IPA-Bericht

|  |
| --- |
| Erweiterung der Sicherheit durch WatchGuard Endpoint-Protection mit Firewall |
| Dylan Nideröst |
| 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** |
| 25.03.2024 |  | V0.1 |
| 26.03.2024 |  | V0.2 |
| 27.03.2024 |  | 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](#_Toc159585254)

[Teil 1: Aufbau und Organisation 6](#_Toc159585255)

[Aufgabenstellung 6](#_Toc159585256)

[Kandidat 6](#_Toc159585257)

[Titel 6](#_Toc159585258)

[Beschreibung 6](#_Toc159585259)

[Ausgangslage 6](#_Toc159585260)

[Detaillierte Aufgabenstellung 6](#_Toc159585261)

[Individuelle Bewertungskriterien 8](#_Toc159585262)

[Mittel und Methoden 15](#_Toc159585263)

[Vorkenntnisse 15](#_Toc159585264)

[Vorarbeiten 15](#_Toc159585265)

[Neue Lerninhalte 15](#_Toc159585266)

[Arbeiten in den letzten 6 Monaten 15](#_Toc159585267)

[Tage, an welchen an der Facharbeit gearbeitet wird 15](#_Toc159585268)

[Bemerkungen 15](#_Toc159585269)

[Projektaufbauorganisation 16](#_Toc159585270)

[Lehrbetrieb und Durchführungsort 16](#_Toc159585271)

[Verantwortliche Fachkraft 16](#_Toc159585272)

[Berufsbildnerin 16](#_Toc159585273)

[Hauptexperte 16](#_Toc159585274)

[Nebenexperten 16](#_Toc159585275)

[Fachthema 16](#_Toc159585276)

[Deklaration der Vorarbeiten 17](#_Toc159585277)

[Projektmanagement 18](#_Toc159585278)

[Zeitplanung 19](#_Toc159585279)

[Meilensteine 19](#_Toc159585280)

[Zeitplan 20](#_Toc159585281)

[Arbeitsjournal 21](#_Toc159585282)

[Tag 1 - 25.03.2024 21](#_Toc159585283)

[Tag 2 - 26.03.2024 22](#_Toc159585284)

[Tag 3 - 27.03.2024 23](#_Toc159585285)

[Tag 4 - 02.04.2024 24](#_Toc159585286)

[Tag 5 - 03.04.2024 25](#_Toc159585287)

[Tag 6 - 05.04.2024 26](#_Toc159585288)

[Tag 7 - 08.04.2024 27](#_Toc159585289)

[Tag 8 - 09.04.2024 28](#_Toc159585290)

[Tag 9 - 10.04.2024 29](#_Toc159585291)

[Tag 10 - 12.04.2024 30](#_Toc159585292)

[Teil 2: Projekt 31](#_Toc159585293)

[Kurzfassung 31](#_Toc159585294)

[Informieren 32](#_Toc159585295)

[Wissensbeschaffung 32](#_Toc159585296)

[Vorbereitete Testumgebung 32](#_Toc159585297)

[Planen 33](#_Toc159585298)

[Vorgehensweise 33](#_Toc159585299)

[Datensicherung: 33](#_Toc159585300)

[Konfigurationsplan 34](#_Toc159585301)

[Appoval-Meeting Planung 34](#_Toc159585302)

[Testumgebung: 35](#_Toc159585303)

[Testkonzept 37](#_Toc159585304)

[Entscheiden 38](#_Toc159585305)

[Approval-Meeting 38](#_Toc159585306)

[Änderungen an der Testumgebung 40](#_Toc159585307)

[Festlegung externer Hilfestellung 41](#_Toc159585308)

[Realisieren 42](#_Toc159585309)

[Versionsverwaltung einsetzen 42](#_Toc159585310)

[Öffnen der Testumgebung 43](#_Toc159585311)

[Installieren von WatchGuard EPDR 43](#_Toc159585312)

[Drei Grundschutzstufen einrichten 43](#_Toc159585313)

[Webzugriffskontrolle bearbeiten 43](#_Toc159585314)

[Erstellung der Firewall-Policies 43](#_Toc159585315)

[Verhinderung spezifischer Software-Installation 43](#_Toc159585316)

[Mailalarmierung einrichten 43](#_Toc159585317)

[Kontrollieren 44](#_Toc159585318)

[Testfälle 44](#_Toc159585319)

