Agrarfrost GmbH

Projektdokumentation

Zum Abschlussprojekt der Ausbildung zum

Fachinformatiker – Systemintegration

Einführung einer Schwachstellenmanagement-Software, um Schwachstellen der IT-Systeme zu erkennen und zu managen

Prüfung: Winter 2023

Prüfungsteilnehmer:
Finn Schröder
XXXXXXXXXXX
XXXXXXXXXXX

Ausbildungsbetrieb:
Agrarfrost GmbH
Aldrup 3
27793 Wildeshausen

Projektverantwortlicher:
Marcel Plate

Inhaltsverzeichnis

1. Projektbeschreibung

1.1 Einleitung

Das Projekt „Einführung einer Schwachstellenmanagement-Software, um Schwachstellen der IT-Systeme zu erkennen und zu managen“ wurde im Rahmen der Berufsausbildung zum Fachinformatiker für Systemintegration durchgeführt. Diese Dokumentation enthält die Tätigkeiten und Ergebnisse dieses Projekts.

1.2 Ausbildungsbetrieb

Die Agrarfrost GmbH ist ein mittelständisches Familienunternehmen in der Lebensmittelindustrie, welches Kartoffelprodukte herstellt und international vertreibt. Das Unternehmen beschäftigt insgesamt etwa 850 Mitarbeiter. Als IT-Abteilung betreuen wir die IT-Systeme aller Standorte des Unternehmens. Dazu gehören die zwei Produktionsstandorte Aldrup und Oschersleben, sowie Kartoffelläger der Tochterunternehmen, dessen IT-Systeme ebenfalls von uns verwaltet werden. Jährlich werden etwa 250.000 Tonnen Kartoffeln verarbeitet.

1.3 Aufgabenstellung

Da die Verfügbarkeit und Funktionalität der IT-Systeme von Agrarfrost für nahezu alle Prozesse des Unternehmens enorm wichtig sind, ist der Sicherheit dieser Systeme vor äußeren Bedrohungen ebenfalls eine große Bedeutung zuzuweisen. Aus diesem Grund und der EU-Richtlinie NIS2, welche im Oktober 2024 in Kraft tritt, hat sich das Unternehmen dazu entschieden eine Schwachstellenmanagement-Software einzuführen. Dadurch möchte das Unternehmen die rechtlichen Anforderungen erfüllen und die IT-Systeme präventiv vor möglichen Cyberangriffen durch Ausnutzung von Schwachstellen schützen.

Im Rahmen dieses Projektes soll die Auswahl und Implementierung einer solchen Schwachstellenmanagement Software stattfinden.

1.4 Projektteam

Das Projektteam bestand aus dem Projektverantwortlichem Herr Plate und mir. Herr Plate initiierte das Projekt und stand in seiner Funktion als Informationssicherheitsbeauftragter für Fragen und Anforderungen beratend zur Seite.

1.5 Projektumfang

Der zeitliche Umfang des Projektes wurde auf 40 Arbeitsstunden festgelegt.

2. Planungsphase

2.1 Ablauf der Planungsphase

Zu Beginn des Projektes erfolgte ein Kick-Off-Meeting zwischen Marcel Plate, dem Informationssicherheitsbeauftragten (kurz ISB) der Firma, und mir. In diesem Meeting wurde zunächst der Bedarf einer solchen Software, aufgrund des bisherigen Umgangs mit Schwachstellen, sowie durch die Anforderungen einer abgeschlossenen Cyber-Versicherung und der aufkommenden Regulierung durch die NIS2 Richtlinie, besprochen. Die Verantwortung, das Projekt durchzuführen, wurde daraufhin an mich übertragen. Als erstes sollte die aktuelle Situation beschrieben, und die sich daraus ergebenen Probleme genannt werden, um daraufhin die Anforderungen an eine Schwachstellenmanagement-Software zu definieren. Aus diesen Anforderungen sollte dann ein Soll-Konzept erstellt werden. Als nächstes musste die Struktur des Projektes zeitlich geplant werden. Daraufhin sollten auf Grundlage des Soll-Konzepts mögliche Anbieter ausgewählt werden.

