauf laufenden Dienste schlecht konfiguriert sind, Sicherheitslücken enthalten oder nicht gepatcht sind. Einige Ports sind nur intern gedacht, wie z. B. SMB für interne Datei- und Druckfreigaben. Der vertikale Scan untersucht ein einzelnes System auf erreichbare TCP-/UDP-Ports.
Erforderliche Informationen	◗ Ereigniscodes NET01 oder NET02 ◗ Quell-IP, von dieser Adresse wird der Scan durchgeführt ◗ Ziel-IP, auf dieser Adresse oder in diesem Netz/Subnetz wird der Scan durchgeführt ◗ Ziel-Port(s) = Portrange, mit dem der Scan ausgeführt wird ◗ Optional: Portscan_Arten zur automatischen Erkennung der Portscan-Arten ◗ Schwellenwert_Port_Anzahl als Schwellenwert für die Anzahl der geprüften Ports pro Zeiteinheit, z. B. 100 Ports/Sekunde
Benötigte Positiv- und Negativlisten	◗ Negativliste <NL_ZUGELASSENEZIELSYSTEME_01>: Systeme/Services, bei denen Portscans zugelassen sind ◗ Negativliste <NL_ZUGELASSENEQUELLSYSTEME_01>: Quell-IPs, die Portscans durchführen dürfen ◗ Positivliste <PL_VERBOTENEZIELSYSTEME_01>: Systeme/Services, auf denen Portscans auf keinen Fall durchgeführt werden dürfen ◗ Positivliste <PL_VERBOTENEQUELLSYSTEME_01>: Quell-IPs, die Portscans auf keinen Fall ausführen dürfen
Empfohlener Reaktionstyp	Warnmeldung oder via Mail
Kritikalität	2 (hoch)
Dringlichkeit	2 (schnell)
Typische True Positives (kritisch)	◗ Ein vertikaler Scan wurde an einem nicht erlaubten Zielsystem aus <PL_VERBOTENEZIELSYSTEME_01> festgestellt, oder die Quell-IP ist in <PL_VERBOTENEQUELLSYSTEME_01> enthalten und daher nicht berechtigt, Scans durchzuführen.
Typische True Negatives (unkritisch)	◗ Ein vertikaler Scan wurde durchgeführt an einem System, das gescannt werden darf oder aber auf einer der Negativlisten steht.
Typische False Positives (unkritisch)	◗ Schwachstellenscan oder Penetrationstest, der nicht vorher angekündigt wurde (z. B. im Rahmen einer Sicherheitsüberprüfung)
Typische False Negatives (kritisch)	◗ Ein vertikaler Scan wurde festgestellt unter Beteiligung eines Systems, das fälschlicherweise in einer der Negativlisten aufgeführt ist, oder die Mengengerüste für das Auslösen des UC wurden nicht erfüllt.
Fachliche Beschreibung der Regel	WENN Ereignis E = NET01 ODER NET02 EINTRITT, UND Auftreten >= Schwellenwert_Port_Anzahl UND Quell-IP ist nicht enthalten in <NL_ZUGELASSENEQUELLSYSTEME_01> ODER Quell-IP ist enthalten in <PL_VERBOTENEQUELLSYSTEME_01> UND Ziel-IP ist konstant UND Ziel-Port ist unterschiedlich UND Ziel-IP ist nicht enthalten in <NL_ZUGELASSENEZIELSYSTEME_01> ODER Ziel-IP ist enthalten in <PL_VERBOTENEZIELSYSTEME_01> DANN löse aus Empfohlener Schwellenwert: Schwellenwert_Port_Anzahl = 100 Portanfragen/Sekunde

→

Gruppierung	**Empfehlung:** Gruppierung nach Quelle, falls möglich auch eine Gruppierung z. B. nach Systemen, Zonen, Schutzbedarf **Begründung:** Quellen von Portscans und somit potenziell unterschiedliche Akteure werden zusammengefasst.
Optionen und Anmerkungen	Es ist ein grundlegender Use-Case. Es wird angenommen, dass die unterschiedlichen Arten von Portscans automatisch erkannt werden, wie bspw. (Auflistung nur als Beispiel und nicht abschließend): ◗ Ping-Sweep-Scan, ICMP-Echo-Requests ◗ TCP-Connect, Vanilla-Scan, normaler Scan ◗ TCP-SYN-Scan, TCP-half-open-Scan, halber Scan ◗ Strobe-Scan, Scan von nur wenigen Top 10, Top 20 oder Top 100 Ports ◗ UDP-Scan ◗ FTP-Bounce-Scan, über einen FTP-Server geleitete Scans ◗ Xmas-Scans, Manipulation von PSH-, URG- und FIN-Flags der TCP-Header ◗ FIN-Scan, nur FIN-Flag gesetzt ◗ NULL-Scan, keine Flags gesetzt ◗ RST-Scan, nur RST-Flag gesetzt ◗ Stealth-Scans, verschiedene Techniken zur Verschleierung von Scans
Empfohlene Reaktion	Ein Portscan ist nicht sofort ein Angriff. Trends und Häufigkeiten sollten im Blick behalten werden. Situations- und organisationsabhängige Rahmenbedingungen sind ebenfalls zu berücksichtigen.
Referenz ATT&CK Techniques	T1595 [D] (Active Scanning), T1590 [G] (Gather Victim Network Information)
Referenz BSI	NET.3.2 Firewall NET.3.4 Network Access Control
Referenz ATT&CK Tactics	Reconnaissance

3.9.18 B18 – Keine Daten von Protokollquelle

ID	B18
Name	Keine Daten von Protokollquelle
Kurzbeschreibung mit Detektionsziel	Es fließen keine Daten mehr – entweder ist das System offline oder aber die Verbindung wurde unabsichtlich oder gezielt unterbrochen. Somit wird dem auswertenden System die Datenbasis entzogen.
Adressierte Risiken	Der Ausfall einer Protokollquelle bedeutet, dass die Möglichkeit der Auswertung und der Korrelation von Protokollen gestört sein kann oder sogar nicht mehr möglich ist. Damit wird zudem die Option eingeschränkt, Zusammenhänge oder potenzielle Angriffsvektoren zu erkennen.
Erforderliche Informationen	◗ IDs der Quellsysteme Q; IP/Hostname ◗ Ereigniscode HB01 auf dem überwachenden (SIEM-)System ◗ Zeitintervall T für Quellsystem, in dem stets Daten zu liefern sind ◗ Geräteliste <GL_SYSTEME_01>: IP-Adressen oder Hostnamen der Systeme, die überwacht werden sollen
Benötigte Positiv- und Negativlisten	◗ Positivliste <PL_SYSTEME_01>: IP-Adressen oder Hostnamen der Systeme, deren Protokollübermittlung an das überwachende System auf keinen Fall ausfallen darf ◗ Negativliste <NL_SYSTEME_01>: IP-Adressen oder Hostnamen der Systeme, die zwar Protokolle ans überwachende System senden sollten, aber z. B. vorübergehend nicht in Betrieb sind oder aus einem anderen Grund Protokolle nicht senden müssen.
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	3 (sehr hoch) für Systeme auf der Positivliste 2 (hoch) für alle anderen Systeme
Dringlichkeit	2 (schnell)
Typische True Positives (kritisch)	◗ Die Netzwerkverbindung zwischen auswertendem System und Quelle ist unterbrochen (z. B. FW-Regel, Routing). ◗ Das Quellsystem ist ausgefallen. ◗ Die Protokollierung wurde deaktiviert.
Typische True Negatives (unkritisch)	◗ Die Protokollübermittlung zwischen Quelle und überwachendem System funktioniert korrekt und im vorgeschriebenen Zeitraum.
Typische False Positives (unkritisch)	◗ Das Quellsystem ist planmäßig offline. ◗ Es werden Wartungsarbeiten am System ausgeführt, z. B. Updates oder Hardwareveränderungen. ◗ Es wurde vergessen, das System in <NL_SYSTEME_01> einzutragen.
Typische False Negatives (kritisch)	◗ Das HB01-Ereignis zum Quellsystem wird auf dem auswertenden System nicht mehr überwacht, bspw. weil das System fälschlicherweise in <NL_SYSTEME_01> eingetragen wurde. ◗ Das Quellsystem steht fälschlicherweise nicht in <GL_SYSTEME_01>.

→

Fachliche Beschreibung der Regel	Falls HB01.fail nicht unterstützt wird: WENN das Ereignis HB01 für Quellsystem Q in Zeitintervall T nicht EINTRITT, UND Q ist enthalten in <PL_SYSTEME_01> ODER Q ist enthalten in <GL_SYSTEME_01> UND Q ist nicht enthalten in <NL_SYSTEME_01> DANN löse aus Falls HB01.fail unterstützt wird: WENN das Ereignis HB01.fail für Quellsystem Q EINTRITT, UND Q ist enthalten in <PL_SYSTEME_01> ODER Q ist enthalten in <GL_SYSTEME_01> UND Q ist nicht enthalten in <NL_SYSTEME_01> DANN löse aus Empfohlener Schwellenwert: In beiden Varianten sollte T passend anhand der Kritikalität der Systeme gewählt werden. Richtwert hierfür ist T = 5 min.
Gruppierung	**Empfehlung:** Gruppierung nach Quellsystem Q **Begründung:** Wiederholtes Ausbleiben der Protokollquelle wird systemweise zusammengefasst, und beim zeitgleichen Ausfall mehrerer Systeme sind diese einfach zu identifizieren.
Optionen und Anmerkungen	◗ Viele zur Überwachung eingesetzte Technologien bieten kein explizites Ereignis an, das darauf hinweist, dass eine Protokollquelle noch Daten liefert bzw. keine mehr liefert. Hier hilft es, jedwedes Ereignis, das von der Quelle kommt, als HB01 zu interpretieren. Hierfür ist die erste Regel gedacht. Im Regeltext wurde auf diese explizite Ausprägung für alle Ereignisse verzichtet, da für die Überwachung wesentliche Ereignisse genutzt werden sollten, die möglichst eine vollständig funktionierende Protokollierung nachweisen oder zumindest wesentlich sind, aber auch regelmäßig auftreten. Eine Umsetzungsmöglichkeit wäre, bestimmte Programme oder Aktivitäten auf dem System per Zeitplanung regelmäßig (z. B. 1x/min) ausführen zu lassen, und diese als HB01 zu verwenden. HB01 ist mit diesem Ansatz idealerweise eine Untermenge aller möglichen Ereignisse E, als Rückfalloption ist aber das Verwenden beliebiger Ereignisse E eine Option. ◗ Falls das überwachende System die Funktionalität bietet, ein HB01.fail-Ereignis zu erzeugen, wenn eine Protokollübermittlung im vorgeschriebenen Zeitraum T nicht erfolgt, so lässt sich die Regel wie im zweiten Fall oben umschreiben und wird so meist effizienter.
Empfohlene Reaktion	Bei einem Ausfall der Protokollübertragung sollte im ersten Schritt geprüft werden, ob das Quellsystem noch aktiv ist (z. B. per Monitoring-System). Wenn das der Fall ist, sollte im nächsten Schritt die Netzwerkverbindung zum Quellsystem überprüft werden. Ist beides in Ordnung, so sollte unverzüglich mit der tieferen Analyse begonnen werden.
Referenz ATT&CK Techniques	T1562 [G] (Impair Defenses)
Referenz BSI	OPS.1.1.5 Protokollierung
Referenz ATT&CK Tactics	Defense Evasion

3.9.19 B19 – Technisches Konto – Sperrung aufgrund zu vieler fehlgeschlagener Anmeldeversuche

ID	B19
Name	Technisches Konto – Sperrung aufgrund zu vieler fehlgeschlagener Anmeldeversuche
Kurzbeschreibung mit Detektionsziel	Technische Benutzer werden selten verändert und Fehlanmeldungen finden üblicherweise nicht statt. Sie sind oftmals für kritische Prozesse in Gebrauch und können daher durch bspw. Brute-Force-Angriffe oder wiederholte manuelle Versuche automatisch gesperrt werden und so Schäden in (Geschäfts-)Prozessen verursachen. Daher ist eine Erkennung einer automatischen Sperrung wichtig.
Adressierte Risiken	Sind automatische Sperren auch für technische Benutzer aktiviert, so sind diese sehr einfach von einem Angreifer zu sperren und Prozesse störbar, was fehlerhafte Verarbeitungen in Prozessketten und somit wirtschaftliche Schäden verursachen kann. Zudem können Sicherungs- und Sicherheitsprozesse gestört werden, bspw. wenn ein für regelmäßige Backups oder die Übertragung von Protokolldateien verwendeter Benutzer durch einen Angriff für kurze Zeit gezielt blockiert wird.
Erforderliche Informationen	Ereignis: – Ereigniscode LOCK01 für Sperrung eines Benutzers – Benutzer U1, der gesperrt wurde – Zielsystem Z, auf dem der Benutzer gesperrt wird – Optional: Benutzer U2, der die Anmeldung versuchte, die zur Sperrung führte – Optional: Quellsystem Q, dessen Zugriffsversuch zur Sperrung führte Liste: Liste der technischen Benutzer, um sie von anderen Benutzern zu unterscheiden. Dies kann auch über andere Kriterien wie eine Namenskonvention geschehen. Im Folgenden wird von einer Liste ausgegangen, da diese meist ohnehin für gesonderte von der Software fest vorgegebene Benutzer benötigt wird.
Benötigte Positiv- und Negativlisten	◗ Positivliste <PL_RELEVANTENUTZER_01>: Liste der technischen bzw. für diesen Use-Case relevanten Benutzer je System oder global ◗ Negativliste <NL_IRRELEVANTESYSTEME_01>: Liste der Systeme, auf denen die Sperrung der technischen Benutzer unproblematisch ist, bspw. Entwicklungs- oder Testsysteme ohne Bedeutung für den operativen Betrieb
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	Entspricht SBF
Dringlichkeit	2 (hoch)
Typische True Positives (kritisch)	◗ Ein Angreifer versucht erfolglos, sich Zugriff auf einen Benutzer zu verschaffen, und verursacht dabei eine Sperrung. ◗ Ein Angreifer verursacht bewusst die Sperrung eines für wichtige Prozesse maßgeblichen Benutzers.
Typische True Negatives (unkritisch)	◗ Der Benutzer ist kein technischer Benutzer. ◗ Die Sperrung erfolgte nicht aufgrund fehlgeschlagener Anmeldungen, sondern wegen manueller Sperrung.
Typische False Positives (unkritisch)	◗ Fehlkonfiguration eines automatisierten Prozesses, bspw. falscher Benutzer oder falsches Passwort ◗ Fehlende Synchronisation bei zentral verwalteten Benutzern mit betroffenem System ◗ Der Benutzer ist kein technischer Benutzer.
Typische False Negatives (kritisch)	◗ Eine automatisierte Sperrung von Benutzern ist nicht konfiguriert. ◗ Die Positivliste <PL_RELEVANTENUTZER_01> erfasst nicht alle relevanten Benutzer. ◗ Die Negativliste <NL_IRRELEVANTESYSTEME_01> enthält falsche oder unzulässige Einträge, bspw. weil ein Angreifer es geschafft hat, sich auf dieser einzutragen oder eintragen zu lassen oder weil nach einem Aufgabenwechsel die Benutzerkennung nicht entfernt wurde. ◗ Ein Angreifer führt die Fehlversuche jenseits des Zeitfensters durch, in dem eine automatische Sperrung greift. ◗ Ein systemübergreifender Benutzer wird vom Angreifer abwechselnd auf verschiedenen Systemen verwendet, sodass eine Sperrung nicht auftritt. ◗ Ein Angreifer führt Anmeldeversuche durch; aufgrund von ständig laufenden automatisierten Prozessen mit korrektem Passwort greift die automatische Sperrung nicht. ◗ Ein Angreifer kennt das Passwort nicht, kann jedoch einen Prozess ausführen, bspw. ein für Mitarbeiter zugängliches Skript mit dem darin hinterlegten Benutzer und korrektem Passwort, das zu einer erfolgreichen Anmeldung führt. Der Angreifer ruft diesen Prozess oft genug zwischen fehlerhaften Anmeldeversuchen mit unterschiedlichen Passwörtern auf, sodass die automatische Sperrung nicht greift.

→

Fachliche Beschreibung der Regel	WENN das Ereignis LOCK01.* für System Z mit Benutzer U1 EINTRITT, UND (U1,Z) oder (U1,*) ist enthalten in <PL_RELEVANTENUTZER_01> UND Z ist nicht enthalten in <NL_IRRELEVANTESYSTEME_01> DANN löse aus
Gruppierung	**Empfehlung:** Gruppierung nach Kombination Benutzer mit System (U1,Z) **Begründung:** So ist eine Identifikation der betroffenen Benutzer mit einzelnen Systemen möglich.
Optionen und Anmerkungen	◗ Dieser Use-Case funktioniert nur, wenn tatsächlich auch eine automatisierte Sperrung nach einer festen Zahl von Fehlversuchen durchgeführt wird. Häufig wird für technische Benutzer eine derartige automatisierte Sperre aus betrieblichen Überlegungen heraus nicht umgesetzt. In einem solchen Fall sollten andere Use-Cases, die wiederholte Fehlversuche detektieren, implementiert werden. Zudem können die Erfolgsaussichten für automatisierte Zugriffsversuche durch eine am System eingestellte Verzögerungszeit nach einem erfolglosen Anmeldeversuch stark reduziert werden. ◗ Da ein Angriff zur Provokation einer automatischen Sperrung neben der Kenntnis oder der Vermutung (bspw. verbreitete und öffentlich dokumentierte eingebaute Benutzer) von verwendeten Benutzern keinerlei besonderes Wissen oder Fähigkeiten erfordert, ist er sehr einfach durchzuführen. ◗ Eine Variante dieses Use-Case besteht darin, grundsätzlich für besonders kritische Benutzer eine Sperrung zu überwachen, egal ob diese aufgrund von fehlerhaften Anmeldungen oder manueller Sperrung erfolgte. Das differenziert das Szenario zwar nicht, ist bei besonders kritischen Prozessen jedoch meist zweitrangig. ◗ Der Use-Case könnte besondere Fälle noch berücksichtigen, bspw. wenn U1=U2, also der Benutzer sich selbst versucht anzumelden. Er ist zwar dann immer noch gesperrt worden, aber ein Sicherheitsbezug ist weniger wahrscheinlich, da der Benutzer selbst dies verursachte. In den meisten Fällen ist dies dann ein Konfigurations- oder Prozessfehler in der Automatisierung. Nichtsdestotrotz ist auch hier ein bewusster Angriff nicht ganz auszuschließen, da ein Angreifer Zugriff auf bspw. ein Skript haben könnte und damit versucht, eine Anmeldung durchzuführen, obwohl diese aus Sicherheitsgründen vorsorglich gesperrt wurde, und so trotzdem indirekt eine Sperrung auslöst.
Empfohlene Reaktion	Eine entsprechend schnelle Reaktion abhängig von der Kritikalität des Prozesses ist erforderlich. Bei wirtschaftlich relevanten Prozessen ist dies offenkundig. Aber auch bei Sicherungs- und Sicherheitsprozessen können die Folgen von nur kurzen Unterbrechungen sehr weitreichend sein und erfordern ... ◗ im Fall von Sicherungssystemen: Sicherstellung korrekter und konsistenter Backups und Ähnliches. Es könnten bspw. differenzielle Backups nicht mehr funktionieren und somit könnte möglicherweise ein eine Woche später erfolgreicher Angriff nicht mehr durch das Rückspielen der Sicherungskopien mitigiert werden. ◗ im Fall von Sicherheitssystemen: zur Erkennung von Angreifern vor Spurenverwischung schnelle Maßnahmen. Idealerweise sollte die Kritikalität der Prozesse bereits vorher identifiziert und erfasst sein, um in der Situation keine Zeit zu verlieren.
Referenz ATT&CK Techniques	T1087 [G] (Account Discovery), T1531 [D] (Account Access Removal), T1110 [D] (Brute Force)
Referenz BSI	ORP.4 Identitäts- und Berechtigungsmanagement
Referenz ATT&CK Tactics	Discovery, Credential Access, Impact

3.9.20 B20 – Erfolgreicher Login nach fehlgeschlagenen Anmeldeversuchen

ID	B20
Name	Erfolgreicher Login nach fehlgeschlagenen Anmeldversuchen
Kurzbeschreibung mit Detektionsziel	Wiederholte fehlgeschlagene Anmeldeversuche sollen detektiert werden.
Adressierte Risiken	Da ein Risiko erst dann eintritt, wenn ein erfolgreicher Anmeldeversuch auf verdächtig viele fehlgeschlagene folgt, soll beim erfolgreichen Einloggen dieser Use-Case einen Alarm auslösen. Dies könnte einen erfolgreichen Zugang durch Unbefugte darstellen. **Hinweis:** Grundsätzlich lang andauernde fehlerhafte Anmeldeversuche sollten über einen anderen UC detektiert werden.
Erforderliche Informationen	◗ Ereignis: – Ereigniscode für Logins, erfolgreich AUTH01.succ und fehlgeschlagen AUTH01.fail – Benutzer U, der die Aktivität durchführt – Zielsystem Z, auf dem die Aktivität durchgeführt wird ◗ Zeitraum t und Schwellenwert s der Anzahl von Einlogversuchen, ab denen in Reihe stattfindende fehlgeschlagene Logins als verdächtig eingestuft werden
Benötigte Positiv- und Negativlisten	◗ Negativliste <NL_ZUGELASSENENUTZER_01>: Benutzer je System oder global, bei denen dieses Verhalten zugelassen wird (bspw. wegen bekannten technischen Fehlimplementierungen) ◗ Negativliste <NL_ZUGELASSENESYSTEME_01>: Systeme, bei denen dieses Verhalten zugelassen wird (bspw. wegen bekannten technischen Fehlimplementierungen oder aufgrund ihrer Netzexponiertheit)
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	Entspricht SBF
Dringlichkeit	2 (hoch)
Typische True Positives (kritisch)	◗ Angreifer probieren verschiedene Passwörter für ein Benutzerkonto aus und schaffen es, nach s oder mehr Fehlversuchen Zugang zu erlangen.
Typische True Negatives (unkritisch)	◗ Ein Benutzer vertippt sich, jedoch höchstens *s* Mal, und verwendet dann das korrekte Passwort. ◗ Das System oder der Benutzer steht auf einer Negativliste.
Typische False Positives (unkritisch)	◗ Ein automatisierter Prozess versucht sich in einem System anzumelden, jedoch besteht noch kein Zugang oder das eingestellte Passwort ist falsch. Zu einem späteren Zeitpunkt wird der Zugang eingerichtet oder das eingestellte Passwort beim Prozess korrigiert, der Prozess meldet sich erfolgreich an und die Warnmeldung wird ausgelöst. ◗ Ein Benutzer vertippt sich bei seiner interaktiven Anmeldung wiederholt und verwendet schließlich das korrekte Passwort. ◗ Ein Benutzer wird von Personen – bspw. ein privilegierter Benutzer durch zwei Administratoren – für unterschiedliche Aufgaben auf dem gleichen System von unterschiedlichen Quellsystemen Q1 und Q2 aus gleichzeitig auf Z verwendet. Nun treffen bei einem Wert von s = 4 im gleichen Zeitraum t jeweils zwei fehlgeschlagene Anmeldungen von Q1 und Q2 und anschließend von Q1 eine erfolgreiche Anmeldung ein. Somit löst der Use-Case zwar grundsätzlich korrekt aus, muss bei der Analyse jedoch differenziert werden.
Typische False Negatives (kritisch)	◗ Benutzer/Systeme stehen auf Negativlisten, obwohl dies inkorrekt ist. ◗ Die Folge von fehlerhaften und erfolgreichen Anmeldungen findet über einen längeren Zeitraum als t statt und fällt so nicht auf. ◗ Das System, auf dem Angreifer sich versuchen anzumelden, sperrt nach spätestens s fehlgeschlagenen Zugangsversuchen den Zugang, sodass selbst bei einem dann korrekten Passwort ein anderes Ereignis als AUTH01.succ auftritt. ◗ Ein Angreifer verwendet nach weniger als s Fehlversuchen das korrekte Passwort. ◗ Angreifer melden sich zwar erfolglos und wiederholt an, jedoch verteilt über mehrere Systeme Z1..Zn, sodass die Bedingungen des Use-Case nicht erfüllt werden. Insbesondere für übergreifende Benutzer wie bspw. fest im Betriebssystem eingebaute Benutzer (»Administrator« für Windows, »root« für Linux/Unix, Domain-Administrator-Konten bei Active Directory mit mehreren Domain-Servern usw.) ist dies möglich. ◗ Angreifer verwenden Ereignisse, die nicht im Use-Case benutzt werden. Beispielsweise könnte ein interner Angreifer einen legitimen Zugang haben, nutzt diesen und versucht dann auf einen anderen Benutzer zu wechseln. Wird hierbei ein anderes Ereignis vom System protokolliert als das in der Implementierung des Use-Case verwendete, so löst der Use-Case nicht aus.

