|  |
| --- |
| Erweiterung der Sicherheit durch WatchGuard Endpoint-Protection mit Firewall |
| Dylan Nideröst  IPA-Bericht |
| 25.03. bis 12.04.2024 |

Erweiterung der Sicherheit durch WatchGuard Endpoint-Protection mit Firewall  
Individuelle Praktische Arbeit

***Infos zum Autor:***

**Name:**   
**Abteilung:** RC-CH SI RSS-EMEA CE CS DEX ISC  
**Telefon:** +41 79 894 15 79  
**E-Mail:**  dylan.nideroest@siemens.com  
**Adresse:** D4 Business Village Luzern  
 Platz 3  
 6039 Root, Schweiz

# Änderungsnachweis

|  |  |  |
| --- | --- | --- |
| **Datum** | **Aktivität** | **Dokument-Version** |
| 04.03.2024 | Erstellung des Dokuments, Übertitel, Inhaltsverzeichnis, Formatierung, Vorlagen Arbeitsjournal und Verzeichnisse | V0.0 |
| 25.03.2024 | Dokumentation Teil 1 abgeschlossen, Phase «Informieren» abgeschlossen, mit Phase «Planen» begonnen, sowie Lernjournal Tag 1 ausgefüllt | V0.1 |
| 26.03.2024 | Planung des Grundschutzstufen-Konzepts abgeschlossen, Planung des Approval-Meetings abgeschlossen, mit der Planung des Testkonzepts begonnen | V0.2 |
| 27.03.2024 | Planung des Testkonzepts abgeschlossen. Planen-Phase abgeschlossen. Approval-Meeting und Protokollierung abgeschlossen, sowie resultierende Änderungen an der Testumgebung und der Grundschutzstufen notiert. Festlegung Externer Hilfestellung dokumentiert. Abschluss der Entscheiden-Phase | V0.3 |
| 02.04.2024 |  | V0.4 |
| 03.04.2024 |  | V0.5 |
| 05.04.2024 |  | V0.6 |
| 08.04.2024 |  | V0.7 |
| 09.04.2024 |  | V0.8 |
| 10.04.2024 |  | V0.9 |
| 12.04.2024 |  | V1.0 |

Tabelle Änderungsnachweis

Inhaltsverzeichnis

[Änderungsnachweis 2](#_Toc162444307)

[Teil 1: Aufbau und Organisation 6](#_Toc162444308)

[Aufgabenstellung 6](#_Toc162444309)

[Kandidat 6](#_Toc162444310)

[Titel 6](#_Toc162444311)

[Ausgangslage 6](#_Toc162444312)

[Detaillierte Aufgabenstellung 6](#_Toc162444313)

[Mittel und Methoden 16](#_Toc162444314)

[Vorkenntnisse 16](#_Toc162444315)

[Vorarbeiten 16](#_Toc162444316)

[Neue Lerninhalte 16](#_Toc162444317)

[Arbeiten in den letzten 6 Monaten 16](#_Toc162444318)

[Tage, an welchen an der Facharbeit gearbeitet wird 16](#_Toc162444319)

[Bemerkungen 16](#_Toc162444320)

[Projektaufbauorganisation 17](#_Toc162444321)

[Lehrbetrieb und Durchführungsort 17](#_Toc162444322)

[Verantwortliche Fachkraft 17](#_Toc162444323)

[Berufsbildnerin 17](#_Toc162444324)

[Hauptexperte 17](#_Toc162444325)

[Nebenexperten 17](#_Toc162444326)

[Fachgebiete 17](#_Toc162444327)

[Deklaration der Vorarbeiten 18](#_Toc162444328)

[Projektmanagement 21](#_Toc162444329)

[Zeitplanung 22](#_Toc162444330)

[Meilensteine 22](#_Toc162444331)

[Zeitplan 23](#_Toc162444332)

[Arbeitsjournal 24](#_Toc162444333)

[Tag 1 - 25.03.2024 24](#_Toc162444334)

[Tag 2 - 26.03.2024 26](#_Toc162444335)

[Tag 3 - 27.03.2024 28](#_Toc162444336)

[Tag 4 - 02.04.2024 29](#_Toc162444337)

[Tag 5 - 03.04.2024 30](#_Toc162444338)

[Tag 6 - 05.04.2024 31](#_Toc162444339)

[Tag 7 - 08.04.2024 32](#_Toc162444340)

[Tag 8 - 09.04.2024 33](#_Toc162444341)

[Tag 9 - 10.04.2024 34](#_Toc162444342)

[Tag 10 - 12.04.2024 35](#_Toc162444343)

[Teil 2: Projekt 36](#_Toc162444344)

[Kurzfassung 36](#_Toc162444345)

[Informieren 37](#_Toc162444346)

[Wissensbeschaffung 37](#_Toc162444347)

[Vorbereitete Testumgebung 37](#_Toc162444348)

[Planen 38](#_Toc162444349)

[Vorgehensweise 38](#_Toc162444350)

[Datensicherung: 38](#_Toc162444351)

[Konfigurationsplan 39](#_Toc162444352)

[Appoval-Meeting Planung 48](#_Toc162444353)

[Testkonzept 49](#_Toc162444354)

[Entscheiden 56](#_Toc162444355)

[Approval-Meeting 56](#_Toc162444356)

[Änderungen an der Testumgebung 57](#_Toc162444357)

[Festlegung externer Hilfestellung 59](#_Toc162444358)

[Realisieren 61](#_Toc162444359)

[Versionsverwaltung einsetzen 61](#_Toc162444360)

[Öffnen der Testumgebung 62](#_Toc162444361)

[Installieren von WatchGuard EPDR 62](#_Toc162444362)

[Drei Grundschutzstufen einrichten 62](#_Toc162444363)

[Webzugriffskontrolle bearbeiten 62](#_Toc162444364)

[Erstellung der Firewall-Policies 62](#_Toc162444365)

[Verhinderung spezifischer Software-Installation 62](#_Toc162444366)

[Mailalarmierung einrichten 62](#_Toc162444367)

[Kontrollieren 63](#_Toc162444368)

[Testfälle 63](#_Toc162444369)

[Auswerten 71](#_Toc162444370)

[Stand der Endpoint-Protection 71](#_Toc162444371)

[Erweiterungsmöglichkeiten 71](#_Toc162444372)

[Vollständigkeitstest 72](#_Toc162444373)

[Schlusswort 73](#_Toc162444374)

[Glossar 74](#_Toc162444375)

[Quellenverzeichnis 74](#_Toc162444376)

[Abbildverzeichnis 75](#_Toc162444377)

[Tabellenverzeichnis 76](#_Toc162444378)

[Anhang 77](#_Toc162444379)

[Datenname? 77](#_Toc162444380)

# Teil 1: Aufbau und Organisation

## Aufgabenstellung

### Kandidat

|  |  |  |  |
| --- | --- | --- | --- |
| *Name* | Nideröst | *Vorname* | Dylan |
| *Fachrichtung* | Systemtechnik | *Lehrgang:* | 2020 |
| *Telefon* | 079 894 15 79 | *Mail:* | dylan.nideroest@siemens.com |

Tabelle Kandidat

### Titel

Erweiterung der Sicherheit durch WatchGuard Endpoint-Protection mit Firewall

### Ausgangslage

Um bei Infrastrukturen ohne physikalische Firewall dennoch für Sicherheit sorgen zu können, müssen mit der Endpoint-Protection-Lösung "WatchGuard EPDR" diverse Sicherheitsaspekte abgedeckt werden. Dies umfasst: Kontrollierter Zugriff auf Webseiten, White-/ Black-Listing und Port-Regeln in der integrierten Software-Firewall. Dabei sollen für verschiedene Sicherheitsstufen, welche im Rahmen dieser Arbeit auch konzipiert werden, unterschiedliche Default-Konfigurations-Profile erstellt werden, welche schlussendlich auf den Kundensystemen (Server oder Clients) angewendet werden können. Sämtliche Konfigurationen dieser Lösung erfolgen durch eine zentrale managed Cloud, welche beim Anbieter gehostet wird. Diese Cloud ist mit einem gegebenen Administratoren-Account zugänglich und muss nicht aufgesetzt werden.

### Detaillierte Aufgabenstellung

1. Grundschutzstufen Sicherheit

Ein Konzept für drei Grundschutzstufen bezüglich der Sicherheit ist zu erstellen. Pro Grundschutzstufe ist ein eigenes Profil innerhalb von WatchGuard zu erstellen. Die verschiedenen Grundschutzstufen umfassen strengere oder weniger strengere Richtlinien:

Grundschutzstufe I: Minimum an Sicherheit wird geboten

Grundschutzstufe II: Erhöhte Sicherheit wird geboten

Grundschutzstufe III: Die maximal erreichbare Sicherheit wird geboten

Die WatchGuard Einstellungen und Features dürfen mindestens ab Stufe II nicht durch den Benutzer veränderbar sein.

Die Grundschutzstufen sind in den folgenden Aufgabenstellungen zu berücksichtigen.

2. Approval-Meeting

Zur Bewilligung des Grundschutzstufen-Konzepts wird vom Kandidaten ein Approval-Meeting mit den entsprechenden Personen einberufen. Das Konzept wird vom Kandidaten vorgestellt. Das Konzept wird besprochen und die Ergebnisse werden in einem Protokoll festgehalten.

3. Kontrollierter Zugriff auf Webseiten

a) Der Zugriff auf Webseiten ist sinngemäss einzuschränken.

b) Auf die Firewall muss jederzeit vom Server aus zugegriffen werden können.

c) Die Funktion von Siemens-Anlagen muss vollumfänglich gewährleistet sein und darf nicht eingeschränkt werden.

4. Firewall-Regeln

a) Die Kommunikation wird mittels Firewall-Regeln sinngemäss eingeschränkt.

b) Siemens-Anlagen kommunizieren über verschiedenste URLs und Ports mit dem Internet, um Funktionen wie z.B Fernzugriff zu ermöglichen. Die benötigten Kommunikationswege müssen eruiert werden. Die Funktion von Siemens-Anlagen muss vollumfänglich gewährleistet sein und darf nicht eingeschränkt werden.

5. Verhinderung von spezifischer Software-Installation

Die Installation von spezifischer Software wird verhindert. Der Kandidat eruiert selbstständig Software, welche für bösartige Zwecke eingesetzt werden kann, und blockiert diese. Hierbei soll die Funktionalität dieser Blockierung sichergestellt werden, sodass die Konfiguration für spätere Zwecke als Grundlage verwendet werden kann.

6. Monitoring - Mail-Alert

a) Beim Versuch der Installation von blockierter Software wird die verantwortliche Person per Mail alarmiert.

b) Die verantwortliche Person des Systems wird bei allgemeinen bedrohlichen Situationen per Mail informiert.

c) Die verantwortliche Person des Systems wird zu einem sinnvoll gewählten Intervall mit einem Bericht über die Gesundheit der Systeme und deren Vorfälle informiert.  
Im Bericht soll die verantwortliche Person des Systems über folgende Punkte informiert werden:

- Wird die aktuelle Konfiguration auf dem Endpoint (Client/Server) angewendet und synchronisiert?

- Wurden Malware Aktivitäten festgestellt?

- Sind Risiken vorhanden?

- Sind Angriffsindikatoren (IOAs) vorhanden?

7. Active Directory-Sync

Die Domäne ist mit der WatchGuard Umgebung so zu verknüpfen, sodass die Benutzer und Gruppen vom Active Directory synchronisiert werden und in der WatchGuard Cloud vorhanden sind. Hiermit wird ermöglicht, dass sich berechtigte Benutzer zu einem späteren Zeitpunkt beim Einsatz von Cloud-Devices mit ihrem Active Directory Benutzerkonto anmelden können.

Die Active Directory Struktur darf nicht über die WatchGuard-Cloud veränderbar sein.

8. Dashboard

In der WatchGuard-Cloud ist unter dem erfassten System ein Dashboard zu erstellen, welches folgende Informationen darstellt:

- Geschützte und ungeschützte Endpoints

- Warnmeldungen / Fehler

- Aktuelle Lizenz-Situation

9. Dokumentation

Die Dokumentation umfasst vor allem:

a) Konzept Grundschutzstufe

b) Beschrieb der Konfiguration der verschiedenen Grundschutz-Profile

c) Testergebnisse der durchgeführten Testszenarien

Die Einbindung der Grundschutzprofile auf produktiven Kundensystem ist nicht Bestandteil dieser IPA.