2.2 IST-Analyse

Für die IT-Systeme des Unternehmens gibt es bislang keinen automatisierten oder manuell durchgeführten, definierten Management Prozess, um Schwachstellen aufzudecken und zu schließen. Lediglich für Windows-Systeme werden regelmäßig die neuesten Updates ausgerollt. Andere Updates und Fehlkonfigurationen, welche zu Schwachstellen auf den IT-Systemen führen, werden derzeit nur nach dem Bekanntwerden dieser Schwachstellen behoben. Dies erfolgt manuell durch Internetrecherchen der Administratoren. Da der Einsatz von verschiedenen Legacy-Systemen[1], aufgrund von Softwarekompatibilität, nicht vermeidbar ist, können Softwareaktualisierungen auf den betroffenen Systemen nicht bedingungslos durchgeführt werden.

Diese manuelle Vorgehensweise nimmt zum einen viel Zeit in Anspruch, zum anderen ist es so unmöglich kontinuierlich alle Schwachstellen für alle Systeme zu kennen und zu schließen.

2.2.1 Ermittlung der Geräteanzahl

Um bei den ausgewählten Anbietern ein Angebot für die Lizensierung unserer Geräte anzufragen, musste zunächst die Anzahl der Geräte ermittelt werden. Hierfür wurde das bereits vorhandene Asset Management[2] System zur Hilfe genommen. Die Geräte wurden in verschiedenen Geräteklassen unterteilt. Dabei wurde beschlossen, dass Mobilgeräte, wie Firmenhandys und Tablets, nicht berücksichtigt werden sollten, da diese Geräte zukünftig mit einem Mobile Device Management (kurz. MDM)[3] überwacht und abgesichert werden.

Geräteklasse	Anzahl
Workstation	772
Server	164
Netzwerkinfrastruktur	
Switch	172
Router	37
Access Points	113
Telefonie	392
Drucker	219
Produktionsmaschinen	800
Sicherheit	
Kameras	122
Zutrittskontrolle	19
Sensoren & Alarmanlagen	30
Sonstige	50
Gesamt	**3433**

Tabelle 1 - Ermittlung der Geräteanzahl

Es ergab sich eine Gesamtzahl von 3433 Assets. Da diese Anzahl in Zukunft weiterwachsen wird, hat man sich dazu entschieden, bei den Anbietern die Lizensierung von 3500 Assets anzufragen.

[1] Siehe Glossar: Legacy-Systeme
[2] Siehe Glossar: Asset Management
[3] Siehe Glossar: MDM

2.3 SOLL-Konzept

Mit dem Abschluss des Projektes soll eine Lösung implementiert sein, welche auf allen IT-Systemen Schwachstellen mithilfe von CVE-Listen[4] identifiziert. Diese sollen automatisch anhand von Wichtigkeit der betroffenen Systeme und Auswirkungen der Schwachstellen, sowie aktuellem Risiko, bewertet werden. Diese automatisch vorgenommene Einordnung der Schwachstellen soll auch manuell angepasst werden können, so dass eine eigene Gewichtung stattfinden kann. Zudem soll die eingeführte Software-Anleitungen dafür bieten, wie die Sicherheitslücken geschlossen werden können. Dadurch sollen die Verantwortlichen der IT-Abteilung einen Überblick über die Schwachstellen der Systeme erhalten und diese kontinuierlich schließen. Die eingeführte Lösung soll den Fortschritt dieses Prozesses darstellen können.

2.4 Marktüberblick

Eine umfangreiche Marktanalyse hat ergeben, dass es mehrere Lösungen gibt, welche die beschrieben Anforderungen erfüllen. Darunter sowohl kommerzielle Anbieter als auch eine kostenlose Open Source[5] Lösung. Wir haben uns dazu entschieden die Lösungen der Anbieter Crowdstrike, Rapid7 und die Open Source Lösung von Greenbone zu vergleichen.

2.4.1 Crowdstrike – Falcon Spotlight

Crowdstrike bietet mit Falcon Spotlight eine Cloud basierte Lösung, welche die Daten über die Systeme mithilfe von lokalen Agenten auf den Zielsystemen sammelt. Dieser Agent sendet die Daten über das Internet an die Cloud, wo die Daten anschließend ausgewertet und dargestellt werden. Die Verwaltung erfolgt über ein Webinterface im Browser, welche über das Internet aufrufbar ist.

Falcon Spotlight wurde in die Auswahl mit aufgenommen, da das Unternehmen bereits die Endpoint Protection Lösung des Anbieters im Einsatz hat und die für diese Lösung benötigten Agenten somit bereits auf den Systemen installiert sind. Zudem kann die Lösung in die bereits bestehende Webinterface eingebunden werden.