→

Fachliche Beschreibung der Regel	WENN die Ereignisse E für System Z mit Benutzer U in Zeitraum t EINTRETEN, UND (U,Z) und (U,*) ist nicht enthalten in <NL_ZUGELASSENENUTZER_01> UND Z ist nicht enthalten in <NL_ZUGELASSENESYSTEME_01> UND E[1..s] = AUTH01.fail UND E[s+1] = AUTH01.succ DANN löse aus s und t müssen passend für die Systeme und Benutzer gewählt werden. Richtwerte hierfür sind s = 4 und t = 2 Minuten.
Gruppierung	**Empfehlung:** Gruppierung nach Kombination Benutzer mit System (U,Z) **Begründung:** So ist eine Identifikation der betroffenen Benutzer mit einzelnen Systemen möglich.
Optionen und Anmerkungen	◗ Die Wahl der Ereignisse, die die Systeme für AUTH01.succ und AUTH01.fail verwenden und die in der technischen Implementierung des Use-Case berücksichtigt werden, müssen sorgfältig gewählt und insbesondere bei Systemupdates regelmäßig überprüft werden. Beispielsweise könnten durch ein Update andere oder neue Ereignisse für spezifische Situationen geschrieben werden, die dann nicht berücksichtigt werden. ◗ Dieser Use-Case muss durch andere Use-Cases flankiert werden, die bspw. über einen längeren Zeitraum laufende fehlschlagende Brute-Force-Attacken erkennen. ◗ Der Use-Case sollte zudem dahingehend geprüft werden, ob unterschiedliche Varianten (besonders die Werte s und t) für unterschiedliche Systeme und Benutzertypen sinnvoll sind, um typische False Positives zu reduzieren. Beispielsweise könnten bei häufigen erzwungenen Passwortwechseln viele Benutzer sich anfangs mehr als s Mal vertippen. ◗ Gegebenenfalls lohnt es sich zudem, das Quellsystem Q zu berücksichtigen: Anstatt nur die Kombination <U,Z> zu verwenden, könnte auch <U,Q,Z> verwendet werden. Dies kann False Positives wie die Benutzung weniger privilegierter Benutzer durch mehrere Personen reduzieren, jedoch auch bei Angriffen von mehreren Quellen gleichzeitig eine rechtzeitige Erkennung verhindern. Auch hier empfiehlt sich eine differenzierte Betrachtung. ◗ Nicht nur fehlerhafte Anmeldungen mit Passwörtern, sondern auch die Verwendung falscher Schlüssel sollte berücksichtigt werden (bspw. bei SSH-Anmeldungen auf Linux/Unix-Systemen).
Empfohlene Reaktion	Die typischen False-Positive-Szenarien sollten schnell geprüft werden, da bei einem tatsächlichen Angriff ein Angreifer sich bereits erfolgreich Zugang verschafft hat.
Referenz ATT&CK Techniques	T1110 [D] (Brute Force), T1087 [G] (Account Discovery), T1078 [D] (Valid Accounts)
Referenz BSI	ORP.4 Identitäts- und Berechtigungsmanagement
Referenz ATT&CK Tactics	Initial Access, Privilege Escalation, Defense Evasion, Persistence

3.9.21 B21 – Technisches Konto – fehlgeschlagener interaktiver Anmeldeversuch

ID	B21
Name	Technisches Konto – fehlgeschlagener interaktiver Anmeldeversuch
Kurzbeschreibung mit Detektionsziel	Technische Benutzer werden üblicherweise für automatisierte Prozesse genutzt und sollten daher nicht interaktiv verwendet werden. Nur in Ausnahmefällen sind sie interaktiv zu nutzen, und dieser oder ein unberechtigter Fall sollen erkannt werden.
Adressierte Risiken	Technische Benutzer haben meist hohe Rechte, um ihre Aufgaben zu erfüllen. Das kann bspw. Zugriff auf alle Dateien und Laufwerke für einen Backup-Benutzer oder Administrator-Rechte für Deploymentzwecke sein. Gelingt einem bösartigen Akteur der Zugriff auf einen solchen Benutzer, so kann je nach Berechtigungen auf sämtliche Rechner und Daten zugegriffen werden oder eine Exfiltration, Manipulation oder Zerstörung von Daten durchgeführt werden. Im Fall eines fehlgeschlagenen Zugriffs hat sich ein Risiko noch nicht materialisiert. Aber wiederholte Versuche sollten überwacht werden, um rechtzeitig eingreifen zu können.
Erforderliche Informationen	◗ Ereignis: – Ereigniscode AUTH01 für Anmeldung und die Möglichkeit, zwischen interaktiver und nicht interaktiver Anmeldung zu unterscheiden. Besteht diese nicht (kein technisches Merkmal beim Anmeldeereignis, kein unterschiedliches verwendetes Programm/Shell/... im Anschluss etc.), so ist dieser Use-Case für solche Systeme bzw. Anwendungen nicht umsetzbar. – Benutzer B, der die Aktivität durchführt – Zielsystem Z, auf dem die Aktivität durchgeführt wird – Quellsystem Q, von dem aus die Aktivität durchgeführt wird ◗ <GL_TECHNISCHENUTZER-GLOBAL_01>: globale Liste technischer Benutzer TB ◗ <GL_TECHNISCHENUTZER-SYSTEM_01>: Liste technischer Benutzer TB je Zielsystem Z in Kombination (TB,Z) ◗ Technische Benutzer je System oder global, die (auch) interaktiv genutzt werden dürfen (siehe Positiv- und Negativlisten)
Benötigte Positiv- und Negativlisten	◗ Positivliste <PL_TECHNISCHENUTZER_01>: Technische Benutzer, bei deren versuchtem interaktivem Einsatz immer gewarnt werden sollte. Inhalt sind Kombinationen (TB,Z,Q) mit – TB: Benutzer-ID – Z: Zielsystem oder '*' (für global), für das die Benutzer-ID als kritisch gilt – Q: Quellsystem oder '*' (für global), für das die Benutzer-ID in Kombination mit einem Zielsystem als Verbindung als kritisch gilt ◗ Negativliste <NL_TECHNISCHENUTZER_01>: Technische Benutzer, die global, je System oder in speziellen Verbindungen zulässig sind. Inhalt sind Kombinationen (TB,Z,Q) mit – TB: Benutzer-ID – Z: Zielsystem oder '*' (für global), für das die Benutzer-ID als unkritisch gilt – Q: Quellsystem oder '*' (für global), für das die Benutzer-ID in Kombination mit einem Zielsystem als Verbindung als unkritisch gilt **Hinweis:** Im Fall von '*' ist jeder Wert enthalten, es gilt also: Ein Benutzer B1 und ein System S1 sind enthalten in (B1,S1) sowie in (B1,*) oder (*,S1).
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	2 (hoch)
Dringlichkeit	1 (normal)

→

Typische True Positives (kritisch)	◗ Es wird von einem Angreifer versucht, das Passwort des technischen Benutzers zu erraten. ◗ Das Gleiche wie oben, aber bei zahlreichen Versuchen in kurzer Zeit gilt die besondere Kategorie »Brute-Force-Attacke«. ◗ Zugriff auf Daten oder Systeme mit besonderen Rechten werden versucht.
Typische True Negatives (unkritisch)	◗ Passwörter sind korrekt gesetzt und der technische Benutzer darf verwendet werden. Keine Alarmierung. ◗ Es ist kein technischer Benutzer, der verwendet wird, und er steht daher auch nicht auf der Liste und verursacht keine Alarmierung. ◗ Es ist ein System, auf dem eine Überwachung nicht für nötig gehalten wird (abgeschottete Sandbox oder Entwicklungssystem o. Ä.).
Typische False Positives (unkritisch)	◗ Das Passwort des technischen Benutzers wurde verändert, aber noch nicht in allen automatisierten Prozessen (bspw. Skripten) angepasst. In diesem Fall kann hierüber zeitnah eine mögliche Betriebsstörung identifiziert werden (Backups funktionieren nicht mehr o. Ä.). ◗ Ein technischer Benutzer muss in einem Ausnahmefall, bspw. aufgrund von Programmlogik oder erforderlichen Berechtigungen, manuell genutzt werden und der Benutzer hat sich vertippt.
Typische False Negatives (kritisch)	◗ Ein technischer Benutzer ist nicht in der zentralen Liste der technischen Benutzer erfasst. ◗ Ein technischer Benutzer steht fälschlicherweise auf der Negativliste. ◗ Das verwendete Zielsystem wird nicht überwacht oder die Protokollierung ist auf diesem nicht (ausreichend) aktiv.
Fachliche Beschreibung der Regel	WENN das Ereignis AUTH01.fail für System Z von System Q aus mit Benutzer B EINTRITT, UND (B,Z,Q) ist enthalten in <PL_TECHNISCHENUTZER_01> ODER (B,Z,Q) ist nicht enthalten <NL_TECHNISCHENUTZER_01> UND B ist enthalten in <GL_TECHNISCHENUTZER-GLOBAL_01> ODER (B,Z) ist enthalten in <GL_TECHNISCHENUTZER-SYSTEM_01> DANN löse aus
Gruppierung	**Empfehlung:** Gruppierung nach der Kombination (B,Z) **Begründung:** So ist eine Identifikation der verwendeten Benutzer mit einzelnen Systemen möglich.
Optionen und Anmerkungen	Die vorgeschlagene Regel hat mehrere Stufen und benötigt mehrere Informationen: ◗ Ein technischer Benutzer TB muss auf einer Liste sein, die ihn als technischen Benutzer identifiziert. Dies ist insofern erforderlich, weil die meisten Systeme keine klaren technischen Unterscheidungsmöglichkeiten zwischen Benutzertypen für technische Prozesse und für Nutzung durch Personen bieten. Diese Listen müssen gepflegt werden. Sie können natürlich, sofern vorhanden, auch durch entsprechende Benutzer- und Berechtigungsmanagementsysteme verwaltet bzw. daraus erzeugt werden (bspw. Active Directory mit entsprechenden Strukturen oder Unix-Systeme mit Mitgliedschaft in entsprechenden Gruppen).

→

Optionen und Anmerkungen (Fortsetzung)	◗ Bezüglich des Regelwerks oben gilt: – Ein TB sollte immer in entweder <GL_TECHNISCHENUTZER-GLOBAL_01> oder <GL_TECHNISCHENUTZER-SYSTEM_01> enthalten sein, nicht nur in der Positivliste <PL_TECHNISCHENUTZER_01>. – Das Regelwerk ermöglicht mehrere Unterscheidungen: 1. Der fehlgeschlagene interaktive Login mit einem TB erzeugt grundsätzlich eine Warnmeldung. 2. Steht der TB nicht in <PL_TECHNISCHENUTZER_01>, so kann er über <NL_TECHNISCHENUTZER_01> ausgeschlossen werden. 3. Steht der TB in <PL_TECHNISCHENUTZER_01>, so wird ein fehlgeschlagener Anmeldeversuch immer einen Alarm auslösen, auch wenn er nicht als technischer Benutzer in den allgemeinen Listen ausgezeichnet ist. Dies soll verhindern, dass versehentlich der TB nicht als technischer Benutzer klassifiziert wurde. Schließlich überschreibt die Aufnahme in <PL_TECHNISCHENUTZER_01> bewusst eine mögliche Ausnahmeregelung in <NL_TECHNISCHENUTZER_01>. **Beispiel:** Ein Benutzer U1 soll generell bei fehlgeschlagener Anmeldung eine Warnmeldung auslösen, aber nicht a) wenn er auf den Systemen Z1-Z3 verwendet wird, b) jedoch immer, wenn er von den am Internet hängenden Systemen Q1 & Q2 aus verwendet wird. Dann würden die folgenden Listen diese Informationen enthalten: <GL_TECHNISCHENUTZER-GLOBAL_01>: U1 <NL_TECHNISCHENUTZER_01>: (U1,Z1,*), (U1,Z2,*), (U1,Z3,*) <PL_TECHNISCHENUTZER_01>: (U1,*,Q1), (U1,*,Q2) ◗ Grundsätzlich sollte die Aufnahme in Negativlisten hier sorgfältig geprüft werden. Fehlgeschlagene Anmeldungen sollten selten vorkommen, doch ggf. gibt es aufgrund von betrieblichen Abläufen oder gezielten Testfällen Gründe, dass bestimmte technische Benutzer öfter fehlgeschlagene Anmeldungen durchführen. ◗ Grundsätzlich kann der Use-Case auch als Bericht aufgesetzt werden. Dies muss mit der Kritikalität der technischen Benutzer abgewogen werden. ◗ Eine Weiterentwicklung besteht hier darin, erst nach einer gewissen Anzahl fehlerhafter Anmeldungen zu reagieren. Hintergrund hierfür dürften aber nur vorübergehende technische Probleme sein, gerade bei technischen Benutzern sollten fehlerhafte Anmeldungen sehr selten vorkommen.
Empfohlene Reaktion	Bei diesem Use-Case ist zunächst noch kein Schaden entstanden, da die Anmeldung fehlgeschlagen war. Gerade bei technischen Benutzern sind Anmeldefehler aber unüblich – »Vertippen« und ähnliche Fehlerquellen gibt es hier nicht. Besonderes Augenmerk sollte auf Folgendes gelegt werden: 1. Die fehlgeschlagene Verwendung unterschiedlicher TB vom gleichen System aus (→ System möglicherweise kompromittiert, Angreifer probiert verschiedene Benutzer aus) 2. Das Auftreten einer hohen Frequenz von fehlerhaften Anmeldungen mit dem TB (→ Brute-Force-Attacke) Überdies kann das Fehlschlagen von Anmeldungen – wenn es eine legitime Anwendung ist – auf die Störung von Betriebsprozessen hindeuten, die schnell behoben werden sollte.
Referenz ATT&CK Techniques	T1110 [G] (Brute Force), T1087 [G] (Account Discovery)
Referenz BSI	ORP.4 Identitäts- und Berechtigungsmanagement
Referenz ATT&CK Tactics	Discovery, Credential Access

3.9.22 B22 – Technisches Konto – erfolgreiche interaktive Anmeldung

ID	B22
Name	Technisches Konto – erfolgreiche interaktive Anmeldung
Kurzbeschreibung mit Detektionsziel	Technische Benutzer werden üblicherweise für automatisierte Prozesse genutzt und sollten daher nicht interaktiv verwendet werden. Nur in Ausnahmefällen sind sie interaktiv zu nutzen, und dieser Ausnahmefall oder ein unberechtigter Fall sollen erkannt werden.
Adressierte Risiken	Technische Benutzer haben meist hohe Rechte, um ihre Aufgaben zu erfüllen. Das kann bspw. Zugriff auf alle Dateien und Laufwerke für einen Backup-Benutzer oder Administrator-Rechte für Deploymentzwecke sein. Gelingt einem bösartigen Akteur der Zugriff auf einen solchen Benutzer, so kann je nach Berechtigungen auf sämtliche Rechner und Daten zugegriffen werden oder eine Exfiltration, Manipulation oder Zerstörung von Daten durchgeführt werden. Im Fall eines erfolgreichen Zugriffs hat sich ein potenzielles Risiko materialisiert. Hierauf sollte zeitnah reagiert werden.
Erforderliche Informationen	◗ Ereignis: – Ereigniscode AUTH01 für Anmeldung und die Möglichkeit, zwischen interaktiver und nicht interaktiver Anmeldung zu unterscheiden. Besteht diese nicht (kein technisches Merkmal beim Anmeldeereignis, kein unterschiedliches verwendetes Programm/Shell/... im Anschluss etc.), so ist dieser Use-Case für solche Systeme bzw. Anwendungen nicht umsetzbar. – Benutzer B, der die Aktivität durchführt – Zielsystem Z, auf dem die Aktivität durchgeführt wird – Quellsystem Q, von dem aus die Aktivität durchgeführt wird ◗ <GL_TECHNISCHENUTZER-GLOBAL_01>: globale Liste technischer Benutzer TB (TB) ◗ <GL_TECHNISCHENUTZER-SYSTEM_01>: Liste technischer Benutzer TB je Zielsystem Z in Kombination (TB,Z) ◗ Technische Benutzer je System oder global, die (auch) interaktiv genutzt werden dürfen (siehe Positiv- und Negativlisten)
Benötigte Positiv- und Negativlisten	◗ Positivliste <PL_TECHNISCHENUTZER_01>: Technische Benutzer, bei deren erfolgreichem interaktivem Einsatz immer gewarnt werden sollte. Inhalt sind Kombinationen (TB,Z,Q) mit – TB: Benutzer-ID – Z: Zielsystem oder '*' (für global), für das die Benutzer-ID als kritisch gilt – Q: Quellsystem oder '*' (für global), für das die Benutzer-ID in Kombination mit einem Zielsystem als Verbindung als kritisch gilt ◗ Negativliste <NL_TECHNISCHENUTZER_01>: Technische Benutzer, die global, je System oder in speziellen Verbindungen zulässig sind. Inhalt sind Kombinationen (TB,Z,Q) mit – TB: Benutzer-ID – Z: Zielsystem oder '*' (für global), für das die Benutzer-ID als unkritisch gilt – Q: Quellsystem oder '*' (für global), für das die Benutzer-ID in Kombination mit einem Zielsystem als Verbindung als unkritisch gilt **Hinweis:** Im Fall von '*' ist jeder Wert enthalten, es gilt also: Ein Benutzer B1 und ein System S1 sind enthalten in (B1,S1) sowie in (B1,*) oder (*,S1).
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	3 (sehr hoch)
Dringlichkeit	2 (schnell)
Typische True Positives (kritisch)	◗ Ein Angreifer hat erfolgreich einen technischen Benutzer übernommen, bspw. nach vorangegangenen fehlgeschlagenen Versuchen. ◗ Zugriff auf Daten oder Systeme mit besonderen Rechten finden erfolgreich statt.
Typische True Negatives (unkritisch)	◗ Passwörter sind korrekt gesetzt und der technische Benutzer darf verwendet werden. Keine Alarmierung. ◗ Es ist kein technischer Benutzer, der verwendet wird, und er steht daher auch nicht auf der Liste und verursacht keine Alarmierung. ◗ Es ist ein System, auf dem eine Überwachung nicht für nötig gehalten wird (abgeschottete Sandbox oder Entwicklungssystem o. Ä.).

→

Typische False Positives (unkritisch)	◗ Der verwendete Benutzer ist gar kein technischer Benutzer und steht nur versehentlich auf den entsprechenden Listen. ◗ Es soll bei Anmeldung des technischen Benutzers nicht alarmiert werden, dieser ist aber nicht auf der Negativliste oder steht versehentlich auf der Positivliste. ◗ Es gibt einen genehmigten Ausnahmefall, in dem der Benutzer verwendet werden darf.
Typische False Negatives (kritisch)	◗ Ein technischer Benutzer ist nicht in der zentralen Liste der technischen Benutzer erfasst. ◗ Ein technischer Benutzer steht fälschlicherweise auf der Negativliste. ◗ Das verwendete Zielsystem wird nicht überwacht oder die Protokollierung ist auf diesem nicht (ausreichend) aktiv.
Fachliche Beschreibung der Regel	WENN das Ereignis AUTH01.succ für System Z von System Q aus mit Benutzer B EINTRITT, UND (B,Z,Q) ist enthalten in <PL_TECHNISCHENUTZER_01> ODER (B,Z,Q) ist nicht enthalten <NL_TECHNISCHENUTZER_01> UND B ist enthalten in <GL_TECHNISCHENUTZER-GLOBAL_01> ODER (B,Z) ist enthalten in <GL_TECHNISCHENUTZER-SYSTEM_01> DANN löse aus
Gruppierung	**Empfehlung:** Gruppierung nach der Kombination (B,Z) **Begründung:** So ist eine Identifikation der verwendeten Benutzer mit einzelnen Systemen möglich.
Optionen und Anmerkungen	Die vorgeschlagene Regel hat mehrere Stufen und benötigt mehrere Informationen: ◗ Ein technischer Benutzer TB muss auf einer Liste sein, die ihn als technischen Benutzer identifiziert. Dies ist erforderlich, weil die meisten Systeme keine klaren technischen Unterscheidungsmöglichkeiten zwischen Benutzertypen für technische Prozesse und für Nutzung durch Personen bieten. Diese Listen müssen gepflegt werden. Sie können natürlich, sofern vorhanden, auch durch entsprechende Benutzer- und Berechtigungsmanagementsysteme verwaltet bzw. daraus erzeugt werden (bspw. Active Directory mit entsprechenden Strukturen oder Unix-Systeme mit Mitgliedschaft in entsprechenden Gruppen). ◗ Bezüglich des Regelwerks oben gilt: – Ein TB sollte immer in entweder <GL_TECHNISCHENUTZER-GLOBAL_01> oder <GL_TECHNISCHENUTZER-SYSTEM_01> enthalten sein, nicht nur in der Positivliste <PL_TECHNISCHENUTZER_01>. – Das Regelwerk ermöglicht mehrere Unterscheidungen: 1. Der erfolgreiche interaktive Login mit einem TB erzeugt grundsätzlich eine Warnmeldung. 2. Steht der TB nicht in <PL_TECHNISCHENUTZER_01>, so kann er über <NL_TECHNISCHENUTZER_01> ausgeschlossen werden. 3. Steht der TB in <PL_TECHNISCHENUTZER_01>, so wird eine erfolgreiche Anmeldung immer einen Alarm auslösen, auch wenn er nicht als technischer Benutzer in den allgemeinen Listen ausgezeichnet ist. Dies soll verhindern, dass versehentlich der TB nicht als technischer Benutzer klassifiziert wurde. Schließlich überschreibt die Aufnahme in <PL_TECHNISCHENUTZER_01> bewusst eine mögliche Ausnahmeregelung in <NL_TECHNISCHENUTZER_01>. **Beispiel:** Ein Benutzer U1 soll generell bei erfolgreicher Anmeldung eine Warnmeldung auslösen, aber nicht a) wenn er auf den Systemen Z1-Z3 verwendet wird, b) jedoch immer, wenn er von den am Internet hängenden Systemen Q1 & Q2 aus verwendet wird. Dann würden die folgenden Listen diese Informationen enthalten: <GL_TECHNISCHENUTZER-GLOBAL_01>: U1 <NL_TECHNISCHENUTZER_01>: (U1,Z1,*), (U1,Z2,*), (U1,Z3,*) <PL_TECHNISCHENUTZER_01>: (U1,*,Q1),(U1,*,Q2) – Grundsätzlich sollte die Aufnahme in Negativlisten hier sorgfältig geprüft werden. Erfolgreiche Anmeldungen mit technischen Benutzern sollten selten und nur in genehmigten Einzelfällen vorkommen, doch ggf. gibt es aufgrund von betrieblichen Abläufen oder gezielten Testfällen Gründe, dass bestimmte technische Benutzer öfter Anmeldungen durchführen müssen.

→

Empfohlene Reaktion	Bei diesem Use-Case ist bereits ein potenzieller Schaden in der Entstehung, wenn die Anmeldung erfolgreich war und ein potenzieller Angreifer nun die besonderen Rechte des technischen Benutzers nutzen kann. Eine schnelle, der Kritikalität des technischen Benutzers angemessene Reaktion mit Prüfung der Frage der Legitimation (genehmigter Einzelfall?) sollte stattfinden, damit im Fall eines bösartigen Akteurs schnell Benutzer und Systeme gesperrt werden bzw. generell der Schaden eingedämmt werden kann.
Referenz ATT&CK Techniques	T1110 [G] (Brute Force), T1078 [D] (Valid Accounts)
Referenz BSI	ORP.4 Identitäts- und Berechtigungsmanagement
Referenz ATT&CK Tactics	Credential Access, Initial Access, Privilege Escalation, Defense Evasion, Persistence

3.9.23 B23 – Benutzer administriert sich selbst

ID	B23
Name	Benutzer administriert sich selbst
Kurzbeschreibung mit Detektionsziel	Die Veränderung von Rechten des eigenen Benutzerkontos soll detektiert werden.
Adressierte Risiken	Die Administration des eigenen Benutzerkontos könnte auf eine Rechteausweitung oder Rechtereduktion hindeuten.
Erforderliche Informationen	◗ Zielbenutzer ZB, an dessen Konto die Änderung durchgeführt wird ◗ Quellbenutzer QB, der die Änderung durchführt ◗ Zielsystem Z ◗ Quellsystem Q ◗ Ereigniscode ACCT01 für Berechtigungsänderungen an Benutzern ◗ Negativ- und Positivlisten
Benötigte Positiv- und Negativlisten	◗ Positivliste <PL_NUTZER_01>: Benutzer, bei denen eine Rechteänderung durch sich selbst immer eine Warnung auslösen sollte. Inhalt sind Kombinationen (ZB,QB,Z,Q) mit – ZB: Zielbenutzer (z. B. Benutzer-ID oder Account-Name) – QB: Quellbenutzer (z. B. Benutzer-ID oder Account-Name) – Z: Zielsystem oder '*' (für global), für das der Benutzer als kritisch gilt – Q: Quellsystem oder '*' (für global), für das der Benutzer in Kombination mit einem Zielsystem als Verbindung als kritisch gilt. Beispielsweise würde («Administrator», «Administrator», *, *) die Änderung des Benutzers »Administrator« durch sich selbst von allen Systemen aus an allen Systemen anzeigen. ◗ Negativliste <NL_NUTZER_01>: Benutzer, für die global, je System oder in speziellen Verbindungen eine Rechteänderung durch sich selbst zulässig ist. Inhalt sind Kombinationen (ZB,QB,Z,Q) mit – ZB: Zielbenutzer (z. B. Benutzer-ID oder Account-Name) – QB: Quellbenutzer (z. B. Benutzer-ID oder Account-Name) – Z: Zielsystem oder '*' (für global), für das der Benutzer als unkritisch gilt – Q: Quellsystem oder '*' (für global), für das der Benutzer in Kombination mit einem Zielsystem als Verbindung als unkritisch gilt. Beispielsweise würde ("Administrator", "Administrator", *, *) die Änderung des Benutzers "Administrator" durch sich selbst von allen Systemen aus an allen Systemen ausnehmen. **Hinweis:** Im Fall von‚*' ist jeder Wert enthalten, es gilt also: Ein Benutzer B1 und ein System S1 sind enthalten in (B1,S1) sowie in (B1,*) oder (*,S1), bzw. Benutzer B1 und B2, System S1 und S2 sind enthalten in (*,B2,S1,S2), (B1,B2,*,*) usw.
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	2 (hoch)
Dringlichkeit	3 (sehr hoch)
Typische True Positives (kritisch)	◗ Eine Schadsoftware oder ein Angreifer nutzt eine Softwarelücke aus, um einem normalen Benutzer höhere Rechte zu verschaffen und diesen anschließend zu verwenden. ◗ Es werden bewusst Rechte in einem Benutzer reduziert, der diese benötigt, wodurch bspw. automatisierte Prozesse nicht mehr funktionieren (Änderungen an technischen Benutzern). ◗ Eine Schadsoftware oder ein Angreifer entzieht den üblichen Administratoren die Rechte, die Systeme zu verwalten, und sperrt sie so aus oder verhindert Möglichkeiten zum Eingriff.
Typische True Negatives (unkritisch)	◗ Ein Benutzer, der auf der Negativliste steht, administriert die eigenen Rechte in einem genehmigten Vorgang.
Typische False Positives (unkritisch)	◗ Ein Benutzer, der nicht auf der Negativliste steht, administriert die eigenen Rechte in einem genehmigten Vorgang. ◗ Ein Benutzer, der in einem solchen Fall die Veränderung vornehmen darf, steht fälschlicherweise auf der Positivliste.
Typische False Negatives (kritisch)	◗ Ein Benutzer steht fälschlicherweise auf der Negativliste. ◗ Es werden nicht alle Änderungsmöglichkeiten für die Rechte an einem Benutzer überwacht. Beispielsweise wenn Systeme die Änderungen über Einträge in Konfigurationsdateien oder Tabellen in Datenbanksystemen zulassen und dieser Vorgang nicht überwacht wird.