Die Arbeiten erfolgen ausschliesslich auf einem zur Verfügung gestellten Testsystem

Individuelle Bewertungskriterien

|  |  |
| --- | --- |
| *Nummer Katalog-Kriterium - Bezeichnung* | |
| Leitfrage 1, Monitoring (Alarmierung) | |
| *Definition (Leitfrage)* | |
| Werden die eingerichteten Kontakte zu den richtigen Zeiten alarmiert? Werden die Kontakte über die verlangten Medien (Mail, SMS etc.) kontaktiert? | |
| *Gütestufe 3* | *Gütestufe 2* |
| Im Alarmfall werden die richtigen Kontakte zu den richtigen Zeiten mit den richtigen Medien alarmiert. Die richtige Person erhält nach einem sinnvoll gewählten Intervall einen Bericht über die Gesundheit der Systeme und deren bedrohlichen Vorfälle. | Im Alarmfall werden die richtigen Kontakte zu den richtigen Zeiten mit den richtigen Medien alarmiert. |
| *Gütestufe 1* | *Gütestufe 0* |
| Im Alarmfall werden die richtigen Kontakte alarmiert. | Im Alarmfall werden keine Kontakte alarmiert (Alarmierung nicht oder fehlerhaft eingerichtet) |

Tabelle Bewertungskriterium 1

|  |  |
| --- | --- |
| *Bezeichnung* | |
| Leitfrage 2, Kontrollierter Zugriff auf Webseiten | |
| *Definition (Leitfrage)* | |
| Ist der Webzugriff auf allen drei Konfigurationsprofilen eingeschränkt? | |  |
| *Gütestufe 3* | *Gütestufe 2* |
| Der Webzugriff ist auf allen Konfigurationsprofilen eingeschränkt und funktionsfähig. Die Konfigurationen unterscheiden sich aufgrund der Grundschutzstufe und ergeben Sinn. Die Firewall ist erreichbar. | Der Webzugriff ist auf zwei Konfigurationsprofilen eingeschränkt und funktionsfähig. Die Konfigurationen unterscheiden sich aufgrund der Grundschutzstufe. |
| *Gütestufe 1* | *Gütestufe 0* |
| Der Webzugriff ist auf einem Konfigurationsprofil eingeschränkt und funktionsfähig. | Der Webzugriff ist auf keinem Konfigurationsprofil eingeschränkt und nicht funktionsfähig. |

Tabelle Bewertungskriterium 2

|  |  |
| --- | --- |
| *Bezeichnung* | |
| Leitfrage 3, Firewall-Policies | |
| *Definition (Leitfrage)* | |
| Wird die Kommunikation innerhalb des Netzwerks mittels Firewall-Regeln sinngemäss eingeschränkt? | |
| *Gütestufe 3* | *Gütestufe 2* |
| Die Firewall ist auf allen Konfigurationsprofilen aktiviert und die Regeln sind funktionsfähig. Die Regeln unterscheiden sich aufgrund der Grundschutzstufen. | Die Firewall ist auf zwei Konfigurationsprofilen aktiviert und die Regeln sind funktionsfähig. |
| *Gütestufe 1* | *Gütestufe 0* |
| Die Firewall ist auf einem Konfigurationsprofil aktiviert und die Regeln sind funktionsfähig. | Die Firewall ist auf keinem Konfigurationsprofil aktiviert und/oder die Regeln sind nicht funktionsfähig. |

Tabelle Bewertungskriterium 3

|  |  |
| --- | --- |
| *Bezeichnung* | |
| Leitfrage 4, Verhinderung von spezifischer Software-Installation | |
| *Definition (Leitfrage)* | |
| Wird die Installation von spezifischer Software sinngemäss verhindert? | |
| *Gütestufe 3* | *Gütestufe 2* |
| Die Profile sind gemäss Grundschutzstufen so konfiguriert, dass unterschiedliche Software-Installation blockiert wird. Die Verantwortliche Person des Systems wird per Mail alarmiert. | Die Installation von spezifischer Software wird verhindert. Es wird keine Alarmierung per Mail ausgelöst. |
| *Gütestufe 1* | *Gütestufe 0* |
| Die Blockierung ist für eine Software konfiguriert, aber sie kann trotzdem installiert werden. | Keine Software wird blockiert. |

Tabelle Bewertungskriterium 4

|  |  |
| --- | --- |
| *Bezeichnung* | |
| Leitfrage 5, Konzept Grundschutzstufen | |
| *Definition (Leitfrage)* | |
| Wird das Konzept unter Berücksichtigung von Security-Aspekten sinnvoll aufgebaut? | |
| *Gütestufe 3* | *Gütestufe 2* |
| I. Unterschiede zwischen den drei Grundschutz-Stufen sind im Konzept klar ersichtlich.  II. Die Unterschiede dieser Stufen sind aus Sicht von Security sinnvoll gewählt, sodass diese später als Grundlage dienen können. (Niedrige Sicherheit, Mittlere Sicherheit, Hohe Sicherheit).  III. Die Entscheidung dieser Unterschiede werden in der Dokumentation begründet. | Zwei Aspekte werden erfüllt. |
| *Gütestufe 1* | *Gütestufe 0* |
| Ein Aspekt wird erfüllt. | Kein Aspekt wird erfüllt. |

Tabelle Bewertungskriterium 5

|  |  |
| --- | --- |
| *Bezeichnung* | |
| Leitfrage 6, Approval-Meeting | |
| *Definition (Leitfrage)* | |
| Ist das Approval-Meeting Zielführend und werden Ergebnisse festgehalten? | |
| *Gütestufe 3* | *Gütestufe 2* |
| I. Der Kandidat erstellt eine Termineinladung, ist vorbereitet und stellt das Konzept vor.  II. Eine Diskussionsrunde zur Besprechung von Änderungen wird eröffnet.  III. Die Ergebnisse werden in einem Protokoll festgehalten. | Zwei Aspekte werden erfüllt |
| *Gütestufe 1* | *Gütestufe 0* |
| Ein Aspekt wird erfüllt. | Kein Aspekt wird erfüllt. |

Tabelle Bewertungskriterium 6

|  |  |
| --- | --- |
| *Bezeichnung* | |
| Leitfrage 7, Dokumentation | |
| *Definition (Leitfrage)* | |
| Werden die Konfigurationen innerhalb des Profils dokumentiert und entsprechend begründet? | |
| *Gütestufe 3* | *Gütestufe 2* |
| Pro Grundschutzstufe wird begründet:  I. Weshalb die verwendeten Webkategorien/URLs zugelassen oder blockiert werden  II. Weshalb die verwendeten Ports zugelassen oder blockiert werden  III. Weshalb die gewählte Software spezifisch blockiert wird  IV. Weshalb die Alarmierung per Mail eingerichtet wird | Zwei Aspekte werden erfüllt |
| *Gütestufe 1* | *Gütestufe 0* |
| Ein Aspekt wird erfüllt. | Kein Aspekt wird erfüllt. |

Tabelle Bewertungskriterium 7

### Mittel und Methoden

Für die Lösung dieser IPA wird dem Kandidaten ein Testsystem mit virtuellen Servern/Clients zur Verfügung gestellt. Der Kandidat verfügt über einen Administratoren-Account auf dem WatchGuard Account, um das Produkt auf dem Testsystem zu integrieren und konfigurieren. Die IPA soll mit der Projektmanagement-Methode "IPERKA" durchgeführt werden.

### Vorkenntnisse

Da das Produkt neu eingeführt werden soll, sind Vorkenntnisse beschränkt verfügbar. Das Wissen ist der IPA jedoch gerecht. (-> siehe "Vorarbeiten")

### Vorarbeiten

Der Kandidat hat sich selbständig mit dem Produkt vertraut gemacht und sich in kleinerem Rahmen mit den Funktionen auseinandergesetzt. Unklarheiten hat er selbst mit dem Hersteller geklärt. Es ist bereits sichergestellt, dass die benötigten Personen für das Approval-Meeting während der IPA sofort zur Verfügung stehen, um Verzögerungen zu verhindern. Benötigte Lizenzen für die vollständige Durchführung der IPA sind vorhanden.

### Neue Lerninhalte

Erstellung Konzept für Grundschutzstufen und deren Umsetzung:  
Als Quelle steht ihm das Internet und der Hersteller zur Verfügung. Das Approval-Meeting soll dem Lernenden ebenfalls die Möglichkeit geben, dies als Quelle nutzen zu können.

### Arbeiten in den letzten 6 Monaten

- Hauptaufgabe: Mitverantwortung der cRSP-Plattform zur Verwaltung von Remotezugriffen auf Kundensysteme und Applikationen, Bearbeitung von Supportanfragen

- Vorkonfiguration von Gateway-Geräten, welche von Technikern vor Ort in Betrieb genommen werden

- Aufbau und Betreuung von Netzwerken

- Aufbau und Betreuung von Domänenstrukturen

### Tage, an welchen an der Facharbeit gearbeitet wird

Root: 25. Bis 27. März 2024 und 02.Bis 03. Sowie 08. Bis 10. und 12. April 2024 (10 Tage – Abgabe 12. April 2024 spätestens 18:00:00:000 Uhr Einsendung auf PKorg)

### Bemerkungen

Abwesenheiten der VF vor der Facharbeit:  
12.01.2024 - 21.01.2024  
19.02.2024 - 25.02.2024

## Projektaufbauorganisation

### Lehrbetrieb und Durchführungsort

*Firma:* Siemens Schweiz AG, Smart Infrastructure  
*Adresse:* Business Village D4, 6039 Root

### Verantwortliche Fachkraft

*Name:* Timon Hochstrasser  
*Geschäftsadresse:* Duggingerstrasse 23, 4153 Reinach, Schweiz  
*Tel. Geschäft:* +41 79 714 84 91  
*E-Mail:* timon.hochstrasser@siemens.com

### Berufsbildnerin

*Name:* Melanie Fahrner  
*Geschäftsadresse:* Freilagerstrasse 40, 8047 Zürich   
*Tel. Mobil:* +41 79 754 38 63  
*E-Mail:* melanie.fahrner@siemens.com

### Hauptexperte

*Name:* Ruedi Kubli  
*Tel. Mobil:* +41 79 655 88 88   
*E-Mail:* [ruedi.kubli@gmx.ch](mailto:ruedi.kubli@gmx.ch)

### Nebenexperten

*Name:* Alexander Bösch   
*Tel. Mobil:* +41 79 533 26 65  
*E-Mail:* [alexander@boesch.be](mailto:alexander@boesch.be)

### **Fachgebiete**

**Umfeld und Branche der Arbeit**: Information und Kommunikation

**Arbeitsgebiet**: Sicherheitsinfrastruktur (Firewall, DMZ, IDS, ...)

**Plattform**: Windows

**Technologiebereich**: Keine Programmiersprache

## Deklaration der Vorarbeiten

Als Vorarbeit wurde über das Produkt «WatchGuard EPDR» recherchiert. Ich habe ein-Konto mit dem Namen «dylan.nideroest» unter «deu.cloud watchguard.com» von unserem internen Administrator erhalten und eine Zweifaktorauthentifizierung über die App «AuthPoint» eingerichtet. Es wurde mir ein interner Testclient zur Verfügung gestellt, auf dem die EPDR-Software installiert und von der Cloud aus gesteuert und getestet werden konnte. Das Ziel der Tests war es, mich mit der Umgebung vertraut zu machen, die Funktionen und Einstellungen, sowie die Firewall der Software kennenzulernen. Es wurden auch praktische Tests mit den Technikern im Büro durchgeführt, welche diverse Siemens-Geräte über ihre Servern betreuen. Dies war notwendig, um die Erreichbarkeit besagter Geräte mit aktivierter Webzugriffskontrolle und Firewall zu testen.

Für die IPA wurde eine separate Testumgebung auf einem Testserver im Serverraum des Büros eingerichtet. Dies beinhaltet:

* 1 x Windows Server 2016 als Hyper-V-Host
* 1 x virtueller Windows Server 2022
* 1 x virtueller Windows 10 Client

Beide Geräte sind via «Common Remote Service Plattform (cRSP)» der Siemens mit einer Remotedesktopverbindung erreichbar. Auf den Servern befinden sich benötigte Testprogramme, sowie später WatchGuard EPDR installiert. Die beiden virtuellen Maschinen werden mit der WatchGuard-Cloud kommunizieren und von meinem persönlichen Laptop aus, anhand der vorgegebenen Bewertungskriterien, konfiguriert.

In der Abbildung auf der nächsten Seite wurde die Struktur der Testumgebung visuell veranschaulicht.

Aufbau der IPA-Testumgebung:

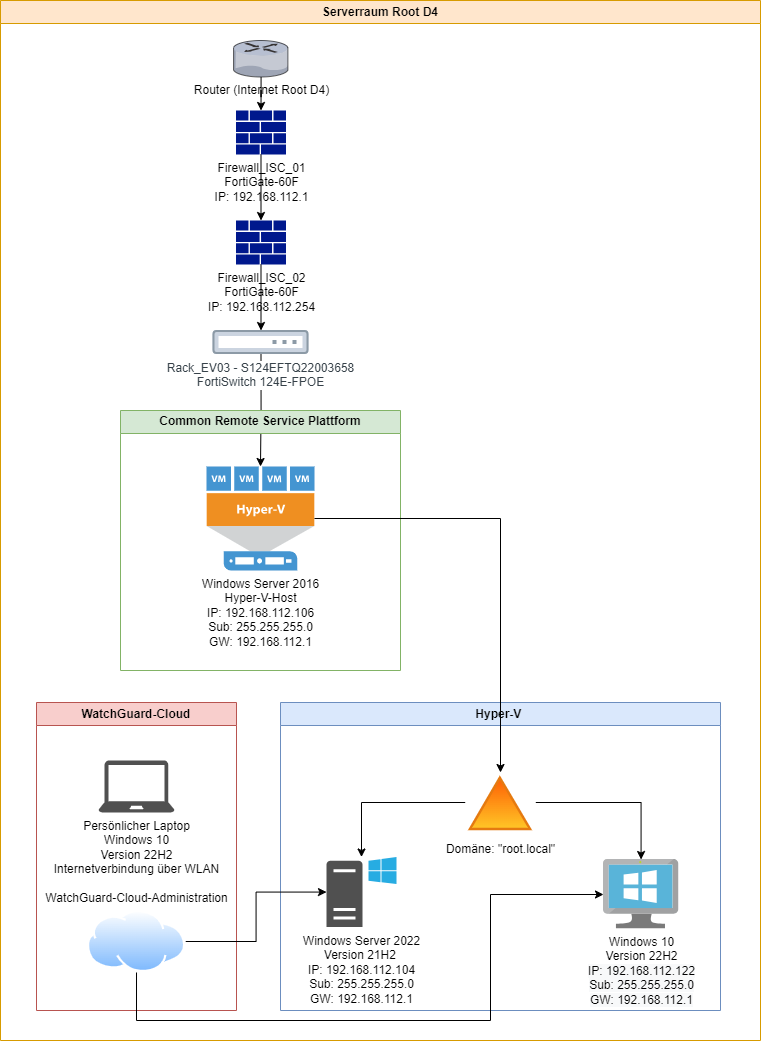


Abbildung Testumgebung

Der Plan der Testumgebung enthält die verschiedenen **Geräte** der Testumgebung, **Firmwareversion** der relevanten Geräte**,** **Adressierung**. Einige Punkte sind nicht im Plan ersichtlich. Diese werden aus dem Grund hier aufgeführt:

**Hardware-Version aller Windows-Geräte:** Version 9.0  
**Schnittstellen**: Privates Netzwerk  
**Örtlichkeiten:** Physischer Windows 10 Computer  
*Standort Host:* D4 Business Village Luzern  
 Platz 3  
 6039 Root, Schweiz  
**Zugang:** Remoteverbindung über SSL-VPN und cRSP  
**Ansprechpartner:** Andrin Egger  
**Leitungsbezeichner:** Andrin Egger

Das Internet in Root, sowie die entsprechenden Firewalls wurden nur spärlich beschrieben, da ich die exakten Konfigurationen dazu nicht preisgeben darf. Der Plan der Testumgebung ist dazu da, damit man den Test nachvollziehen kann.