Aufgrund der benötigten Agenten für die Erfassung der Daten, deckt Falcon Spotlight allein nicht alle IT-Systeme des Unternehmens ab, da dieser nicht auf allen Systemen installiert werden kann. Da das Unternehmen jedoch bereits die Agenten von Crowdstrike für die Endpoint Protection im Einsatz hat, und die Schwachstellenmanagement Lösung mit demselben Agenten arbeitet und in die bestehende Weboberfläche integriert werden kann, wurde entschieden, diese Lösung zu testen.

Um die Anforderung, alle IT-Systeme abzudecken, zu erfüllen, wird hierzu also noch eine weitere Software benötigt, welche die üblichen Systeme (Switches, Router, Firewalls) auf Schwachstellen überprüft. In diesem Fall wurde OpenVAS als Ergänzung in Betracht gezogen, um die Lösung zu vervollständigen.

2.4.2 Greenbone – OpenVAS

Die Community Edition von OpenVAS ist ein Open Source Projekt, welches auf einem Linux Server installiert werden kann. Es bietet die Möglichkeit, Geräte über das Netzwerk zu scannen. Dabei werden die Systeme auf offene Ports und Fehlkonfigurationen durch vordefinierte Schwachstellentests geprüft. Dazu greift das System auf eine Datenbank zurück, welche diese Tests bereitstellt. Anschließend werden die Ergebnisse dieser Tests mit einer Datenbank an bekannten Schwachstellen verglichen.

[4] Siehe Glossar: CVE
[5] Siehe Glossar: Open Source

OpenVAS bietet die Möglichkeit alle IT-Systeme auf Schwachstellen zu scannen. Daher wurde zum einen in Betracht gezogen, ob OpenVAS als einzige Lösung für alle Systeme implementiert werden soll, oder in Kombination mit Falcon Spotlight von Crowdstrike.

OpenVAS wird direkt vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlen und wurde deshalb in diese Auswahl mit aufgenommen[6].

2.4.3 Rapid7 – InsightVM

Rapid7 bietet mit InsightVM eine Lösung, welche die Geräte sowohl mit installierten Agenten als auch mit Scans über das Netzwerk auf Schwachstellen prüfen kann. Somit können auch mit dieser Lösung alle Geräte gescannt werden. Die Installierten Agenten bieten den Vorteil, dass nicht jedes System aktiv über das Netzwerk gescannt werden muss, was weniger Netzwerkauslastung verursacht.

Es ist eine hybride Lösung, wobei der Netzwerkscanner und die Datenbank für die Speicherung der Daten, sowie die Auswertung der Schwachstellen, auf einem On Premise Server betrieben werden. Einige Funktionalitäten, wie eine Dashboard Ansicht und die Erstellung von Berichten werden in der Public Cloud von Rapid7 bereitgestellt. Durch Menüpunkte in der Weboberfläche des On Premise Servers sind diese Funktionalitäten aufrufbar.

Rapid7 wurde aufgrund der Marktführenden Position und sehr großen Erfahrung im Bereich Schwachstellenmanagement in die Auswahl aufgenommen.

2.5 Lösungskonzepte im Überblick

1.	2.	3.
Crowdstrike Falcon Spotlight für Endgeräte + OpenVAS für übliche Geräte	OpenVAS für alle Geräte	Rapid7 InsightVM für alle Geräte
Cloud + On Premise	On Premise	Cloud + On Premise

Tabelle 2 - Lösungskonzepte im Überblick

2.6 On Premise oder Cloud

Die vorgestellten Lösungen verfolgen bei der Wahl zwischen On Premise oder Cloud unterschiedliche Ansätze. Da sich die Netzwerkscanner der Lösungen OpenVAS und InsightVM im internen Netzwerk befinden müssen, um die Zielsysteme zu erreichen, müssen diese On Premise betrieben werden. Dieser Server kann entweder virtualisiert oder als physische Hardware installiert werden. Das Unternehmen besitzt mit VMware eine virtuelle Infrastruktur, welche ausreichende Ressourcen für die benötigten Server besitzt und auf der auch alle anderen neuen Systeme bereitgestellt werden. Das Bereitstellen einer virtuellen Maschine bietet den Vorteil, dass die benötigten Ressourcen für die Testphase zunächst minimal gehalten werden können und bei einem Übergang in den Produktivbetrieb anschließend ohne großen Aufwand hochskaliert und an temporäre Leistungsspitzen angepasst werden können.

Daher wurde entschieden, die benötigten Server virtuell bereitzustellen. Da es sich bei den gesammelten Daten der Lösungen nicht um personenbezogene Daten handelt, wird auch die Umsetzung der Cloud basierten Lösungen von Crowdstrike und Rapid7 nicht ausgeschlossen.