→

Fachliche Beschreibung der Regel	WENN das Ereignis ACCT01 für Benutzer ZB durch den Benutzer QB EINTRITT, UND ZB = QB UND (ZB,QB,Z,Q) ist nicht enthalten in <NL_NUTZER_01> ODER (ZB,QB,Z,Q) ist enthalten in <PL_NUTZER_01> DANN löse aus
Gruppierung	**Empfehlung:** Gruppierung nach Kombination (ZB,QB) **Begründung:** Änderungen an Benutzerkonten erfolgen oftmals nicht nur auf einem System, sondern systemübergreifend. Somit wird der Fokus auf die Kombination verursachender und betroffener Benutzer gelegt und die Analyse erleichtert.
Optionen und Anmerkungen	◗ Der Use-Case warnt in allen Fällen, wo Benutzer sich selbst administrieren und nicht dediziert ausgenommen sind. Grundsätzlich sollte dies immer überwacht und in organisatorischen Richtlinien untersagt werden, dass sich Administratoren selbst ihre eigenen Rechte ändern – dies sollte immer durch einen Kollegen bzw. eine Kollegin vorgenommen werden, um diesen Angriffsvektor zu schließen. Zudem sollte dieser Fall sehr selten vorkommen, auch wenn es nur einen einzelnen Administrator in der Organisation gibt. ◗ Für den Fall, dass Administrationskonten immer auf Rechteveränderung überprüft werden sollen, bspw. um das Entfernen der Rechte anderer Administratoren durch einen einzelnen zu erkennen, so setzt man diese in der Positivliste ein (z. B. (Administrator A,*,*,*), (Administrator B,*,*,*) usw.). Gerade bei einem Angreifer, der sich selbst einen eigenen Administrationsbenutzer schaffen konnte, ist dies eine sinnvolle Warnmaßnahme, um ggf. noch eingreifen zu können, da eine Sperrung von Administratoren schneller auffallen könnte als ein (teilweiser) Rechteentzug. ◗ Eine alternative Umsetzung wäre, anstelle des direkten Vergleichs »ZB = QB«, lediglich über die Positivliste einen Abgleich zu machen. Dann müssten für alle möglichen Administratoren X die Einträge grundsätzlich so gepflegt werden, dass (X,X,*,*) enthalten ist. ◗ Eine weitere Option ist es, statt auch für Versuche nur erfolgreiche Änderungen zu überwachen (ACCT01.succ). Dies kann in Einzelfällen sinnvoll sein, generell wird hiervon aber abgeraten, da so die Vorwarnzeit erheblich verkürzt wird. **Hinweis:** Es sollten auch indirekte Rechteänderungen überwacht werden, z. B. Veränderung an Zuweisung von Rollen, die entsprechende Rechte geben.
Empfohlene Reaktion	Änderungen an Benutzern durch sich selbst sind grundsätzlich kritisch und sollten aufgrund des hohen Schadenspotenzials möglichst schnell geprüft werden.
Referenz ATT&CK Techniques	T1078 [G] (Valid Accounts), T1098 [D] (Account Manipulation)
Referenz BSI	ORP.4 Identitäts- und Berechtigungsmanagement
Referenz ATT&CK Tactics	Initial Access, Privilege Escalation, Persistence, Defense Evasion

3.9.24 B24 – Administration von Benutzerkonten

ID	B24
Name	Administration von Benutzerkonten
Kurzbeschreibung mit Detektionsziel	Die Änderung von Benutzerkonten ist ein kritischer Vorgang der IT-Sicherheit. Der Use-Case soll sicherstellen, dass entsprechende Änderungen nur von berechtigten Administratoren durchgeführt werden.
Adressierte Risiken	Bei unberechtigtem Zugriff können über diesen Weg unerwünschte Konten eingerichtet werden, einschließlich privilegierter Rechte. Bleiben solche Änderungen unerkannt, können Angreifer im Nachgang mit scheinbar legitimen Rechten uneingeschränkten Zugriff auf die Assets der Organisation erlangen. Dadurch besteht das Risiko, dass Unberechtigte Zugriff auf zu schützende Daten haben oder Berechtigte keinen Zugriff mehr auf Daten haben, die zur Erfüllung ihrer Arbeitsaufgaben notwendig sind.
Erforderliche Informationen	◗ Benutzer B, der Änderungen der Benutzerstruktur vornimmt ◗ Benutzer U, an dessen Konto die Änderung durchgeführt wird ◗ System Z, auf dem Änderungen der Benutzerstruktur vorgenommen wird ◗ Ereigniscodes ACCT03, ACCT04 und ACCT05 für Anlegen, Modifikationen und Löschungen von Benutzern ◗ Negativ- und Positivlisten
Benötigte Positiv- und Negativlisten	◗ Negativliste <NL_ZUGELASSENENUTZERBEARBEITUNG_01>: Benutzer B, die die Erlaubnis haben, Benutzerkonten ohne Warnmeldung zu verändern ◗ Negativliste <NL_ZUGELASSENESYSTEMEBEARBEITUNG_01>: Systeme Z, auf denen Benutzerkonten ohne Warnmeldung verändert werden dürfen ◗ Positivliste <PL_SENSIBLESYSTEME_01>: Administrationssysteme Z zur Benutzerverwaltung (z. B. AD-Server), deren Nutzung prinzipiell zu überwachen ist (Vorrangigkeit gegenüber <NL_ZUGELASSENENUTZERBEARBEITUNG_01> und <NL_ZUGELASSENESYSTEMEBEARBEITUNG_01>) ◗ Positivliste <PL_SENSIBLENUTZER_01>: Benutzer B, die Benutzerstrukturen nicht verändern dürfen, aber bspw. nicht gelöscht werden können oder bei Updates wiederholt angelegt werden
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	2 (hoch)
Dringlichkeit	2 (schnell)
Typische True Positives (kritisch)	◗ Es wurden Benutzerkonten von nicht autorisierten Personen oder Systemen verändert (Benutzer wurde neu angelegt, gelöscht oder verändert).
Typische True Negatives (unkritisch)	◗ Es wurden Änderungen der Benutzerkonten von legitimierten Personen oder Systemen durchgeführt. Die Akteure wurden korrekt in den Negativlisten hinterlegt.
Typische False Positives (unkritisch)	◗ Es treten Warnmeldungen auf, die durch Änderungen von Benutzern oder Systemen ausgelöst wurden, die dazu berechtigt sind. Es wurde vergessen, diese Akteure in die Negativlisten aufzunehmen.
Typische False Negatives (kritisch)	◗ Wichtige Administratoren wurden vergessen in die Positivlisten aufzunehmen. Manipulationen auf diesen Systemen bleiben daher unerkannt.
Fachliche Beschreibung der Regel	WENN das Ereignis ACCT03 oder ACCT04 oder ACCT05 durch Benutzer B an Benutzer U auf System Z EINTRITT, UND Z ist enthalten in <PL_SENSIBLESYSTEME_01> ODER U ist enthalten in <PL_SENSIBLENUTZER_01> ODER B ist nicht enthalten in <NL_ZUGELASSENENUTZERBEARBEITUNG_01> UND Z ist nicht enthalten in <NL_ZUGELASSENESYSTEMEBEARBEITUNG_01> DANN löse aus

→

Gruppierung	**Empfehlung:** Gruppierung nach Kombination (U,Z) von betroffenem Benutzerkonto U und Zielsystem Z **Begründung:** Gerade bei Anpassung an Benutzerkonten finden oft mehrere Änderungen auf einmal statt. So kann z. B. ein Benutzerkonto angelegt und anschließend mit weiteren Details versehen werden. Derartige Änderungen sind gruppiert einfacher zu prüfen. Die Aufnahme des Zielsystems hilft bei der Übersicht. Werden allerdings Änderungen entsprechend der hier aufgeführten Ereigniscodes stets auf zahlreichen Systemen durchgeführt, so kann es sinnvoll sein, nur nach U zu gruppieren.
Optionen und Anmerkungen	◗ Es ist darauf zu achten, dass bei der Erstellung der Listen mögliche Verknüpfungen lokaler Anmeldesysteme mit Anmeldesystemen bei einem Cloud-Anbieter berücksichtigt werden. ◗ Privilegierte Default-Konten, die die Administration von Benutzerkonten erlauben, sind nach Möglichkeit zu deaktivieren. Ist dies nicht möglich, sind diese in die Positivliste <PL_SENSIBLENUTZER_01> aufzunehmen.
Empfohlene Reaktion	Besteht der Verdacht, dass ein Benutzer oder ein System oder ein Angreifer, der vorgibt dieser Benutzer zu sein, Benutzerkonten ohne Genehmigung angelegt, geändert oder gelöscht hat, sollten im Zweifelsfall zunächst diese Änderungen wieder rückgängig gemacht werden. Im Nachgang ist dann ausreichend Zeit, den Vorgang genau zu untersuchen, um festzustellen, ob die Änderungen legitim waren oder nicht.
Referenz ATT&CK Techniques	T1078 [G] (Valid Accounts), T1098 [G] (Account Manipulation), T1136 [D] (Create Account), T1531 [D] (Account Access Removal)
Referenz BSI	OPS.1.1.2 Ordnungsgemäße IT-Administration ORP.4 Identitäts- und Berechtigungsmanagement
Referenz ATT&CK Tactics	Initial Access, Persistence, Privilege Escalation, Impact

3.9.25 B25 – Administration von Rechten

ID	B25
Name	Administration von Rechten
Kurzbeschreibung mit Detektionsziel	Typischerweise dürfen nur wenige Personen oder Systeme Berechtigungen von Benutzern oder Rollen verändern. Wenn andere als diese Benutzer Veränderungen vornehmen, soll dies detektiert werden. Besonders für kritische Konten sollte diese Prüfung immer erfolgen.
Adressierte Risiken	Durch die zu detektierenden Aktivitäten können Benutzern oder Rollen höhere Rechte erteilt werden, als dies notwendig oder vorgesehen ist, oder für Prozesse wichtigen Benutzern Berechtigungen entzogen werden. Dadurch besteht das Risiko, dass Unberechtigte Zugriff auf zu schützende Daten haben oder den Geschäftsbetrieb stören können.
Erforderliche Informationen	◗ Benutzer B oder System Q, der oder das Berechtigungsänderungen vornimmt ◗ Benutzer D oder Rolle R, an denen die Berechtigungsänderungen vorgenommen werden ◗ Ereigniscode ACCT01 für Rechteänderungen an Benutzern ◗ Ereigniscode ACCT02 für Rechteänderungen an Rollen (beinhaltet auch Gruppenrichtlinien oder mit Rollen vergleichbare Objekte) ◗ Negativ- und Positivlisten
Benötigte Positiv- und Negativlisten	◗ Negativliste <NL_ZUGELASSENENUTZERBEARBEITUNG_01>: Benutzer, die die Erlaubnis haben, Benutzerkonten ohne Warnmeldung zu verändern ◗ Negativliste <NL_ZUGELASSENENUTZERBEARBEITUNG_02>: Systeme, die die Erlaubnis haben, Benutzerkonten ohne Warnmeldung zu verändern ◗ Negativliste <NL_ZUGELASSENEROLLENBEARBEITUNG_01>: Benutzer, die die Erlaubnis haben, Rollen ohne Warnmeldung zu verändern ◗ Negativliste <NL_ZUGELASSENEROLLENBEARBEITUNG_02>: Systeme, die die Erlaubnis haben, Rollen ohne Warnmeldung zu verändern ◗ Positivliste <PL_SENSIBLENUTZER_01>: Benutzer, an denen keine Änderungen vorgenommen werden dürfen, ohne dass dies dediziert geprüft wird (Vorrangigkeit gegenüber <NL_ZUGELASSENENUTZERBEARBEITUNG_01>) ◗ Positivliste <PL_SENSIBLEROLLEN_01>: Rollen/Gruppen, an denen keine Änderungen vorgenommen werden dürfen, ohne dass dies dediziert geprüft wird (Vorrangigkeit gegenüber <NL_ZUGELASSENEROLLENBEARBEITUNG_01>)
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	2 (hoch)
Dringlichkeit	2 (schnell)
Typische True Positives (kritisch)	◗ Es wurden Berechtigungen von Benutzerkonten oder Rollen durch nicht autorisierte Personen oder Systeme verändert.
Typische True Negatives (unkritisch)	◗ Es wurden Änderungen der Benutzerrechte oder Rollen von legitimierten Personen oder Systemen durchgeführt. Die Akteure wurden korrekt in den Negativlisten hinterlegt.
Typische False Positives (unkritisch)	◗ Es wurden Änderungen der Benutzerrechte oder Rollen von legitimierten Personen oder Systemen durchgeführt. Die Akteure wurden nicht in den Negativlisten hinterlegt.
Typische False Negatives (kritisch)	◗ Wichtige zu überwachende Benutzerkonten oder Rollen wurden nicht in den Positivlisten hinterlegt, oder auf den Negativlisten sind Systeme oder Benutzer hinterlegt, die nicht befugt sind, Änderungen durchzuführen.

→

Fachliche Beschreibung der Regel	WENN das Ereignis ACCT01 durch Benutzer B oder System Q für Benutzer D EINTRITT, UND D ist enthalten in <PL_SENSIBLENUTZER_01> ODER B ist nicht enthalten in <NL_ZUGELASSENENUTZERBEARBEITUNG_01> UND Q ist nicht enthalten in <NL_ZUGELASSENENUTZERBEARBEITUNG_02> ODER das Ereignis ACCT02 durch Benutzer B oder System Q für Rolle R EINTRITT, UND R ist enthalten in <PL_SENSIBLEROLLEN_01> ODER B ist nicht enthalten in <NL_ZUGELASSENEROLLENBEARBEITUNG_01> UND Q ist nicht enthalten in <NL_ZUGELASSENEROLLENBEARBEITUNG_02> DANN löse aus
Gruppierung	**Empfehlung:** Gruppierung nach Kombination (Ereigniscode, D, R) von Ereignis, betroffenem Benutzerkonto (falls existent) und betroffener Rolle (falls existent). Alternativ, wenn eine unterschiedliche Gruppierung anhand des Ereigniscodes möglich ist, für ACCT01 nach Kombination (B,Q,D) und für ACCT02 nach (B,Q,R). **Begründung:** Es ist wichtig, schnell einen Überblick über betroffene Rollen und Benutzer zu bekommen, um eine Priorisierung effektiv durchführen zu können. Entsprechend sollte eine diesem Ziel zuträgliche Gruppierung gewählt werden.
Optionen und Anmerkungen	◗ Ein Verdachtsfall auf unrechtmäßige Rechteveränderung muss immer im Kontext betrachtet werden. Nicht nur die Erweiterung, sondern auch der Entzug von Berechtigungen kann geschäftsschädigende Konsequenzen haben. Werden bspw. Überwachungssystemen Rechte entzogen, so können diese möglicherweise nicht mehr Protokolle lesen, die sie überwachen sollen, oder Maßnahmen ergreifen. Unter Umständen funktionieren auch geschäftsrelevante Prozesse nicht mehr, wenn technischen Benutzern die nötigen Berechtigungen fehlen.
Empfohlene Reaktion	Besteht der Verdacht, dass ein Benutzer oder ein System oder ein Angreifer, der vorgibt, dieser Benutzer zu sein, die Rechte eines Benutzers ohne Genehmigung verändert hat, sollten im Zweifelsfall zunächst diese Änderungen wieder rückgängig gemacht werden. Im Nachgang ist dann genau zu untersuchen, ob die Änderungen legitim waren oder nicht. Zudem sollte geprüft werden, ob es im Kontext möglicher Rechteveränderungen weitere Auffälligkeiten gibt. Gibt es auch Hinweise aus anderen Use-Cases? Beispielsweise, dass der Benutzer seit der Erweiterung viele Uploads intern oder nach außen durchgeführt hat.
Referenz ATT&CK Techniques	T1078 [G] (Valid Accounts), T1098 [D] (Account Manipulation)
Referenz BSI	ORP.4 Identitäts- und Berechtigungsmanagement
Referenz ATT&CK Tactics	Privilege Escalation

3.9.26 B26 – Änderungen an Regelwerken oder Konfigurationen

ID	B26
Name	Änderungen an Regelwerken oder Konfigurationen
Kurzbeschreibung mit Detektionsziel	Wenn die Regelwerke bzw. der »Inhalt« von Sicherheitslösungen, bspw. Regeln von Firewall-, SIEM-, Antivirus-, IDS-Systemen, geändert werden, so soll dies erkannt und auf Rechtmäßigkeit und Fehler geprüft werden.
Adressierte Risiken	Eine Änderung an den Regeln von Sicherheitssystemen könnte eine bewusste Öffnung von Sicherheitslöchern oder die Ausschaltung von Überwachungssystemen als Ziel haben und den Nutzen der Lösungen einschränken oder aufheben.
Erforderliche Informationen	◗ Ereigniscode CONFIG03 ◗ Benutzer B, der die Änderungen durchführt ◗ Sicherheitslösung S, für die die Änderung durchgeführt wird. Wenn dies nicht differenzierbar ist, dann entspricht dies dem betroffenen System. ◗ IDS-Logs, AV-Logs, Firewall-Logs, Systemlogs und Ähnliches
Benötigte Positiv- und Negativlisten	◗ Negativliste <NL_NUTZER_01>: Liste im Format (B,S) mit B: autorisierte Benutzer, die Änderungen durchführen dürfen S: Sicherheitslösungen, für die die Änderungen durch B durchgeführt werden dürfen
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	2 (hoch)
Dringlichkeit	2 (schnell)
Typische True Positives (kritisch)	◗ Ein Angreifer hat Änderungen an Regelwerken vorgenommen. ◗ Von einem (autorisierten) Benutzer wurden versehentlich Änderungen vorgenommen.
Typische True Negatives (unkritisch)	◗ Genehmigte und dokumentierte Änderungen wurden von einem autorisierten Benutzer vorgenommen.
Typische False -Positives (unkritisch)	◗ Ein autorisierter Benutzer hat eine genehmigte und dokumentierte Änderung vorgenommen, stand jedoch nicht auf der Negativliste. ◗ Ein Benutzer, der grundsätzlich nicht auf der Negativliste stehen darf, hat in einem genehmigten Ausnahmefall eine dokumentierte Änderung vorgenommen.
Typische False Negatives (kritisch)	◗ Ein Benutzer hat eine Änderung vorgenommen und steht fälschlicherweise auf der Negativliste. ◗ Ein Benutzer hat eine Änderung vorgenommen und steht auf der Negativliste, aber es gibt keinen dokumentierten und genehmigten Auftrag hierfür.
Fachliche Beschreibung der Regel	WENN das Ereignis CONFIG03 durch Benutzer B für die Sicherheitslösung S EINTRITT, UND (B,S) ist nicht enthalten in <NL_NUTZER_01> DANN löse aus
Gruppierung	**Empfehlung:** Gruppierung nach Kombination (B,S) von Benutzer und Sicherheitslösung **Begründung:** Änderungen sind in Gruppierungen je Sicherheitslösung und Benutzer effektiver zu kontrollieren.

→

Optionen und Anmerkungen	◗ Dieser Use-Case überwacht, dass Änderungen an Sicherheitssystemen nicht unbemerkt erfolgen. Es wird somit sichergestellt, dass diese Systeme auch tatsächlich noch ihren Zweck erfüllen. ◗ Je nach Art der überwachten Systeme kann es sein, dass Konfigurationsänderungen an Regelwerken häufig vorgenommen werden. So werden typischerweise Antivirus-Systeme eher selten umkonfiguriert, Firewallregeln jedoch häufig. Daher wird hier über die Negativliste die Zahl der Warnmeldungen eingeschränkt, indem sie autorisierte Benutzer ausschließt. Da hierbei Fehler in der Umsetzung geschehen können und so zu Sicherheitslücken führen, ist eine Ausnahme von der Alarmierung sorgsam abzuwägen. ◗ Es gibt verschiedene Ausbaumöglichkeiten, bspw. anstatt pauschal nur für bestimmte Aktivitäten je System Benutzer zu autorisieren.
Empfohlene Reaktion	Überprüfung und tiefergehende Analyse.
Referenz ATT&CK Techniques	T1562 [D] (Impair Defenses)
Referenz BSI	Keine Entsprechung
Referenz ATT&CK Tactics	Defense Evasion

3.9.27 B27 – Benutzer erhält besondere privilegierte Rechte

ID	B27
Name	Benutzer erhält besondere privilegierte Rechte
Kurzbeschreibung mit Detektionsziel	Es soll erkannt werden, wenn ein Benutzer mit besonders kritischen Rechten ausgestattet wird, bspw. die Aufnahme in die Administratorgruppe, Vergabe von Debug-Berechtigungen, root-Rechte, SAP_ALL etc.
Adressierte Risiken	Benutzerkonten mit hohen Rechten sind häufig das Ziel von Angreifern, um sich so mehr Möglichkeiten zu verschaffen, bspw. auf weitere Systeme zuzugreifen oder sich zu persistieren. Daher sollte insbesondere eine unbeabsichtigte Zuweisung von erhöhten Rechten verhindert werden. Alternativ versuchen Angreifer existierende Benutzerkonten mit erhöhten Rechten auszustatten oder anzulegen. Eine schnelle Erkennung verringert so ihre Möglichkeiten und begrenzt die Risiken.
Erforderliche Informationen	◗ Ereignis: – Ereignis E mit Ereigniscodes ACCT01 und ACCT03 – Benutzerkonto B, mit dem die Aktivität durchgeführt wird – Benutzerkonto D, dessen Rechte erweitert werden – Rechte R, die dem Benutzerkonto D zugewiesen werden – Gruppe G mit privilegierten Rechten, der der Benutzer zugewiesen wird
Benötigte Positiv- und Negativlisten	◗ Positivliste <PL_PRIVRECHTE_01>: Liste privilegierter Rechte, die überwacht werden sollen. Enthält typischerweise die von den Systemen gemeldeten Zeichenfolgen, die die entsprechenden Rechte darstellen. ◗ Negativliste <NL_AUTHNUTZER_01>: Liste der Benutzerkonten, die für die Durchführung der Zuweisung von erhöhten Rechten freigegeben sind. Diese Liste sollte sorgsam überwacht werden und idealerweise nur technische Benutzerkonten von automatisierten Prozessen aus bspw. Benutzerverwaltungssystemen enthalten. ◗ Negativliste <NL_AUTHNUTZER_02>: Liste der Benutzerkonten, die für den Erhalt der Zuweisung von erhöhten Rechten freigegeben sind. Diese Liste sollte sorgsam überwacht werden und idealerweise nur technische Benutzerkonten von automatisierten Prozessen enthalten, bspw. wenn durch eine Software oder einen Betriebssystemprozess regelmäßig temporär privilegierte Rechte benötigt werden. ◗ Positivliste <PL_PRIVGRUPPEN_01>: Liste von Gruppen mit privilegierten Berechtigungen, die bei Zuweisung von Benutzern diesen entsprechende zu überwachende Rechte geben
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	3 (sehr hoch)
Dringlichkeit	3 (unverzüglich)
Typische True Positives (kritisch)	◗ Privilegierte Rechte wurden einem Benutzerkonto über direkte Zuweisung erteilt. ◗ Privilegierte Rechte wurden einem Benutzerkonto über die Aufnahme in eine Gruppe mit privilegierten Rechten erteilt.
Typische True Negatives (unkritisch)	◗ Es werden keine privilegierten Rechte zugewiesen oder Benutzerkonten in Gruppen mit privilegierten Rechten aufgenommen. ◗ Durchführende oder empfangende Benutzerkonten stehen berechtigt auf einer Ausnahmeliste.
Typische False Positives (unkritisch)	◗ Fehler in der Listenpflege: Es sind nicht privilegierte Rechte oder Gruppen enthalten; für die Durchführung oder den Erhalt der Zuweisung befugte Benutzer sind nicht aufgenommen usw. ◗ Ein Softwareprozess benötigt neuerdings, bspw. nach einem Softwareupdate oder der Nutzung neuer Funktionalitäten, erhöhte Berechtigungen und weist diese Benutzern zu. ◗ Es finden Zuweisungen statt, die grundsätzlich nicht zulässig sind, aber für einen besonderen Einzelfall genehmigt wurden.
Typische False Negatives (kritisch)	◗ Fehlerhaft gepflegte Listen, bspw. fehlen zu überwachende Rechte oder Gruppen oder unzulässige Benutzerkonten sind freigegeben.