[Auswerten 52](#_Toc159585320)

[Stand der Endpoint-Protection 52](#_Toc159585321)

[Erweiterungsmöglichkeiten 52](#_Toc159585322)

[Vollständigkeitstest 53](#_Toc159585323)

[Schlusswort 54](#_Toc159585324)

[Glossar 55](#_Toc159585325)

[Quellenverzeichnis 55](#_Toc159585326)

[Abbildverzeichnis 56](#_Toc159585327)

[Tabellenverzeichnis 57](#_Toc159585328)

[Anhang 58](#_Toc159585329)

[Datenname? 58](#_Toc159585330)

# 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

### Beschreibung

Auf einem PC wird WatchGuard Endpoint Protection installiert. Dabei werden innerhalb von drei Sicherheitsstufen mehrere Sicherheitsregeln definiert, die den Computer effektiv schützen sollten. Die Funktionalität und der Nutzen der EPDR-Software sollten getestet und umgesetzt werden können.

### Ausgangslage

Um bei Infrastrukturen ohne physikalische Firewall dennoch für Sicherheit sorgen zu können, müssen mit der Endpoint-Protection-Lösung "WatchGuard" 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 unterschiedliche Default-Konfigurations-Profile erstellt werden, welche schlussendlich auf den Kundensystemen angewendet werden können.

### 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 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) 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.

6. Monitoring - Mail-Alert

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

7. 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, Grundschutzstufen Sicherheit | |
| *Definition (Leitfrage)* | |
| Sind die drei Grundschutzstufen sinnvoll konzipiert und umgesetzt? | |
| *Gütestufe 3* | *Gütestufe 2* |
| Alle drei Grundschutzstufen sind sinnvoll konzipiert und umgesetzt. | Zwei der drei Grundschutzstufen sind sinnvoll konzipiert und umgesetzt. |
| *Gütestufe 1* | *Gütestufe 0* |
| Eine der drei Grundschutzstufen ist sinnvoll konzipiert und umgesetzt. | Keine der drei Grundschutzstufen sind sinnvoll konzipiert und umgesetzt. |

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, Testing | |
| *Definition (Leitfrage)* | |
| Werden die in der Aufgabe erwähnten Ziele sinnvoll mittels Testing überprüft? | |
| *Gütestufe 3* | *Gütestufe 2* |
| Sämtliche in der Aufgabe erwähnten Ziele wurden zielführend getestet und in einem Testprotokoll festgehalten. Es werden sinnvolle Tools für das Testing eingesetzt. | Nicht alle Ziele wurden mit dem Testing überprüft. Das Testprotokoll ist vorhanden |
| *Gütestufe 1* | *Gütestufe 0* |
| Es wurden wenige Tests durchgeführt, die Testszenarien sind jedoch nicht zielführend. | Es wurden keine Tests durchgeführt |

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  IIII. 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.

### 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.

### 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.-27. März 2024 & 02.-03 + 08.-10. + 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)

### **Fachthema**

## Deklaration der Vorarbeiten

Aufbau der Testumgebung:

Abbildung Testumgebung

## Projektmanagement

## Zeitplanung

In diesem Kapitel wird der Zeitplan der IPA beschrieben.

### Meilensteine

### Zeitplan

Abbildung Zeitplan

## Arbeitsjournal

### Tag 1 - 25.03.2024

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

Tabelle Tätigkeiten Tag1

Reflexion:

|  |
| --- |
|  |

Hilfe:

|  |
| --- |
|  |

### Tag 2 - 26.03.2024

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

Tabelle Tätigkeiten Tag2

Reflexion:

|  |
| --- |
|  |

Hilfe:

|  |
| --- |
|  |

### Tag 3 - 27.03.2024

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

Tabelle Tätigkeiten Tag3

Reflexion:

|  |
| --- |
|  |

Hilfe:

|  |
| --- |
|  |

### 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:

Umsetzung:

Ergebnis:

## Informieren

### Wissensbeschaffung

### Vorbereitete Testumgebung

## Planen

### Vorgehensweise

### Datensicherung:

### Konfigurationsplan

#### Webzugriffskontrolle

#### Grundschutzstufen-Konzept

### Appoval-Meeting Planung

#### Konzept

### Testumgebung:

### Testkonzept

|  |  |  |  |
| --- | --- | --- | --- |
| Nr. | Name | Beschreibung | Testumgebung |
| *Black-Box-Tests (Funktioniert die Webzugriffskontrolle? Funktionieren die Warnmeldungen? Funktioniert die Programmblockierung? )* | | | |
| 1 |  |  |  |
| Erwartetes Ergebnis | | | |
|  | | | |
| 2 |  |  |  |
| Erwartetes Ergebnis | | | |
|  | | | |
| 3 |  |  |  |
| Erwartetes Ergebnis | | | |
|  | | | |
| *White-Box-Tests (Funktionieren die Firewall-Regeln? Funktioniert der Virenschutz?)* | | | |
| 4 |  |  |  |
| Erwartetes Ergebnis | | | |
|  | | | |
| 5 |  |  |  |
| Erwartetes Ergebnis | | | |
|  | | | |
| 6 |  |  |  |
| Erwartetes Ergebnis | | | |
|  | | | |
| *Connectivity-Tests (Sind die Webseiten erreichbar? Funktioniert die cRSP-RDP-Session noch?)* | | | |
| 7 |  |  |  |
| Erwartetes Ergebnis | | | |
|  | | | |
| 8 |  |  |  |
| Erwartetes Ergebnis | | | |
|  | | | |

Tabelle Testkonzept

Wie wird getestet:

Hyperterminal:

Hercules:

AMTSO – Security Features – Check

## Entscheiden

### Approval-Meeting

Protokoll:

Aufbau Grundschutzstufen:

### Änderungen an der Testumgebung

### Festlegung externer Hilfestellung

Ansprechpersonen:

Probleme:

Erarbeitete Lösungen:

* .
* .
* .

## 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 Begriffen alphabetisch sortiert.

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

Tabelle Glossar

# Quellenverzeichnis

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

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

Tabelle Quellenverzeichnis

# Abbildverzeichnis

[Abbildung 1 Testumgebung 17](file:///C:\Users\z00476rn\Desktop\2_Lehrjahr\63_WatchGuard_IPA\Vorlagen\05_Nideröst_IPA-Bericht.docx#_Toc160200958)

[Abbildung 3 Zeitplan 20](file:///C:\Users\z00476rn\Desktop\2_Lehrjahr\63_WatchGuard_IPA\Vorlagen\05_Nideröst_IPA-Bericht.docx#_Toc160200959)

[Abbildung 7 cRSP Anmeldung an Client 43](#_Toc160200960)

# Tabellenverzeichnis

[Tabelle 1 Änderungsnachweis 2](#_Toc160200966)

[Tabelle 2 Kandidat 6](#_Toc160200967)

[Tabelle 3 Bewertungskriterium 1 8](#_Toc160200968)

[Tabelle 4 Bewertungskriterium 2 9](#_Toc160200969)

[Tabelle 5 Bewertungskriterium 3 10](#_Toc160200970)

[Tabelle 6 Bewertungskriterium 4 11](#_Toc160200971)

[Tabelle 7 Bewertungskriterium 5 12](#_Toc160200972)

[Tabelle 8 Bewertungskriterium 6 13](#_Toc160200973)

[Tabelle 9 Bewertungskriterium 7 14](#_Toc160200974)

[Tabelle 11 Tätigkeiten Tag1 21](#_Toc160200975)

[Tabelle 12 Tätigkeiten Tag2 22](#_Toc160200976)

[Tabelle 13 Tätigkeiten Tag3 23](#_Toc160200977)

[Tabelle 14 Tätigkeiten Tag4 24](#_Toc160200978)

[Tabelle 15 Tätigkeiten Tag5 25](#_Toc160200979)

[Tabelle 16 Tätigkeiten Tag6 26](#_Toc160200980)

[Tabelle 17 Tätigkeiten Tag7 27](#_Toc160200981)

[Tabelle 18 Tätigkeiten Tag8 28](#_Toc160200982)

[Tabelle 19 Tätigkeiten Tag9 29](#_Toc160200983)

[Tabelle 20 Tätigkeiten Tag10 30](#_Toc160200984)

[Tabelle 24 Testkonzept 36](#_Toc160200985)

[Tabelle 26 Vollständigkeitstest 53](#_Toc160200986)

[Tabelle 27 Glossar 55](#_Toc160200987)

[Tabelle 28 Quellenverzeichnis 55](#_Toc160200988)

# Anhang

### Datenname?