[6] Siehe Quellen: BSI-Empfehlung für OpenVAS

3. Angebots und Testphase

3.1 Kontaktaufnahme mit ausgewählten Anbietern

Um Angebote und Testlizenzen von den Anbietern zu bekommen, musste nur für die Lösungen Falcon Spotlight und InsightVM der Kontakt zu den Anbietern aufgenommen werden. OpenVAS konnte direkt über eine Installationsanleitung installiert werden.

Die Einholung eines ersten Angebots für Falcon Spotlight erfolgte über unseren bereits bestehenden Kontakt von Crowdstrike, welche uns sehr zeitnah ein Angebot zukommen ließ. Dabei wurde uns auch die Lösung „Exposure Management“ von Crowdstrike empfohlen, welche zusätzlich zum darin enthaltenen Vulnerability Management mit Falcon Spotlight noch weitere Features beinhaltet. Um einen sogenannten Scope Creep, also die schleichende Ausweitung des Projektes, zu verhindern, wurde diese Lösung von mir nicht betrachtet. Der Projektverantwortliche Herr Plate prüfte jedoch, ob die angebotene Lösung einen Mehrwert bietet. Letztlich wurde beschlossen, dass die zusätzlich angebotene Lösung „Exposure Management“ keine Vorteile bietet, welche wir in naher Zukunft nutzen würden, und einen Aufpreis rechtfertigen. Somit beschränkte sich die Auswahl weiterhin auf Falcon Spotlight. Zeitnah wurde auch eine Webdemonstration der Software vereinbart, wobei die grundlegenden Funktionen erläutert wurden.

Mit dem Anbieter Rapid7 bestand bislang noch kein Kontakt. Nach der Kontaktaufnahme über ein Formular zur Produktanfrage auf deren Internetseite, meldete sich der Anbieter per Telefon und es wurde ein erstes Meeting für eine Webdemonstration des Produkts vereinbart, wobei ein vielversprechender erster Eindruck der Software erlangt wurde. Am Ende dieses Meetings wurde bereits ein unverbindlicher Preis genannt. Daraufhin wurde ein weiteres Meeting für die Installation einer Testversion vereinbart.

3.2 Vorbereitung der Server

Für die Installation der Testversion von InsightVM und OpenVAS wurde jeweils ein On Premise Server benötigt. Ausgehend von der Entscheidung, die vorhandene virtualisierte Infrastruktur zu nutzen, wurden diese Server mithilfe des Hypervisors-vSphere bereitgestellt.

Für InsightVM wurde ein Windows Server 2022 mit 4 CPU-Kernen, 16GB RAM und 250 GB Festplattenspeicher bereitgestellt. Die Anforderungen an diesen Server wurden vor in einer E-Mail mitgeteilt. Für die Windows Server Version wird mindestens die Version 2016 benötigt. Es wurde entschieden die Version 2022 zu nutzen, da man somit auf dem aktuellen Stand ist und Agrarfrost sich momentan in einem Prozess befindet, bei dem nach Möglichkeit alle Server auf die Version 2022 geupdatet werden. Dieser Server wurde anschließend manuell in die Domaine aufgenommen, wodurch er durch die globalen Gruppenrichtlinie automatisch in die Verwaltung des Windows Server Update Service (WSUS) aufgenommen wurde.

Für OpenVAS wird ein Linux Server mit mindestens 2 CPU-Kernen, 4GB RAM und 20GB freiem Festplattenspeicher benötigt. Die Linux Distribution war zwischen Debian, Ubuntu, Fedora und CentOS frei wählbar. Da für die Linux basierten Server im Unternehmen Debian als Betriebssystem verwendet wird, wurde auch für diesen Server Debian in der Version 12 gewählt, um die Homogenität der Serverlandschaft zu wahren. Zudem wurde direkt bei der Installation SSH und der Apache Web-Server installiert, um den Server später per SSH zu administrieren und das Webinterface von OpenVAS aufzurufen.

3.3 Netzwerkeinrichtung

Den beiden Servern wurde jeweils eine freie IPv4 Adresse in einem Subnetz für Server statisch zugewiesen. Die Ermittlung dieser freien Adressen erfolgte über das Eintragen der Server im eigenen Asset Management der Firma. Dabei werden den Systemen freie Adressen zugewiesen. Der DHCP-Server des Unternehmens ist über ein File-Export mit diesem System verbunden, wodurch die Eindeutigkeit der IP-Adressen gewahrt ist.