→

Fachliche Beschreibung der Regel	WENN das Ereignis E=ACCT01 von Rolle R durch Benutzerkonto B für Benutzerkonto D ODER E=ACCT03 von Gruppe G durch Benutzerkonto B für Benutzerkonto D EINTRITT, UND E=ACCT01 UND R ist enthalten in <PL_PRIVRECHTE_01> ODER E=ACCT03 UND G ist enthalten in <PL_PRIVGRUPPEN_01> UND B ist nicht enthalten in <NL_AUTHNUTZER_01> ODER D ist nicht enthalten in <NL_AUTHNUTZER_02> DANN löse aus
Gruppierung	**Empfehlung:** Gruppierung nach Benutzerkonto B **Begründung:** Multiple Aktivitäten durch denselben Benutzer werden zusammengefasst.
Optionen und Anmerkungen	◗ Privilegierte Rechte sollten so sparsam wie möglich Benutzerkonten zugewiesen oder verwendet werden. Neben einer regelmäßigen Rezertifizierung der Rechte sollte die Zuweisung direkt überwacht werden. ◗ Die obige Regel kann hierfür noch weiter ausgebaut werden: Beispielsweise könnte die Liste <NL_AUTHNUTZER_02> um die pro Benutzerkonto genehmigten privilegierten Rechte als Dimension erweitert werden. ◗ Auch der umgekehrte Fall könnte implementiert werden: Werden den Administratoren bzw. den für den Zweck der Berechtigungsadministration zugewiesenen Benutzerkonten die privilegierten Rechte entzogen, so könnte dies eine Aktivität von bereits auf den Systemen aktiven Angreifern sein, um der Organisation die Möglichkeiten zum Eingreifen zu nehmen.
Empfohlene Reaktion	Unverzügliche Kontrolle, ob die Zuweisung freigegeben ist. Falls nicht, entsprechende Analysen und Reaktionen wie das Zurücksetzen der Rechte einleiten.
Referenz ATT&CK Techniques	T1098 [D] (Account Manipulation), T1068 [G] (Exploitation for Privilege Escalation)
Referenz BSI	OPS.1.1.2 Ordnungsgemäße IT-Administration ORP.4 Identitäts- und Berechtigungsmanagement
Referenz ATT&CK Tactics	Privilege Escalation

3.9.28 B28 – Logins zu ungewöhnlichen Zeiten

ID	B28
Name	Logins zu ungewöhnlichen Zeiten
Kurzbeschreibung mit Detektionsziel	Beispielsweise finden außerhalb der Arbeitszeiten Logins – insbesondere privilegierte wie von Administratoren – in Systemen statt. Dies könnte ein Hinweis auf Zugriff eines Angreifers von außerhalb oder eine Malware-Aktivität sein.
Adressierte Risiken	Logins zu unüblichen Zeiten können auf ein unerwünschtes Eindringen von Angreifern hinweisen. Auslöser können sowohl Datenverbindungen von Personen als auch von maliziöser Software sein.
Erforderliche Informationen	◗ Ereigniscode AUTH01 für eine Anmeldung mit einem Benutzerkonto ◗ Zeitraum „time_ok", der die üblichen Arbeitszeiten beschreibt ◗ Zeit t, bei der der Login erfolgt ◗ Benutzername B, mit dem der Login stattfindet ◗ IP-Adresse IP, von der aus der Zugriff durchgeführt wird ◗ Optional: System Z, auf dem der Login erfolgt
Benötigte Positiv- und Negativlisten	◗ Optional: Positivliste <PL_SENSIBLESYSTEME_01>: Systeme Z, die mit diesem Use-Case zu überwachen sind ◗ Negativliste <NL_ZUGELASSENEIPS_01>: zulässige IP-Adressen (z. B. Jump-Hosts oder Managementsysteme)
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	1 (normal)
Dringlichkeit	2 (schnell 2)
Typische True Positives (kritisch)	◗ Es erfolgt auf einem System ein Login zu unüblichen Zeiten.
Typische True Negatives (unkritisch)	◗ Es erfolgt auf einem System ein Login zu üblichen Zeiten.
Typische False Positives (unkritisch)	◗ Die Negativliste <NL_ZUGELASSENEIPS_01> ist falsch gepflegt. Dadurch fehlen darin IP-Adressen, von denen aus der Login eigentlich zulässig ist. Daher werden unkritische Fehlalarme ausgelöst.
Typische False Negatives (kritisch)	◗ Der Login erfolgte auf einem System, das überwacht werden soll, aber versehentlich nicht in <PL_SENSIBLESYSTEME_01> steht. ◗ Der Login erfolgte von einer IP-Adresse, die versehentlich in <NL_ZUGELASSENEIPS_01> aufgeführt ist, aber eigentlich nicht zugelassen ist.
Fachliche Beschreibung der Regel	WENN das Ereignis AUTH01 mit Benutzer B zum Zeitpunkt t von IP aus auf System Z EINTRITT, UND t ist nicht innerhalb time_ok UND IP ist nicht enthalten in <NL_ZUGELASSENEIPS_01> UND Z ist enthalten in <PL_SENSIBLESYSTEME_01> (optional) DANN löse aus
Gruppierung	**Empfehlung:** Gruppierung nach Benutzer B **Begründung:** Arbeitet ein Benutzer außerhalb der üblichen Arbeitszeit, so können schnell zahlreiche Systeme verwendet werden. Die Gruppierung nach dem Benutzer fasst dies zusammen und verhindert eine unnötig große Zahl einzelner Warnmeldungen.

→

Optionen und Anmerkungen	◗ In größeren Organisationen mit weltweit verteilten Standorten sollten die üblichen Geschäftszeiten (time_ok) mit den jeweiligen Geolokationen verknüpft werden. ◗ Es kann auch hilfreich sein, Negativlisten einzuführen, um genehmigte Wartungsarbeiten außerhalb der Bürozeiten abzufangen.
Empfohlene Reaktion	Verdächtige Logins sind mit dem Benutzer im Nachgang abzusprechen. Im Fall eines Logins mit einem administrativen Account sollte dies mit hoher Priorität erfolgen.
Referenz ATT&CK Techniques	T1078 [G] (Valid Accounts)
Referenz BSI	ORP.4 Identitäts- und Berechtigungsmanagement
Referenz ATT&CK Tactics	Initial Access, Privilege Escalation

3.9.29 B29 – Mehrfach fehlgeschlagene Anmeldeversuche über längeren Zeitraum

ID	B29
Name	Mehrfach fehlgeschlagene Anmeldeversuche über längeren Zeitraum
Kurzbeschreibung mit Detektionsziel	Es soll erkannt werden, wenn ein Angreifer über einen längeren Zeitraum versucht, sich in ein Benutzerkonto einzuloggen. Hierbei geht es um »slow attacks«, also um Angriffe, bei denen bewusst in längeren Zeitabständen wie bspw. alle 10 min, jede 1 h oder einem ähnlichen Zeitfenster ein Versuch gestartet wird, um keine Aufmerksamkeit zu erregen. Wenn erfolgreiche Anmeldungen dazwischenliegen, so soll der Alarm nicht ausgelöst werden, da dies sonst sehr viele False Positives verursachen kann.
Adressierte Risiken	Erkennen eines langlaufenden Angriffs, der von anderen Use-Cases aufgrund eines längeren Abstandes nicht erkannt wird
Erforderliche Informationen	◗ Ereignis: – Ereigniscodes AUTH01.* für Anmeldung (erfolgreich + abgelehnt) – Benutzer B, der die Aktivität versucht durchzuführen – Zielsystem Z, auf dem die Aktivität durchgeführt wird – Quellsystem Q, von dem aus die Aktivität durchgeführt wird ◗ Benutzer je System oder global, bei denen dieses Verhalten zulässig oder besonders unzulässig ist (siehe Positiv- und Negativlisten) ◗ Angabe eines Gesamtzeitraums t, der betrachtet wird ◗ Angabe eines Zeitabstands bzw. Intervalls i, in dem ein erfolgloser Login geprüft wird. t muss durch i ganzzahlig teilbar sein. ◗ Angabe eines Schwellenwerts n, der die Zahl der mindestens aufgetretenen Versuche festlegt, ab dem eine Warn- oder Berichtsmeldung erfolgt.
Benötigte Positiv- und Negativlisten	◗ Positivliste <PL_NUTZER_01>: Benutzer, bei deren erfolgreichem Einsatz immer gewarnt werden sollte. Inhalt sind Kombinationen (B,Z,Q) mit – B: Benutzer-ID – Z: Zielsystem oder '*' (für global), für das die Benutzer-ID als kritisch gilt – Q: Quellsystem oder '*' (für global), für das die Benutzer-ID in Kombination mit einem Zielsystem als Verbindung als kritisch gilt ◗ Negativliste <NL_NUTZER_01>: Benutzer, die global, je System oder in speziellen Verbindungen zulässig sind. Inhalt sind Kombinationen (B,Z,Q) mit – B: Benutzer-ID – Z: Zielsystem oder '*' (für global), für das die Benutzer-ID als unkritisch gilt – Q: Quellsystem oder '*' (für global), für das die Benutzer-ID in Kombination mit einem Zielsystem als Verbindung als unkritisch gilt **Hinweis:** Im Fall von '*' ist jeder Wert enthalten, es gilt also: Ein Benutzer B1 und ein System S1 sind enthalten in (B1,S1) sowie in (B1,*) oder (*,S1).
Empfohlener Reaktionstyp	Bericht
Kritikalität	2 (hoch)
Dringlichkeit	1 (normal)

→

Typische True Positives (kritisch)	◗ Ein Angreifer versucht über einen längeren Zeitraum, Benutzer und Passwortkombinationen zu erraten bzw. mittels vorhandener Listen und Brute-Force-Attacken durchzuprobieren.
Typische True Negatives (unkritisch)	◗ Ein solches Verhalten tritt von Quellsystemen aus auf, für die dies zulässig ist, bspw. eigene Schwachstellenscanner oder Pentest-Systeme. ◗ Es tritt für Benutzer auf der Negativliste auf, die aufgrund eines bekannten fehlerhaften Verhaltens sonst immer wieder unnötig alarmiert würden, bspw. bei fehlerhafter Passwortsetzung in einem Quellsystem, das nicht in der Hoheit der Organisation liegt und bei dem die Korrektur stets lange dauert.
Typische False Positives (unkritisch)	◗ Es gab einen Passwortwechsel für den Benutzer und der aufrufende Prozess fragt nur in längeren Zeitabständen an. ◗ Das Quellsystem ist ein für einen solchen Zweck erlaubtes System wie ein Schwachstellenscanner oder ein Pentest-System, das aber nicht auf der Liste steht. ◗ i, t und s sind in der Kombination zu empfindlich eingestellt.
Typische False Negatives (kritisch)	◗ i, t und s sind in der Kombination zu unempfindlich eingestellt. ◗ Benutzer oder Quell-/Zielsysteme stehen fälschlicherweise auf einer Negativliste.
Fachliche Beschreibung der Regel	Im Folgenden ist ◗ Minimum(a,b): die Minimum-Funktion, die die kleinere Zahl von zwei Zahlen a und b zurückgibt ◗ Summe (s1, s2, ...): gibt die Summe der Zahlen bzw. Vorkommen von s1+s2+... wieder ◗ t_# = t / i ◗ i_x mit x=[1..t_#] das Intervall, das an x-ter Stelle steht **Beispiel:** t=24h und i=10 min, dann ist t_x = 24 * 60 min / 10 min = 144 und i_x mit x=[1..144], es gibt also 144 zu betrachtende Intervalle. WENN die Ereignisse E für System Z von System Q aus mit Benutzer B im Zeitraum t EINTRETEN, UND E[1..i_x] != AUTH01.succ UND Summe (Minimum(Summe(E[1..i_x] = AUTH01.fail), 1) UND (B,Z,Q) ist nicht enthalten in <NL_NUTZER_01> ODER (B,Z,Q) ist enthalten in <PL_NUTZER_01>) >= n DANN löse aus Empfohlene Schwellenwerte: i, t und s müssen passend für die Systeme und Benutzer gewählt werden. Richtwerte hierfür sind t = 24 h, i=10 min und n = 24.
Gruppierung	**Empfehlung:** Gruppierung nach der Kombination (B,Z,Q) **Begründung:** So ist eine Identifikation der verwendeten Benutzer zusammen mit den beteiligten Systemen möglich. Über eine Häufigkeitsanalyse lassen sich so schnell Priorisierungen durchführen.

→

Optionen und Anmerkungen	◗ Dieser Use-Case ist je nach technischen Möglichkeiten sehr unterschiedlich zu implementieren. Wird eine Auswertung mittels Skripten oder eines SIEM-Systems mit Gruppierungs- und Zählfunktionen durchgeführt, so sieht eine Umsetzung dem oben angeführten recht ähnlich. Bei SIEM-Systemen, die Ereignisse in einem Zwischenspeicher halten und in (nahezu) Echtzeit warnen, wird sich dies wiederum sehr davon unterscheiden, da hier »nach vorne« geprüft wird. Grundsätzlich ist der Ablauf wie folgt: 1. Prüfe für den gewählten Zeitraum, dass es keine erfolgreichen Anmeldungen in der Kombination Benutzer, Ziel und Quelle gibt. 2. Zähle die Zahl der Intervalle, in denen mindestens ein fehlgeschlagener Anmeldungsversuch in der Kombination Benutzer, Ziel und Quelle vorgekommen ist, zusammen. 3. Berücksichtige dabei, ob es Anmeldeversuche in Kombination Benutzer, Ziel und Quelle gibt, die ausgenommen sind. 4. Prüfe, ob die sich ergebende Gesamtzahl über dem Schwellenwert liegt und löse die Warnmeldung bzw. den Bericht entsprechend aus. ◗ Dieser Use-Case kann entweder als Warnmeldung oder als Bericht implementiert werden. Aufgrund der typischerweise längeren Zeit, bis ein Angreifer einen Erfolg erzielt, der meist großen Ressourcen-Aufwände für die Ermittlung dieses Ergebnisses und der potenziell großen Zahl der Ergebnisse, die zu überprüfen sind, wird ein Bericht mit einer täglichen Auswertung empfohlen. ◗ Die Standardimplementierung oben sieht vor, dass stets eine Kombination aus Benutzer, Zielsystem und Quellsystem verwendet wird, um die Wahrscheinlichkeit von False Positives zu reduzieren. Würden bspw. nur Benutzer berücksichtigt werden, so würden fehlerhafte Aufrufe von einzelnen Benutzern insgesamt angezeigt werden, auch wenn sie voneinander unabhängig sind. Eine solche Generalisierung, auch nur in Kombination mit einem Zielsystem, mag in manchen Fällen sinnvoll sein, meistens ist sie jedoch zu empfindlich. ◗ Negativlisten sollten sorgsam geprüft werden, da diese Art eines regelmäßig fehlerhaften Zugriffversuchs eher untypisch ist.
Empfohlene Reaktion	Üblicher Prozess der Überprüfung
Referenz ATT&CK Techniques	T1110 [G] (Brute Force), T1087 [G] (Account Discovery)
Referenz BSI	ORP.4 Identitäts- und Berechtigungsmanagement
Referenz ATT&CK Tactics	Initial Access, Discovery

→

3.9.30 B30 – Zugriff auf PAM-verwaltete Systeme ohne PAM

ID	B30
Name	Zugriff auf PAM-verwaltete Systeme ohne PAM
Kurzbeschreibung mit Detektionsziel	PAM steht für Privileged Account Management, ein Verfahren, das spezielle Identitäten mit privilegierten Berechtigungen im Rahmen eines Identity-Managements verwaltet. Benutzer dürfen sich auf PAM-verwalteten Systemen üblicherweise nur mit nicht privilegierten Berechtigungen anmelden und müssen bei Bedarf über die PAM-Lösung Berechtigungen freischalten oder (kurzfristig) gültige Passwörter für speziell reservierte Benutzer mit hohen Privilegien erhalten. Angreifer können sich jedoch bei Erlangung entsprechender Zugriffsinformationen unter Umständen direkt an den Zielsystemen anmelden, ohne über die kontrollierten und gesteuerten Prozesse der PAM-Lösung zu gehen.
Adressierte Risiken	Haben Angreifer Kenntnis der erforderlichen Zugangsinformationen für PAM-verwaltete privilegierte Benutzerkonten, so können sie sich direkt auf Zielsystemen anmelden. Sind die verwendeten Benutzerkonten in der Überwachung ausgenommen, da sie eigentlich über die PAM-Lösung abgesichert sein sollten, so können Angreifer umfangreiche Aktivitäten ohne Kontrolle durchführen.
Erforderliche Informationen	◗ Ereigniscodes AUTH01.* für Anmeldung (erfolgreich + abgelehnt) ◗ Zielsystem Z, auf dem die Anmeldung erfolgt ◗ Benutzerkonto B, mit dem eine Anmeldung versucht wird ◗ Quellsystem Q, von dem aus die Anmeldung erfolgt ◗ <GL_PAM_01>: Liste im Format (Z,Q,B) mit Z: IP-Adressen oder Hostnamen der Systeme, die mit diesem Use-Case zu überwachen sind Q: Für Z zuständiges PAM-System B: Benutzerkonten je Zielsystem Z, die mittels der PAM-Lösung Q verwaltet werden
Benötigte Positiv- und Negativlisten	–
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	2 (hoch)
Dringlichkeit	2 (schnell)
Typische True Positives (kritisch)	◗ Es erfolgt eine Anmeldung auf einem PAM-verwalteten System über einen Non-PAM-Zugriff.
Typische True Negatives (unkritisch)	◗ Es erfolgt eine Anmeldung über einen Non-PAM-Zugriff auf ein PAM-verwaltetes System, das nicht in der Liste steht und auch nicht überwacht werden muss.
Typische False Positives (unkritisch)	◗ Es erfolgt eine Anmeldung über einen Non-PAM-Zugriff auf ein PAM-verwaltetes System. Das System muss nicht überwacht werden, wurde aber versehentlich in die Überwachung aufgenommen.
Typische False Negatives (kritisch)	◗ Es erfolgt eine Anmeldung über einen Non-PAM-Zugriff auf ein PAM-verwaltetes System. Versehentlich wurde das betreffende Zielsystem nicht in die Überwachung aufgenommen.
Fachliche Beschreibung der Regel	WENN das Ereignis AUTH01.* auf Zielsystem Z mit Benutzer B von Quellsystem Q EINTRITT, UND Z und B sind enthalten (Z,*,B) UND (Z,Q,B) ist nicht enthalten in <GL_PAM_01> DANN löse aus
Gruppierung	**Empfehlung:** Gruppierung nach der Kombination (B, Z) von verwendetem Benutzerkonto B und Zielsystem Z **Begründung:** Die Trennung der unterschiedlichen privilegierten Zugriffe erleichtert die Übersicht in der Auswertung, gerade wenn mehrere Anmeldungen mit dem gleichen Benutzerkonto auf einem System erfolgen.

→

Optionen und Anmerkungen	◗ Dieser Ansatz hier geht davon aus, dass für die Verwendung privilegierter Zugriffe spezielle Benutzerkonten (eigene IDs) verwendet werden. Diese sind normalerweise mit einem geheimen bzw. zufällig generierten Passwort versehen, das nur der PAM-Lösung bekannt ist. Der Zugriff erfolgt transparent über die PAM-Lösung, sie wird also als Sprungserver verwendet. ◗ Wenn keine speziellen Benutzerkonten für privilegierte Zugriffe vorgesehen sind, so lässt sich das ebenfalls abbilden, indem automatisiert temporär die entsprechende Kombination (Z,Q,B) in die <GL_PAM_01> oder eine weitere Negativliste aufgenommen wird. ◗ Für Notzugänge, bspw. wenn die PAM-Lösung ausfallen sollte, werden oftmals separate Konten angelegt, deren Passwörter auf andere Weise (bspw. Safe) verwaltet werden. Diese sollten als spezielle Konten über andere Use-Cases überwacht werden.
Empfohlene Reaktion	Die eintreffenden Warnmeldungen sollten schnell untersucht werden, da es hier um privilegierte Anmeldungen geht und der Angreifer somit hohe Zugriffsrechte im Zielsystem hat.
Referenz ATT&CK Techniques	T1078 [D] (Valid Accounts)
Referenz BSI	ORP.4 Identitäts- und Berechtigungsmanagement
Referenz ATT&CK Tactics	Initial Access, Persistence

3.9.31 B31 – Verwendung kritischer Funktionen

ID	B31
Name	Verwendung kritischer Funktionen
Kurzbeschreibung mit Detektionsziel	Die Nutzung kritischer Funktionen wie Debugger auf Produktionssystemen, Kommandos zum Löschen oder Verschlüsseln aller Daten (rm * -f -r, encrypt...) oder für bestimmte Anwendungen besonders kritische Funktionen (SQL-Kommandos in SAP o. Ä.) soll überwacht werden, um eine schnelle Reaktion zu erlauben.
Adressierte Risiken	Kritische Funktionen können Spuren verwischen, Zugriff auf üblicherweise nicht zugängliche Informationen ermöglichen oder Manipulation inklusive Löschung von Daten ermöglichen. Beispielsweise ist beim Einsatz von Debuggern keine nachträgliche Kontrolle mehr möglich (Datenzugriffe und -änderungen im Speicher, Überspringen von Logfunktionen etc.). Die Nutzung derartiger Funktionen soll erkannt werden.
Erforderliche Informationen	◗ Ereignis: – Ereigniscode PSTART02 für Aufruf/Ausführung von Funktionen – Programm P – Funktion F – Benutzer U, der die Aktivität durchführt – Prozess/Programm A, das bzw. in dem diese Funktionen ausgeführt werden – Zielsystem Z, auf dem die Aktivität durchgeführt wird
Benötigte Positiv- und Negativlisten	◗ Positivliste <PL_SENSIBLESYSTEMEUNDPROZESSE_01>: kritische Funktionen je System, je Prozess, je System und Prozess, global oder in weiteren Kombinationen ◗ Negativliste <NL_ZUGELASSENENUTZER_01>: Benutzerkonten je System/Prozess/global, bei denen die Nutzung dieser Funktionen zulässig ist ◗ Negativliste <NL_ZUGELASSENESYSTEMEUNDPROZESSE_01>: Systeme oder Prozess/Programm je System, bei denen dieses Verhalten zugelassen wird
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	Entspricht SBF
Dringlichkeit	2 (hoch)
Typische True Positives (kritisch)	◗ Eine kritische Funktion wird in einem Programm aufgerufen, für das der Benutzer nicht autorisiert ist (bspw. Debugger auf Produktionssystem wird genutzt, um Berechtigungsprüfungen zu überspringen).
Typische True Negatives (unkritisch)	◗ Eine nicht kritische Funktion wird aufgerufen. ◗ Der Benutzer, der die kritische Funktion aufruft, ist autorisiert, diese zu verwenden.
Typische False Positives (unkritisch)	◗ Eine autorisierte, möglicherweise einmalige Tätigkeit wie die Behebung einer Störung oder Nutzung einer kritischen Funktion findet statt, ohne dass der Benutzer oder das entsprechende System auf einer Negativliste steht. ◗ Die Negativlisten sind nicht korrekt oder vollständig gepflegt.
Typische False Negatives (kritisch)	◗ Die Positivliste der kritischen Funktionen ist nicht vollständig bzw. aktuell. ◗ Benutzer, Systeme oder Prozesse stehen in den Negativlisten, für die eine Freigabe nicht existiert. ◗ Das verwendete Benutzerkonto ist kompromittiert.
Fachliche Beschreibung der Regel	WENN das Ereignis PSTART02 für Programm P für Funktion F auf System Z mit Benutzer U EINTRITT, UND (F,*), (F,P), (F,P,Z), ... sind enthalten in <PL_SENSIBLESYSTEMEUNDPROZESSE_01>, UND (U,*), (U,Z), (U,P,*), … sind nicht enthalten in <NL_ZUGELASSENENUTZER_01> UND Z oder (P,Z) sind nicht enthalten in <NL_ZUGELASSENESYSTEMEUNDPROZESSE_01> DANN löse aus

→

Gruppierung	**Empfehlung:** Kombination Benutzer mit Programm und System (U,P,Z) **Begründung:** So ist eine Gruppierung möglich, die nicht zu granular ist und beim Überblick hilft.
Optionen und Anmerkungen	◗ Optional könnte der Elternprozess hinzugenommen werden, um noch genauer die Negativlisten zu gestalten. Beispielsweise können in Systemen teilweise Funktionen andere Funktionen intern aufrufen, was dann in Ordnung ist, auch wenn es indirekt durch Benutzer geschieht, die nicht dafür befugt sind. ◗ Das Quellsystem könnte hinzugenommen werden, um die Nutzung nur durch bestimmte Systeme zu erlauben. Im Fall von Housekeeping oder Backups durch zentrale Systeme könnte dies sinnvoll sein. ◗ Manchmal kann es vorkommen, dass gleiche Kommandos unterschiedliche Bedeutung in unterschiedlichen Programmen haben. Daher empfiehlt es sich, wenn die Information über das verwendete Programm zur Verfügung steht, Funktionen mit Programmen in der Positivliste zu kombinieren. Ebenso können die eigentlich kritischen Funktionen auf manchen Systemen unkritische Funktionen sein, bspw. Löschkommandos oder Debugger auf Entwicklungssystemen. ◗ Es sollten mindestens solche Kommandos ausgenommen werden, die Folgendes ermöglichen: – Das (massenweise) Löschen von Daten – Stoppen von für den Betrieb wesentlichen Systemservices – Unmittelbare Beeinträchtigung der Lauffähigkeit des Systems (BIOS-Flash, – Löschen/Formatieren Datenträger) – Nutzung von Debugging-Funktionen – Mitlesen oder Mitschneiden von Daten – Ausführen von Kommandos durch einen anonymen Benutzer (z. B. SQL-Kommandos aus Applikationsebene oder OS-Kommandos aus Applikation oder Datenbank) – Verschlüsseln von Daten – Verändern der Netzwerkkonfiguration – Anlegen von Benutzerkonten auf einem Nicht-Standard-Weg (z. B. direkter Eintrag von Nutzern in SQL-Tabelle für eine Applikation, anstatt über vorhandene Applikationsverwaltungsfunktionen zu gehen)
Empfohlene Reaktion	Üblicher Prozess der Überprüfung
Referenz ATT&CK Techniques	T1548 [G] (Abuse Elevation Control Mechanism), T1057 [G] (Process Discovery), T1082 [G] (System Information Discovery), T1049 [G] (System Network Connections Discovery), T1033 [G] (System Owner/User Discovery), T1007 [G] (System Service Discovery), T1124 [G] (System Time Discovery), T1531 [G] (Account Access Removal), T1485 [G] (Data Destruction), T1486 [G] (Data Encrypted for Impact), T1565 [G] (Data Manipulation), T1561 [G] (Disk Wipe), T1495 [G] (Firmware Corruption), T1490 [G] (Inhibit System Discovery), T1489 [G] (Service Stop), T1529 [G] (System Shutdown/Reboot)
Referenz BSI	Keine Entsprechung
Referenz ATT&CK Tactics	Defense Evasion, Discovery, Impact

3.9.32 B32 – Systemkommunikation in externe Netze

ID	B32
Name	Systemkommunikation in externe Netze
Kurzbeschreibung mit Detektionsziel	Dieser Use-Case soll Systemkommunikation zu externen Netzen erkennen, die nicht zulässig ist, bspw. von internen Netzen/Systemen direkt ins Internet oder zu Dienstleister-/Cloud-Infrastruktur, für die keine Notwendigkeit besteht.
Adressierte Risiken	Nicht freigegebene Kommunikation in externe Netze kann auf bösartige Aktivitäten wie bspw. Exfiltration oder Command-and-Control-Aktivitäten im Rahmen einer Schadsoftware hindeuten. Des Weiteren können hiermit indirekte Security-Risiken wie Schatten-IT oder fehlerhafte Konfigurationen von Systemen erkannt werden.
Erforderliche Informationen	◗ Ereignis E: Jede Art von Ereigniscode mit Informationen über die Herkunft, bspw. IP-Adressen oder Hostnamen/FQDN. Mindestens NET01 sollte darunter sein. ◗ Quellsystem Q mit Herkunftsinformation ◗ Zielsystem Z, auf das zugegriffen wird
Benötigte Positiv- und Negativlisten	◗ Negativliste <NL_NETZE_01>: Liste der durch die Organisation selbst grundsätzlich zugelassenen externen Netze ◗ Positivliste <PL_NETZE_01>: Liste der durch die Organisation selbst als in jedem Fall unzulässig eingestuften externen Netzwerke bzw. Endpunkte ◗ Negativliste <NL_ENDPUNKTE_01>: Liste der durch die Organisation selbst grundsätzlich zugelassenen Endpunkte, die in externe bzw. nicht interne Netze kommunizieren dürfen. Typischerweise sind dies Firewalls am Perimeter, Proxy-Systeme, Nameserver und Ähnliches. ◗ <GL_NETZEINTERN_01>: Liste der eigenen Netze bzw. Endpunkte
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	2 (hoch)
Dringlichkeit	2 (schnell)
Typische True Positives (kritisch)	◗ Ein System kommuniziert mit externen Netzen oder Endpunkten, die als besonders kritisch eingestuft wurden. ◗ Ein System kommuniziert mit externen Netzen oder Endpunkten, obwohl es dies nicht sollte. Beispielsweise könnten Desktops/Notebooks direkt mit dem Internet kommunizieren, obwohl sie nach Organisationsvorgaben immer über einen geschützten Proxy gehen müssen. ◗ Ein neues Netz oder System, das nicht existieren sollte (Schatten-IT), kommuniziert mit externen Netzen.
Typische True Negatives (unkritisch)	◗ Systeme auf einer der Negativlisten sind Quelle oder Ziel der Kommunikation.
Typische False Positives (unkritisch)	◗ Die Listen sind nicht korrekt gepflegt: Es fehlen bspw. interne Netze auf den entsprechenden Listen oder finden sich fälschlicherweise auf der Positivliste. ◗ Systeme, die in bzw. mit externen Netzen kommunizieren müssen, waren nicht bekannt und wurden daher nicht auf Negativlisten aufgenommen. ◗ Netzwerkverbindungen sind zusammengebrochen, bspw. bei einer Stateful Firewall, sodass Antwortpakete wie eine neue Verbindung erscheinen, obwohl sie eigentlich zu einer extern eröffneten Verbindung gehören und möglicherweise zulässig sind. ◗ Ein grundsätzlich nicht zulässiger, aber im speziellen Fall autorisierter Zugriff findet statt.
Typische False Negatives (kritisch)	◗ Es sind Netze oder Endpunkte fälschlicherweise in den Negativlisten enthalten. ◗ Der Datenverkehr zwischen internen und externen Netzen wird nicht vollständig erfasst bzw. nicht alle relevanten Ereignisse werden ausgewertet.

