

Abnahmeprotokoll

Projekttitel: **Netzwerkanalyse eines Enterprise Netzwerks (Argos)**
Auftraggeber: **Christian Schöndorfer, August Hörandl**
Auftragnehmer: **Lorenz Stechauner / Argos**
Schuljahr: **2019/20** Klasse: **5CN**

VERSION	DATUM	AUTORIN/AUTOR	ÄNDERUNG
v1.0	31.03.2020	Lorenz Stechauner	Erstellung
V2.0	01.04.2020	Thomas Hilscher	Abnahme der Ziele

Inhaltsverzeichnis

1	Grundlage der Abnahme	2
2	Bedeutung der Abnahme	2
3	Abnahmekriterien	3
3.1	Hauptziele	3
3.2	Optionale Ziele	6
4	Unterzeichnung	8

1 Grundlage der Abnahme

Die gegenständliche Abnahme basiert auf dem Vertrag und Projektauftrag vom 18.09.2019, Argos_DA_Antrag_v1.1.pdf.

2 Bedeutung der Abnahme

- Der Auftraggeber bestätigt mit der Abnahme die inhaltliche und ablauftechnische Ordnungsgemäßheit sowie die Vollständigkeit der Installation und der damit verbundenen Dokumentationen. Sämtliche Dienstleistungen, die zur Erreichung der definierten Projektziele erforderlich sind, wurden zur Gänze erbracht.
- Beim Auftreten von Mängeln, die in ihrem Verhalten die Funktionsfähigkeit des Vertragsgegenstandes einschränken oder behindern, erfolgt eine neuerliche Abnahme der beanstandeten Punkte (Nachabnahme) nach Behebung durch den Auftragnehmer (wesentliche Mängel), was zu einem nur teilweise oder einem nicht erfüllten Ziel führt. Wesentliche Mängel müssen bei expliziter Aufforderung innerhalb eines gemeinsam definierten Zeitraumes vom Auftragnehmer behoben werden. Ein wesentlicher Mangel beschreibt in jedem Fall eine grobe Beeinträchtigung der Grundfunktion.
- Mängel, die eine Verwendung des Vertragsgegenstandes weder behindern noch einschränken, werden abgenommen. Unwesentliche Mängel sind als Ablehnungsgrund für die Abnahme nicht zulässig und gelten daher als erfüllt. Ein unwesentlicher Mangel beschreibt jene Fehler, welche die Funktionsweise der Implementation nicht beeinträchtigen.
- Mit dem Datum der Unterzeichnung gilt das angeführte Projekt mit Ausnahme der Beanstandungen wesentlicher Mängel als abgenommen. Darüberhinausgehende Änderungen und Erweiterungen am Vertragsgegenstand müssen zwischen Auftraggeber und Auftragnehmer vereinbart und als neue Aufträge in Rechnung gestellt werden.
- Die Nichterfüllung optionaler Ziele kann nicht als Grund einer Nichtabnahme herangezogen werden. Sollte ein optionales Ziel nicht erfüllt oder nur teilweise erfüllt worden sein, so muss es nicht nachgebracht werden.

3 Abnahmekriterien

3.1 Hauptziele

Ziel	Zielerreichung
<p>Ziel H1 Sammlung der Log-Daten</p> <p>Es wird eine geeignete Syslog-Server-Lösung ausgewählt und aufgesetzt welche Syslog-Nachrichten von diversen Geräten sammelt und an einem zentralisierten Ort speichert.</p>	<input checked="" type="checkbox"/> erfüllt <input type="checkbox"/> teilweise erfüllt <input type="checkbox"/> nicht erfüllt
Anmerkung: <input checked="" type="checkbox"/>	

Ziel	Zielerreichung
<p>Ziel H2 Implementierung einer Packet Capture Lösung</p> <p>Ein Programm wird erstellt, welches Pakete aus einem Netzwerk (z.B. Port-Mirror auf einem Switch) mittels Deep Packet Inspection verarbeitet und gegebenenfalls an eine Speicherlösung weiterleitet.</p>	<input checked="" type="checkbox"/> erfüllt <input type="checkbox"/> teilweise erfüllt <input type="checkbox"/> nicht erfüllt
Anmerkung:	