3.3.1 Interne Firewall

Da die Server für OpenVAS und InsightVM für die Scans alle internen Netzwerke erreichen und dabei alle Ports der Zielgeräte prüfen müssen, wurde für die beiden Server auf der internen Firewall, welche für den Traffic im internen Netzwerk des Unternehmens eingesetzt wird, eine Richtlinie erstellt, welche dies ermöglicht.

Da der volle Zugriff auf alle Netzwerke von einem einzelnen Host allein ein Sicherheitsrisiko darstellt, bietet InsightVM die Möglichkeit mehrere Server in den einzelnen Netzwerkbereichen zu platzieren. Für die Testphase wurde jedoch nur ein zentraler Server betrieben.

3.3.2 Externe Firewall

Für die Installation benötigten beide Server auch Zugriff auf das Internet. Die Installationsdatei für InsightVM konnte dem Server über das interne Netz zur Verfügung gestellt werden, jedoch benötigte die Aktivierung die Testlizenz das Internet. InsightVM gibt in der Installationsanleitung eine Liste an Adressen heraus, welche erreicht werden müssen. Auf der externen Firewall wurde eine Richtlinie für den Zugriff auf die genannten Adressen erstellt.

OpenVAS benötigte für die Installation den Zugriff auf den Repository-Server[7]. Auch hierfür wurde eine Richtlinie auf der externen Firewall erstellt.

Die Lösung Falcon Spotlight erhält die Daten über Schwachstellen von den Agents. Da Agrarfrost bereits Falcon Complete als Endpoint Protection im Einsatz hat und dafür derselbe Agent verwendet wird, sind die benötigten Firewall-Richtlinien hierfür bereits vorhanden.

3.4 InsightVM Installation

Die Installation der voll umfänglichen Testversion wurde zusammen mit dem Vertriebspartner der Rapid7 durchgeführt. Anschließend wurde die Software aktiviert und die Testphase konnte beginnen. Für die Einführung in die Software stand der Mitarbeiter des Vertriebspartners ebenfalls eine weitere halbe Stunde zur Verfügung.

3.5 OpenVAS Installation

Zugriff per SSH

Die Installation, sowie die Anpassung von Konfigurationsdateien erfolgte über das Command Line Interface (CLI), auf welche Remote per SSH zugegriffen wurde.

ssh orgavas@192.0.2.1

Greenbone stellt für die Installation zwei Möglichkeiten bereit. Wir entschieden uns für die Installation mit Containern[8]. Dafür wurde zunächst ein Benutzer erstellt, auf welchem die Dienste laufen sollten. Anschließend wurde Docker installiert, um daraufhin die benötigten Container herunterzuladen. Dabei kam es zu einem Fehler, aufgrund eines fehlenden öffentlichen Schlüssels, welcher als Teil einer asymmetrischen Verschlüsselung für die Prüfung der Authentizität und Integrität der Pakete verwendet wird. Das Problem wurde behoben, indem

[7] Siehe Glossar: Repository Server
[8] Siehe Glossar: Container

der öffentliche Schlüssel manuell mit dem folgenden Befehl von einem Schlüsselserver heruntergeladen wurde.
sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys

Jetzt konnten die Container heruntergeladen und gestartet werden. Danach war die Weboberfläche von OpenVAS bereits über den Local Host und Port 9392 aufrufbar. Um die Weboberfläche von anderen Systemen aufrufen zu können, wurde nun die Konfigurationsdatei von Docker so angepasst, dass alle IP-Adressen den Dienst erreichen können. Außerdem wurde der Port 9392 auf der Firewall des Debian Servers für ein und ausgehende Verbindungen freigeschaltet. Nun konnte die Weboberfläche auch von Remote Systemen im internen Netzwerk aufgerufen werden. Nach dem ersten Start von OpenVAS mussten die aktuellen Datenbanken für CVEs, NVTs, Portlisten, Scankonfigurationen. heruntergeladen werden. Nachdem dies abgeschlossen war, konnten auch hier die ersten Scans auf ausgewählte Systeme durchgeführt werden.