→

Fachliche Beschreibung der Regel	WENN das Ereignis E EINTRITT, UND Q ist enthalten in <GL_NETZEINTERN_01> UND Z ist enthalten in <PL_NETZE_01> ODER Q ist nicht enthalten in <NL_ENDPUNKTE_01> UND Z ist nicht enthalten in <NL_NETZE_01> UND Z ist nicht enthalten in <GL_NETZEINTERN_01> DANN löse aus
Gruppierung	**Empfehlung:** Gruppierung nach System Z **Begründung:** Die Kommunikation zu einem externen Zielpunkt wird zusammengefasst.
Optionen und Anmerkungen	◗ Werden Netze, insbesondere die internen Netze, korrekt eingepflegt und die Aufnahme von eigenen Endpunkten in Negativlisten restriktiv gehandhabt, kann dieser Use-Case sehr viele Bedrohungsszenarien abdecken. So ist bspw. unerheblich, auf welche Art und Weise (Protokolle, Ports etc.) oder mit welcher Verschleierungstaktik (Verschlüsselung, Codierung, Verschleierung etc.) gearbeitet wird – wenn eine Quelle-Ziel-Kommunikation stattfindet, die grundsätzlich nicht sein darf, so wird dies erkannt. Dies funktioniert allerdings nur eingeschränkt für freigegebene Endpunkte und solche, die als Zwischenstation dienen, wie z. B. Proxy-Systeme. Hier müssen weitere Maßnahmen ergriffen werden. ◗ Nicht zulässige Kommunikation aus dem eigenen Netz in externe Netze ist generell kritisch, da das eigene Netz der Organisation wohlbekannt und zumindest der Perimeter klar abgesteckt sein dürfte. Abgesehen von Fehlern in der Listenpflege oder in kurzen Zeiträumen von Umbaumaßnahmen dürften False Positives hier eher ungewöhnlich sein und selten auftreten. Je nachdem, in welcher Situation die Organisation ist, kann es daher auch sinnvoll sein, die Kritikalität auf 3 (sehr hoch) zu setzen. ◗ Eine Ausbaumöglichkeit für diesen Use-Case wäre die Aufnahme von Punkt-zu-Punkt-Verbindungen in Negativ- und Positivlisten. Somit könnten gezielt einzelne Verbindungsstrecken freigegeben oder überwacht werden. ◗ Solange nicht aufgrund von Fehlkonfigurationen im Netz oder von Netzwerkproblemen die Zahl der durch erfolglose Versuche ausgelösten Warnmeldungen zu groß wird, sollten sowohl erfolgreiche als auch erfolglose Versuche des Zugriffs auf externe Netze überwacht werden: Bei erfolgreichen Zugriffen hat sich ein Risiko wahrscheinlich bereits manifestiert, bei erfolglosen gibt es wertvolle Hinweise auf laufende und noch nicht völlig erfolgreiche maliziöse Aktivitäten (bspw. Schadsoftware, die erfolglos versucht, Kontakt zu einem Command-and-Control-Server aufzunehmen). Ist dies aber nicht erwünscht, so kann anstelle von »E« »E.fail« überwacht werden.
Empfohlene Reaktion	Es sollten zunächst Fehler ausgeschlossen werden (Antwortpakete statt eigenständiger Verbindungen von intern nach extern, kein offenkundiger Fehler bei internen Netzen o. Ä.). Ist dies geschehen, so ist zügig in die Analyse inklusive Umfeldanalyse einzusteigen.
Referenz ATT&CK Techniques	T1071 [G] (Application Layer Protocol), T1132 [G] (Data Encoding), T1001 [G] (Data Obfuscation), T1568 [G] (Dynamic Resolution), T1573 [G] (Encrypted Channel), T1008 [G] (Fallback Channels), T1665 [G] (Hide Infrastructure), T1104 [G] (Multi-Stage Channels), T1095 [G] (Non-Application Layer Protocol), T1571 [G] (Non-Standard Port), T1572 [G] (Protocol Tunneling), T1090 [G] (Proxy), T1219 [G] (Remote Access Software), T1102 [G] (Web Service), T1020 [D] (Automatic Exfiltration), T1030 [D] (Data Transfer Size Limits), T1048 [D] (Exfiltration Over Alternative Protocol), T1041 [D] (Exfiltration Over C2 Channel), T1011 [G] (Exfiltration Over Other Network Medium), T1567 [G] (Exfiltration Over Web Service), T1029 [D] (Scheduled Transfer)
Referenz BSI	Keine Entsprechung
Referenz ATT&CK Tactics	Command and Control, Exfiltration

3.9.33 B33 – Unzulässige Systemkommunikation erkennen

ID	B33
Name	Unzulässige Systemkommunikation erkennen
Kurzbeschreibung mit Detektionsziel	Es soll unzulässige Kommunikation zwischen Systemen oder Netzwerksegmenten der Organisation identifiziert werden. Dieser Use-Case hilft, die Ausbreitung von Angreifern im Netz (»Lateral Movement«) und die Ausspähung des Netzwerks (»Discovery«) zu erkennen.
Adressierte Risiken	Wenn Angreifer in ein Netz eingedrungen sind, so versuchen sie zunächst, Informationen über die Umgebung zu erlangen und sich auf weiteren Systemen Zugang zu verschaffen. Dies sind wesentliche Voraussetzungen für die nächsten Schritte bzgl. Ausspähung von Daten, die Erhöhung von Zugriffsrechten und Weiteres.
Erforderliche Informationen	◗ Ereignis E: Jede Art von Ereigniscode mit Informationen über die Herkunft, bspw. IP-Adressen oder Hostnamen/FQDN. Mindestens NET01 sollte darunter sein. ◗ Quellsystem Q mit Herkunftsinformation ◗ Zielsystem Z, auf das zugegriffen wird
Benötigte Positiv- und Negativlisten	◗ Negativliste <NL_NETZWERKKOMMUNIKATION_01>: Liste über grundsätzlich zulässige Kommunikation zwischen Netzen. Inhalt ist (QN,ZN) mit – QN: Quellnetz/Endpunkt, von dem die Kommunikation ausgeht – ZN: Zielnetz/Endpunkt, zu dem die Kommunikation erfolgt Typischerweise erlaubt eine Organisation nur die Kommunikation zwischen bestimmten Netzen, diese wären hier einzutragen. ◗ Positivliste <PL_NETZWERKKOMMUNIKATION_01>: Liste über dediziert nicht zulässige Verbindungen. Inhalt ist (QN,ZN) mit – QN: Quellnetz/Endpunkt, von dem die Kommunikation ausgeht – ZN: Zielnetz/Endpunkt, zu dem die Kommunikation erfolgt Hiermit können einzelne Verbindungen untersagt werden, bspw. wenn sich ein kritischer Endpunkt in einem Zielnetz befindet, alle anderen in diesem Netz aber für die Kommunikation zugelassen sind. ◗ Negativliste <NL_NETZENDPUNKTE-QUELLE_01>: Netze/Endpunkte, von denen als Quelle alle Kommunikation grundsätzlich zulässig ist. ◗ Negativliste <NL_NETZENDPUNKTE-ZIEL_01>: Netze/Endpunkte, zu denen als Ziel alle Kommunikation grundsätzlich zulässig ist.
Empfohlener Reaktionstyp	Bericht
Kritikalität	1 (Normal)
Dringlichkeit	1 (Normal)
Typische True Positives (kritisch)	◗ Eine Kommunikation zwischen Netzen bzw. Endpunkten, die dafür nicht freigegeben ist oder die explizit untersagt ist, hat stattgefunden.
Typische True Negatives (unkritisch)	◗ Nur zulässige Kommunikation findet statt.
Typische False Positives (unkritisch)	◗ Die Listen sind nicht korrekt gepflegt, bspw. sind nicht alle zulässigen bekannten Netz-zu-Netz-Verbindungen enthalten. ◗ Bisher nicht bekannte, aber zulässige Verbindungen fehlen in den Listen. ◗ Ein grundsätzlich nicht zulässiger, aber im speziellen Fall autorisierter Zugriff findet statt.
Typische False Negatives (kritisch)	◗ Netze bzw. Endpunkte befinden sich auf den Negativlisten, die nicht zulässig sind. ◗ Der Datenverkehr wird nicht vollständig erfasst bzw. nicht alle relevanten Ereignisse werden ausgewertet.

→

Fachliche Beschreibung der Regel	WENN das Ereignis E EINTRITT, UND (QN,ZN) ist enthalten in <PL_NETZWERKKOMMUNIKATION_01> ODER ZN ist enthalten in <PL_NETZENDPUNKTE-ZIEL_01> ODER (QN,ZN) ist nicht enthalten in <NL_NETZWERKKOMMUNIKATION_01> UND QN ist nicht enthalten in <NL_NETZENDPUNKTE-QUELLE_01> DANN löse aus
Gruppierung	**Empfehlung:** Kombination von (QN,ZN) **Begründung:** Kommunikationsstrecken werden sichtbar und lassen sich bspw. anhand ihres Datenvolumens und der Art der Kommunikation leichter priorisieren.
Optionen und Anmerkungen	◗ Grundsätzlich kann bei einer sich nur selten ändernden Netzwerkstruktur auch auf Warnmeldung umgestellt werden. Allerdings gibt es in einem Netzwerk häufig Änderungen, bspw. werden neue Systeme oder neue Software eingeführt bzw. nach Softwareupdates kommunizieren Systeme über neue Strecken miteinander oder es gibt Erweiterungen und Umstrukturierungen. Daher wird im Normalfall ein regelmäßiger Bericht zielführender sein. ◗ Der Use-Case könnte auch weiter verfeinert werden, um bspw. bestimmte Ports bzw. Portranges gezielt freizugeben oder zu überwachen. Dies ist jedoch sehr aufwendig und deshalb außer für bestimmte Einzelfälle nicht zielführend. ◗ Dieser Use-Case kann nur dann seine Wirkung entfalten, wenn eine grundlegende Segmentierung im Netz vorliegt. Ist das Netz komplett flach aufgebaut oder dürfen alle Systeme mit allen kommunizieren, so ist eine Umsetzung ggf. sinnlos. Beispiele für geeignete Einsatzszenarien: – Produktivnetze sind von Test- und Entwicklungsnetzen getrennt, und direkte Zugriffe von Entwicklung auf Produktion sind unzulässig und sollen überwacht werden. – Internet-Gateways dürfen nur von bestimmten Systemen genutzt werden und ein direkter Zugriff durch andere soll kontrolliert werden. – Anwendungssysteme haben eigene Subnetze und dürfen nur über ein zentrales Netz kommunizieren, bspw. über ein API-Management-System.
Empfohlene Reaktion	Überprüfung der Kommunikation und tiefergehende Analyse
Referenz ATT&CK Techniques	T1580 [G] (Cloud Infrastructure Discovery), T1526 [G] (Cloud Service Discovery), T1619 [G] (Cloud Storage Object Discovery), T1046 [D] (Network Service Discovery), T1135 [D] (Network Share Discovery), T1018 [D] (Remote System Discovery), T1210 [G] (Exploitation of Remote Services), T1570 [D] (Lateral Tool Transfer), T1021 [G] (Remote Services), T1080 [G] (Taint Shared Content), T1074.002 [G] (Remote Data Staging)
Referenz BSI	Keine Entsprechung
Referenz ATT&CK Tactics	Discovery, Lateral Movement, Collection

3.9.34 B34 – Unbekanntes Gerät entdeckt

ID	B34
Name	Unbekanntes Gerät entdeckt
Kurzbeschreibung mit Detektionsziel	Ein unbekanntes Gerät wird anhand von Kommunikationsverhalten oder im Rahmen einer Service Discovery erkannt.
Adressierte Risiken	Angreifer können Geräte im Netzwerk platzieren, mithilfe derer sie Informationen gewinnen oder Angriffe fahren. Dabei können sie sich gegen die Organisation selbst wenden oder auch andere Ziele außerhalb des Netzes angreifen.
Erforderliche Informationen	◗ Ereignis E: Jede Art von Ereigniscode mit Informationen über die Herkunft, bspw. IP-Adressen, Ethernet-Adressen oder Hostnamen/FQDN. Mindestens NET01 sollte darunter sein, DET01 – falls entsprechende Systeme als Informationsgeber existieren – sollte als Zielsystem hier die Informationen über erkannte Geräte liefern. ◗ Quellsystem Q mit Herkunftsinformation ◗ Zielsystem Z, auf das zugegriffen wird
Benötigte Positiv- und Negativlisten	◗ Negativliste <NL_ERLAUBTEENDPUNKTE_01>: Liste über alle bekannten Endpunkte ◗ <GL_NETZEINTERN_01>: Liste der eigenen internen Netze
Empfohlener Reaktionstyp	Warnmeldung oder als Bericht
Kritikalität	2 (hoch)
Dringlichkeit	2 (schnell)
Typische True Positives (kritisch)	◗ Angreifer haben ein Gerät im Netzwerk platziert.
Typische True Negatives (unkritisch)	◗ Bekannte Geräte kommunizieren oder werden erkannt.
Typische False Positives (unkritisch)	◗ Kommunikationsverhalten eines zulässigen Geräts wurde erkannt, aber nicht in der Negativliste gepflegt. ◗ Externe Netze wurden als interne eingetragen.
Typische False Negatives (kritisch)	◗ Falsche, veraltete oder unvollständige Einträge in den Listen ◗ Geräte sind im Netz, kommunizieren aber (noch) nicht oder zumindest nicht mit überwachten Systemen. ◗ Zulässige Geräte wurden von Angreifern durch unzulässige ersetzt und werden durch die gewählte Implementierung der Überwachung nicht erkannt.
Fachliche Beschreibung der Regel	WENN das Ereignis E EINTRITT, UND Q ist enthalten in <GL_NETZEINTERN_01> UND Q ist nicht enthalten in <NL_ERLAUBTEENDPUNKTE_01> ODER Z ist enthalten in <GL_NETZEINTERN_01> UND Z ist nicht enthalten in <NL_ERLAUBTEENDPUNKTE_01> DANN löse aus
Gruppierung	**Empfehlung:** Wenn technisch möglich, nach Q oder Z als einzelner Wert (nicht Kombination (Q,Z)). Ist dies technisch nicht möglich, dann nach Ereigniscode E. **Begründung:** Unbekannte Geräte können auf Basis unterschiedlicher Ereignisse gefunden werden. Dabei können sie sowohl als Quelle als auch als Ziel in Erscheinung treten. Idealerweise lassen sich die Geräte über ihre IP-Adressen/Hostnamen gruppieren. Ist dies technisch nicht möglich, so ist der Ereigniscode E eine alternative Option.

→

Optionen und Anmerkungen	◗ Dieser Use-Case ist einfach in der reinen Regelumsetzung, benötigt jedoch stets aktuelle Informationen über die Geräte der Organisation. Dies ist ab einer gewissen Gesamtzahl an Geräten und abhängig von Veränderungen der Gerätelandschaft aufwendig. Alternativ wird ein zentraler, automatisiert gepflegter Datenbestand (bspw. CMDB) benötigt. Zudem kann die Auswertung bei einer großen Zahl von Geräten hohe Anforderungen an die Leistung der auswertenden Software stellen. ◗ Ist eine (nahezu) Echtzeit-Auswertung nicht möglich, so bietet sich die Umsetzung als Bericht anstelle einer Warnmeldung an. Eine mindestens tägliche Auswertung wird empfohlen. ◗ Der Use-Case kann in verschiedener Hinsicht ausgebaut werden. ◗ **Beispiele:** – Die Art des Geräts kann als Dimension aufgenommen werden, bspw. wenn eine Service Discovery offene Linux-typische Ports oder OS-Fingerprints bei einem eigentlich als Windows geführten System erkennt. – Virtuelle Geräte werden über das hier vorgestellte Verfahren grundsätzlich ebenfalls erkannt, können aber in Spezialfällen erweiterte Informationen und ein Regelwerk benötigen. Zudem sollten hierzu dediziert Ereignisse, die die Anlage von virtuellen Geräten dokumentieren, in die Überwachung aufgenommen werden.
Empfohlene Reaktion	Zunächst sollten mögliche Fehler in den Listen, bspw. aufgrund von Verzögerungen zwischen dem genehmigten Einbringen eines neuen Gerätes ins Netzwerk und dem Hinzufügen zu den Listen, ausgeschlossen werden. Anschließend erfolgen die Analyse und Einleitung geeigneter Gegenmaßnahmen.
Referenz ATT&CK Techniques	T1200 [D] (Hardware Additions), T1578.002 [D] (Modify Cloud Compute Infrastructure: Create Cloud Instance)
Referenz BSI	INF: Infrastruktur
Referenz ATT&CK Tactics	Initial Access, Defense Evasion

3.9.35 B35 – Erkennung unerwünschter Software

ID	B35
Name	Erkennung unerwünschter Software
Kurzbeschreibung mit Detektionsziel	Die Verwendung von unerwünschter Software soll erkannt werden und einen Alarm auslösen. Das benötigt typischerweise Informationen über gestartete Prozesse auf den zu überwachenden Systemen und eine gepflegte Liste der unerwünschten Software.
Adressierte Risiken	Der Einsatz unerwünschter Software kann viele Gründe haben: Zum einen ist der Klassiker ein Angriffsversuch durch Hacker per Malware. Zum anderen gehören hierzu aber auch reguläre Netzwerk-Analysetools wie Sniffer-Programme, die in der Lage sind, den gesamten ein- und ausgehenden Verkehr von einem mit dem Netzwerk verbundenen Computer aufzuzeichnen, einschließlich sensibler Informationen wie Benutzernamen und nicht verschlüsselter Passwörter. Oft werden solche Programme nicht nur von Administratoren zur Fehleranalyse genutzt, sondern auch von Angreifern, um an vertrauliche Informationen zu gelangen. Das rechtzeitige Erkennen und Unterbinden solcher Aktivitäten ist ein Baustein zur Abwehr von Cyberangriffen.
Erforderliche Informationen	◗ Ereignis: – Ereigniscodes ALERT01 oder PSTART01 – Programmname PNAME, wird verwendet für automatisches Prüfen der Prozessliste auf den Endgeräten gegen eine Ausschlussliste – Gerät Z, auf dem das Programm ausgeführt wird – Auf Netzwerkebene ein Monitoring-Tool für Protokollanalyse (Netflow) – Ausschlussliste <GL_SOFTWARE_01>, die alle Namen der unerwünschten Softwareprozesse bzw. Programmnamen enthält
Benötigte Positiv- und Negativlisten	◗ Negativliste <NL_HOSTS_01>: Systeme, auf denen unerwünschte Programme im Bedarfsfall ausgeführt werden dürfen ◗ Positivliste <PL_HOSTS_01>: Systeme, auf denen unerwünschte Programme auf keinen Fall ausgeführt werden dürfen (wegen hohen Schutzbedarfs)
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	2 (hoch)
Dringlichkeit	2 (hoch)
Typische True Positives (kritisch)	◗ Eine bekannt unerwünschte Software wurde gefunden.
Typische True Negatives (unkritisch)	◗ Keine unerwünschte Software gefunden.
Typische False Positives (unkritisch)	◗ Zu genehmigten Analysezwecken wurde ein Sniffer-Programm auf einem Endgerät installiert und verwendet. Das Gerät wurde aber nicht in die Negativliste <NL_HOSTS_01> eingetragen und löst daher einen Alarm aus.
Typische False Negatives (kritisch)	◗ Neue Malware, die nicht vom AV-Programm erkannt wird. ◗ Es wurden unerwünschte Programme verwendet, die nicht in der Ausschlussliste <GL_SOFTWARE_01> aufgeführt sind. Beispielsweise, weil das Programm neu ist oder bisher unbekannt war.

→

Fachliche Beschreibung der Regel	WENN Ereignis ALERT01 für System Z ODER Ereignis PSTART01 auf System Z EINTRITT, UND PNAME enthalten in <GL_SOFTWARE_01> UND Z nicht enthalten in <NL_HOSTS_01> ODER Z enthalten in <PL_HOSTS_01> DANN löse aus
Gruppierung	**Empfehlung:** Gruppierung nach System Z **Begründung:** Wiederholte Verwendungen der gleichen bzw. der Einsatz unterschiedlicher unerwünschter Software wird je System zusammengefasst.
Optionen und Anmerkungen	◗ Um ein PSTART01-Ereignis zu erhalten, bieten verschiedene Systeme die Möglichkeit, dies zu konfigurieren. Sollte ein System nicht so konfiguriert werden können, dass Prozessstarts im Ereignislog aufgezeichnet werden können, so kann man alternativ regelmäßig ein Skript ausführen lassen, das die aktuelle Prozessliste scannt und beim Auftreten bestimmter Prozesse ein entsprechendes Ereignis erzeugt. ◗ Optional kann zusätzlich eine Liste geführt werden, über die auch unerwünschte Fernzugriffssoftware (z. B. PC Anywhere oder VNC) erkannt wird.
Empfohlene Reaktion	Die Ausführung unerwünschter Software ist aus Organisationssicht eine latente Bedrohung. Entsprechende Meldungen sollten daher unverzüglich nachverfolgt und im aufgetretenen Umfeld bewertet werden, z. B. durch SOC-Analysten oder ggf. CISO.
Referenz ATT&CK Techniques	T1204 [G] (User Execution), T1659 [G] (Content Injection), T1189 [G] (Drive-by Compromise), T1059 [G] (Command and Scripting Interpreter), T1203 [G] (Exploitation for Client Execution), T1072 [G] (Software Deployment Tools)
Referenz BSI	OPS.1.1.4 Schutz vor Schadprogrammen
Referenz ATT&CK Tactics	Initial Access, Execution

3.9.36 B36 – Herunterladen bösartiger Inhalte

ID	B36
Name	Herunterladen bösartiger Inhalte
Kurzbeschreibung mit Detektionsziel	Es soll erkannt werden, wenn Dateien mit bösartigen Inhalten heruntergeladen werden. Bösartige Inhalte umfassen unter anderem Schadsoftware in Windows-EXE-Dateien oder bösartige Makros in Office-Dateien.
Adressierte Risiken	Sind Dateien mit bösartigen Inhalten auf IT-Systemen vorhanden und werden aktiv, so können diese eine Vielzahl von schädlichen Aktivitäten durchführen. Dazu gehören u. a. Verschlüsselungstrojaner (Ransomware) und Datenabfluss.
Erforderliche Informationen	Ereignisse: ◗ Ereigniscode ALERT01 ◗ Sicherheitssystem mit dedizierter Prüfung von Schadcode oder Hashwerten (Prüfsummen) von bekannten Schadcodes, üblicherweise Firewall-, Proxy-, Antivirus- oder IDS/IPS-Systeme ◗ System Z, auf das der Inhalt heruntergeladen wird ◗ Liste <GL_HASHWERTE_01> mit Liste von Hashwerten bekannt bösartiger Schadprogramme oder ähnlichen Inhalten
Benötigte Positiv- und Negativlisten	◗ Negativliste <NL_ZUGELASSENESYSTEME_01>: Systeme, auf denen das Herunterladen von unerwünschten Programmen oder Ähnlichem im Bedarfsfall durchgeführt werden dürfen ◗ Positivliste <PL_SENSIBLESYSTEME_01>: Systeme, auf denen das Herunterladen von unerwünschten Programmen oder Ähnlichem auf keinen Fall durchgeführt werden dürfen (z. B. wegen hohen Schutzbedarfs) ◗ Negativliste <NL_HASHWERTE_01> mit einer Liste von Hashwerten sicherer Inhalte, die nicht blockiert werden dürfen, um False Positives zu vermeiden. ◗ Positivliste <PL_HASHWERTE_01> mit einer Liste von Hashwerten bekannt bösartiger Schadprogramme oder ähnlichen Inhalten, die dediziert immer als bösartig zu behandeln sind
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	2 (hoch)
Dringlichkeit	2 (schnell)
Typische True Positives (kritisch)	◗ Heruntergeladene Datei/Programm wird anhand des Hashwerts erkannt und ist bösartig. ◗ Datei/Programm steht auf einer Positivliste.
Typische True Negatives (unkritisch)	◗ Heruntergeladene Datei/Programm ist nicht bösartig und wird auch nicht erkannt. ◗ Datei/Programm steht berechtigterweise auf einer Negativliste.
Typische False Positives (unkritisch)	◗ Heruntergeladene Datei/Programm wird anhand des Hashwerts erkannt, ist aber nicht bösartig. ◗ Datei/Programm steht fälschlicherweise auf einer Positivliste.
Typische False Negatives (kritisch)	◗ Heruntergeladene Datei/Programm wird anhand des Hashwerts nicht erkannt, ist aber bösartig. ◗ Datei/Programm steht fälschlicherweise auf einer Negativliste.
Fachliche Beschreibung der Regel	WENN Ereignis ALERT01 für System Z EINTRITT, UND Hashwert des Inhalts ist enthalten in <PL_HASHWERTE_01> ODER System Z ist enthalten in <PL_SENSIBLESYSTEME_01> ODER Hashwert des Inhalts ist enthalten in <GL_HASHWERTE_01> UND System Z ist nicht enthalten in <NL_ZUGELASSENESYSTEME_01> UND Hashwert des Inhalts ist nicht enthalten in <NL_HASHWERTE_01> DANN löse aus
Gruppierung	**Empfehlung:** Gruppierung nach Z **Begründung:** Multiple Downloads werden je System zusammengefasst und erleichtern so die Analyse.