## Projektmanagement

In diesem Kapitel wird die angewendete Projektmanagementmethode definiert. Diese wurde anhand der Kriterien und meiner bisherigen Erfahrung gewählt. Die Kriterien bilden die Titel und die Grundlage für das Vorgehen in den Kapiteln des zweiten Teils sowie die Meilensteine für das .

IPERKA

Abbildung IPERKA

In der Abbildung ist der Aufbau der IPERKA Projektmethode ersichtlich. Der Name setzt sich aus den verschiedenen Buchstaben zusammen, welche jeweils für die einzelnen Phasen der Methode stehen. IPERKA eignet sich vor allem für Projekte, mit klaren Strukturen in der zuerst das Projekt komplett geplant und dann umgesetzt wird.

Ich habe die Projektmethode gewählt, da sie gut geeignet für die meisten Projekte ist, die wenig unvorhergesehene äussere Einflüsse und in einer kurzen Zeitspanne durchgeführt werden müssen. Ebenfalls habe ich auf Basis von IPERKA alle meine bisherigen Schul-, sowie Geschäfts Projekte durchgeführt.

## Zeitplanung

In diesem Kapitel wird der Zeitplan der IPA beschrieben. Auf der nächsten Seite wird die Zeitplanung als Gantt-Diagramm dargestellt.

### Meilensteine

Ich habe mehrere Meilensteine auf Basis von IPERKA und des Kriterienkatalogs in das Gantt-Diagramm eingeführt. Diese dienen dazu, dem Zeitplan mehr Struktur zu verleihen und dem Prozess des Projektes besser folgen zu können.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nr. | Bezeichnung | Beschreibung | Datum | Zeit |
| 1 | IPA Bericht Teil 1 fertig | Der Teil 1 des IPA-Berichts wurde dokumentiert mitsamt Aufgabenstellung, Projektaufbauorganisation und Zeitplanung. Die Vorlagen der Arbeitsjournale wurden erstellt und werden im Laufe des Projekts ausgefüllt. | 25.03.2024 | 13:00 Uhr |
| 2 | Phase Informieren / Planen abgeschlossen | Die Informieren- und Planen-Phase wurde abgeschlossen. Dazu gehören die Kurzfassung, geleistete Wissensbeschaffung sowie ein Beschrieb der Testumgebung. | 27.03.2024 | 10:00 Uhr |
| 3 | Phase Entscheiden abgeschlossen | Das Protokoll des Approval-Meetings wird ausgefüllt, der Aufbau der Grundschutzstufen, resultierende Änderungen | 02.04.2024 | 09:00 Uhr |
| 4 | Phase Realisieren abgeschlossen | Alle Grundschutzstufen und dazugehörende Konfigurationen wurden abgeschlossen und dokumentiert. Für Techniker und zukünftige WatchGuard-Administratoren wurde je eine Anleitung erstellt. | 09.04.2024 | 15:00 Uhr |
| 5 | Phase Kontrollieren abgeschlossen | Die Grundfunktionalitäten des EPDR und die definierten Testfälle wurden getestet und dokumentiert. | 10.04.2024 | 14:00 Uhr |
| 6 | Phase Auswerten abgeschlossen | Die letzten Vollständigkeitstests wurden durchgeführt, sowie Erweiterungsmöglichkeiten und das Schlusswort notiert. | 12.04.2024 | 15:00 Uhr |
| 7 | Abgabe der IPA-Dokumentation | Die IPA-Dokumentation wurde abgeschlossen, kontrolliert und wird nun vor 18:00 Uhr abgegeben. | 12.04.2024 | 16:00 Uhr |

Tabelle Meilensteine

### Zeitplan

Abbildung Zeitplan

## Arbeitsjournal

### Tag 1 - 25.03.2024

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nr. | Tätigkeit | | Soll-Zeit | Ist-Zeit |
| 1 | IPA-Bericht Teil 1 abgeschlossen. | | **05:00h** | **05:00h** |
| Erfolge:  Ich konnte heute den Teil 1 der Dokumentation abschliessen. Die Zeitplanung wurde erstellt. Aber auch die restlichen Pendenzen des Teil 1 wurden wie geplant durchgeführt und stellte sich als sehr realistisch geplant heraus.  Probleme:  Ich hatte ein wenig länger als geplant beim Beschreiben der Testumgebung, da ich auch noch mit Draw.io den Plan aufgezeichnet und beschrieben habe.  Lösung & Lösungsvarianten:  Ich hatte zwei Möglichkeiten, da ich nun Zeit verloren hatte, musste ich beim Rest entweder etwas schneller arbeiten oder einen Schritt überspringen der länger dauert als andere. Beides wurde schliesslich kombiniert, da ich am Anfang schon weniger lange für das Ausfüllen des Teil 1 benötigte war ich immer noch im Zeitplan und konnte dank des schnelleren Tempos bereits mit der Planung beginnen. | | | | |
| 2 | Phase Informieren abgeschlossen. | | **03:00h** | **02:00h** |
| Erfolge:  Ich konnte alle Einträge in der Informieren-Phase ausfüllen und dies sogar um eine Stunde schneller als geplant.  Probleme:  Ich hatte eine kurze Schreibblockade, da ich nicht wusste, wie ich das Thema richtig beschreiben sollte.  Lösung & Lösungsvarianten:  Ich hätte eine ausführliche Liste mit meinem in der Informieren-Liste erworbenen Wissen eintragen können, doch ich entschied mich für einen Fliesstext, der das Wesentliche zusammenfasst und werde dann später in der Entscheidungs- und Realisieren-Phase genauer auf die Erkenntnisse eingehen, oder die Liste noch nachtragen. | | | | |
| 3 | | Mit Planung des Grundschutzstufen-Konzepts begonnen. | **00:00h** | **01:00h** |
| Erfolge:  Ich bin stolz, dass ich bereits am ersten Tag ein wenig mit der Planung beginnen konnte. Ich habe das Grundgerüst in der Dokumentation erstellt und kann am nächsten Tag mit der Planung des Grundschutzkonzepts abschliessen.  Probleme:  Es entstanden keine Probleme, da ich innerhalb einer Stunde nur die Formatierung, Tabellen erstellen und das Vorgehen bei der Planung dokumentieren konnte.  Lösung & Lösungsvarianten:  Da keine Probleme aufgetreten sind, benötigte ich auch keine Lösung. | | | | |
| Total: | | | **08:00h** | **08:00h** |

Tabelle Tätigkeiten Tag1

Reflexion:

|  |
| --- |
| Ich habe motiviert in den Tag gestartet und diese Motivation konnte ich mehr oder weniger den ganzen Tag beibehalten. Abgesehen von kurzen Momenten, an denen ich nicht wusste, was ich schreiben wollte, konnte ich meine gesetzten Ziele erreichen. Ich bin der Meinung, dass ich den Informieren-Teil noch ausführlicher hätte dokumentieren können und werde möglicherweise die Pufferzeit dazu verwenden. Auf das Zeitmanagement muss ich Acht geben, doch momentan bin ich sehr gut im Zeitplan unterwegs. |

Hilfe:

|  |
| --- |
| Ich habe das mich in WatchGuard über die Cloud () eingeloggt und das Manual () geöffnet, um die IPERKA-Phasen besser beschreiben zu können, doch abgesehen davon benötigte ich keine Hilfe und war eher den ganzen Tag mit der Dokumentation beschäftigt. |

(Quellenverzeichnis zwischen den Klammern referenzieren)

### Tag 2 - 26.03.2024

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nr. | Tätigkeit | | Soll-Zeit | Ist-Zeit |
| 1 | Planung des Grundschutzstufen-Konzepts abgeschlossen. | | **04:00** | **05:00** |
| Erfolge:  Ich konnte die gesamte Planung für das Grundschutzstufenkonzept abschliessen und bin sehr zufrieden mit dem geschriebenen. Es beschreibt die gesamt, geplante Umgebung ausführlich, was nützlich beim Planen des Approval-Meetings sein wird.  Probleme:  Da ich eine gute Beschreibung diesmal priorisierte, war ich um eine Stunde langsamer als geplant, obwohl ich bereits gestern mit der Beschreibung begonnen habe.  Lösung & Lösungsvarianten:  Ich hatte die Möglichkeit die Planung des Approval-Meetings vorzuziehen, doch ich habe mich dagegen entschieden, da die Planung sonst weniger ausführlich geworden wäre. Da ich für eine erfolgreiche Realisierung eine gute Planung benötige, legte ich grossen Wert auf eine genaue Planung. Ich arbeitete dafür ein wenig schneller während der Planung für das Approval-Meeting. | | | | |
| 2 | Approval-Meeting Planung abgeschlossen. | | **02:00** | **02:00** |
| Erfolge:  Ich konnte die Planung für das Approval Meeting abschliessen und habe zusätzlich eine PowerPoint-Präsentation für das Meeting am nächsten Tag erstellt, um meinen Zuhörern das Konzept besser vorstellen zu können.  Probleme:  Eine PowerPoint-Präsentation zum Konzept zu erstellen war zeitaufwändiger als gedacht.  Lösung & Lösungsvarianten:  Ich habe die PowerPoint Präsentation dann eher basierend auf die Punkte erstellt, die ich bereits in der Planung aufgeschrieben habe. Die Präsentation hat jetzt mehr Text, doch das wird den Fluss der Präsentation nicht stören. Was noch funktioniert hätte, wäre die Präsentation mit Zeigen der Dokumentation zu führen, doch ich wollte die Idee visuell ansprechender präsentieren. | | | | |
| 3 | | Mit Planung des Testkonzepts begonnen. | **02:00** | **01:00** |
| Erfolge:  Ich konnte mit der Planung des Testkonzepts beginnen und das Grundgerüst aufstellen und bereits die Anzahl und Richtung der Tests definieren.  Probleme:  Da ich länger für die Planung des Grundschutzkonzepts hatte, konnte ich mit dem Testkonzept nicht zur geplanten Zeit beginnen.  Lösung & Lösungsvarianten:  Stattdessen nehme ich mir nun am nächsten Tag mehr Zeit für das Testkonzept. Eine andere Lösung wäre es, die Entscheidungsphase zu kürzen, doch es ist mir wichtig die zwei Stunden Zeit zu nehmen, um das Ganze genau zu beschreiben. | | | | |
| Total: | | | **08:00h** | **08:00h** |

Tabelle Tätigkeiten Tag2

Reflexion:

|  |
| --- |
| Der heutige Tag kam mir anfangs recht fordernd vor, ich habe lange für das Planen des Konzepts benötigt und kam mit dem Rest in Verzug. Daraufhin kam ich ein wenig in Zeitstress, da ich der Planung nicht mehr genau folgen konnte und so schneller arbeiten musste. Ich konnte aber auch viel dazulernen und versuche mein Zeitmanagement durch die nun sehr ausführlich beschriebene Planung morgen besser in den Griff zu kriegen. |

Expertenbesuch:

|  |
| --- |
| Heute kam auch Herr Kubli zu Besuch und es wurde das weitere Vorgehen besprochen. Er gab mir auch viele Tipps und Tricks wie ich die Versionierung, das Testkonzept, Lernjournal, die Kopf- und Fusszeile, sowie Backup besser beschreibt und dokumentiert. Seine Vorschläge werden in den kommenden Phasen eingebaut, um die Arbeit professioneller zu gestalten. |

Hilfe:

|  |
| --- |
| Hilfestellungen beanspruchte ich heute von Nico Dahinden, einem unserer Mitarbeiter im Navigator. Somit konnte ich die URLS der Navigator-Apps besser erklären und benötigte nicht ständig auf der Siemens-Plattform zu suchen, um Informationen zu URLs und Geräten zu finden. ()  Ich habe ein Mail an Herrn Timo Kirchem verfasst, ob man von den Konfigurationen in der WatchGuard-Cloud ein Backup machen kann. Ich erwarte bald eine Antwort.  Ebenfalls hat mir Herr Kubli wie im Reiter «Expertenbesuch» erwähnt, wichtige Fragen zu den genannten Themen oben beantwortet und mir das weitere Vorgehen erklärt. |