3.6 Testphase in Testumgebung

Für die Lösung Falcon Spotlight, war keine Testumgebung notwendig. Die Daten wurden bereits von allen Systemen gesammelt, auf denen der Agent installiert war. Dies trifft auf nahezu alle Windows, Linux und macOS Geräte zu. Da die Lösungen InsightVM und OpenVAS mit dem Active-Scanning[9] Ansatz arbeiten und dies unter Umständen zum Ausfall eines Systems führen kann, wurden für die Testphase anfangs von jeder Geräteklasse zunächst nur einzelne oder wenige Geräte ausgewählt, bei denen ein Ausfall keine kritischen Auswirkungen hätte. Dafür wurde ein Windows Client, ein Switch, ein IP-Telefon, ein Access-Point, sowie ein Multifunktionsdrucker bereitgestellt. Für die Scans lassen sich in InsightVM und OpenVAS Ziele erstellen. Diese basieren auf den IP-Adressen der Zielgeräte. Dort können entweder einzelne IP-Adressen, IP-Ranges (z.B. 172.16.0.0 – 172.31.255.255) oder Subnetzwerke in der CIDR-Notation (z.B. 10.0.1.0/24) angegeben werden. Für die ersten Testgeräte wurden die Ziel-IP-Adressen einzeln vorgegeben.

Beide Lösungen können sowohl authentifizierte als auch unauthentifizierte Scans durchführen. Für authentifizierte Scans benötigen sie dafür die Anmeldeinformationen der entsprechenden Ziele für die einzelnen Services (z.B. SSH, SMB, ESXi). Diese Anmeldeinformationen können definiert und bestimmten Zielen zugewiesen werden. Beide Systeme besitzen unterschiedliche Scan-Einstellungen. Diese unterscheiden sich in den Diensten, welche untersucht werden. Somit lassen sich zum Beispiel Scans durchführen, welche Hosts lediglich auf Erreichbarkeit mittels ICMP-Datenpaket prüfen. Die empfohlenen Scan Konfigurationen dienen dazu die meisten Schwachstellen zu identifizieren. Auf die ausgewählten Ziele wurden authentifizierte Scans durchgeführt. Während des Scans wurde die Systemauslastung der Zielgeräte überwacht. Dabei ließen sich keine nennenswerten Auswirkungen feststellen.

Nachdem diese ersten Scans erfolgreich und ohne Systemausfälle abgeschlossen waren, wurden die Ergebnisse miteinander verglichen. Als sichergestellt war, dass die Scans auf die ausgewählten Geräte keine Auswirkungen hatten, wurde die Auswahl an Geräten vergrößert. Da das Unternehmen einzelne Subnetzwerke für bestimmte Geräte besitzt, wurden die Ziele anhand dieser Subnetzwerke definiert.

Die Ausweitung der Testphase führte zu einer Auslastung der Rechenressourcen des OpenVAS-Servers. Die Anfangs zugewiesenen 2 CPU-Kerne mit 8GHz waren voll ausgelastet. Auch der freie Arbeitsspeicher und Festplattenspeicher wurde immer geringer. Der virtuellen

[9] Siehe Glossar: Active-Scanning

Maschine wurden daraufhin zwei zusätzliche CPU-Kerne, 4GB mehr RAM und 40 GB mehr Festplattenspeicher zugewiesen, um den Anforderungen gerecht zu werden.

3.7 Angebotsvergleich

3.7.1 Kostenübersicht

Der Vergleich der Angebote für Falcon Spotlight und InsightVM brachte eine Herausforderung mit sich. Ausgehend von der Berechnung der Anzahl der Assets wurde beschlossen, für InsightVM die Lizensierung von 3500 Assets zu betrachten. Da für Falcon Spotlight jedoch nur 750 Geräte lizensiert werden sollten, wären diese zwei Angebote mit unterschiedlichen Geräteanzahlen kostentechnisch nicht direkt vergleichbar. Um die Kosten der Lösungen Falcon Spotlight und InsightVM miteinander zu vergleichen, wurden deshalb für InsightVM von Rapid7 zwei Angebote angefragt. Zum einen lag ein Angebot für dieselbe Anzahl an Assets, wie für Falcon Spotlight lizensiert werden würden vor, welche bei 750 Stück lag. Zum anderen lag ein Angebot für die Lizensierung von 3500 Assets vor.