→

Optionen und Anmerkungen	◗ Dies ist ein grundlegender Use-Case. Er beschreibt die grundsätzliche Erkennung von Schadsoftware auf Systemen der Infrastruktur. ◗ Die Erkennung benötigt einerseits eine Negativliste mit Hashwerten wichtiger Programme oder ähnlicher Inhalte zur Vermeidung von False Positives, kann andererseits aber auch Listen mit Hashwerten bösartiger Inhalte nutzen, die zur Erkennung herangezogen werden. Diese Listen mit Hashwerten müssen nicht lokal erstellt werden, sondern können von einem Dienstleister, bspw. in Form eines Cloud-Dienstes, bereitgestellt werden. Diese sollten regelmäßig in kurzen Zyklen aktualisiert werden.
Empfohlene Reaktion	Da bösartige Inhalte einen sehr großen Schaden verursachen können, muss auf dieses Ereignis schnell reagiert werden.
Referenz ATT&CK Techniques	T1072 [G] (Software Deployment Tools), T1204 [G] (User Execution)
Referenz BSI	OPS.1.1.4 Schutz vor Schadprogrammen
Referenz ATT&CK Tactics	Execution, Initial Access

3.9.37 B37 – Datenausleitung

ID	B37
Name	Datenausleitung
Kurzbeschreibung mit Detektionsziel	Ausleitung ungewöhnlich hoher Datenmengen, Baseline um ein Mehrfaches überschritten, spezifische Schwellenwerte notwendig
Adressierte Risiken	Wenn Angreifer nach einem erfolgreichen Eindringen in fremde IT-Systeme interessante Daten entdeckt haben, werden diese in der Regel über Standardprotokolle auf eigene Systeme der Angreifer ins Internet ausgeleitet, um mit dem Material die angegriffene Organisation bspw. erpressen zu können. Die dafür zu übertragenden Datenmengen können entsprechend hoch sein. Solche signifikant großen Datenvolumina sollen mit diesem Use-Case erkannt werden.
Erforderliche Informationen	Perimeter-Logs (üblicherweise der Firewall) ◗ IP-Adressen oder Hostnamen von Geräten G, die das höchste Datenvolumen ins Internet gesendet haben – IP_volumen oder Z_volumen ◗ Übertragenes Datenvolumen D_volumen ◗ Zeitraum t_volumen, in dem D_volumen von IP_volumen oder von Z_volumen übertragen wurde ◗ Schwellenwert S_volumen (D_volumen/t_volumen), ab dem das Datenvolumen als verdächtig eingestuft werden soll
Benötigte Positiv- und Negativlisten	◗ Negativliste <NL_HOSTSMITHOHEMVOLUMEN_01>: IP-Adressen oder Hostnamen von internen Geräten, die aus betrieblicher Sicht ein so hohes Datenvolumen generieren, dass es regelmäßig über dem Schwellenwert S_volumen liegt. ◗ Positivliste <PL_KRITISCHEHOSTS_01>: IP-Adressen oder Hostnamen von Geräten, die aus betrieblicher Sicht niemals den Schwellenwert S_volumen überschreiten. Sollte trotzdem eine Detektion erfolgen, müssen diese Vorgänge zwingend einen Alarm auslösen, auch wenn sie in der Negativliste <NL_HOSTSMITHOHEMVOLUMEN_01> enthalten sind (Vorrangigkeit).
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	2 (hoch)
Dringlichkeit	2 (hoch)
Typische True Positives (kritisch)	◗ Der definierte Schwellenwert für das zulässige Datenvolumen einer Verbindung wird bei einem zu überwachenden IT-Gerät überschritten.
Typische True Negatives (unkritisch)	◗ Der definierte Schwellenwert für das zulässige Datenvolumen einer Verbindung wird bei einem IT-Gerät aus der Negativliste <NL_HOSTSMITHOHEMVOLUMEN_01> überschritten.
Typische False Positives (unkritisch)	◗ Ein Alarm wird für die Datenverbindung eines IT-Gerätes ausgelöst, das bekanntermaßen den definierten Schwellenwert überschreitet, aber versehentlich nicht in die Negativliste <NL_HOSTSMITHOHEMVOLUMEN_01> aufgenommen wurde.
Typische False Negatives (kritisch)	◗ Die Volumenmessung D_volumen kann nicht für alle Protokolle durchgeführt werden. Sollte daher die Exfiltration über ein unübliches Protokoll erfolgen, das am Perimeter weder geblockt noch protokolliert wird, so bleibt die Ausleitung unerkannt (bspw. DNS).
Fachliche Beschreibung der Regel	FÜR JEDES IP-Gerät oder Z-Gerät G BERECHNE VG = Volumen(G) in Zeitraum t WENN VG >= S_volumen UND G ist nicht enthalten in <NL_HOSTSMITHOHEMVOLUMEN_01> ODER G ist enthalten in <PL_KRITISCHEHOSTS_01> DANN löse aus
Gruppierung	**Empfehlung:** Es ist sinnvoll, die IT-Geräte in Gruppen zusammenzufassen und jeweils unterschiedliche Schwellenwerte zu definieren. Insbesondere die Nutzung von Cloud-Diensten kann hohe Datenvolumina nach außen erfordern, trotzdem ist dies legitim. **Begründung:** Mithilfe einer Gruppierung wird die Trefferquote und Wirksamkeit des Use-Case stark erhöht.

→

Optionen und Anmerkungen	◗ Die Festlegung des richtigen Schwellenwertes <S_volumen> ist nicht einfach. ◗ Sie ist sehr individuell und organisationsspezifisch. ◗ Im ersten Schritt sollte das Netz oder auch einzelne Netzsegmente längere Zeit beobachtet werden, um das »Grundrauschen« (Baseline) zu bestimmen. Erfahrungsgemäß ist das 3- bis 4-fache Datenvolumen der Baseline ein praktikabler Start für den Schwellenwert. ◗ Falls es das Segmentierungsmodell hergibt, kann der Use-Case auch auf interne Datentransfers erweitert werden. **Grund:** Gerne werden von den Angreifern erbeutete Daten intern an frequentierte Übergabepunkte verschoben, um sie erst von dort aus nach außen zu senden, z. B. in unauffällige Cloud-Dienste. **Hinweis:** In einem fortgeschrittenen Stadium des Use-Case ist es sinnvoll, die Negativ- und Positivlisten auch für gezielte Strecken festzulegen. Beispielsweise darf ein internes Gerät nur zu einer bestimmten Ziel-IP höhere Datenvolumen übertragen, sodass nur für diese Verbindung ein Eintrag auf der Negativliste aufgeführt wird.
Empfohlene Reaktion	Im Fall einer Warnmeldung ist eine möglichst schnelle Prüfung des Vorgangs angeraten. Der Vorgang der Exfiltration steht am Ende der ATT&CK Tactics [MITRE 2025b]. In diesem Fall ist die Unterbindung zeitkritisch, da möglicherweise weiterhin vertrauliche Daten nach außen gesendet werden.
Referenz ATT&CK Techniques	T1020 [G] (Automated Exfiltration), T1048 [G] (Exfiltration Over Alternative Protocol), T1041 [G] (Exfiltration Over C2 Channel), T1011 [G] (Exfiltration Over Other Network), T1567 [G] (Exfiltration Over Web Service), T1029 [G] (Scheduled Transfer), T1537 [G] (Transfer Data to Cloud Account)
Referenz BSI	Keine Entsprechung
Referenz ATT&CK Tactics	Exfiltration

3.9.38 B38 – Erkennung bösartiger Zugriffe von externen Systemen auf interne Systeme

ID	B38
Name	Erkennung bösartiger Zugriffe von externen Systemen auf interne Systeme
Kurzbeschreibung mit Detektionsziel	Zugriffe durch bekannt bösartige Hosts, bspw. von Bots in Botnetzen, sind ein deutlicher Hinweis auf Angriffe. Diese sollen erkannt werden.
Adressierte Risiken	Jede Art von Risiken, die durch extern durchgeführte Angriffe entstehen können Werden Zugriffe externer bösartiger Hosts im internen Netz erkannt, so sind Angreifer bereits eingedrungen.
Erforderliche Informationen	◗ Ereignis E: Jede Art von Ereigniscode mit Informationen über die Herkunft, bspw. IP-Adressen oder Hostnamen/FQDN. Mindestens NET01 sollte darunter sein. ◗ Quellsystem Q mit Herkunftsinformation ◗ Zielsystem Z, auf das zugegriffen wird ◗ Information über bösartig eingestufte Hosts, bspw. via Threat Intelligence oder aus externen oder internen Informationsquellen
Benötigte Positiv- und Negativlisten	◗ Positivliste <PL_EIGENE_01>: Liste der durch die Organisation selbst als bösartig verifizierten oder eingestuften Hosts, z. B. aufgrund eines laufenden Angriffs ◗ Negativliste <NL_EIGENE_01>: Liste der durch die Organisation selbst als nicht bösartig verifizierten oder eingestuften Hosts, z. B. um keine False Positives aufgrund der in einer Threat-Intelligence-Datenquelle fehlerhaft aufgeführten Hosts zu erhalten ◗ <GL_MALHOSTS_01>: Liste potenziell bösartiger Hosts, bspw. aus Threat-Intelligence-Quellen oder automatisch oder manuell befüllt aufgrund verdächtigen Verhaltens ◗ Negativliste <NL_HOSTS_01>: Liste der eigenen Hosts, für die keine Warnmeldung ausgelöst werden soll. Dies sind typischerweise Hosts am Perimeter, können aber auch solche sein, die für Testzwecke vorgesehen sind und nur statistisch oder auf andere Weise ausgewertet werden sollen.
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	2 (hoch)
Dringlichkeit	3 (unverzüglich)
Typische True Positives (kritisch)	◗ Angreifer sind in das interne Netz eingedrungen und sind dort aktiv. ◗ Schadsoftware ist in der Organisation aktiv und wird von außen gesteuert.
Typische True Negatives (unkritisch)	◗ Hosts am Perimeter, die auf einer Negativliste stehen, werden gescannt. ◗ Zugriffe finden von einem nicht bösartigen bzw. als nicht bösartig eingestuften oder verifizierten Host statt.
Typische False Positives (unkritisch)	◗ Zugreifende Hosts sind als bösartig klassifiziert, sind es aber nicht wirklich. ◗ Die Positivlisten enthalten fehlerhafte oder nicht mehr aktuelle Einträge. ◗ Der Zugriff erfolgt nicht ins interne Netz, sondern nur am Perimeter, und dieser ist nicht vollständig in den entsprechenden Listen gepflegt.
Typische False Negatives (kritisch)	◗ Bösartige Hosts sind nicht als solche erkannt. ◗ Hosts stehen auf Negativlisten, obwohl sie dort nicht stehen sollten.

→

Fachliche Beschreibung der Regel	WENN das Ereignis E EINTRITT, UND Q ist enthalten in <PL_EIGENE_01> ODER Q ist enthalten in <GL_MALHOSTS_01> UND Q ist nicht enthalten in <NL_EIGENE_01> UND Z ist nicht enthalten in <NL_HOSTS_01> ODER Z ist enthalten in <NL_HOSTS_01> UND E != NET01 DANN löse aus
Gruppierung	**Empfehlung:** Gruppierung nach Quelle Q **Begründung:** Die Quellen und somit potenziell unterschiedliche Akteure werden zusammengefasst.
Optionen und Anmerkungen	◗ Hier wird empfohlen, Zugriffsversuche auf den Perimeter auszuschließen, weil typischerweise fortwährend aus dem Internet gescannt wird. Erfolgreiche Zugriffe müssen unterschieden werden: Reine Netzwerkereignisse sind in der Regel unkritisch. Sind es jedoch erfolgreiche Login-Ereignisse oder dergleichen, so könnten sich Angreifer erfolgreich auf einem Server, einer Firewall o. Ä. Zugriff verschafft haben. Somit haben sie von dort aus dann Zugriff auf das interne Netz. Dem sollte dringend nachgegangen werden. ◗ Der Use-Case kann grundsätzlich auch auf erfolgreiche Zugriffe eingeschränkt werden. Allerdings wird dies nicht empfohlen, da hier bereits Zugriffe von außen ins interne Netz erfolgen. ◗ Die sogenannte »Threat Intelligence« wird heutzutage immer wichtiger. So bieten zahlreiche Unternehmen entsprechende Informationen über als Verdachtsfälle eingestufte Hosts an. Diese Informationen bilden dann die Basis für die <GL_MALHOSTS_01>. ◗ Die Organisation kann zudem auch eigene grundsätzliche Risikobetrachtungen einfließen lassen wie: – Dürfen Teilnehmer aus dem TOR-Netzwerk (https://www.torproject.org/) anonym zugreifen? – Soll über öffentlich verfügbare anonymisierende Proxys zugegriffen werden können? – Gibt es Länder oder Netzwerke, aus denen Zugriffe sehr unüblich wären? Entsprechende Hosts bzw. Netzwerke können dann in <GL_MALHOSTS_01> hinzugefügt werden.
Empfohlene Reaktion	Überprüfung der Zugriffe, insbesondere der Quellhosts, und auf welche Ziele und wie tief im internen Netz zugegriffen wird. Zudem sollte überprüft werden, ob bereits von Zielen aus weitere Zugriffe nach innen oder außen stattfinden. Dies könnte ein Hinweis auf Ausbreitung der Angreifer im Netz sein (»Lateral Movement«). Eine schnelle Reaktion ist unabdingbar und könnte als Maßnahme eine Sperrung des Zugriffs von den entsprechenden Quellen, bspw. über Firewall, und die Isolation interner betroffener Systeme beinhalten.
Referenz ATT&CK Techniques	T1659 [G] (Content Injection), T1190 [D] (Exploit Public-Facing Application), T1133 [D] (External Remote Services), T1078 [G] (Valid Accounts), T1105 [G] (Ingress Tool Transfer)
Referenz BSI	SYS.1.1.A2 Authentisierung an Servern SYS.1.1.A27 Hostbasierte Angriffserkennung
Referenz ATT&CK Tactics	Initial Access, Command and Control

3.9.39 B39 – Erkennung interner Zugriffe von bekannt bösartigen Hosts

ID	B39
Name	Erkennung interner Zugriffe von bekannt bösartigen Hosts
Kurzbeschreibung mit Detektionsziel	Zugriffe auf bekannt bösartige Hosts sind ein deutlicher Hinweis auf Angriffe oder auf deren Vorbereitung. Bösartige Hosts können bspw. »Command & Control Server« (C&C) sein, bei denen sich bereits in der Organisation befindliche Schadsoftware meldet. Oder eine Phishing-Seite, auf die die eigenen Benutzer zugreifen, was den Abfluss von Credentials oder eine Einbringung von Schadsoftware zur Folge haben kann.
Adressierte Risiken	Jede Art von Risiken, die durch Angreifer im Netz entstehen können. Werden Zugriffe aus dem internen Netz auf externe bösartige Hosts erkannt, so sind Angreifer bereits eingedrungen.
Erforderliche Informationen	◗ Ereignis E: Jede Art von Ereigniscode mit Informationen über das Ziel, bspw. IP-Adressen oder Hostnamen/FQDN. Mindestens NET01 sollte darunter sein. ◗ Quellsystem Q ◗ Zielsystem Z, auf das zugegriffen wird ◗ Information über als bösartig eingestufte Hosts, bspw. via Threat Intelligence oder aus externen oder internen Informationsquellen
Benötigte Positiv- und Negativlisten	◗ Positivliste <PL_EIGENE_01>: Liste der durch die Organisation selbst als bösartig verifizierten oder eingestuften Hosts, z. B. aufgrund eines laufenden Angriffs ◗ Negativliste <NL_EIGENE_01>: Liste der durch die Organisation selbst als nicht bösartig verifizierten oder eingestuften Hosts, z. B. um keine False Positives aufgrund der in einer Threat-Intelligence-Datenquelle fehlerhaft aufgeführten Hosts zu erhalten ◗ <GL_MALHOSTS_01>: Liste potenziell bösartiger Hosts, bspw. aus Threat-Intelligence-Quellen oder automatisch oder manuell befüllt aufgrund verdächtigen Verhaltens ◗ Negativliste <NL_HOSTS_01>: Liste der eigenen Hosts, für die keine Warnmeldung ausgelöst werden soll. Dies können bspw. abgesicherte Systeme sein, die ein Security-Team zur Überprüfung verdächtiger Seiten verwendet.
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	3 (sehr hoch)
Dringlichkeit	3 (unverzüglich)
Typische True Positives (kritisch)	◗ Eine Schadsoftware meldet sich bei einem C&C-Server. ◗ Angreifer exfiltrieren Daten aus dem Netzwerk.
Typische True Negatives (unkritisch)	◗ Das Security-Team untersucht von abgesicherten Systemen aus die verdächtigen Ziele und diese stehen auf einer Negativliste. ◗ Zugriffe finden auf einen nicht bösartigen bzw. als nicht bösartig eingestuften oder verifizierten Host statt.
Typische False Positives (unkritisch)	◗ Das Security-Team untersucht von abgesicherten Systemen aus die verdächtigen Ziele. Diese abgesicherten Systeme stehen aber nicht auf einer Negativliste. ◗ Zielhosts sind als bösartig klassifiziert, sind es aber nicht wirklich. ◗ Die Positivlisten enthalten fehlerhafte oder nicht mehr aktuelle Einträge.
Typische False Negatives (kritisch)	◗ Bösartige Hosts sind nicht als solche erkannt. ◗ Hosts stehen auf Negativlisten, obwohl sie dort nicht stehen sollten. ◗ Der Datenverkehr fällt nicht auf, da die Zielsysteme nicht im internen Netzwerk liegen und Systeme, die den Netzwerkverkehr überwachen, nicht existieren oder unzureichend konfiguriert sind.

→

Fachliche Beschreibung der Regel	WENN Ereignis E EINTRITT, UND Z ist enthalten in <PL_EIGENE_01> ODER Z ist enthalten in <GL_MALHOSTS_01> UND Z ist nicht enthalten in <NL_EIGENE_01> UND Q ist nicht enthalten in <NL_HOSTS_01> DANN löse aus
Gruppierung	**Empfehlung:** Gruppierung nach System Z **Begründung:** Kommunikation zu einem externen Zielpunkt wird zusammengefasst.
Optionen und Anmerkungen	◗ Hier wird nicht empfohlen, Zugriffe vom Perimeter aus auszuschließen, da diese üblicherweise nicht selbst Verbindungen zu externen Systemen aufbauen sollten. In Sonderfällen kann dies erforderlich sein, bspw. wenn Verbindungen in definierte Systeme von Partnern stattfinden. Dann sollten diese nach Möglichkeit genau eingeschränkt und nur die Kombinationen von Quelle und Ziel ausgenommen werden. ◗ Die sogenannte »Threat Intelligence« wird heutzutage immer wichtiger. So bieten zahlreiche Unternehmen entsprechende Informationen über als Verdachtsfälle eingestufte Hosts ein. Diese Informationen bilden dann die Basis für die <GL_MALHOSTS_01>. ◗ Die Organisation kann zudem auch eigene grundsätzliche Risikobetrachtungen einfließen lassen wie: – Dürfen Benutzer der Organisation das TOR-Netzwerk (https://www.torproject.org/) nutzen? – Sollen öffentlich verfügbare anonymisierende Proxys genutzt werden können? Oder VPN-Anbieter? – Gibt es Länder oder Netzwerke, auf die Zugriffe sehr unüblich wären und nicht zur üblichen Geschäftstätigkeit gehören? Entsprechende Hosts bzw. Netzwerke können dann in <GL_MALHOSTS_01> hinzugefügt werden.
Empfohlene Reaktion	Überprüfung der Zugriffe, insbesondere der Zielhosts, und von welchen Quellsystemen im internen Netz zugegriffen wird. Zudem sollte überprüft werden, ob weitere Zugriffe nach innen oder außen von diesen Systemen aus stattfinden. Dies könnte ein Hinweis auf Ausbreitung der Angreifer im Netz sein (»Lateral Movement«). Eine schnelle Reaktion ist unabdingbar und könnte als Maßnahme eine Sperrung des Zugriffs von den entsprechenden Zielen, bspw. über Firewall, und die Isolation interner betroffener Systeme beinhalten.
Referenz ATT&CK Techniques	T1071 [G] (Application Layer Protocol), T1659 [G] (Content Injection), T1568 [G] (Dynamic Resolution), T1573 [G] (Encrypted Channel), T1008 [G] (Fallback Channels), T1665 [G] (Hide Infrastructure), T1095 [G] (Non-Application Layer Protocol), T1571 [G] (Non-Standard Port), T1572 [G] (Protocol Tunneling), T1020 [G] (Automated Exfiltration), T1030 [G] (Data Transfer Size Limits), T1048 [G] (Exfiltration over Alternative Protocol), T1041 [G] (Exfiltration Over C2 Channel), T1567 [G] (Exfiltration Over Web Service), T1029 [G] (Scheduled Transfer)
Referenz BSI	Keine Entsprechung
Referenz ATT&CK Tactics	Command and Control, Exfiltration

3.9.40 B40 – Ungewöhnliche Netzwerkaktivität außerhalb der Geschäftszeiten

ID	B40
Name	Ungewöhnliche Netzwerkaktivität außerhalb der Geschäftszeiten
Kurzbeschreibung mit Detektionsziel	Wenn ein zu überwachender Parameter über einem Schwellwert liegt innerhalb der zu definierenden Nicht-Geschäftszeiten, dann soll ein Alarm ausgelöst werden [→Hinweise auf Exfiltration].
Adressierte Risiken	Aktivitäten außerhalb der üblichen Geschäftszeiten sind möglich, aber nicht die Regel. Je nach Geschäftsmodell der Organisation und Ausgestaltung der Arbeitsverträge der Mitarbeiter ist es ggf. sinnvoll, solche ungewöhnlichen Ereignisse zu registrieren und nachzuverfolgen. Oft können mithilfe solcher Use-Cases Angriffsversuche oder sogar erfolgreiche Angriffe schon in einem sehr frühen Stadium erkannt werden.
Erforderliche Informationen	◗ Geschäftszeiten (Zeitraum) GZ, z. B. Mo-Fr 09:00 - 18:00 h, exkl. gesetzliche Feiertage im (Bundes-) Land ◗ Schwellenwert(e) thr_traffic (1 ... n) für den Netzwerkverkehr (Durchsatz/Zeiteinheit) an bestimmten Messpunkten im Netz (1 … n) ◗ Netzwerkverkehr traffic (1 ... n) (Durchsatz/Zeiteinheit) an den Messpunkten (1 … n) zum Zeitpunkt t
Benötigte Positiv- und Negativlisten	Negativliste <NL_WARTUNG_01>: als Ausnahme für Wartungsfenster an den Messpunkten (1 … n)
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	2 (hoch)
Dringlichkeit	1 (normal)
Typische True Positives (kritisch)	◗ Außerhalb der definierten Geschäftszeiten wird eine zu überwachende Netzwerkaktivität erkannt und gemeldet.
Typische True Negatives (unkritisch)	◗ Außerhalb der definierten Geschäftszeiten erfolgt eine Netzwerkaktivität, die nicht überwacht werden soll.
Typische False Positives (unkritisch)	◗ Außerhalb der definierten Geschäftszeiten wird eine zu überwachende Netzwerkaktivität erkannt und gemeldet, bei der es sich um eine geplante Wartung handelt. Es wurde vergessen, diese Maßnahme in der Negativliste einzutragen.
Typische False Negatives (kritisch)	◗ Außerhalb der definierten Geschäftszeiten wird eine zu überwachende Netzwerkaktivität nicht erkannt, weil diese Maßnahme fälschlicherweise in der Negativliste eingetragen wurde oder weil vergessen wurde, eine bereits abgeschlossene Maßnahme wieder auszutragen.
Fachliche Beschreibung der Regel	WENN traffic (1 … n) > thr_traffic (1 … n) UND t nicht innerhalb von GZ UND t nicht aufgeführt in <NL_WARTUNG_01> DANN löse aus
Gruppierung	Keine Empfehlung