### Tag 3 - 27.03.2024

|  |  |  |  |
| --- | --- | --- | --- |
| Nr. | Tätigkeit | Soll-Zeit | Ist-Zeit |
| 1 | Planung des Testkonzepts abgeschlossen. Planen-Phase abgeschlossen. | **03:00** | **04:00** |
| Erfolge:  Ich konnte das ganze Testkonzept dokumentieren und habe es zusätzlich mit Bildern aus dem Plan der Testumgebung ausgestattet. Somit kann eine aussenstehende Person die geplanten Tests besser nachvollziehen. Das Konzept ist mir sehr ausführlich gelungen und somit konnte die Planungs-Phase beendet werden.  Probleme:  Ich habe lange am Testkonzept geschrieben, da ich die Bilder erst noch selbst erstellen musste und kam somit in Verzug mit dem Beginn der Entscheidungsphase.  Lösung & Lösungsvarianten:  Ich habe mir vorgenommen, das Protokoll für das Approval-Meeting so ausführlich wie möglich zu machen, um so wenig Zeit wie möglich zu verlieren. Dies führte glücklicherweise dazu, dass ich sogar schneller als geplant mit dem nächsten Schritt fertig wurde. | | | |
| 2 | Approval-Meeting und Protokollierung abgeschlossen, sowie resultierende Änderungen an der Testumgebung und der Grundschutzstufen notiert. | **04:00** | **02:00** |
| Erfolge:  Ich kam sehr schnell vorwärts mit der Dokumentation des Approval-Meetings, da ich ein ausführliches Protokoll bereits während dem Meeting geführt hatte, und nur noch einfügen musste. Ich fand auch, dass ich meine Idee gut vorstellen konnte und viel wertvolles Feedback bekommen habe.  Probleme:  Es traten während der Präsentation und der Protokollierung keine Probleme auf. Die Änderungen waren gut nachvollziehbar und konnten somit auch gut dokumentiert werden.  Lösung & Lösungsvarianten:  Da keine Probleme aufgetreten sind, benötigte ich auch keine Lösung. | | | |
| 3 | Festlegung Externer Hilfestellung dokumentiert. Abschluss der Entscheiden-Phase | **01:00** | **02:00** |
| Erfolge:  Durch die schnelle Abarbeitung des Approval-Meetings und Dokumentation der Änderungen an der Testumgebung konnte ich nun länger als geplant an der Hilfestellung arbeiten und sie schneller abschliessen.  Probleme:  Ich musste alte Mailverläufe durchsuchen und hatte lange bis ich die Fehler und Lösungen richtig zusammenfassen konnte, wodurch ich ein wenig in Zeitstress geriet.  Lösung & Lösungsvarianten:  Ich konnte mich nur auf die Suchfunktion in Outlook beschränken. Mit Ihrer Hilfe konnte ich viele der alten Mailverläufe wieder finden und sparte wertvolle Zeit. Ich habe mir noch Zeit auf Dienstag eingeplant, wollte dort aber gerne und so früh wie möglich mit der Realisierung beginnen. | | | |
| Total: | | **08:00h** | **08:00h** |

Tabelle Tätigkeiten Tag3

Reflexion:

|  |
| --- |
| An der Dokumentation wurde heute viel geschrieben, ich konnte die Pendenzen vom gestrigen Tag aufarbeiten und somit zwei IPERKA-Phasen abschliessen, sowie nächstes Mal mit der Realisieren-Phase beginnen. Ein Vorgeschmack auf die IPA-Präsentation erhielt ich heute während des Approval-Meetings. Obwohl es gut lief, bin ich der Meinung, dass ich es besser hätte vorbereiten können. Jedoch habe ich eine Menge Feedback und Änderungen vorgeschlagen bekommen. Mit ihrer Hilfe kann die Dokumentation und das Endprodukt nur noch besser werden. |

Hilfe:

|  |
| --- |
| Hilfestellung erhielt ich heute von Timon Hochstrasser und Maurizio Taglialatela. Sie haben mir während des Approval-Meetings ein ausführliches Feedback gegeben, dessen Ergebnisse ich dokumentiert und damit begonnen habe, sie in die Dokumentation und später dann auch in die Realisierung einzubauen. |

### Tag 4 - 02.04.2024

|  |  |  |  |
| --- | --- | --- | --- |
| Nr. | Tätigkeit | Soll-Zeit | Ist-Zeit |
| 1 |  |  |  |
| Erfolge:  Probleme:  Lösung & Lösungsvarianten: | | | |
| 2 |  |  |  |
| Erfolge:  Probleme:  Lösung & Lösungsvarianten: | | | |
| Total: | | **08:00h** | **08:00h** |

Tabelle Tätigkeiten Tag4

Reflexion:

|  |
| --- |
|  |

Hilfe:

|  |
| --- |
|  |

### Tag 5 - 03.04.2024

|  |  |  |  |
| --- | --- | --- | --- |
| Nr. | Tätigkeit | Soll-Zeit | Ist-Zeit |
| 1 |  |  |  |
| Erfolge:  Probleme:  Lösung & Lösungsvarianten: | | | |
| 2 |  |  |  |
| Erfolge:  Probleme:  Lösung & Lösungsvarianten: | | | |
| Total: | | **08:00h** | **08:00h** |

Tabelle Tätigkeiten Tag5

Reflexion:

|  |
| --- |
|  |

Hilfe:

|  |
| --- |
|  |

### Tag 6 - 05.04.2024

|  |  |  |  |
| --- | --- | --- | --- |
| Nr. | Tätigkeit | Soll-Zeit | Ist-Zeit |
| 1 |  |  |  |
| Erfolge:  Probleme:  Lösung & Lösungsvarianten: | | | |
| 2 |  |  |  |
| Erfolge:  Probleme:  Lösung & Lösungsvarianten: | | | |
| Total: | | **08:00h** | **08:00h** |

Tabelle Tätigkeiten Tag6

Reflexion:

|  |
| --- |
|  |

Hilfe:

|  |
| --- |
|  |

### Tag 7 - 08.04.2024

|  |  |  |  |
| --- | --- | --- | --- |
| Nr. | Tätigkeit | Soll-Zeit | Ist-Zeit |
| 1 |  |  |  |
| Erfolge:  Probleme:  Lösung & Lösungsvarianten: | | | |
| 2 |  |  |  |
| Erfolge:  Probleme:  Lösung & Lösungsvarianten: | | | |
| Total: | | **08:00h** | **08:00h** |

Tabelle Tätigkeiten Tag7

Reflexion:

|  |
| --- |
|  |

Hilfe:

|  |
| --- |
|  |

### Tag 8 - 09.04.2024

|  |  |  |  |
| --- | --- | --- | --- |
| Nr. | Tätigkeit | Soll-Zeit | Ist-Zeit |
| 1 |  |  |  |
| Erfolge:  Probleme:  Lösung & Lösungsvarianten: | | | |
| 2 |  |  |  |
| Erfolge:  Probleme:  Lösung & Lösungsvarianten: | | | |
| Total: | | **08:00h** | **08:00h** |

Tabelle Tätigkeiten Tag8

Reflexion:

|  |
| --- |
|  |

Hilfe:

|  |
| --- |
|  |

### Tag 9 - 10.04.2024

|  |  |  |  |
| --- | --- | --- | --- |
| Nr. | Tätigkeit | Soll-Zeit | Ist-Zeit |
| 1 |  |  |  |
| Erfolge:  Probleme:  Lösung & Lösungsvarianten: | | | |
| 2 |  |  |  |
| Erfolge:  Probleme:  Lösung & Lösungsvarianten: | | | |
| Total: | | **08:00h** | **08:00h** |

Tabelle Tätigkeiten Tag9

Reflexion:

|  |
| --- |
|  |

Hilfe:

|  |
| --- |
|  |

### Tag 10 - 12.04.2024

|  |  |  |  |
| --- | --- | --- | --- |
| Nr. | Tätigkeit | Soll-Zeit | Ist-Zeit |
| 1 |  |  |  |
| Erfolge:  Probleme:  Lösung & Lösungsvarianten: | | | |
| 2 |  |  |  |
| Erfolge:  Probleme:  Lösung & Lösungsvarianten: | | | |
| Total: | | **08:00h** | **08:00h** |

Tabelle Tätigkeiten Tag10

Reflexion:

|  |
| --- |
|  |

Hilfe:

|  |
| --- |
|  |

# Teil 2: Projekt

## Kurzfassung

Kurze Ausgangssituation:

Bisher wurde WatchGuard im Betrieb bei einigen Kunden bereits verwendet. Wir benutzen ein Konto für unsere Branch Central in der Zentralschweiz und erstellten Konten für unsere diversen Systeme, welche wir mit der WatchGuard EPDR Lizenz und dessen Agent ausstatteten und auf den entsprechenden Computern unserer Kunden installierten. Dahinter wurden die Standardeinstellungen für die Gruppe, in welcher sich alle Computer befinden, kopiert und innerhalb der Webzugriffskontrolle so abgeändert, dass es die meisten Siemens-Webseiten bestimmter Kontroller und Konfigurationsfenster erlaubt. Die Firewall blieb deaktiviert, um den Fernzugriff auf den Systemen bei der Installation des Webzugriffs nicht zu verlieren. Es gab jedoch immer wieder Probleme mit blockierten URLs für unsere Siemens-Geräte, die nur mühsam gelöst werden konnten, da die Ursache des Problems mangels Wissen über die diversen Cloudfunktionen, nicht bekannt war. Der Kunde konnte nicht aus verschiedenen Angeboten wählen und konnte die Einstellungen nicht einsehen und erhielt auch keine Informationen oder Sicht auf den Sicherheitsstatus des Computers. Dies sollte sich mit dem Einsatz einer besser durchdachten Webzugriffskonfiguration, der Firewall und Operator-Zuweisung, sowie neuer Grundschutzstufen und automatischen E-Mailwarnungen sowie Berichte an den Kunden und Techniker ändern.

Umsetzung:

Ergebnis:

## Informieren

### Wissensbeschaffung

Da mir das Produkt des WatchGuard EPDR noch ziemlich neu war, musste ich mich zuerst mit den Funktionen, Einstellungen und Möglichkeiten der Cloud-Plattform vertraut machen, da sie alle Einstellungen anzeigt, verwaltet und steuert. Dies umfasst das Studium der Dokumentation des Herstellers. Es gibt innerhalb der Cloud-Management-Plattform einen Button mit Fragezeichen. Dessen Link verweist auf eine Website, die das Vorgehen mit der WatchGuard EPDR-Software gut erklärt.

Wie man Kontos, Grundschutzstufen erstellt, Firewalleinstellungen tätigt, Syncs ausführt und viel weiteres fand ich alles in der Dokumentation des WatchGuard Help Centers. Ich stellte ebenfalls Fragen an unseren WatchGuard-Kontakt Timo Kirchem (Sales Engineer) aus Deutschland, der mich via Mail mit der Beantwortung meiner Fragen unterstützte.

Ich interpretierte den Auftrag so, dass das Erstellen einer neuen Lösung für unser Endpoint-Protection Angebot oberste Priorität hatte. Durch Lesen der Dokumentation wird vieles klarer, doch es musste auch praktisch ausprobiert werden und ich machte mich im Geschäft und Internet schlau, welche Ports, Kategorien und URLs am besten freigegeben werden sollten, um unsere Siemens-Anlagen erreichbar zu halten, Remotedesktopverbindung zu ermöglichen und eine Lösung für das Problem mit den blockierten URLs finden.

### Vorbereitete Testumgebung

Um meine Erfahrungen zu bestätigen, verwendete ich meine Testumgebung. Es ist nicht selbstverständlich, dass meine getätigten Einstellungen sofort und richtig funktionieren. Ich informierte mich über die Synchronisationszeit der Cloud zum Computer, wie lange ein Active-Directory Sync braucht und in welchen Intervallen der Kunde/Techniker seine Nachrichten erhält.

Aber auch die diversen Tools, welche ich zu Testzwecken verwende, mussten zuerst gefunden und deren Nutzung theoretisch wie praktisch beherrscht werden. Auch dazu benötigte ich Unterstützung und bereits eine klare Vorstellung des Endprodukts, welche mit der Zeit immer ausgeprägter wurde.

Kurz zusammengefasst war meine grösste Informationsquelle das Internet, dicht gefolgt vom Austausch mit unserem Kontakt des Sales Engineer und dann gesammelte Erfahrung über die Dokumentation und unsere Techniker.

Die wichtigsten Quellen und Links werden im Quellenverzeichnis dargestellt und erklärt. Die kurz erwähnten, neuen Erkenntnisse werden in die Dokumentation der Realisierung eingebaut.

## Planen

### Vorgehensweise

Die Vorgehensweise richtet sich stark nach dem Zeitplan. Zuerst werden die einzelnen IPERKA-Phasen dokumentiert. Von Informieren bis Planen wird nur in der Doku gearbeitet und nichts physisch auf der Umgebung realisiert. Ausser die Testumgebung benötigt wichtige Änderungen. Sobald die Realisieren-Phase beginnt, werden die genannten Konfigurationen vorgenommen und die Realisierung, sowie alle wichtigen neuen Erkenntnisse eingesetzt und dokumentiert.

### Datensicherung:

Als Datensicherung werde ich ein öffentliches GitHub Projekt mit dem Namen: «IPA\_Nideroest\_2024» mit meinem privaten Konto «DNideroest» verwenden. Auf diesem GitHub werden alle wichtigen Dokumente und Dateien am Ende des Tages hochgeladen und versioniert.

Alle IPA-Files sind gleichzeitig auf meinem Arbeitslaptop lokal auf dem Ordner «D:\Projects\IPA\_Projekt\_Dylan» gespeichert. Dieser Ordner wird mithilfe des Programms GitKraken jeweils immer am Ende des Arbeitstages auf das GitLab Projekt «IPA\_Nideroest\_2024» geladen.

Das Programm funktioniert ähnlich wie das Git-Bash-Terminal, sobald ich eine Änderung an den Files vornehme, zum Beispiel ein neues Wort in die Dokumentation schreibe erscheint die Änderung im mittleren Graph zuoberst als «Work In Progress». Die geänderten Files werden rechts unter «Unstaged Files» aufgelistet. Ein Bild, das Software, Screenshot, Multimedia-Software, Grafiksoftware enthält.

Automatisch generierte Beschreibung

Abbildung GitKraken geänderte Files «stagen»

Ich kann dann eine Beschreibung im Reiter «Commit Message» eintragen und schliesslich die Änderungen übernehmen. Wenn ich nun noch den Button «Push» drücke, werden die Änderungen auch auf das GitLab-Projekt kopiert.