Zur Veröffentlichung wurden alle externen Angebote zensiert

	Produkt		
Kostenart	**Crowdstrike Falcon Spotlight**	**Rapid7 InsightVM**	**Greenbone OpenVAS**
Anschaffungskosten	- €	XXXXXXX €	- €
Servicekosten	XXXXXXX €	XXXXXXX €	- €
Lizenzkosten	XXXXXXX €	XXXXXXX €	- €
Lizenzkosten Server	- €	XXXXXXX €	- €
Abschreibungskosten für Server	- €	XXXXXXX €	XXXXXXX €
Kosten für Backups und Service	- €	XXXXXXX €	XXXXXXX €
Summe	**XXXXXXX €**	**XXXXXXX €**	**XXXXXXX €**

Tabelle 3 - Kostenübersicht für 1 Jahre (750 Assets)

Es stellte sich heraus, dass Falcon Spotlight im Vergleich zu InsightVM die deutlich kostengünstigere Lösung ist. Die Lizensierung der 750 Assets ist bei InsightVM zwar etwas günstiger, jedoch kommen dort höhere Servicekosten und Kosten für eine Ersteinrichtung sowie die Kosten für den virtuellen Server hinzu. Bei OpenVAS beschränken sich die Kosten aufgrund der Open Source Lösung auf die Abschreibungskosten der Hardware, sowie Wartungs- und Backupkosten. Insgesamt gibt es somit einen sehr großen Kostenunterschied zwischen den verschiedenen Lösungen. Hierbei ist zu beachten, dass die Kosten für InsightVM bei der Lizensierung von 3500 Assets noch einmal erheblich höher sind, wie nachfolgend zu sehen.

	Produkt
Kostenart	**Rapid7 - InsightVM**
Anschaffungskosten	XXXXXXX €
Servicekosten	XXXXXXX €
Lizenzkosten (3500)	XXXXXXX €
Lizenzkosten Server	XXXXXXX €
Abschreibungskosten für Server	XXXXXXX €
Kosten für Backups und Service	XXXXXXX €
Summe	**XXXXXXX €**

Tabelle 4 - Kostenübersicht Rapid7 InsightVM für 1 Jahr (3500 Assets)

3.7.2 Nutzwertanalyse

Im nächsten Schritt sollte nun eine Nutzwertanalyse der verschiedenen Softwarelösungen durchgeführt werden, um zu entscheiden, welche der Lösungen für unsere Anforderungen die geeignetste ist und ob ein Aufpreis gegenüber den anderen Lösungen gerechtfertigt und hinnehmbar ist. Für die Nutzwertanalyse wurden ausgehend von den definierten Anforderungen Kriterien bestimmt und nach Wichtigkeit für das Unternehmen bewertet. Diese Kriterien lassen sich in die drei Bereiche „Optik & Bedienbarkeit“, „Funktionalität“ und „Anbieter“ unterteilen. Die Gewichtung der Kriterien erfolgte auf einer Skala von 1 bis 5, wobei 1 für „nicht wichtig“ und 5 für „besonders wichtig“ steht. Je nachdem, wie sehr die Lösung das Kriterium erfüllt, wurden Punkte von 0 bis 5 vergeben. Erfüllte die Software das Kriterium im vollen Umfang, wurden 5 Punkte vergeben. Wurde es gar nicht erfüllt wurden 0 Punkte vergeben.

Optik und Bedienbarkeit - Nutzwertanalyse

Alle Systeme erfüllen die grundlegenden Anforderungen an die Software, bezüglich einer graphischen Oberfläche für die Bedienung und Auswertung der Schwachstellen. Allerdings waren die Benutzeroberflächen teilweise unterschiedlich aufgebaut und es gab Unterschiede in der Intuitiven Bedienung der Lösungen.

		Software					
Kriterium	**Gewichtung**	**CrowdStrike Falcon Spotlight**		**Rapid7 InsightVM**		**Greenbone OpenVAS**	
		Wert	Ergebnis	Wert	Ergebnis	Wert	Ergebnis
Benutzeroberfläche	3	5	15	4	12	3	9
Intuitive Bedienbarkeit	5	4	20	3	15	3	15
Summe	8	9	**35**	7	27	6	24

Tabelle 5 - Nutzwertanalyse Optik & Bedienbarkeit

Von allen drei Lösungen hatte Falcon Spotlight die sowohl beste Benutzeroberfläche, was die optische Darstellung anbelangt, als auch die beste Intuitive Bedienbarkeit. Alle Funktionen ließen sich ohne großen Suchaufwand finden und waren an logischen Stellen positioniert. Allgemein ging die Bedienung im Vergleich zu InsightVM deutlich besser von der Hand. Auffällig ist in diesem Zusammenhang auch OpenVAS. Dass die kommerziellen Lösungen optisch besser abschneiden würden, war zu erwarten. Allerdings lag OpenVAS im Bereich intuitive Bedienbarkeit zwar hinter Falcon Spotlight, konnte jedoch mit InsightVM mithalten. Falcon Spotlight hat mit etwas Abstand den besten Eindruck hinterlassen und OpenVAS und InsightVM liegen erstaunlich dicht beieinander