→

Optionen und Anmerkungen	◗ Die Umsetzung des Use-Case kann sehr komplex werden, wenn die Standorte der Organisation über viele Zeitzonen verteilt sind oder die Mitarbeiter international unterwegs sind und entsprechend der Zeitverschiebung in ihrer gewohnten Businessumgebung arbeiten. Hier empfiehlt sich die Verwendung von Templates, die von den jeweiligen Standorten gepflegt werden. Auch Homeoffice-Optionen der Mitarbeiter können die Umsetzung erschweren. ◗ Der Auslöser des Use-Case ist im vorgestellten Beispiel zur Vereinfachung auf erhöhten Netzwerkverkehr beschränkt. Selbstverständlich können auch andere Parameter als Indikatoren hinzugezogen werden. Beispielsweise direkte Zugriffe auf kritische Fileserver-Systeme oder Logins. ◗ Die Anzahl an falsch positiven Warnmeldungen aus diesem Use-Case kann sehr groß werden. Es bedarf bei der Einführung daher einer längeren Einschwingphase, bis die organisationsspezifische Arbeitsumgebung und die beteiligten Parameter in ein vertretbares Gleichgewicht gebracht worden sind.
Empfohlene Reaktion	Je nach Parameter sind Warnmeldungen aus diesem Use-Case als unspezifischer Hinweis zu verstehen: Es wird lediglich angezeigt, dass im Vergleich zur normalen Arbeitsweise eine Abweichung stattgefunden hat. Daher sollten die Meldungen mit normaler Dringlichkeit bearbeitet, und nur im Zusammenhang mit den Ereignissen anderer Use-Cases oder Logauswertungen bewertet werden.
Referenz ATT&CK Techniques	T1046 [G] (Network Service Discovery), T1135 [G] (Network Share Discovery), T1018 [G] (Remote System Discovery)
Referenz BSI	Keine Entsprechung
Referenz ATT&CK Tactics	Discovery

3.9.41 B41 – Unzulässiger Zugriff auf sensible Daten

ID	B41
Name	Unzulässiger Zugriff auf sensible Daten
Kurzbeschreibung mit Detektionsziel	Besonders die sensiblen Daten sind üblicherweise auf einen Personenkreis eingeschränkt. Dazu gehören bspw. streng vertrauliche Geschäftsdaten oder Gesundheitsdaten. Zugriff auf diese – inkl. Veränderung/Löschung – sollte erkannt werden. Daten können klassifiziert und gekennzeichnet sein, müssen es aber nicht.
Adressierte Risiken	Ein Angreifer kann bei Zugriff auf sensible Daten diese ausspähen und monetarisieren bzw. bei einer Veränderung bzw. Verschlüsselung der Daten hohen Schaden verursachen. Dieser Use-Case umfasst auch die Verschlüsselung durch Ransomware.
Erforderliche Informationen	◗ Ereigniscodes: DATA01 oder DATA02 ◗ Benutzer B, der die Aktivität durchführt ◗ Datei bzw. Daten D, auf die zugegriffen wird ◗ <GL_SENSIBLEDATEIPFADE_01>: Liste von Dateien oder Verzeichnissen (=Speicherorte) mit vertraulichen Daten, z. B. besonders sensible Daten, und den jeweils berechtigten Benutzergruppen oder den einzelnen Benutzern (= berechtigte Benutzerkonten), denen diese bereitgestellt werden ◗ Liste der berechtigten Benutzerkonten für die jeweiligen Speicherorte
Benötigte Positiv- und Negativlisten	◗ Negativliste <NL_UNWICHTIGEDATEIPFADE_01>: Liste von Dateien oder Unterverzeichnissen innerhalb definierter Speicherorte, die nicht überwacht werden sollen
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	2 (hoch)
Dringlichkeit	2 (schnell)
Typische True Positives (kritisch)	◗ Ein unberechtigter Benutzer oder ein Angreifer versucht unerlaubt auf eine Datei mit sensiblen Daten zuzugreifen.
Typische True Negatives (unkritisch)	◗ Ein erfolgreicher berechtigter Zugriff wird protokolliert.
Typische False Positives (unkritisch)	◗ Ein berechtigter Benutzer greift auf sensible Daten zu, ist jedoch nicht als berechtigter Account registriert.
Typische False Negatives (kritisch)	◗ Ein Benutzer steht auf der Liste berechtigter Benutzer, obwohl er nicht berechtigt sein sollte. ◗ Eine Datei innerhalb eines definierten Speicherorts steht fehlerhaft auf der Negativliste <NL_UNWICHTIGEDATEIPFADE_01>.
Fachliche Beschreibung der Regel	WENN das Ereignis DATA01 oder DATA02 mit Benutzer B für Dateien oder Daten D EINTRITT, UND D ist nicht enthalten in <NL_UNWICHTIGEDATEIPFADE_01> UND (D,*) ist enthalten in <GL_SENSIBLEDATEIPFADE_01> UND (D,B) ist nicht enthalten in <GL_SENSIBLEDATEIPFADE_01> DANN löse aus

→

Gruppierung	**Empfehlung:** Gruppierung nach Benutzer B **Begründung:** Beim Zugriff auf Daten können schnell zahlreiche Warnmeldungen erzeugt werden. Die Zusammenfassung nach dem durchführenden Benutzer B hilft den Überblick zu wahren und schnell möglicherweise kompromittierte Benutzerkonten zu erkennen.
Optionen und Anmerkungen	◗ Die Menge der besonders zu schützenden sensiblen Daten ist in der Regel eingeschränkt und überschaubar. Während allgemein für bspw. Geschäftsdaten komplette Verzeichnisse bzw. Laufwerksfreigaben als Speicherorte angegeben werden, können bei den zu schützenden Daten auch einzelne Dateien angegeben werden.
Empfohlene Reaktion	Prüfung, warum ein Zugriff erfolgte und ob ggf. ein Benutzerkonto kompromittiert wurde
Referenz ATT&CK Techniques	T1005 [G] (Data from Local System), T1039 [G] (Data from Network Shared Drive), T1025 [G] (Data from Removable Media)
Referenz BSI	ORP.4 Identitäts- und Berechtigungsmanagement
Referenz ATT&CK Tactics	Collection

3.9.42 B42 – Unzulässiger Zugriff auf System- und Konfigurationsdaten

ID	B42
Name	Unzulässiger Zugriff auf System- und Konfigurationsdaten
Kurzbeschreibung mit Detektionsziel	Zugriff auf Passworttabellen, Passwortdateien, trusted destinations (bspw. in SAP) usw. soll erkannt werden. Das beinhaltet auch Manipulationen.
Adressierte Risiken	Ein unberechtigter Zugriff auf geschützte Daten, insbesondere Authentifizierungsinformationen, kann einem Angreifer Informationen über weitere Zugänge und damit den Einstieg in das Lateral Movement ermöglichen. Werden solche Daten verändert, kann ein Angreifer ggf. seine Rechte eskalieren.
Erforderliche Informationen	◗ Die Ereigniscodes DATA01 oder DATA02 ◗ Benutzers B, der Zugriffe durchführt ◗ Gruppe G, in der Benutzer B Mitglied ist ◗ Datei FILE oder Verzeichnis DIR, auf das zugegriffen wird ◗ <GL_SENSIBLEDATEIEN_01>: Liste von Dateien (FILE) oder Verzeichnissen (DIR), die überwacht werden sollen ◗ <GL_ERFORDERLICHERECHTE_01>: Liste mit zusätzlichen zu überwachenden Dateien (FILE) und Verzeichnissen (DIR) bzw. Speicherorten und die für diese erforderlichen Berechtigungen bzw. Berechtigungsstufen ◗ <GL_ZUGRIFFSRECHTE_01>: Liste mit den Berechtigungen bzw. Berechtigungsstufen der Benutzer ◗ Tabelle der berechtigten Benutzer (B) und/oder Benutzergruppen (G) mit den Berechtigungen für die jeweiligen Verzeichnisse (DIR) und/oder Dateien (FILE) ◗ Liste von Ausnahmen, z. B. nicht überwachte Dateien, wenn sonst Verzeichnisse angegeben sind ◗ Optional: Tabelle von Dateien und Berechtigungen außerhalb der überwachten Verzeichnisse
Benötigte Positiv- und Negativlisten	◗ Negativliste <NL_AUSNAHMEN_01>: Liste von Dateien oder Verzeichnissen von Speicherorten, auf die zugegriffen werden darf ◗ Negativliste <NL_ZUGRIFFSRECHTE_01>: Liste mit den zugelassenen Berechtigungen
Empfohlener Reaktionstyp	Warnmeldung
Kritikalität	2 (hoch)
Dringlichkeit	2 (schnell)
Typische True Positives (kritisch)	◗ Ein unberechtigter Benutzer oder ein Angreifer versucht unerlaubt auf eine Datei mit geschützten Daten zuzugreifen.
Typische True Negatives (unkritisch)	◗ Ein erfolgreicher berechtigter Zugriff findet statt.
Typische False Positives (unkritisch)	◗ Ein berechtigter Benutzer greift auf geschützte Daten zu, ist jedoch nicht auf einer der erforderlichen Freigabelisten registriert.
Typische False Negatives (kritisch)	◗ Ein Benutzer steht auf der Liste berechtigter Benutzer, obwohl er nicht berechtigt sein sollte. ◗ Eine Datei außerhalb der definierten Speicherorte steht fälschlicherweise nicht auf der Liste zu überwachender Dateien oder Verzeichnisse bzw. Speicherorte. ◗ Eine Datei innerhalb eines definierten Speicherorts steht fälschlicherweise auf einer Negativliste.

→

Fachliche Beschreibung der Regel	WENN Ereignis DATA01 ODER Ereignis DATA02 durch Benutzer B mit Benutzergruppe G für Datei FILE oder Verzeichnis DIR EINTRITT, UND DIR oder FILE ist in <GL_SENSIBLEDATEIEN_01> UND DIR oder FILE ist nicht enthalten in <NL_AUSNAHMEN_01> UND die Kombination (B/G, DIR/FILE) ist nicht enthalten in <NL_ZUGRIFFSRECHTE_01> ODER DIR oder FILE ist enthalten in <GL_ERFORDERLICHERECHTE_01> UND für die erforderliche Berechtigung bzw. Berechtigungsstufe R für den Zugriff auf DIR/FILE gemäß <GL_ERFORDERLICHERECHTE_01> gilt: (B,R) ist nicht enthalten in <GL_ZUGRIFFSRECHTE_01> DANN löse aus
Gruppierung	**Empfehlung:** Gruppierung nach Benutzer B **Begründung:** Beim Zugriff auf Daten können schnell zahlreiche Warnmeldungen erzeugt werden. Die Zusammenfassung nach dem durchführenden Benutzer B hilft den Überblick zu wahren und schnell möglicherweise kompromittierte Benutzerkonten zu erkennen.
Optionen und Anmerkungen	◗ Die Menge der zu schützenden Daten ist in der Regel deutlich kleiner als die Menge der Geschäftsdaten. Während bei Geschäftsdaten komplette Verzeichnisse bzw. Laufwerksfreigaben als Speicherorte angegeben werden, können bei besonders zu schützenden Daten auch einzelne Dateien angeführt werden. ◗ Der Use-Case hier stellt zwei Möglichkeiten dar, um Daten zu schützen: 1. Nach Speicherort und dedizierter Berechtigung: Der Zugriff auf den Speicherort, typischerweise Dateien oder Verzeichnisse, löst keinen Alarm aus, sofern die entsprechenden Benutzer bzw. Berechtigungsgruppen auf einer Negativliste stehen. 2. Nach Speicherort und (abstrakten) Berechtigungen oder Berechtigungsstufen: Hier können Klassifikationen abstrakt mit abgebildet werden. Beispielsweise könnte eine Datei als »Streng vertraulich« markiert sein, und alle Benutzer, die nach einer Liste das Recht haben, auf Daten mit der Eigenschaft »Streng vertraulich« zuzugreifen, können so ausgeschlossen werden.
Empfohlene Reaktion	Prüfung, warum ein Zugriff erfolgte und ggf., ob ein Benutzerkonto kompromittiert wurde
Referenz ATT&CK Techniques	T1005 [D] (Data from Local System), T1039 [D] (Data from Network Shared Drive), T1025 [D] (Data from Removable Media)
Referenz BSI	ORP.4 Identitäts- und Berechtigungsmanagement
Referenz ATT&CK Tactics	Collection

3.10 Dokumentation von Use-Cases und Use-Case-Umsetzungen

Use-Cases sollten einheitlich dokumentiert werden. Auch wenn der Use-Case-Katalog bei der Umsetzung eine gute Basisüberwachung sicherstellt, so kann es zusätzlichen individuellen Bedarf an Überwachung je Organisation geben. Beispielsweise könnten spezifische Use-Cases erforderlich sein, die konkrete riskante Operationen in unternehmenseigenen Anwendungssystemen überwachen sollen, wie etwa Hinweise auf Umgehung eines vorgesehenen Vier-Augen-Prinzips bei Freigaben. In einem solchen Fall wird die gleiche Art der Dokumentation wie für die Use-Cases dieses Katalogs gemäß dem Template empfohlen, nur eben mit organisationsspezifischen Inhalten (eigene IDs, fachliche Regeln usw.).

Die beiden folgenden Tabellen 10 und 11 sind in zwei Blöcke unterteilt:

- Der »Zuordnungsblock« (linker Block) dient der Zuordnung der Begriffe des PDCA-Zyklus gemäß Abbildung 1 auf Seite 8.
- Der »Beschreibungsblock« (rechter Block) beschreibt Use-Cases bzw. Use-Case-Umsetzungen in Zeilen und Spalten wie folgt:
  - Farblich hinterlegte Zeilen (in Reihenfolge):
    - Dunkelblau: Daten zur Spezifizierung und Identifikation des Use-Case und der Umsetzung
    - Rosa: Wesentliche Verwaltungsinformationen
    - Grau: Alle Informationen, die notwendig sind, um den Use-Case und die Umsetzung zu implementieren und bei Auslösung zu bearbeiten
    - Rot und grün: Grenzfälle der Detektionsmöglichkeiten
    - Gelb: Fachliche Beschreibung der Prüfregel und, sofern sinnvoll, auch deren Gruppierungsmöglichkeit. Zudem sind in Tabelle 11 im gelben Bereich noch die technische Regel (siehe Erläuterung zu Tabelle 11) sowie Auslösebedingungen enthalten.
    - Hellorange: Empfehlungen für Sonderfälle (Zeile »Optionen und Anmerkungen«) sowie zu Handlungsempfehlungen (»Empfohlene Reaktion«) auf Basis der Erfahrung der Autoren
    - Grau: Soweit vorhanden Hinweise zu unterstützenden Referenzenmodellen
  - Spalten:
    - Erste Spalte: Feldnamen bzw. Kurzbezeichnung der Information
    - Zweite Spalte: Wesentlichkeit des Feldes in drei Varianten:
      - **Erforderlich**: Dieses Feld bzw. diese Information sollte auf jeden Fall dokumentiert werden.
      - **Empfohlen**: Dieses Feld bzw. diese Information sollte für die Aufnahme geprüft werden. Als Grundannahme gilt, dass das Feld dokumentiert wird.

Zuordnung zu den Elementen in **Abbildung 1**	**Bezeichnung**	**erforderlich / empfohlen / optional**	**Inhalte**
	ID	erforderlich	im Unternehmen vergebene ID für diesen Use-Case
	Name	erforderlich	Bezeichnung des Use-Cases
	Kurzbeschreibung mit Detektionsziel	erforderlich	Beschreibung, was detektiert werden soll
	Adressierte Risiken	erforderlich	Beschreibung, welche Risiken adressiert werden
	Verantwortliche	erforderlich	Verantwortliche für den Use-Case
	Stand	erforderlich	Datum dieser Beschreibung
	Letzte Prüfung	erforderlich	Datum der letzten Prüfung: Prüfung ob dieser Use-Case erforderlich ist, die genannten Risiken adressiert und die Detektionsziele erfüllt sind.
	Status	erforderlich	Status dieses Use-Cases, beispielsweise entwurf, freigegeben, nicht anzuwenden
Ereignis Listen	Erforderliche Informationen	erforderlich	erforderliche Informationen bzw. Daten
	Benötigte Positiv- und Negativlisten	erforderlich	Listenaufstellung mit Inhalten, soweit erforderlich
	Reaktionstyp	erforderlich	Warnmeldung, Bericht, andere ...
	Kritikalität	erforderlich	normal (1), hoch (2), sehr hoch (3)
	Dringlichkeit	erforderlich	normal (1), schnell (2), unverzüglich (3)
Regel-optimierung	Typische True-Positives (kritisch)	empfohlen	Auflistung der Arten von True-Positives, also Fälle korrekter Detektionen
	Typische True-Negatives (unkritisch)	empfohlen	Auflistung der Arten von True-Negatives, also in welchen Fällen gewollt nicht detektiert werden soll
	Typische False-Positives (unkritisch)	empfohlen	Auflistung der Arten von False-Positives, also in welchen Fällen detektiert werden könnte, obwohl das grundsätzlich nicht erwünscht ist
	Typische False-Negatives (kritisch)	empfohlen	Auflistung der Arten von False Negatives, also wenn tatsächliche Fälle nicht detektiert werden könnten
Prüfregel, Auslösung	Fachliche Beschreibung Regel	erforderlich	Fachliche Beschreibung, wie der Use-Case funktioniert
	Gruppierung	empfohlen	Nach was werden die detektierten Ereignisse bzw. erstellten Warnmeldungen gruppiert
	Optionen und Anmerkungen	optional	Ergänzungen, bspw. Sonderverhalten, Spezialfälle, besondere Art der Durchführung, Abhängigkeiten oder ähnliches
Reaktion	Reaktion	erforderlich	Welche typischen Reaktionen hier durchgeführt werden. Dies kann abstrakt ("allgemeine Detail- und Umfeldanalyse") oder konkret ("Überprüfung ob betroffenes Benutzerkonto jünger als 1 Tag ist, falls ja Aktivität ... durchführen")
	Referenz ATT&CK Techniques	empfohlen	Referenz ATT&CK Techniques und Subtechniques, siehe hier: https://attack.mitre.org/tactics/enterprise/
	Referenz BSI	empfohlen	Referenz BSI IT-Grundschutz wenn möglich
	Referenz ATT&CK Tactics	erforderlich	Die Zuordnung zu den entsprechenden ATT&CK Tactics, siehe hier: https://attack.mitre.org/tactics/enterprise/

Tabelle 10: Steckbrief für Use-Cases

- **Optional**: Dieses Feld bzw. diese Information kann hilfreich sein und sollte für die Aufnahme geprüft werden.

- Dritte Spalte: Beschreibung des Inhalts

Für die Umsetzungen gilt das Gleiche wie für Use-Cases: Vor, während und nach der Umsetzung ist eine einheitliche und ausreichend detaillierte Dokumentation erforderlich. Tabelle 11 zeigt die Empfehlungen, was im Rahmen der technischen Umsetzung dokumentiert werden sollte.

Dies ist die gleiche Art der Dokumentation wie bei der Beschreibung der Use-Cases, es sind lediglich ein paar Informationen hinzugekommen. Besonders hervorzuheben sind hier die folgenden Punkte:

- Während sich die Dokumentation im Kapitel über die Use-Cases auf eine abstrakte Ebene beschränkte, sind hier konkrete Umsetzungen zu dokumentieren. Die Anzahl der Use-Case-Umsetzungen kann größer oder auch kleiner sein als die Zahl der Use-Cases:
  - Beispiel 1 (größere Zahl der Umsetzungen): Ein Unternehmen setzt die Use-Cases B01 bis B09, also Auswertungsniveau 1, um. Hierfür benötigt es jedoch 15 unterschiedliche Umsetzungen, die diese Use-Cases abdecken, weil unterschiedliche Umsetzungen für die verschiedenen Assetklassen dies erfordern.
  - Beispiel 2 (kleinere Zahl der Umsetzungen): : Ein Unternehmen setzt die Use-Cases B01 bis B14 und zwei spezifische eigene S01 und S02 um. Für die gesamte Umsetzung benötigt es 20 unterschiedliche Umsetzungen, wobei 12 für die Umsetzung von B01 bis B14 und die verbliebenen acht für die Umsetzung von

Zuordnung zu den Elementen in **Abbildung 1**	**Bezeichnung**	**erforderlich / empfohlen / optional**	**Inhalte**
	ID	erforderlich	im Unternehmen vergebene ID für diese Use-Case-Umsetzung
	Name	erforderlich	Bezeichnung der Use-Case-Umsetzung
	Kurzbeschreibung mit Detektionsziel	erforderlich	Beschreibung, was diese konkrete Ausprägung detektieren soll
	Adressierte Risiken	erforderlich	Beschreibung, welche Risiken durch diese konkrete Ausprägung adressiert werden
	Verantwortliche	erforderlich	Verantwortliche für die Umsetzung
	Stand	erforderlich	Datum dieser Beschreibung
	Letzte Prüfung	erforderlich	Datum der letzten Prüfung dieser Umsetzung auf Wirksamkeit
	Status	erforderlich	Status dieser Umsetzung, typischerweise Entwurf, Produktiv, Obsolet
Ereignis Listen	Erforderliche Informationen	erforderlich	für die Umsetzung erforderliche Informationen bzw. Daten
	Benötigte Positiv- und Negativlisten	erforderlich	Listenaufstellung mit Inhalten, soweit erforderlich
	Reaktionstyp	erforderlich	Warnmeldung, Bericht, andere ...
	Kritikalität	erforderlich	normal (1), hoch (2), sehr hoch (3)
	Dringlichkeit	erforderlich	normal (1), schnell (2), unverzüglich (3)
	Priorität	empfohlen	Je kleiner, desto wichtiger. Berechnet sich grundsätzlich P = 10 - Kritikalität * Dringlichkeit
Regel-optimierung	Typische True-Positives (kritisch)	empfohlen	Auflistung der Arten von True-Positives, also Fälle korrekter Detektionen durch die Umsetzung
	Typische True-Negatives (unkritisch)	empfohlen	Auflistung der Arten von True-Negatives, also in welchen Fällen die Umsetzung gewollt nicht detektiert werden soll
	Typische False-Positives (unkritisch)	empfohlen	Auflistung der Arten von False-Positives, also in welchen Fällen die Umsetzung detektieren könnte, obwohl das grundsätzlich nicht erwünscht ist
	Typische False-Negatives (kritisch)	empfohlen	Auflistung der Arten von False-Negatives, also wenn tatsächliche Fälle durch die Umsetzung nicht detektiert werden könnten
Prüfregel, Auslösung	Fachliche Beschreibung Regel	erforderlich	Fachliche Beschreibung der Umsetzung
	Technische Regel	erforderlich	Technische Beschreibung (konkretes Regelwerk) der Umsetzung. Sollte ebenfalls die Frequenz, also wie oft die Regel ausgeführt wird (Echtzeit, alle 5 min, jede Stunde, ...) beinhalten.
	Auslösebedingungen	optional	Was muss getan werden, um den Use-Case auszulösen.
	Assetklassen	erforderlich	Für welche Assetklassen (Windows-Server, Firewall-System-Modell xy, ...) die Detektion in dieser Form funktioniert.
	Gruppierung	empfohlen	Nach was werden die durch die Umsetzung detektierten Ereignisse bzw. erstellten Warnmeldungen gruppiert
	Hinweise und Anmerkungen	optional	Ergänzungen zu der Umsetzung, bspw. Sonderverhalten, Spezialfälle, besondere Art der Durchführung, Abhängigkeiten oder ähnliches
Reaktion	Reaktion	erforderlich	Welche typischen Reaktionen hier durchgeführt werden. Dies kann abstrakt ("allgemeine Detail- und Umfeldanalyse") oder konkret ("Überprüfung ob betroffenes Benutzerkonto jünger als 1 Tag ist, falls ja Aktivität ... durchführen")
	Referenz Use-Cases	erforderlich	Die IDs, z.B. B01, der durch diese Umsetzung abgedeckten Use-Cases sollten hier referenziert werden.
	Referenz ATT&CK Techniques	empfohlen	Referenz ATT&CK Techniques und Subtechniques, siehe hier: https://attack.mitre.org/tactics/enterprise/
	Referenz BSI	empfohlen	Referenz BSI IT-Grundschutz wenn möglich
	Referenz ATT&CK Tactics	erforderlich	Die Zuordnung zu den entsprechenden ATT&CK Tactics, siehe hier: https://attack.mitre.org/tactics/enterprise/

Tabelle 11: Steckbrief zur einheitlichen Dokumentation von Use-Case-Umsetzungen

S01 und S02 benötigt werden. Hier werden weniger Umsetzungen für die Use-Cases aus dem Use-Case-Katalog benötigt, weil mehrere Use-Cases in einer Umsetzung zusammengefasst werden konnten.

- Es wird empfohlen, die Use-Cases und ihre Umsetzungen über das Feld »Referenz Use-Cases« »zusammenzuhalten« – also ein Mapping zwischen den Use-Cases aus dem Katalog und den in einer Organisation umgesetzten Use-Cases durchzuführen. Dies vereinfacht die Strukturierung und hilft dabei, den Überblick zu wahren.
- Der Inhalt der Felder bezieht sich – bis auf die Referenzen – stets auf die konkrete, individuelle Umsetzung in einer Organisation. Daher wird in Feldern wie »ID« auch nicht ein »B07« o.Ä. erwartet, sondern eine durch die Organisation vergebene ID, z.B. »UCU-07-01«. Wenn ein Use-Case aus diesem Katalog wie bspw. »B07« umgesetzt würde, so wäre dies im Referenzfeld »Referenz Use-Cases« als »B07« zu dokumentieren.
- Zusätzliches Feld »Technische Regel«:
  Für die eher abstrakte Beschreibung der Use-Cases wie in diesem Katalog war dies unnötig bzw. nicht beschreibbar, da keine konkrete technische Umsetzung für eine konkrete Assetklasse mit einer konkreten Technologie dokumentiert wurde. Bei der Umsetzungsdokumentation ist dies jedoch zwingend erforderlich. Es könnte bspw. ein Skript wie das PowerShell-Skript aus dem Umsetzungsbeispiel im vorigen Kapitel sein, eine SIEM-Regel oder Ähnliches. Wird die Überprüfung nur manuell vorgenommen, so ist deren Beschreibung direkt oder als Referenz hier zu dokumentieren.
- Feld »Fachliche Regel«:
  Die Informationen im Feld »Technische Regel« können sehr komplex sein und insbesondere bei einem möglichen späteren Technologiewechsel die Organisation vor Schwierigkeiten stellen. Beispiele für solche Umstiege wären der Wechsel von einer Skriptsprache in eine andere (z.B. PowerShell zu Python) oder von skriptbasierter Auswertung auf die Implementierung in einem SIEM-System. Möglicherweise ist zu diesem Zeitpunkt das Wissen über die genaue Funktionsweise der Umsetzung nicht mehr vorhanden oder die Dokumentation selbst ist nicht ausreichend. Hierfür ist es hilfreich, wenn im Feld »Fachliche Regel« eine kurze Zusammenfassung in natürlicher Sprache steht, die die wesentlichen Punkte der Funktionsweise der Umsetzung beschreibt.
- Zusätzliches Feld »Assetklassen«:
  Hier wird dokumentiert, für welche Assetklassen diese Umsetzung den beschriebenen bzw. referenzierten Use-Case abdeckt.
- Zusätzlich ist es wichtig zu dokumentieren, wann die Umsetzung in der beschriebenen Form erfolgte und wann sie durch wen zuletzt geprüft wurde.
- Die Use-Cases und ihre Umsetzung sollten in einem regelmäßigen Zyklus daraufhin überprüft (»rezertifiziert«) werden, ob sie noch gültig sind und ihren Zweck noch erfüllen.