Ein Bild, das Text, Screenshot, Software, Multimedia-Software enthält.

Automatisch generierte BeschreibungEin Bild, das Text, Schrift, Screenshot, Zahl enthält.

Automatisch generierte Beschreibung

Abbildung Mit GitKraken eine Versionierung auf GitLab erstellen

### Konfigurationsplan

Um einen besseren Überblick über meine Testumgebung zu erhalten, beinhaltet dieses Kapitel einen Konfigurationsplan. Alle Konfigurationen und Pendenzen werden hier aufgelistet. Diese werden dann auf die verschiedenen Grundschutzstufen angewendet. Es ist wichtig, dass wir alle Siemenseigenen Geräte trotz eingeschalteter Webzugriffskontrolle und Firewall immer noch erreichen können

#### Webzugriffskontrolle

|  |  |
| --- | --- |
| **Offene Kategorien** | **Begründung** |
| Bürozusammenarbeit | Das Öffnen dieser Kategorie ermöglicht es den Kunden über Office-Anwendungen wie Word und PowerPoint ihre Daten zu teilen und gemeinsam an den Dokumenten zu arbeiten. Wenige Kunden benötigen diese Funktion. Sie wird nur freigegeben, wenn der Kunde dies wünscht. |
| Informationstechnologie | Unsere Techniker stellten fest, dass ohne die Freigabe dieser Kategorie das OpenVPN-GUI nicht funktioniert und der Windows Smartscreen die Installation des Leitsystems blockiert. Aus diesem Grund wurde die gesamte Kategorie freigegeben. |
| Private IP-Adressen | Die Privaten IP-Adressen müssen immer erreichbar sein, da wir im Geschäft, wie auch beim Kunden nutzen, damit Geräte innerhalb eines Netzwerkes miteinander kommunizieren können. |
| **Zugelassene URLs** | **Begründung** |
| update.microsoft.com | Diese URLs werden dazu eingesetzt, um Updates für den Windows-Computer zuzulassen. Die URLs wurden von der bereits bestehenden «Default-Siemens»-Webzugriffskontrolle-Einstellung übernommen. Diese URLs sind offizielle Microsoft-Adressen, die wir für die Systemupdates der Windows-PCs benötigen. |
| http://www.update.microsoft.com |
| http://download.windowsupdate.com |
| http://ds.download.windowsupdate.com |
| http://au.download.windowsupdate.com |
| http://download.microsoft.com |
| http://c.microsoft.com |
| http://stats.update.microsoft.com |
| http://watson.microsoft.com |
| https://12.46.135.194 | Dies ist die Adresse des cRSP SSL-VPN Servers aus Fürth, Deutschland von Siemens, die Freigabe dieser IP ermöglicht es uns über cRSP eine Remotedesktopverbindung aufzustellen. |
| https://194.138.37.194 | Dies ist die Adresse des cRSP SSL-VPN -Servers aus Irving, USA von Siemens, die Freigabe dieser IP ermöglicht es uns über cRSP eine Remotedesktopverbindung aufzustellen |
| https://crsp-sslvpn-nwke-p.siemens.com | Der DNS-Name der IP-Adresse des Irving Servers von Siemens aus den USA. (IP: 194.138.37.194) |
| https://crsp-sslvpn-fth-p.siemens.com | Der DNS-Name der IP-Adresse des Fürth Servers von Siemens aus Deutschland. (IP: 12.46.135.194) |
| https://eadvantage-import.siemens.com/ieg/2\_0/import.html | Dies sind benötigte URLs für das Software-Proxy von Siemens-Navigator. Softwareproxy ist eine Exportsoftware für Daten von Siemens, die auf dem Gebäude Leitsystemserver  installiert wird. Der SW-Proxy scannt das vom Leitsystem erzeugte CSV-File und versendet die Daten via Internet  zum Navigator Datenserver. Die Anwendung wird vor allem von Siemens-Navigator Technikern verwendet. |
| https://eadvantage.siemens.com/uaa/login |
| https://eadvantage.siemens.com/ieg/2\_0/import.html |
| https://import.nav2cloud.bt.siemens.cloud |
| https://import.nav2cloud.bt.siemens.cloud/ieg/2\_0/import.html |
| https://ozw.ccp.siemens.com | Dies ist die URL für einen Web-Server, den unsere Synco-Geräte verwenden. Um diese zu erreichen, muss die URL freigeschaltet sein. |
| https://lms.bt.siemens.com | Diese URL ist nötig, um den Flexclient unserer Gebäudeleitsysteme zu erreichen. Der Flexclient ist eine Anwendung für Kunden, um das Desigo CC-Gebäudeleitsystem direkt von ihrem Browser zu erreichen. |
| http://edge-http.microsoft.com | Diese URL erfüllt einen ähnlichen Zweck wie die gstatic-domain und tauchte auf, bevor wir uns auf ein Siemens-Gerät verbinden wollten. Deshalb wird diese freigegeben. |
| http://gstatic.com | gstatic.com ist eine Google-eigene Domain, auf der statische Inhalte gehostet werden. Doch in unserem Falle ist es eine Domain, die auftaucht, bevor wir über Chrome auf unsere Geräte verbinden wollen. Deshalb wird sie freigegeben. |

Tabelle Planung Webzugriffskontrolle

#### Firewall

|  |  |
| --- | --- |
| **Programmregeln** | **Begründung** |
| C:\Windows\System32\mstsc.exe (Zulassen) | Die einzige Programmregel die wir benötigen. «mstsc.exe» ist ein Befehl und erlaubt die Verbindung über Remote Desktop. Dies wird benötigt, um die Computer über Remotedesktop zu erreichen. |
| **Verbindungsregeln/Ports (Zulassen)** | **Begründung** |
| FTP 20 und 21 | FTP dient der Übertragung von Dateien zwischen einem Client und einem Server. Das Tunneling-Protokoll wird von vielen unserer Server und PXWEB Geräte, wie die RSG-Box verwendet. |
| SMTP 25 | Das Protokoll dient dem Austausch von E-Mails zwischen verschiedenen Computer/Gerätenetzen und da unsere Geräte oft eine Alarmabsetzung via Mail über diesen Port verwenden, ist es wichtig, dass der benötigte Port offen ist. |
| DNS 53 | Die Namensauflösung benötigen wir auf all unseren Servern beim Kunden und im Büro und DNS-Anfragen, werden normalerweise per UDP-Port 53 zum Namensserver gesendet. |
| DHCP 67 und 68 | Dieser Port wird benötigt, um die IP-Adressverteilung auf unseren Servern mit DHCP zu gewährleisten. DHCP-Server wartet auf dem UDP-Port 67oder 68 auf solche Nachrichten. Um dann IPs aus seiner eingetragenen Range zu verteilen. |
| HTTP 80 | Der Standard-Netzwerkanschluss, der zum Senden und Empfangen unverschlüsselter Webseitenbenötigt wird. Dies kommt vor allem beim Erreichen unserer PXWEB-Geräte zum Einsatz. |
| NTP 123 | Dieser NTP-Port ermöglicht die Synchronisierung der Uhren unserer PXWEB-Geräte, vor allem der X300-Box, die diesen standardmässig benötigt, dem Desigo CC und all unseren Servern. |
| HTTPS 443 | Als Gegenstück zum http-Port ist dieser Port für verschlüsselte Websites nötig. HTTPS benötigen vor allem unsere Firewalls und alle neueren PXWEB-Geräte. |
| SMTP 587 | Einige unserer Desigo Control Points verwenden den Port 587 zur E-Mailabsetzung. Er liefert also eine ähnliche Funktion wie Port 25 und wird auch freigeschaltet. |
| RDP 3389 | Dieser RDP-Port ermöglicht es uns, via cRSP, eine Fernverbindung zu den Computern unserer Kunden herzustellen. |
| BACF 47808-47840 | Wir haben einige Systeme, die das Transmissionsprotokoll BACF verwenden, um die Geräte im Netz von BACnet anzeigen zu können. Unsere Techniker benötigen dieses Netz und die Range aus freigegebenen Ports, um von Fern aus Störungen zu identifizieren. |

Tabelle Planung Firewall

#### Programmblockierungen und Warnungen

|  |  |
| --- | --- |
| **Blockierte Programme** | **Begründung** |
| Tcpview.exe | TCPView ist ein Windows-Programm, mit dem man detaillierte Auflistungen aller TCP- und UDP-Endpunkte auf dem System anzeigen kann, einschließlich der lokalen Adressen und Remoteadressen sowie des Status der TCP-Verbindungen. TCPView meldet auch den Namen des Prozesses, dem der Endpunkt gehört, somit könnte ein Angreifer dies ausnutzen, um eine Angriffslücke zu finden. Deshalb wird das Programm blockiert. |
| Wireshark.exe | Wireshark ist der bekannteste und am weitesten verbreitete Netzwerk-Sniffer. Mit Wireshark kann ein Angreifer Netzwerk-Pakete bis in das kleinste Bit analysieren, interessanten Traffic filtern und umfassende Auswertungen durchführen. Dies auch alles in fremden Netzwerken, während unsere Kunden dies fast nie benötigen. |
| Advanced\_ip\_scanner.exe | Das Programm ermöglicht es einem Nutzer oder Angreifer alle Geräte im Netzwerk zu sehen und sogar auf diese via Remote oder Browserfenster zu verbinden. Es ist für unsere Techniker sehr nützlich, aber auch ein hohes Sicherheitsrisiko, welches deaktiviert werden muss. |
| Powershell.exe | Mit Windows Powershell können sämtliche internen Funktionen und Einstellungen mit den nötigen Berechtigungen geändert werden. Ein beliebtes Tool für Viren. Das Ausführen des Programms wird deshalb von WatchGuard blockiert. |
| **Warnung** | **Begründung** |
| Malware-Erkennungen | Grundlegend sind alle Warnungsmöglichkeiten in der Cloud aktiviert. Diese 7 Warnungen senden eine Mail, wenn WatchGuard glaubt, einen Angriff der entsprechenden Klasse auf dem Computer erkannt zu haben. Dies wird an Kunden und Techniker versendet und es ist bei Angriffen allgemein von Vorteil so schnell wie möglich zu reagieren. |
| Exploit-Erkennungen |
| PUP-Erkennungen |
| Erkennung von Netzwerkangriffen |
| Eine Malware-URL wird blockiert |
| Phishing erkennen |
| Ein Einbruchsversuch wird blockiert |
| Ein Programm, das gerade klassifiziert wird, wird blockiert | WatchGuard wird eine Mail senden, wenn ein unbekanntes Programm auf dem Computer ausgeführt wird und sendet eine Mail an Kunden und Administrator, um die Installation entweder freizugeben oder zu verweigern. Dies ist wichtig, wenn der Kunde oder Siemens neue Testprogramme auf den Computern mit WatchGuard installieren will. |
| Durch Administrator blockierte Programme | Eine Mail wird immer dann gesendet, wenn einer der 4 blockierten Programme (Wireshark, PowerShell, AIS, Tcpview) versucht wird zu öffnen. Dies könnte ein Anzeichen für einen Angriff sein, da der Kunde im Voraus über diesen Umstand informiert wird. Deshalb ist es wichtig, dass eine Meldung gemacht wird. |
| Eine durch den Administrator zugelassene Datei ist endgültig klassifiziert | Dies ist eine Meldung, die dem Kunden zugespielt wird, sobald der Administrator die Installation seines Programms bewilligt hat. Die Meldung ist wichtig für ihn, damit mit der Arbeit fortgefahren werden kann. |
| Blockierte Geräte | Es wird immer eine Meldung ausgesendet, wenn die Verbindung auf ein Gerät im Netzwerk nicht möglich ist. Jene, die blockiert wurden sollten nicht erreichbar sein, deshalb könnte es sich um einen Angriff handeln. |
| Computer mit Schutzfehlern | Der Computer benötigt eine Aktion, damit WatchGuard seinen Schutz auf den neusten Stand aktualisieren kann. Es meldet die Art der Aktion dem Kunden und dem Techniker. (es handelt sich hierbei meist um einen Neustart des PCs) Somit ist der Kunde informiert und kann die Installation planen. |
| Computer ohne Lizenz | Eine Meldung die für zukünftige Administratoren wichtig ist. Wenn vergessen wird, eine EPDR-Lizenz am Computer zuzuweisen, kommt eine einmalig versendete E-Mail, um den Administrator darauf hinzuweisen. |
| Installationsfehler | Wenn die Installation fehlschlägt, wird man per E-Mail alarmiert. Eine wichtige Funktion, um zu sehen, ob der Kunde noch einige WatchGuard-Ports freischalten muss. |
| Nicht verwaltete Computer erkennen | WatchGuard scannt das Netz des Kunden, um alle PCs zu identifizieren, die kein WatchGuard installiert haben. Somit kann das Angebot dem Kunden auch für seine nun bekannten, restlichen Systeme verkauft werden. |
| Angriffsindikatoren (IOAs) | Dies sind von WatchGuard gewählte, bestätigte Indikatoren, die höchstwahrscheinlich einen Angriff darstellen. Normalerweise sind dies Angriffe in einem frühen Stadium oder im Exploit-Stadium, die keine Malware nutzen. Diese werden standardmässig in einem separaten Reiter alle aktiv gelassen.  Die Funktion, dass eine Mail zur Warnung dem Kunden und Techniker bei Erkennung einer der Angriffsindikatoren gesendet wird, ist aktiviert, um früh Massnahmen gegen mögliche Angreifer vorzunehmen. |

Tabelle Planung Programmblockierung und Warnungen

Die nächsten vier Funktionen werden unabhängig von den Grundschutzstufen eingesetzt:

#### Active Directory-Sync

Kunden, welche ein Active-Directory besitzen, werden die Möglichkeit haben, eine Synchronisation mit WatchGuard von uns durchführen zu lassen. Diese dauert vier Stunden, dabei werden alle bestehenden Useraccounts der Domäne werden erkannt und können in den WatchGuard Produkten «Firebox», «Firecluster» und «Access Point» verwendet werden.