Ziel	Zielerreichung
<p>Ziel H3 Aufbereitung der ASA Log-Daten</p> <p>Ein Programm wird erstellt, welches bereits gesammelte Log-Daten einer Cisco ASA (Firewall) entgegennimmt und aus diesen Daten technisch nicht relevante Informationen entfernt. Dies ist notwendig, da Logs von Cisco darauf ausgelegt sind von einem Menschen gelesen zu werden, dadurch wird die Datenspeicherung und -verarbeitung erschwert.</p>	<input checked="" type="checkbox"/> erfüllt <input type="checkbox"/> teilweise erfüllt <input type="checkbox"/> nicht erfüllt
Anmerkung:	

Ziel	Zielerreichung
<p>Ziel H4 Speicherung und einfache Verarbeitung der Log-Daten</p> <p>Eine für alle anfallenden Log-Daten geeignete Speicherlösung wird ausgewählt und implementiert. Die Speicherlösung muss auf Datenmengen, die in Netzen, wie z.B. einem EDV-Saal der Schule anfallen ausgelegt sein, ohne die Leistungsfähigkeit zu vermindern. Die Daten sollen in eine für möglichst simple Abfragen geeignete Form (z.B. JSON) gebracht und gespeichert werden.</p>	<input checked="" type="checkbox"/> erfüllt <input type="checkbox"/> teilweise erfüllt <input type="checkbox"/> nicht erfüllt
Anmerkung:	

Ziel	Zielerreichung
<p>Ziel H5 Query Language</p> <p>Es wird ein Konzept für eine Query Language ausgearbeitet und implementiert. So soll es möglich werden mit einfachen Abfragen die gespeicherten Daten in passender Form auszugeben.</p>	<input checked="" type="checkbox"/> erfüllt <input type="checkbox"/> teilweise erfüllt <input type="checkbox"/> nicht erfüllt
Anmerkung:	

Ziel	Zielerreichung
<p>Ziel H6 Visualisierung der Daten</p> <p>Daten, die mithilfe der Query Language abgerufen werden, werden in einem Webinterface grafisch dargestellt, um dem Administrator einen einfachen und schnellen Überblick über die gespeicherten Daten zu ermöglichen.</p>	<input checked="" type="checkbox"/> erfüllt <input type="checkbox"/> teilweise erfüllt <input type="checkbox"/> nicht erfüllt
Anmerkung:	

Ziel	Zielerreichung
<p>Ziel H7 Ergänzen der Daten</p> <p>Ein Programm wird erstellt, welches auf Anfrage hin die Daten mit Informationen aus externen, u.a. öffentlich zugänglichen, Datenquellen (z.B. MAC-Adresse wird in Hersteller übersetzt) ergänzt.</p>	<input checked="" type="checkbox"/> erfüllt <input type="checkbox"/> teilweise erfüllt <input type="checkbox"/> nicht erfüllt
Anmerkung:	

Ziel	Zielerreichung
<p>Ziel H8 Datenschutzkonforme Behandlung von Nutzerdaten</p> <p>Es werden Überlegungen zur Datenschutzkonformen Behandlung der Nutzerdaten betreffend der DSGVO getroffen, welche rechtlichen Probleme dadurch entstehen und wie diese für dieses Projekt gelöst werden könnten. Diese Lösungen werden in allen diesbezüglich relevanten Programmen umgesetzt.</p>	<input checked="" type="checkbox"/> erfüllt <input type="checkbox"/> teilweise erfüllt <input type="checkbox"/> nicht erfüllt
Anmerkung:	

Ziel	Zielerreichung
<p>Ziel H9 Vergleichen verschiedener SIEM-Lösungen</p> <p>Es werden verschiedene, bereits bestehende SIEM-Systeme miteinander verglichen und evaluiert welches am besten für den Anwendungsfall dieses Projektes geeignet wäre.</p>	<input checked="" type="checkbox"/> erfüllt <input type="checkbox"/> teilweise erfüllt <input type="checkbox"/> nicht erfüllt
Anmerkung:	

Ziel	Zielerreichung
<p>Ziel H10 Evaluierung von Deep Packet Inspection auf Firewalls</p> <p>Es wird überprüft, ob der Einsatz von Deep Packet Inspection auf Firewalls ausreichend sinnvolle Informationen liefern kann. Zusätzlich wird auch überprüft ob und wie man verschlüsselte Verbindungen (TLS, SSL, ...) mitverfolgen kann.</p>	<input checked="" type="checkbox"/> erfüllt <input type="checkbox"/> teilweise erfüllt <input type="checkbox"/> nicht erfüllt
Anmerkung:	