Es können auch weitere Informationen hinzugefügt werden, jedoch sollten

- bei Use-Cases mindestens die erforderlichen Felder des Steckbriefs aus Tabelle 10 und
- bei Use-Case-Umsetzungen mindestens die erforderlichen Felder des Steckbriefs aus Tabelle 11

enthalten sein.

Die Dokumentation von Use-Cases und Use-Case-Umsetzungen muss nicht tabellarisch erfolgen, sondern kann in der für die Organisation am besten geeigneten Weise geschehen (z.B. Datenbank). Allerdings sollte die Dokumentation

- elektronisch auswertbar erfolgen,
- in derselben Form als Bericht präsentierbar sein (Papierform und elektronisches Dokument) wie in diesem Dokument beschrieben und
- stets mit einem eindeutigen konsistenten Stand zu einem gegebenen Zeitpunkt reproduzierbar sein (Versions-/Änderungskontrolle).

4 Bericht

In Abschnitt 3.10 wurde gezeigt, wie eine Organisation die erforderlichen Use-Cases möglichst strukturiert und standardisiert dokumentieren kann. Darüber hinaus ist es auch sinnvoll, Übersichten zur Verfügung zu stellen, die aufzeigen, welche Use-Cases bei welchen Assetklassen umgesetzt werden. Hierzu finden sich in diesem Kapitel Vorschläge zu geeigneten Berichtsvorlagen. Deren Nutzung hat mehrere Vorteile:

- Die Mitarbeiter selbst haben dadurch eine kompakte Zusammenfassung über die spezifische Auswahl der Use-Cases der Organisation.
- Im Hinblick auf regelmäßige Wirksamkeitsprüfungen der implementierten Angriffserkennung sind Berichte ein unabdingbares Hilfsmittel der Qualitätssicherung oder dienen dazu, in Managementzusammenfassungen einen Einblick in die Sicherheitslage der Organisation geben zu können (Angriffshistorie).
- Eine Berichtsvorlage erhöht die Transparenz der Art und Weise, wie ein Use-Case-Katalog umgesetzt wurde. Das erleichtert sehr den Austausch mit Prüfern oder Revisoren im Rahmen von Audits oder Zertifizierungen.

Abbildung 11 zeigt den Vorschlag für eine Berichtsvorlage für Unternehmen in einem einfachen tabellarischen Format. Zunächst werden im Kopf wesentliche Informationen dargestellt:

- **Unternehmen**: Name der betroffenen Organisation
- **Unternehmensspezifische Risikobewertung bzgl. Assets durchgeführt?**: Angabe, ob eine entsprechende Bewertung durch die Organisation durchgeführt und dokumentiert worden ist.
- **Abgenommen am** und …
- **Abgenommen von**: Wann der Bericht abgenommen und von wem verifiziert wurde, dass die dargestellten Informationen korrekt sind.

Darunter folgen Details: Horizontal aufgetragen sind die in Abschnitt 3.9 beschriebenen 42 Use-Cases mit zunehmendem Auswertungsniveau. Diese werden in der Vertikalen[1] mit den Assetklassen in Beziehung gesetzt, für die der jeweilige Use-Case eingerichtet ist. Ein »X« steht dabei für eine vollständige Umsetzung, ohne Einschränkung. Eine hilfreiche Unterscheidung der Assetklassen ist deren Einteilung in die Typen Anwendungen (A) und Infrastruktur (I).

Im Rahmen von Audits bzw. IT/OT-Prüfungen hilft eine Angabe dazu, ob eine unternehmensspezifische Risikoanalyse bzgl. der Assets durchgeführt wurde. Diese berücksichtigt bekannte Schwachstellen (Sicherheitslücken), Penetration-

1 Sollte aufgrund des Verhältnisses der Zahl der Use-Cases zur Zahl der Assetklassen eine Darstellung mit Use-Cases in der Vertikalen und Assetklassen in der Horizontalen sinnvoller sein, so ist dies ebenfalls zulässig. Voraussetzung ist jedoch, dass alle erforderlichen Informationen weiterhin eindeutig zugeordnet werden können.

Unternehmen	
Unternehmensspezifische Risikobewertung bzgl. Assets durchgeführt?[(a)]	
Abgenommen am	
Abgenommen von	

	Auswertungsniveau	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	3	3	3	4	4	4
Typ	**v Assetklasse | Use-Cases ->**	**B01**	**B02**	**B03**	**B04**	**B05**	**B06**	**B07**	**B08**	**B09**	**B10**	**B11**	**B12**	**B13**	**B14**	**B15**	**B16**	**B17**	**B18**	**B19**	**B20**	**B21**	**B22**	**B23**	**B24**	**B25**	**B26**	**B27**	**B28**	**B29**	**B30**	**B31**	**B32**	**B33**	**B34**	**B35**	**B36**	**B37**	**B38**	**B39**	**B40**	**B41**	**B42**
A/I	Assetklasse 1																																								
A/I	Assetklasse 2																																								
A/I	…																																								
A/I																																									
A/I																																									
A/I																																									
A/I																																									
A/I																																									
A/I																																									
A/I																																									
A/I																																									
A/I																																									
A/I																																									
A/I																																									

Ausfüllen:

- **x** umgesetzt, keine Einschränkung
- **#…** eingeschränkt oder nicht umgesetzt, ID (1, 2, …) mit Begründung und ggf. Risikobewertung
- (a) Angabe, ob eine unternehmensspezifische Risikoanalyse bzgl. der Auswahl der Assets durchgeführt wurde. Im Falle von kritischen Assetklassen sollte auch ein höheres Auswertungsniveau umgesetzt worden sein. Ist dies nicht der Fall muss das Risiko von der Organisation hierzu identifiziert und bewertet worden sein.

Abbildung 11: Generisches Berichtstemplate für einen Use-Case-Katalog

Unternehmen	*Beispiel GmbH*
Unternehmensspezifische Risikobewertung bzgl. Assets durchgeführt?	*Nein*
Abgenommen am	*01.02.2024*
Abgenommen von	*Max Mustermann, CIO*

	Auswertungsniveau ->	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	3	4	4	4
Typ	**v Assetklasse | Use-Cases ->**	**B01**	**B02**	**B03**	**B04**	**B05**	**B06**	**B07**	**B08**	**B09**	**B10**	**B11**	**B12**	**B13**	**B14**	**B15**	**B16**	**B17**	**B18**	**B19**	**B20**	**B21**	**B22**	**B23**	**B24**	**B25**	**B26**	**B27**	**B28**	**B29**	**B30**	**B31**	**B32**	**B33**	**B34**	**B35**	**B36**	**B37**	**B38**	**B39**	**B40**	**B41**	**B42**
I	Windows-Clients	x	x	x	x	x	x	x	x	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
I	Windows-Server	x	x	x	x	x	x	x	x	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
I	Antivirus	x	x	x	x	x	x	x	x	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
I	Internet-Router	1	x	x	x	x	x	x	x	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
I	Mailserver	x	x	x	x	x	x	x	x	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
I	WebProxy	x	x	x	x	x	x	x	x	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
I	Firewall, basic (bis Layer 3)	x	x	x	x	x	x	x	x	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
I	Non-Windows-Server	x	x	x	x	x	x	x	x	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
I	Webserver	x	x	x	x	x	x	x	x	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
I	Active Directory / LDAP	x	x	x	x	x	x	x	x	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
I	WLAN-Router	x	x	x	x	x	x	x	x	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
I	NTP-Programm / - Server	x	x	x	x	x	x	x	x	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
I	Remote-Zugang/VPN	x	x	x	x	x	x	x	x	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
I	eigener DNS-Service	x	x	x	x	x	x	x	x	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
I	Netzwerkdrucker	x	x	x	x	x	x	x	x	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
I	Zentrale Laufwerke	x	x	x	x	x	x	x	x	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
...	--- (weitere)	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Begründungen und Risiken

1 Nicht umgesetzt, weil die Logs in der Appliance gekapselt sind. Risikoakzeptanz: ID xxxx-yyy

Abbildung 12: Bericht des Use-Case-Katalogs der Firma Beispiel GmbH auf Basis des Berichtstemplates

Test-Ergebnisse, sicherheitsrelevante Konfigurationen, Gefährdung durch physischen Zugriff durch Unbefugte sowie weitere für die Organisation spezifische Risiken bzgl. des betroffenen Assets. Diese Risikoanalyse stellt dann die Grundlage dar, um die Use-Cases unternehmensspezifisch auswählen zu können.

Im Fall von kritischen Assetklassen sollte geprüft werden, ob ein höheres Auswertungsniveau der Use-Cases oder zusätzliche spezifische Use-Cases erforderlich sind. Sollte dies zutreffen, jedoch keine entsprechende Umsetzung erfolgen, so müssen die Risiken identifiziert und bewertet worden sein. Diese Risikobewertung sollte idealerweise für ein Audit bzw. eine Prüfung vorliegen.

Zur Veranschaulichung der praktischen Umsetzung findet sich in Abbildung 12 ein ausgefüllter Bericht der Firma Beispiel GmbH.

Es werden alle empfohlenen Use-Cases dieses Katalogs im Auswertungsniveau 1 umgesetzt (B01 – B09), und zwar über alle Stackebenen der Infrastruktur hinweg. Eine Ausnahme ist der Internet-Router im Fall von Use-Case B01 (Löschung von Ereignisprotokollen). Hier wurde das Risiko, dass Protokolle gelöscht werden könnten, von den Verantwortlichen bewertet, akzeptiert und dokumentiert. Als Begründung wird angeführt, dass der Router eine Appliance ist, und aufgrund dieser Kapselung Veränderungen an den Protokollen nicht überwacht werden können.

Ein weiteres Umsetzungsbeispiel zeigt Abbildung 13. Hier wurde das Berichtstemplate um die nicht umgesetzten Teile des generischen Katalogs gekürzt. Es werden nur noch die implementierten Use-Cases notiert.

Unternehmen	*Beispiel GmbH*
Unternehmensspezifische Risikobewertung bzgl. Assets durchgeführt?	*Nein*
Abgenommen am	*01.02.2024*
Abgenommen von	*Max Mustermann, CIO*

	Auswertungsniveau ->	1	1	1	1	1	1	1	1	1
Typ	**v Assetklasse | Use-Cases ->**	**B01**	**B02**	**B03**	**B04**	**B05**	**B06**	**B07**	**B08**	**B09**
I	Windows-Clients	x	x	x	x	x	x	x	x	x
I	Windows-Server	x	x	x	x	x	x	x	x	x
I	Antivirus	x	x	x	x	x	x	x	x	x
I	Internet-Router	1	x	x	x	x	x	x	x	x
I	Mailserver	x	x	x	x	x	x	x	x	x
I	WebProxy	x	x	x	x	x	x	x	x	x
I	Firewall, basic (bis Layer 3)	x	x	x	x	x	x	x	x	x
I	Non-Windows-Server	x	x	x	x	x	x	x	x	x
I	Webserver	x	x	x	x	x	x	x	x	x
I	Active Directory / LDAP	x	x	x	x	x	x	x	x	x
I	WLAN-Router	x	x	x	x	x	x	x	x	x
I	NTP-Programm / - Server	x	x	x	x	x	x	x	x	x
I	Remote-Zugang/VPN	x	x	x	x	x	x	x	x	x
I	eigener DNS-Service	x	x	x	x	x	x	x	x	x
I	Netzwerkdrucker	x	x	x	x	x	x	x	x	x
I	Zentrale Laufwerke	x	x	x	x	x	x	x	x	x
...	--- (weitere)	-	-	-	-	-	-	-	-	-

Begründungen und Risiken

1 Nicht umgesetzt, weil die Logs in der Appliance gekapselt sind. Risikoakzeptanz: ID xxxx-yyy

Abbildung 13: Bericht des Use-Case-Katalogs der Firma Beispiel GmbH auf Basis des gekürzten Berichtstemplates

Das nächste Umsetzungsbeispiel in Abbildung 14 geht noch einen Schritt weiter und ergänzt eigene organisationsspezifische Use-Cases in der gekürzten Katalogdarstellung.

In diesem Beispiel (Abbildung 14) wurde aufgrund seiner Relevanz Use-Case B11 zusätzlich zu den empfohlenen Use-Cases für das Auswertungsniveau 1 in allen Stackebenen der Infrastruktur implementiert. Außerdem ergänzen drei organisationsspezifische Use-Cases (S01, S02, S03) den Katalog. Anwendungssystem 1 wird mit S01 und S02 überwacht, Anwendungssystem 2 mit den 10 in der Tabelle angegebenen Use-Cases (B01-B08, S02, S03). Das Beispiel zeigt, wie granular und kompakt die Darstellung ist, trotz ihres hohen Informationsgehaltes.

Unternehmen	*Beispiel GmbH*
Unternehmensspezifische Risikobewertung bzgl. Assets durchgeführt?	*Ja*
Abgenommen am	*01.02.2024*
Abgenommen von	*Max Mustermann, CIO*

	Auswertungsniveau ->	1	1	1	1	1	1	1	1	1	2	-	-	-
Typ	**v Assetklasse | Use-Cases ->**	**B01**	**B02**	**B03**	**B04**	**B05**	**B06**	**B07**	**B08**	**B09**	**B11**	**S01**	**S02**	**S03**
I	Windows-Clients	x	x	x	x	x	x	x	x	x	x	-	-	-
I	Windows-Server	x	x	x	x	x	x	x	x	x	x	-	-	-
I	Anti-Virus	x	x	x	x	x	x	x	x	x	x	-	-	-
I	Internet-Router	1	x	x	x	x	x	x	x	x	x	-	-	-
I	Mailserver	x	x	x	x	x	x	x	x	x	x	-	-	-
I	WebProxy	x	x	x	x	x	x	x	x	x	x	-	-	-
I	Firewall, basic (bis Layer 3)	x	x	x	x	x	x	x	x	x	x	-	-	-
I	Non-Windows-Server	x	x	x	x	x	x	x	x	x	x	-	-	-
I	Webserver	x	x	x	x	x	x	x	x	x	x	-	-	-
I	Active Directory / LDAP	x	x	x	x	x	x	x	x	x	x	-	-	-
I	WLAN-Router	x	x	x	x	x	x	x	x	x	x	-	-	-
I	NTP-Programm / - Server	x	x	x	x	x	x	x	x	x	x	-	-	-
I	Remote-Zugang/VPN	x	x	x	x	x	x	x	x	x	x	-	-	-
I	eigener DNS-Service	x	x	x	x	x	x	x	x	x	x	-	-	-
I	Netzwerkdrucker	x	x	x	x	x	x	x	x	x	x	-	-	-
I	Zentrale Laufwerke	x	x	x	x	x	x	x	x	x	x	-	-	-
A	Anwendungssystem 1	2	2	2	2	2	2	2	2	2	2	x	x	-
A	Anwendungssystem 2	x	x	x	x	x	x	x	x	2	2	-	x	x
...	--- (weitere)	-	-	-	-	-	-	-	-	-	-	-	-	-

Begründungen und Risiken

1 Nicht umgesetzt, weil die Logs in der Appliance gekapselt sind.
Risikoakzeptanz: ID xxxx-yyy-1

2 Nicht umgesetzt, da die Abdeckung über die Infrastruktur als ausreichend bewertet ist.
Risikoakzeptanz: ID xxxx-yyy-2

Abbildung 14: Bericht des Use-Case-Katalogs der Firma Beispiel GmbH auf Basis des gekürzten und ergänzten Berichtstemplates

5 Zusammenfassung und Ausblick

Ziel des vorliegenden Leitfadens ist es, Leserinnen und Leser das Handwerkszeug für den Aufbau einer Überwachung zur Verfügung zu stellen: Sie können nun die Use-Cases auswählen, dokumentieren, ihren Assetklassen zuordnen, an ihre Gegebenheiten anpassen und mit dem Bericht sowohl den Aufbau ihres eigenen Use-Case-Katalogs steuern als auch überprüfen. Wir wünschen viel Erfolg damit!

Noch abschließend ein Ausblick:

Der hier vorliegende Use-Case-Katalog ist der erste seiner Art und ein Anfang. Er ist sicher nicht abschließend und vollständig. Somit würden wir uns sehr freuen, wenn weitere Interessierte an den zukünftigen Änderungen und Erweiterungen mitarbeiten. Bestimmt gibt es noch weitere Use-Cases, die es wert sind, hier aufgenommen zu werden. Auch können wir uns vorstellen, den Katalog in Zukunft online mit der Möglichkeit eines interaktiven Austauschs im Sinne einer Open-Source-Community zur Verfügung zu stellen. Ob wir dahin kommen, wird davon abhängen, ob Leserinnen und Leser unser Angebot annehmen und ihr Wissen einbringen. Ein weiteres Anliegen ist es, dieses Werk auch in englischer Sprache zu veröffentlichen. Auch hierfür freuen wir uns über Sprachkundige, die uns dabei unterstützen.

Was wir uns zudem für alle wünschen, ist eine standardisierte Protokollierung, in der zumindest die sicherheitsrelevanten Ereignisinformationen einheitlich zur Verfügung gestellt werden. Das würde bedeuten, dass der Aufwand zum Aufbau einer Sicherheitsüberwachung sich deutlich reduziert und für viele Unternehmen, insbesondere auch kleine und mittlere, erschwinglich wird. Wir erhoffen uns, dass dieses Dokument mit seinen Details unter anderem Hersteller hierbei unterstützt. Dafür haben wir bspw. neben den Use-Cases auch die Liste der abstrakten Ereignisdefinitionen und die Berichtstemplates zur Verfügung gestellt. Wenn daraus dann irgendwann 20 % der für eine Angriffserkennung benötigten Protokolldaten standardisiert ausgegeben werden und damit 80 % der Angriffe mit Standardlösungen erkannt werden, wäre uns allen sehr geholfen.

Wir freuen uns über jede Unterstützung! Jede konstruktive Kritik ist willkommen, und alle sind zu uns in die Fachgruppe (als Mitglied oder Gast) eingeladen, um sich an der weiteren Entwicklung und Verbesserung zu beteiligen.

6 Abbildungs- und Tabellenverzeichnis

Abbildungen

Abbildung 1: Funktionaler Ablauf eines IT-Security Use-Case 8
Abbildung 2: Vorgehensschema zur Implementierung von Use-Cases aus dem Katalog 10
Abbildung 3: Zahl der Unternehmen im Vergleich zur Anzahl der Mitarbeiter – KMU beschäftigen den Großteil der Arbeitnehmerinnen und Arbeitnehmer 10
Abbildung 4: Windows Eventlog einer fehlerhaften Anmeldung 11
Abbildung 5 Screenshot ATT&CK Navigator: Abdeckung kombiniert AN1-AN4 22
Abbildung 6 Screenshot ATT&CK Navigator: Abdeckung AN1 23
Abbildung 7 Screenshot ATT&CK Navigator: Abdeckung AN2 24
Abbildung 8 Screenshot ATT&CK Navigator: Abdeckung AN3 25
Abbildung 9 Screenshot ATT&CK Navigator: Abdeckung AN4 26
Abbildung 10: Typischer prozessualer Ablauf einer Use-Case-Umsetzung 28
Abbildung 11: Generisches Berichtstemplate für einen Use-Case-Katalog 123
Abbildung 12: Bericht des Use-Case-Katalogs der Firma Beispiel GmbH auf Basis des Berichtstemplates 124
Abbildung 13: Bericht des Use-Case-Katalogs der Firma Beispiel GmbH auf Basis des gekürzten Berichtstemplates 124
Abbildung 14: Bericht des Use-Case-Katalogs der Firma Beispiel GmbH auf Basis des gekürzten und ergänzten Berichtstemplates 125

Tabellen

Tabelle 1: Use-Case-Zuordnung je Auswertungsniveau 17
Tabelle 2: IT-Landschaft 18
Tabelle 3: Zahl der Use-Cases je Tactic 19
Tabelle 4: Zahl der zugeordneten Techniques je Use-Case 19
Tabelle 5: Use-Case-Zuordnung je Tactic 20
Tabelle 6: Abdeckung Techniques durch Use-Cases 21
Tabelle 7: Liste der abstrakten Ereignisdefinitionen 27
Tabelle 8: Format der im Folgenden beschriebenen Use-Cases 32
Tabelle 9: Wichtige Begriffe des Use-Case-Steckbriefes 32
Tabelle 10: Steckbrief für Use-Cases 120
Tabelle 11: Steckbrief zur einheitlichen Dokumentation von Use-Case-Umsetzungen 121

Varianten

Variante 2a Powershell Script 30
Variante 2b Beispiel einer Ereignisausgabe 30
Variante 3 Festlegung eines Sicherheitssystems 31

7 Abkürzungsverzeichnis

AG	Arbeitsgruppe
AN	Auswertungsniveau
AV	Antivirus
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI-Gesetz
CISO	Chief Information Security Officer
CMDB	Configuration Management Database
DLP	Data Loss Prevention
DNS	Domain Name System
DORA	Digital Operational Resilience Act
FIN	Finish
FQDN	Fully Qualified Domain Name
FW	Firewall
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IKT	Informations- und Kommunikations-technologien
IoC	Indicators of Compromise
IPS	Intrusion Prevention System
ISB	Informationsbeauftragter
IT	Information Technology
MDM	Mobile Device Management
NAC	Network Access Control
NG	Next Generation
NTP	Network Time Protocol
OCSF	Open Cybersecurity Schema Framework
OT	Operation Technology
PAM	Privileged Access Management
PCDA	Plan – Check – Do – Act
PSH	Push Function
PTP	Precision Time Protocol
RST	Reset
SBF	Schutzbedarf
SIEM	Security Information and Event Management
SMB	Server Message Block
SOC	Security Operations Center
SOCaaS	Security Operations Center as a Service
SSH	Secure Shell
TB	Technischer Benutzer
TCP	Transmission Control Protocol
TI	Threat Intelligence
TOTP	Time-based One-Time Password
UC	Use-Case
UDP	User Datagram Protocol
URG	Urgent
UTC	Universal Time Coordinated
VNC	Virtual Network Computing
WAF	Web Application Firewall

8 Literaturverzeichnis

[Bitkom 2024] *Bitkom:* Angriffe auf die deutsche Wirtschaft nehmen zu, August 2024; www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2024.

[BSI 2018] *Bundesamt für Sicherheit in der Informationstechnik (BSI):* Online-Kurs IT-Grundschutz Lerneinheit 2.1: Der Sicherheitsprozess, August 2018; *www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_2_Sicherheitsmanagement/2_01_Sicherheitsprozess.html*.

[BSI 2023] *Bundesamt für Sicherheit in der Informationstechnik (BSI):* IT-Grundschutz-Kompendium (Edition 2023), Februar 2023; *www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html*.

[BSI 2024] *Bundesamt für Sicherheit in der Informationstechnik (BSI):* Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung, November 2024; *www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.pdf*.

[D_STATIS 2025] *Statistisches Bundesamt (Destatis):* Unternehmen, Tätige Personen, Umsatz und weitere betriebs- und volkswirtschaftliche Kennzahlen: Deutschland, Jahre, Unternehmensgröße. Verfügbarer Zeitraum: 2008 – 2022; abgerufen am 13.03.2025; *www-genesis.destatis.de/datenbank/online/statistic/48121/table/48121-0001*.

[IBM 2024] *IBM:* Cost of a Data Breach Report 2024, Juli 2024; *www.ibm.com/downloads/cas/OJLZOEMZ*.

[ISACA 2014] *ISACA:* Leitfaden Cyber-Sicherheits-Check, März 2014; isaca.de/images/Publikationen/Leitfaden/Leitfaden_Cyber-Sicherheits-Check_V1.pdf.

[ISACA 2020] *ISACA:* Leitfaden Cyber-Sicherheits-Check Version 2, Februar 2020; isaca.de/images/Publikationen/Leitfaden/Leitfaden_Cyber-Sicherheits-Check_V2.pdf.

[ISACA 2021] *ISACA:* Leitfaden Cyber-Sicherheits-Check OT, September 2021; isaca.de/images/Publikationen/Leitfaden/Leitfaden_Cyber-Sicherheits-Check_OT.pdf.

[ISACA 2022] *ISACA:* Positionspapier SIEM Vorschlag für einen Protokollierungsstandard, Oktober 2022; isaca.de/images/Publikationen/Positionspapier/ISACA_Germany_-_Positionspapier_SIEM_10-2022.pdf.

[ISACA 2025] ISACA Germany Chapter, abgerufen am 04.05.2025; *www.isaca.de*.

[Mandiant 2024] *Mandiant Consulting:* M-Trends 2024, Mandiant Consulting, April 2024; *cloud.google.com/blog/topics/threat-intelligence/m-trends-2024?hl=en*.

[MITRE 2024] MITRE ATT&CK® Navigator®, mitre-attack.github.io/attack-navigator; abgerufen am 04.12.2024.

[MITRE 2025a] MITRE ATT&CK®, attack.mitre.org; abgerufen am 13.03.2025.

[MITRE 2025b] Enterprise Tactics, attack.mitre.org/tactics/enterprise; abgerufen am 13.03.2025.