#### Managementbericht

Der Managementbericht stellt den monatlichen Bericht dar, den Kunde und Techniker erhalten. Dieser Bericht zeigt den Status der Lizenz, Netzwerksicherheit, ob bestimmte Malware-Erkennungen bestehen, bestehende Risiken, erkannte Angriffsindikatoren und getätigte, sowie verweigerte Zugriffe in der Webzugriffskontrolle.

Folgende Voraussetzungen werden eingebaut:

1. Er sollte immer am letzten Tag des Monats gesendet werden.
2. Die Sendezeit wird mit Kunde und Techniker abgesprochen oder sonst auf 09:00 Uhr gestellt.
3. Der Bericht enthält die Daten des Monats.
4. Die Daten werden von allen Computern im Profil bezogen.
5. Der Bericht wird allen involvierten Technikern und Kunden gesendet.
6. Das Namenskonzept der E-Mail ist:   
   **«WatchGuard Managementbericht» + «Anlagenname ohne Region, Objekt und Equipmentnummer»**   
   Also z.B. «WatchGuard Managementbericht Raiffeisenbank Cham
7. Das Dateiformat ist PDF
8. Die Sprache wird der des Kunden angepasst.  
   Zentralschweiz = Deutsch  
   Westschweiz = Französisch  
   Tessin = Italienisch

#### Operatoren

Es gibt vier Arten von Operatoren in WatchGuard. Dies sind User, welche in einer Weise Zugriff auf die Cloud und deren Systeme haben. Wir verwenden drei der Nutzer:

Helpdesk - Hat Administratorberechtigungen in der Cloud, kann jedoch keine neuen Systeme erstellen oder neue Lizenzen zuweisen, jedoch können die bestehenden in jeder Weise geändert werden. Dieser Operator wird vorzugsweise den Technikern zugeteilt.

Owner - Hat vollständige Administratorberechtigung für alle Profile und Konten in der Cloud, kann jedoch keiner Kontogruppe zugewiesen werden. Dieser Operator ist mir und allen WatchGuard-Administratoren von oberster Ebene zugewiesen worden.

Auditor - Hat Read-Only Berechtigungen, kann also keine Systeme erstellen und bearbeiten. Dieser Operator wird nur auf Wunsch dem Kunden zugewiesen.

Sales – Der vierte Nutzer, welcher nicht verwendet wird. Sie haben automatisch Zugriff auf alle Kontogruppen wie die Owner, können Lizenzen und Kundensysteme anlegen, jedoch ist eine technische Administration wie beim Helpdesk nicht möglich.

#### Kontogruppen

Die Kontogruppen sind Ordner mit einer Sammlung von Kundenanlagen mit einer bestimmten Anzahl von Anlagenprofilen drin. Ihnen werden jeweils die zuständigen Techniker mit Operator «Helpdesk» und auch Kunden mit Operator «Auditor» zugewiesen. Das Namenskonzept ist «Anlagen» \_ «Name des Technikers» Also zum Beispiel: «Anlagen\_Dylan\_Nideröst».

#### Grundschutzstufen-Konzept

|  |  |  |
| --- | --- | --- |
| **Konfiguration** | **Effekt** | **Sicherheitsstufe** |
| **Webzugriffskontrolle: Standardeinstellungen der Kategorien.** | Alle Kategorien geblockt ausser «Informationstechnologie» und «Private IP-Adressen» | Leicht und Mittel |
| **Webzugriffskontrolle: Kategorie «Bürozusammenarbeit»** | Bürozusammenarbeit wird freigeschaltet, wenn der Kunde dies benötigt. | Leicht |
| **Webzugriffskontrolle: Siemens Default Whitelisting** | Das Siemens-Default-Whitelisting bleibt bestehen, um auf alle Siemens-Geräte verbinden zu können. Wir bieten jedoch Whitelisting von URLs an, die der Kunde gerne erreichen würde. | Alle |
| **Firewall: Standardeinstellung «leicht»** | Die Firewall von WatchGuard ist aktiviert und darf vom Kunden konfiguriert werden. | Leicht |
| **Firewall: Standardeinstellung** | Die Firewall von WatchGuard ist aktiviert und darf nicht vom Kunden aktiviert werden. Alle WatchGuard Standard-Regeln sind aktiviert. Traffic ohne vordefinierte Regel wird blockiert. | Mittel und Hoch |
| **Firewall: Verbindungsregeln «Mittel»** | Die Verbindungsregeln besagen, dass folgende Ports ein und ausgehend zugelassen sind:  FTP 20  FTP 21  SMTP 25  DNS 53  DHCP 67  DHCP 68  HTTP 80  NTP 123  HTTPS 443  SMTP 587  RDP 3389  BACF 47808-47840 | Mittel |
| **Firewall: Verbindungsregeln «Hoch»** | Die Verbindungsregeln besagen, dass folgende Ports ein und ausgehend zugelassen sind:  SMTP 25  DNS 53  DHCP 67  DHCP 68  HTTP 80  NTP 123  HTTPS 443  SMTP 587  RDP 3389 | Hoch |
| **Firewall: Alle Einbrüche werden blockiert.** | Die folgenden Einbrüche werden alle von der Firewall des WatchGuard EPDR blockiert:  IP Explicit Path  Land Attack  SYN Flood  TCP Port Scan  TCP Flags Check  Header Lengths  UDP Flood  UDP Port Scan  Smart WINS  Smart DNS  Smart DHCP  ICMP Attack  ICMP Filter Echo Request  Smart ARP  OS Detection | Alle |
| **Firewall: Zugelassene Programmregeln** | Eingehende und Ausgehende Verbindungen werden für C:\Windows\System32\mstsc.exe zugelassen. | Mittel und Hoch |
| **Workstations und Server: Allgemein, Erweiterter Schutz, Virenschutz, Gerätesteuerung und Prüfmodus - Standardeinstellungen** | Alle restlichen Reiter in der WatchGuard-Konfiguration bleiben auf ihren Standardeinstellungen, welche sie bei der Installation erhalten, und sind nicht Teil des IPA-Auftrages. Es werden lediglich Webzugriffskontrolle und Firewall angepasst. | Alle |
| **Programmblockierung:** | Die folgenden Programme werden blockiert:  Wireshark.exe  PowerShell.exe  Advanced IP Scanner.exe  Tcpview.exe | Alle |
| **Warnungen:** | Zu jedem verfügbaren Fall im Warnungen-Reiter wird eine Warnung an Kunde und Techniker sowie Administrator versendet. | Alle |
| **Managementbericht** | Ein Managementbericht wird jeweils am Ende des Monats an Kunden und Techniker versendet. | Alle |
| **Active Directory-Sync** | Sofern ein Active Directory vorhanden ist, werden dessen Daten und Nutzerkontos synchronisiert, um später ein Login auf WatchGuard-Produkte (Firebox & Accesspoints) bereitzustellen. | Alle |

Tabelle Konzept der Grundschutzstufen

### Appoval-Meeting Planung

Beiliegend wird das Approval-Meeting geplant. Für das Meeting wir eine kurze PowerPoint-Präsentation erstellt, welche die wichtigsten Punkte im Programm den Teilnehmern vorstellen sollte. Die PowerPoint-Präsentation wird dem Anhang beigefügt. Alle Aspekte der Planung sollten in das Meeting einfliessen und schliesslich verbessert werden. Ein Protokoll mit den wichtigsten Punkten wird geführt, die erwähnten Verbesserungsvorschläge umgesetzt und in die Dokumentation aufgenommen.

#### Konzept

|  |  |
| --- | --- |
| **Termin** | Der Termin wurde am Dienstag, 26.03.2024 um 12:47 Uhr versendet |
| **Ziel des Meetings** | Bewilligung zum praktischen Einsatz der 3 verschiedenen Grundschutzstufen. |
| **Datum** | 27.03.2024 |
| **Ort** | Onlinebesprechung via Teams |
| **Dauer** | Von 10:00 Uhr bis 11:00 Uhr |
| **Teilnehmer** | WatchGuard-Administratoren: Timon Hochstrasser und Maurizio Taglialatela |
| **Programm** | - Ich stelle die 3 verschiedene Grundschutzstufen vor, die das Netzwerk und die Zugriffe des Kunden unterschiedlich stark sichert.  - Ich zeige auf, wie der Webzugriff und die Firewall funktionieren und verwaltet werden.  - Wie die zuständigen Techniker einbezogen werden.  - Wie der Kunde, die Techniker und WatchGuard-Administratoren bei Fehlern und Änderungen im Schutz benachrichtigt werden.  - Wie die Dokumentation für Kunde, Techniker und Administratoren (Owner) gehandhabt wird.  - Am Ende der Präsentation gibt es eine Feedbackrunde, und ein Fazit, ob und wie das Konzept bewilligt wird.  - Während der gesamten Feedbackrunde werden die Meinungen von mir protokolliert und genutzt, um entsprechende Änderungen am Endprodukt vorzunehmen. |

Tabelle Konzept Approval-Meeting

### Testkonzept

Um das Testkonzept genauer beschreiben zu können, verwende ich leicht veränderte Bilder des Plans, den ich auf Seite 19 im Teil 1 des IPA-Berichts erstellt habe, um das Testkonzept für aussenstehende Personen besser verständlich zu machen.   
  
**1.** Mein persönlicher Laptop wird nur für das Ändern der WatchGuard-Konfiguration verwendet und um eine Verbindung auf den Hostserver herzustellen. **2.** Alle Tests finden in der Domäne des Hostservers zwischen den beiden virtuellen Maschinen statt:

Ein Bild, das Text, Screenshot, Diagramm, parallel enthält.

Automatisch generierte Beschreibung

**2.)**

**1.)**

**1.)**

Abbildung Durchführung der Tests

|  |  |  |
| --- | --- | --- |
| Nr. | Name | Beschreibung |
| *Black-Box-Tests (Funktioniert die Webzugriffskontrolle? Funktionieren die Warnmeldungen? Funktioniert die Programmblockierung? )* | | |
| 1 | Funktioniert die Webzugriffskontrolle? | Es wird versucht auf die Seite Blick.ch und 20min.ch zu navigieren, welche blockiert sein sollten. |
| Testumgebung und Testmittel | | |
|  | | |
| Erwartetes Ergebnis | | |
|  | | |
| 2 | Funktionieren die E-Mail-Benachrichtigungen? | Es wird ein Managementbericht vom letzten Monat auf den 10.04.2024 um 09:00 Uhr an mich selbst versendet und sollte zur vorgegebenen Zeit ankommen. |
| Testumgebung | | |
|  | | |
| Testumgebung und Testmittel | | |
|  | | |
| 3 | Funktionieren die Warnemeldungen und die Programmblockierung? |  |
| Testumgebung und Testmittel | | |
|  | | |
| Erwartetes Ergebnis | | |
|  | | |
| *White-Box-Tests (Funktionieren die Firewall-Regeln? Funktioniert der Virenschutz?)* | | |
| 4 | Funktionieren die Firewall-Verbindungsregeln? (TCP-Ports, ein und ausgehend) |  |
| Testumgebung und Testmittel | | |
|  | | |
| Erwartetes Ergebnis | | |
|  | | |
| 5 | Funktionieren die Firewall-Verbindungsregeln? (UDP-Ports, ein und ausgehend) |  |
| Testumgebung und Testmittel | | |
|  | | |
| Erwartetes Ergebnis | | |
|  | | |
| 6 | Funktioniert der Virenschutz? |  |
| Testumgebung und Testmittel | | |
|  | | |
| Erwartetes Ergebnis | | |
|  | | |
| *Connectivity-Tests (Sind die Webseiten erreichbar? Funktioniert die cRSP-RDP-Session noch?)* | | |
| 7 | Sind freigegebene Webseiten erreichbar? | Es wird getestet, ob die Freigabe der URLs funktioniert, indem die versucht wird eine Firewall innerhalb des Netzes zu erreichen. Die Firewall wurde vorher von der Webzugriffskontrolle freigegeben. |
| Testumgebung und Testmittel | | |
|  | | |
| Erwartetes Ergebnis | | |
|  | | |
| 8 | Funktioniert die cRSP-Verbindung mit Remotedesktop? |  |
| Testumgebung und Testmittel | | |
|  | | |
| Erwartetes Ergebnis | | |
|  | | |

Tabelle Testkonzept

#### Was nicht getestet wird

#### Beschreibung der verwendeten Testtools

Um die White-Box-Tests abzuschliessen, bediene ich mich einer Reihe von Tools, welche die Funktionalität der WatchGuard Firewall und dessen Virenschutz darstellen und testen können.

Hyperterminal:

Hyperterminal ist ein Terminalprogramm von Windows, mit dem man die eingehenden Daten an einer Schnittstelle überprüfen kann. Man kann so nachsehen, ob die Verbindung mit einem Server im selben Netzwerk möglich ist. Dazu gibt man beim ersten Computer, welcher auf die Verbindung oder den Call wartet, die Adresse 127.0.0.1. Dies ist der sogenannte Localhost.

Ein Bild, das Text, Elektronik, Screenshot, Display enthält.

Automatisch generierte BeschreibungEin Bild, das Text, Screenshot, Display, Software enthält.

Automatisch generierte Beschreibung

Abbildung HyperTerminal Computer 1 wartet auf den Call

Die Anfrage wird somit nicht über den Router ins Internet weitergeleitet, sondern bleibt im eigenen System. Localhost hat also die IP-Adresse 127.0.0.1, die auf den Server auf dem eigenen Rechner referiert.