Ziel	Zielerreichung
<p>Ziel H11 Evaluierung des Einsatzes von Deep Learning</p> <p>Es wird überprüft, ob und wie der Einsatz von Deep Learning bzw. Machine Learning dabei helfen kann, aussagekräftige Voraussagen über den Netzwerkverkehr treffen kann.</p>	<input checked="" type="checkbox"/> erfüllt <input type="checkbox"/> teilweise erfüllt <input type="checkbox"/> nicht erfüllt
Anmerkung:	

Ziel	Zielerreichung
Ziel H12 Vergleichen verschiedener KI-Systeme Mögliche Deep Learning Modelle (z.B. Supervised, Unsupervised) werden verglichen und es wird für das Projekt ein geeignetes Modell evaluiert.	<input checked="" type="checkbox"/> erfüllt <input type="checkbox"/> teilweise erfüllt <input type="checkbox"/> nicht erfüllt
Anmerkung:	

3.2 Optionale Ziele

Optionales Ziel	Zielerreichung
Ziel O1 Log-Daten aus dem Schulnetz sammeln Die Geräte im Schulnetz werden so konfiguriert, dass sie relevante Log-Daten an einen Server weiterleiten. Dieser Server kann auch im Schulnetz aufgesetzt werden.	<input type="checkbox"/> erfüllt <input type="checkbox"/> teilweise erfüllt <input checked="" type="checkbox"/> nicht erfüllt
Anmerkung:	

Optionales Ziel	Zielerreichung
Ziel O2 Überprüfung der angewendeten Anonymisierung Es werden diverse „Angriffe“ auf die eigenen Systeme ausgeführt, um zu überprüfen, wie sicher die Anonymisierung (Ziel H9) der personen- und nutzerbezogenen Daten tatsächlich stattgefunden hat. Falls durch eine Analyse der Metadaten trotzdem Benutzer identifizierbar sind, wird versucht dieses Problem zu beheben.	<input type="checkbox"/> erfüllt <input type="checkbox"/> teilweise erfüllt <input checked="" type="checkbox"/> nicht erfüllt
Anmerkung:	

Optionales Ziel	Zielerreichung
Ziel O3 Einsatz von Deep Learning Das in H12ausgewählte Modell wird mit gespeicherten Daten trainiert und erste Ergebnisse werden auf ihre Aussagekraft überprüft.	<input checked="" type="checkbox"/> erfüllt <input type="checkbox"/> teilweise erfüllt <input type="checkbox"/> nicht erfüllt
Anmerkung:	

Optionales Ziel	Zielerreichung
<p>Ziel O4 Packet Capture auf Switch in einem Raum durchführen</p> <p>Die in H2 erstellte Lösung wird auf einen Switch in einem Raum (z.B. Raum 261) eingesetzt, um möglichst aussagekräftige Echtdaten zu erhalten. Weiters wird überprüft wie viel Datendurchsatz in Echtzeit überprüfbar ist und ob dieser für den Anwendungsfall des Projekts ausreicht.</p>	<p> <input checked="" type="checkbox"/> erfüllt <input type="checkbox"/> teilweise erfüllt <input type="checkbox"/> nicht erfüllt </p>
<p>Anmerkung:</p>	

Optionales Ziel	Zielerreichung
<p>Ziel O5 Überprüfung der Leistungsfähigkeit</p> <p>Es wird überprüft, ob die Verarbeitung der anfallenden Dateneiner ausreichend großen Testgruppe (z.B. EDV Saal, Raum 261) durch das gesamte System in Echtzeit möglich ist.</p>	<p> <input type="checkbox"/> erfüllt <input type="checkbox"/> teilweise erfüllt <input checked="" type="checkbox"/> nicht erfüllt </p>
<p>Anmerkung:</p>	

4 Unterzeichnung

Hiermit bestätigen die Unterzeichnenden, dass die Abnahme entsprechend den oben ausgefüllten Abnahmekriterien durchgeführt wurde.

Datum der Unterzeichnung: 01.04.2020

Lorenz Stechauner, PL

Christian Schöndorfer, PA

August Hörandl, PA

Unterschrift

Unterschrift

Unterschrift