Beim zweiten Computer, welcher ebenfalls Hyperterminal installiert hat, wird dann die IP-Adresse des ersten Computers eingetragen. Beim ersten und zweiten Computer wird dann noch der zu testende Port eingetragen und schliesslich ruft der zweite Computer den Ersten an.

Ein Bild, das Text, Elektronik, Screenshot, Display enthält.

Automatisch generierte BeschreibungEin Bild, das Text, Screenshot, Display, Software enthält.

Automatisch generierte Beschreibung

Abbildung HyperTerminal Computer 2 startet den Call mit der IP-Adresse von Computer 1

Danach wird je nach Firewall-Regel des entsprechenden Ports eine Verbindung aufgebaut oder nicht. Wenn die Verbindung aufgebaut und ein Textstring über beide Computer gesendet werden kann, dann ist der Port offen. Wenn nicht, dann ist der Port blockiert.

Ein Bild, das Text, Screenshot, Software, Display enthält.

Automatisch generierte BeschreibungEin Bild, das Text, Screenshot, Software, Computersymbol enthält.

Automatisch generierte Beschreibung

Abbildung Hyperterminal Links Computer 2 und Rechts Computer 1 Ein "Hallo" kann gesendet werden

Hercules:

Hercules ist ein leistungsfähiges Terminalprogramm von HW-Group. In meiner Arbeit benutze ich aber hauptsächlich die Registerkarte „UDP“. Diese ist ein einfaches „Terminal“, das zum Versenden von UDP-Paketnachrichten zwischen meinen beiden Computern benutzt wird.

Der Hauptzweck dieser Registerkarte besteht darin, UDP-Pakete von einem Computer an das Ziel zu senden. In seiner Funktionalität ist es daher ähnlich wie Hyperterminal:

Unter «Module IP», trägt man die IP-Adresse des zweiten Computers ein. Unter «Port» den zu testenden UDP-Port. Unter «Local Port» sollte ein Zweiter, freigegebener UDP-Port angeben werden. Wenn man dann den Button «Listen» betätigt, erscheint in der weissen Konsole unter «Received data» ein grüner Text mit «UDP socket created»

Auf dem zweiten Rechner muss man ähnlich Vorgehen. Unter «Module IP», trägt man nun die IP-Adresse des ersten Computers ein. Bezüglich der Ports tauscht man nun die Plätze der beiden Ports aus dem Terinal des ersten Computers. Also genau umgekehrt. Wenn man dann den Button «Listen» betätigt, erscheint in der weissen Konsole unter «Received data» wieder ein grüner Text mit «UDP socket created»

Nach dem beide Rechner die Übermittlung initiiert haben, kann unter Send bei der ersten Zeile ein beliebiger Textstring eingetragen und via Button «Send» übermittelt werden.

Erscheint der gesendete Textstring unter Received data beim anderen Rechner, funktioniert die Kommunikation. Wenn nicht, ist einer der beiden Ports blockiert.

AMTSO – Security Features – Check

## Entscheiden

### Approval-Meeting

#### Protokoll:

|  |  |  |  |
| --- | --- | --- | --- |
| **Datum:** | **Dauer:** | **Teilnehmer:** | **Anwesend/Abwesend:** |
| 27.03.2024 | 10:00 bis 11:05 Uhr | Timon Hochstrasser | Anwesend |
| Maurizio Taglialatela | Anwesend |
| **Gesprächspunkte und wichtige Entscheidungen:** | | | |
| * Es besteht Verbesserungspotenzial bei der Grundschutzstufe 1, die Programmblockierung ist dort nicht notwendig, wenn der Kunde die Firewall selbst konfigurieren kann. * Die Blockierung von Advanced-IP-Scanner macht wenig Sinn, da es viele andere Gratislösungen gibt. Am besten wird der Port ICMP blockiert. Ausserdem sollte eine Regel zur Freigabe von Modbus eingesetzt werden. * Am besten wird für zusätzliche Sicherheit noch das Regedit blockiert. * Der Kunde muss informiert werden, dass die WatchGuard-Firewall die Windows-Firewall ersetzt und eine Liste mit Empfehlung zum Öffnen der Standard-Ports sollte mit der Kundendokumentation mitgesendet werden. * In der finalen IPA-Präsentation empfiehlt sich eine Matrix der drei verschiedenen Grundschutzstufen. Die URLs und Portfreigaben sollten gruppiert werden und in der Präsentation auf einer Seite dargestellt werden können. * Kann der Zugriff auf die Firewall der Stufe «Leicht» mit einem Passwort geschützt werden? * Die E-Mail-Warnungen sollten nur den verantwortlichen Technikern bei Siemens versendet werden und der Kunde und Techniker erhalten den monatlichen Managementbericht. So wird verhindert, dass der Kunde zu viele E-Mailnachtrichten, erhält, die nur für WatchGuard Nutzer relevant sind. | | | |
| **Nächste Schritte:** | | | |
| * Die Programmblockierung wird für Grundschutzstufe 1 entfernt, was die leichte Stufe auch mehr von der Mittleren abhebt. * Der Advanced-IP-Scanner wird aus der Liste der blockierten Programme entfernt und stattdessen wird ICMP durch die WatchGuard Firewall in der Mittleren und Hohen Grundschutzstufe blockiert. Für Modbus wird der Port 502 freigeschaltet. Der Port kommt in die Kundenempfehlung auf Stufe Leicht und wird als Firewallregel in Stufe Mittel und Hoch eingeführt. * Eine weitere Programmblockierung zur Blockierung von C:\Windows\regedit.exe wird eingeführt. * Innerhalb der Dokumentationen für den Kunden wird eine Liste mit empfohlenen Ports zur Freigabe eingesetzt, sollten Sie die Stufe «Leicht» gewählt haben. * Ich erstelle in der Präsentation eine Matrix mit Übertiteln um die einzelnen Kategorien, URLs und Portfreigaben zu kategorisieren, damit die Erklärung möglichst auf einer Seite Platz hat. * Ich werde nachforschen, ob die Firewall mit einem Passwort geschützt werden kann und das Ergebnis dokumentieren. * Es wird in der Dokumentation für die Techniker und Administratoren beschrieben, wie sie den verantwortlichen Techniker für eine bestimmte Anlage ermitteln können und schliesslich werden die E-Mailwarnungen nur für den besagten Techniker in Kraft gesetzt. Der Managementbericht wird weiterhin für Kunde und Techniker verschickt. | | | |

Tabelle Meetingprotokoll

### Änderungen an der Testumgebung

|  |  |  |
| --- | --- | --- |
| **Konfiguration** | **Effekt** | **Sicherheitsstufe** |
| **Webzugriffskontrolle: Standardeinstellungen der Kategorien.** | Alle Kategorien geblockt ausser «Informationstechnologie» und «Private IP-Adressen» | Leicht und Mittel |
| **Webzugriffskontrolle: Kategorie «Bürozusammenarbeit»** | Bürozusammenarbeit wird freigeschaltet, wenn der Kunde dies benötigt. | Leicht |
| **Webzugriffskontrolle: Siemens Default Whitelisting** | Das Siemens-Default-Whitelisting bleibt bestehen, um auf alle Siemens-Geräte verbinden zu können. Wir bieten jedoch Whitelisting von URLs an, die der Kunde gerne erreichen würde. | Alle |
| **Firewall: Standardeinstellung «leicht»** | Die Firewall von WatchGuard ist aktiviert, ersetzt die Windows Firewall und darf vom Kunden konfiguriert werden. Der Kunde erhält in der Dokumentation eine Liste mit dieser Information und den von uns empfohlenen Portfreigaben. | Leicht |
| **Firewall: Standardeinstellung** | Die Firewall von WatchGuard ist aktiviert und darf nicht vom Kunden aktiviert werden. Alle WatchGuard Standard-Regeln sind aktiviert. Traffic ohne vordefinierte Regel wird blockiert. | Mittel und Hoch |
| **Firewall: Verbindungsregeln «Mittel»** | Die Verbindungsregeln besagen, dass folgende Ports ein und ausgehend zugelassen sind:  FTP 20  FTP 21  SMTP 25  DNS 53  DHCP 67  DHCP 68  HTTP 80  NTP 123  HTTPS 443  MODBUS 502  SMTP 587  RDP 3389  BACF 47808-47840 | Mittel |
| **Firewall: Verbindungsregeln «Hoch»** | Die Verbindungsregeln besagen, dass folgende Ports ein und ausgehend zugelassen sind:  SMTP 25  DNS 53  DHCP 67  DHCP 68  HTTP 80  NTP 123  HTTPS 443  MODBUS 502  SMTP 587  RDP 3389 | Hoch |
| **Firewall: Alle Einbrüche werden blockiert.** | Die folgenden Einbrüche werden alle von der Firewall des WatchGuard EPDR blockiert:  IP Explicit Path  Land Attack  SYN Flood  TCP Port Scan  TCP Flags Check  Header Lengths  UDP Flood  UDP Port Scan  Smart WINS  Smart DNS  Smart DHCP  ICMP Attack  ICMP Filter Echo Request  Smart ARP  OS Detection | Alle |
| **Firewall: ICMP-Block** | Es wird eine Verbindungsregel erstellt, die alle ICMP-Services blockiert. | Mittel und Hoch |
| **Firewall: Zugelassene Programmregeln** | Eingehende und Ausgehende Verbindungen werden für C:\Windows\System32\mstsc.exe zugelassen. | Mittel und Hoch |
| **Workstations und Server: Allgemein, Erweiterter Schutz, Virenschutz, Gerätesteuerung und Prüfmodus - Standardeinstellungen** | Alle restlichen Reiter in der WatchGuard-Konfiguration bleiben auf ihren Standardeinstellungen, welche sie bei der Installation erhalten, und sind nicht Teil des IPA-Auftrages. Es werden lediglich Webzugriffskontrolle und Firewall angepasst. | Alle |
| **Programmblockierung:** | Die folgenden Programme werden blockiert:  Wireshark.exe  PowerShell.exe  Regedit.exe  Tcpview.exe | Mittel und Hoch |
| **Warnungen:** | Zu jedem verfügbaren Fall im Warnungen-Reiter wird eine Warnung an Kunde und Techniker versendet. In der Testumgebung werden sie mir unter der Mail: «dylan.nideroest@siemens.com» gesendet. | Alle |
| **Managementbericht** | Ein Managementbericht wird jeweils am Ende des Monats an Kunden und Techniker versendet. In der Testumgebung werden sie mir unter der Mail: «dylan.nideroest@siemens.com» gesendet. | Alle |
| **Active Directory-Sync** | Sofern ein Active Directory vorhanden ist, in unserem Falle das Active-Directory der Domäne «root», werden dessen Daten und Nutzerkontos synchronisiert, um später ein Login auf WatchGuard-Produkte (Firebox & Accesspoints) bereitzustellen. | Alle |

Tabelle Entschiedene Änderungen an der Testumgebung

### Festlegung externer Hilfestellung

Ich habe mich entschieden, für alle Probleme, die ich nicht selbst lösen konnte, einen externen Ansprechpartner zu Hilfe zu ziehen. Die Lösungen werden kurz aufgeführt, da sie bereits in die IPA integriert wurden oder neu dazukommen. Die Konfigurationen innerhalb der Realisierungsphase wurden mit den hier beschriebenen, erarbeiteten Lösungen ausgestattet.

|  |  |  |
| --- | --- | --- |
| **Ansprechpersonen** | **Probleme** | **Erarbeitete Lösung** |
| -Timo Kirchem  -WatchGuard Sales Engineer Central Europe  -WatchGuard “Owner”  -Kontakt mit dem Hersteller. | Blick.ch konnte nicht blockiert werden, obwohl die URL in der Webzugriffskontrolle zugelassen wurde. | Wenn die URL folgendermassen eingetragen wird, kann die Website erreicht werden:  <https://www.blick.ch> oder  <https://blick.ch> |
| Was beinhaltet die Synchronisation auf dem Endpoint? Z.B Whitelist-Einträge oder Anpassungen der Firewall sollten unmittelbar vom Client übernommen werden?  Wie sieht das Intervall dieser Synchronisation aus und kann dieses angepasst werden? Wenn ja, wo? | Es besteht eine Echtzeitkommunikation des Endpoint mit der WatchGuard Cloud. Dadurch erfolgt ein Sync innerhalb weniger Sekunden.  Je nach Auslastung und Verbindungsqualität kann es sich allerdings bis zu 1 Minute verzögern. Dieser Sync kann manuell von der Konsole im Kundencomputer ausgeführt werden. |
| Woher stammt der Inhalt der Webkategorien? Wird dieser von Ihnen definiert, oder sind dies allgemeine im Internet geltende Kategorien?  Gibt es eine Übersicht, was diese Webkategorien konkret beinhalten? | Der Inhalt der Webkategorien bestimmt WatchGuard zusammen mit Forcepoint. Wenn es nicht klar ist, welcher Kategorie einer URL angehört, kann die Kategorie besagter URL in das Suchfeld dieser Webseite eingetragen und ermittelt werden: <https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Endpoint-Security/manage-settings/configure-authorized-software-settings.html> |
| An einem Profil werden Änderungen via Cloud gemacht. Wie lange dauert es bis der Client diese Anpassung erhält? Wo wird das geloggt? Mit Zeitstempel?  Kann ich mir ein Mail auslösen, wenn die Anpassungen nicht bis zum Client gepusht werden können? (z.B aufgrund mangelnder Netzwerk-Konnektivität) | Im Detail kann dies unter «Last connection & Last settings check» eingesehen werden. Eine Alarmierung für Clients die länger nicht verbunden sind, gibt es als solches nicht.  Für eine Systemüberwachung auf Erreichbarkeit ist die Endpoint Lösung nicht ausgelegt. Da es im Bereich des Endpoint Schutzes immer wieder Systeme gibt, die unregelmäßig oder nur in Intervallen, Online kommen. Hier wäre eine Monitoring Tool bzw Systemüberwachungslösung der Clients die Sinnvollere Lösung.  In der gesamten Cloud Übersicht kann man allerdings sehen ob Clients einzelner Kunden vorhanden sind, die länger als 3, 7 oder 30 Tage nicht verbunden sind. |
| Gäbe es eine Möglichkeit (lokal) ein Backup der getätigten Konfigurationen/Einstellungen zu erstellen? | ANTWORT AUSSTEHEND!!! |
| -Sandro Scalfaro  -Siemens Product Portfolio Management Manager  -WatchGuard-“Owner” auf höchster Ebene | Sandro Scalfaro kontaktierte für mich den WatchGuard-Support bezüglich folgenden Problems:  Es konnte über den Port 517 kommuniziert werden, obwohl dieser blockiert war. | Das Problem bestand darin, dass die NTP-123-Regel weiter oberhalb in der Tabelle mit den Ausnahmen den gesamten ausgehenden Datenverkehr zuließ. Die Regeln gelten von oben nach unten, sodass der gesamte Datenverkehr, der nicht mit den oben genannten Ablehnungsregeln übereinstimmte, schließlich mit NTP123 abgeglichen wurde, welches komplett offen war und alle Verbindungen zuliess. |
| Wie kann ich den Antivirus von WatchGuard EPDR testen? | Die Funktionalität des Antivirus kann mithilfe des Tools auf dieser Webseite ermittelt werden. Eine Testdatei kann dort generiert werden, welches von einer funktionierenden Firewall als Malware erkannt werden sollte. <https://www.amtso.org/security-features-check/> |
| -David Trachsler  -Siemens Techniker  -WatchGuard «Helpdesk» | Ich und David behandelten und testeten folgendes Problem miteinander:  Windows Smartscreen blockiert die Installation eines Desigo CCs. Er kann nicht überprüfen, ob die Software vertrauenswürdig ist. Eine Freigabe muss erstellt werden. | Wenn die Kategorie Informationstechnologie freigegeben wird, kann das Desigo CC installiert werden, ohne dass Smartscreen die Installation blockiert. |
| -Pius Müller  -Siemens Techniker  -WatchGuard «Helpdesk» | Die Open-VPN-GUI-Software wird von WatchGuard blockiert. | Das Open-VPN-GUI kann ebenfalls aktiviert werden, sobald die Kategorie «Informationstechnologie» freigegeben wird. Aufgrund ihrer Wichtigkeit wird die Kategorie nun bei der Erstellung der Grundschutzfunktionen verwendet und zukünftig freigegeben, wenn die Software vorhanden ist. |

Tabelle Festlegung Externer Hilfestellung

## Realisieren

### Versionsverwaltung einsetzen

### Öffnen der Testumgebung

Abbildung cRSP Anmeldung an Client

### Installieren von WatchGuard EPDR

### Drei Grundschutzstufen einrichten

### Webzugriffskontrolle bearbeiten

### Erstellung der Firewall-Policies

### Verhinderung spezifischer Software-Installation

### Mailalarmierung einrichten

## Kontrollieren

### Testfälle

#### Name Test 1

1. Beschreibung des Testsystem

Der Test wird auf dem … ausgeführt, welcher...

1. Testmethode & Testmittel

Es wird ein Black-Box Test / White-Box Test ausgeführt.

1. Testperson & Testzeitpunkt

Dylan Nideröst -> Lehrling viertes Lehrjahr als Informatik Systemtechniker EFZ  
Am (Datum) um (Uhrzeit) ausgeführt.

1. Testszenario

Der Benutzer macht ...

1. Durchführung des Testes / Fazit zum Resultat

Testergebnis: True Positive oder True Negative False Negative

Beschreibung:

Massnahmen/Empfehlungen:

#### Name Test 2

1. Beschreibung des Testsystem

Der Test wird auf dem … ausgeführt, welcher...

1. Testmethode & Testmittel

Es wird ein Black-Box Test / White-Box Test ausgeführt.

1. Testperson & Testzeitpunkt

Dylan Nideröst -> Lehrling viertes Lehrjahr als Informatik Systemtechniker EFZ  
Am (Datum) um (Uhrzeit) ausgeführt.

1. Testszenario

Der Benutzer macht ...

1. Durchführung des Testes / Fazit zum Resultat

Testergebnis: True Positive oder True Negative False Negative

Beschreibung:

Massnahmen/Empfehlungen:

#### Name Test 3

1. Beschreibung des Testsystem

Der Test wird auf dem … ausgeführt, welcher...

1. Testmethode & Testmittel

Es wird ein Black-Box Test / White-Box Test ausgeführt.

1. Testperson & Testzeitpunkt

Dylan Nideröst -> Lehrling viertes Lehrjahr als Informatik Systemtechniker EFZ  
Am (Datum) um (Uhrzeit) ausgeführt.

1. Testszenario

Der Benutzer macht ...

1. Durchführung des Testes / Fazit zum Resultat

Testergebnis: True Positive oder True Negative False Negative

Beschreibung:

Massnahmen/Empfehlungen:

#### Name Test 4

1. Beschreibung des Testsystem

Der Test wird auf dem … ausgeführt, welcher...

1. Testmethode & Testmittel

Es wird ein Black-Box Test / White-Box Test ausgeführt.

1. Testperson & Testzeitpunkt

Dylan Nideröst -> Lehrling viertes Lehrjahr als Informatik Systemtechniker EFZ  
Am (Datum) um (Uhrzeit) ausgeführt.

1. Testszenario

Der Benutzer macht ...

1. Durchführung des Testes / Fazit zum Resultat

Testergebnis: True Positive oder True Negative False Negative

Beschreibung:

Massnahmen/Empfehlungen:

#### Name Test 5

1. Beschreibung des Testsystem

Der Test wird auf dem … ausgeführt, welcher...

1. Testmethode & Testmittel

Es wird ein Black-Box Test / White-Box Test ausgeführt.

1. Testperson & Testzeitpunkt

Dylan Nideröst -> Lehrling viertes Lehrjahr als Informatik Systemtechniker EFZ  
Am (Datum) um (Uhrzeit) ausgeführt.

1. Testszenario

Der Benutzer macht ...

1. Durchführung des Testes / Fazit zum Resultat

Testergebnis: True Positive oder True Negative False Negative

Beschreibung:

Massnahmen/Empfehlungen:

#### Name Test 6

1. Beschreibung des Testsystem

Der Test wird auf dem … ausgeführt, welcher...

1. Testmethode & Testmittel

Es wird ein Black-Box Test / White-Box Test ausgeführt.

1. Testperson & Testzeitpunkt

Dylan Nideröst -> Lehrling viertes Lehrjahr als Informatik Systemtechniker EFZ  
Am (Datum) um (Uhrzeit) ausgeführt.

1. Testszenario

Der Benutzer macht ...

1. Durchführung des Testes / Fazit zum Resultat

Testergebnis: True Positive oder True Negative False Negative

Beschreibung:

Massnahmen/Empfehlungen:

#### Name Test 7

1. Beschreibung des Testsystem

Der Test wird auf dem … ausgeführt, welcher...

1. Testmethode & Testmittel

Es wird ein Black-Box Test / White-Box Test ausgeführt.

1. Testperson & Testzeitpunkt

Dylan Nideröst -> Lehrling viertes Lehrjahr als Informatik Systemtechniker EFZ  
Am (Datum) um (Uhrzeit) ausgeführt.

1. Testszenario

Der Benutzer macht ...

1. Durchführung des Testes / Fazit zum Resultat

Testergebnis: True Positive oder True Negative False Negative

Beschreibung:

Massnahmen/Empfehlungen:

#### Name Test 8

1. Beschreibung des Testsystem

Der Test wird auf dem … ausgeführt, welcher...

1. Testmethode & Testmittel

Es wird ein Black-Box Test / White-Box Test ausgeführt.

1. Testperson & Testzeitpunkt

Dylan Nideröst -> Lehrling viertes Lehrjahr als Informatik Systemtechniker EFZ  
Am (Datum) um (Uhrzeit) ausgeführt.

1. Testszenario

Der Benutzer macht ...

1. Durchführung des Testes / Fazit zum Resultat

Testergebnis: True Positive oder True Negative False Negative

Beschreibung:

Massnahmen/Empfehlungen:

## Auswerten

### Stand der Endpoint-Protection

Die vom Auftraggeber definierten Funktionen wurden umgesetzt…?

Einige Tests waren negativ, da…?

### Erweiterungsmöglichkeiten

* …
* …

### Vollständigkeitstest

In diesem Kapitel werde ich die einzelnen Punkte des Kriterienkatalogs auflisten und in der Doku kontrollieren, ob ich ihn meiner Meinung nach erfüllt habe. Dies ist eine persönliche Checkliste

|  |  |
| --- | --- |
| **IPA-Bewertungskriterien (Leitfragen)** | **Erfüllt? (Ja/Nein)** |
| A1 Projektmanagement und Planung |  |
| A2 Wissensbeschaffung |  |
| A3 Zeitplan |  |
| A4 Konzeptionelle Umsetzung |  |
| A5 Projektumfeld: Systemgrenzen / Schnittstellen zur Aussenwelt |  |
| A6 Testkonzept |  |
| A7 Leistungsfähigkeit |  |
| A8 Selbständiges Arbeiten |  |
| A9 Fachkenntnisse und Anwendungskompetenz |  |
| A10 Anwendung der Fachsprache |  |
| A11 Arbeits- und Fachmethodik |  |
| A12 Organisation der Arbeitsergebnisse |  |
| A13 IPA-Erfüllungsgrad |  |
| B1 Kurzfassung des IPA-Berichtes |  |
| B2 Führung des Arbeitsjournals |  |
| B3 Reflexionsfähigkeit |  |
| B4 Gliederung |  |
| B5 Prägnanz |  |
| B6 Formale Vollständigkeit des IPA-Berichts |  |
| B7 Sprachlicher Ausdruck und Stil / Rechtschreibung und Grammatik |  |
| B8 Darstellung |  |
| B9 Grafiken, Bilder, Diagramme und Tabellen |  |
| B10 Durchführung und Auswertung der Tests |  |

Tabelle Vollständigkeitstest

Ich bin zuversichtlich, dass ich alle Punkte zumindest genügend erfüllt habe. Was ist rot? nicht vollständig so abschliessen konnte, wie ich es geplant habe und ein paar Tests fehlschlugen.

### Schlusswort

#### Reflexion

#### Fazit

# Glossar

Das Glossar zu verwendeten Ausdrücken. Die Tabelle wurde nach Anfangsbuchstaben der Begriffe alphabetisch aufsteigend sortiert.

|  |  |
| --- | --- |
| Begriff | Beschreibung |
|  |  |
|  |  |
|  |  |
|  |  |

Tabelle Glossar

# Quellenverzeichnis

Hier werden die verschiedenen Quellen beschrieben, die ich verwendet habe. Alphabetisch, aufsteigend sortiert.

|  |  |
| --- | --- |
| Name | Quelle/n |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Tabelle Quellenverzeichnis

# Abbildverzeichnis

[Abbildung 1 Testumgebung 19](file:///D:\Projects\IPA_Nideröst_2024\01_Nideröst_IPA-Bericht.docx#_Toc162265161)

[Abbildung 2 IPERKA 20](#_Toc162265162)

[Abbildung 3 Zeitplan 22](file:///D:\Projects\IPA_Nideröst_2024\01_Nideröst_IPA-Bericht.docx#_Toc162265163)

[Abbildung 7 cRSP Anmeldung an Client 45](#_Toc162265164)

# Tabellenverzeichnis

[Tabelle 1 Änderungsnachweis 2](#_Toc162268661)

[Tabelle 2 Kandidat 6](#_Toc162268662)

[Tabelle 3 Bewertungskriterium 1 9](#_Toc162268663)

[Tabelle 4 Bewertungskriterium 2 10](#_Toc162268664)

[Tabelle 5 Bewertungskriterium 3 11](#_Toc162268665)

[Tabelle 6 Bewertungskriterium 4 12](#_Toc162268666)

[Tabelle 7 Bewertungskriterium 5 13](#_Toc162268667)

[Tabelle 8 Bewertungskriterium 6 14](#_Toc162268668)

[Tabelle 9 Bewertungskriterium 7 15](#_Toc162268669)

[Tabelle 10 Meilensteine 21](#_Toc162268670)

[Tabelle 11 Tätigkeiten Tag1 23](#_Toc162268671)

[Tabelle 12 Tätigkeiten Tag2 24](#_Toc162268672)

[Tabelle 13 Tätigkeiten Tag3 25](#_Toc162268673)

[Tabelle 14 Tätigkeiten Tag4 26](#_Toc162268674)

[Tabelle 15 Tätigkeiten Tag5 27](#_Toc162268675)

[Tabelle 16 Tätigkeiten Tag6 28](#_Toc162268676)

[Tabelle 17 Tätigkeiten Tag7 29](#_Toc162268677)

[Tabelle 18 Tätigkeiten Tag8 30](#_Toc162268678)

[Tabelle 19 Tätigkeiten Tag9 31](#_Toc162268679)

[Tabelle 20 Tätigkeiten Tag10 32](#_Toc162268680)

[Tabelle 21 Planung Webzugriffskontrolle 36](#_Toc162268681)

[Tabelle 22 Konzept der Grundschutzstufen 36](#_Toc162268682)

[Tabelle 23 Konzept 36](#_Toc162268683)

[Tabelle 24 Testkonzept 38](#_Toc162268684)

[Tabelle 25 Vollständigkeitstest 55](#_Toc162268685)

[Tabelle 26 Glossar 57](#_Toc162268686)

[Tabelle 27 Quellenverzeichnis 57](#_Toc162268687)

# Anhang

### Datenname?