Funktionalität - Nutzwertanalyse

Kriterium	Gewich-tung	Software					
		CrowdStrike Falcon Spotlight		Rapid7 InsightVM		Greenbone OpenVAS	
		Wert	Ergebnis	Wert	Ergebnis	Wert	Ergebnis
Schwachstellenerkennung (Windows, Linux, macOS)	5	5	25	5	25	3	15
Schwachstellenerkennung (Alle übrigen Geräte)	4	0	0	5	20	5	20
Remediations	5	5	25	3	15	3	15
Bewertung der Schwachstellen	4	5	20	4	16	3	12
Filtermöglichkeiten	3	5	15	2	6	3	9
Berichte	3	4	12	3	9	3	9
Wartungsaufwand	2	5	10	3	6	1	2
			0		0		0
Summe	26	29	**107**	25	97	21	82

Tabelle 6 - Nutzwertanalyse Funktionalität

Auch im Bereich Funktionsumfang erzielte Falcon Spotlight insgesamt das beste Ergebnis. Am wichtigsten war hierbei, wie genau die Systeme Schwachstellen erkennen können. Dazu wurde die Anzahl der gefunden Schwachstellen auf identischen Geräten für alle Lösungen verglichen. Für Windows-Systeme fanden die Systeme Falcon Spotlight und InsightVM fast identische Anzahlen an Schwachstellen, welche auch inhaltlich bis auf ein paar unterschiede sehr übereinstimmend waren. Nur OpenVAS wies hier teilweise deutlich weniger Schwachstellen auf. Für die übrigen Geräte wie Switches, IP-Telefone, Drucker etc. konnte Falcon Spotlight keine Punkte vergeben werden. Insight VM und OpenVAS weisen in diesem Bereich jedoch eine sehr ähnliche Genauigkeit auf. Besonders überzeugte Falcon Spotlight bei der Darstellung von Schwachstellen über alle Systeme hinweg und bei den Filtermöglichkeiten. Bei InsightVM gestaltete sich die Suche nach bestimmen Systemen oder Gruppen von Systemen um diese gezielt nach Schwachstellen zu betrachten deutlich aufwändiger. Dort müssen dafür erst einzelne Auswertungen gebaut werden, welche dann viel mehr Zeit in Anspruch nehmen, wohingegen dies bei Falcon Spotlight über einfache Filter in einer Live-Ansicht direkt möglich war. Da OpenVAS die Schwachstellen nur nach dem CVS-Score bewertet und die anderen Systeme hierbei noch andere Aspekte berücksichtigen, fiel dieses Kriterium bei der Open Source Lösung nicht so gut aus. Überraschend war, wie ähnlich die Lösungen InsightVM und OpenVAS in einigen Aspekten waren. Beide benötigen zu Beginn einen hohen Administrationsaufwand, da die Zielbereiche im Netzwerk, sowie Anmeldeinformationen für den Zugang auf die Systeme, zunächst angelegt werden mussten. Da die Datenbanken von OpenVAS im Command Line Interface des Servers manuell aktuell gehalten werden müssen, fällt der Wartungsaufwand bei dieser Lösung am höchsten aus. Mit Falcon Spotlight liegt praktisch kein Wartungsaufwand vor, da dieser komplett von Crowdstrike übernommen wird. Für InsightVM bleibt ebenfalls die Verwaltung des lokalen Windows Servers. Auffällig ist insgesamt, dass Falcon Spotlight trotz fehlender Punkte beim wichtigen Kriterium „Schwachstellenerkennung auf übrigen Geräten“ am meisten Punkte erhalten hat.

Anbieter - Nutzwertanalyse

		Anbieter					
Kriterium	**Gewichtung**	**CrowdStrike Falcon Spotlight**		**Rapid7 InsightVM**		**Greenbone OpenVAS**	
		Wert	Ergebnis	Wert	Ergebnis	Wert	Ergebnis
Marktposition	2	4	8	5	10	4	10
Schnelligkeit	2	5	10	5	10	0	0
Kundenorientierung	3	5	15	5	15	0	0
Summe	7	14	33	15	**35**	0	10

Tabelle 7 - Nutzwertanalyse Anbieter

Bezüglich des Vergleiches zwischen den Anbietern lässt sich sagen, dass die Anbieter Crowdstrike und Rapid7 sehr kundenorientiert waren. Beide haben sehr kurzfristig auf Anfragen reagiert und waren sehr bemüht bei Nachfragen eine Lösung zu ermöglichen. Rapid7 besitzt, jedoch eine leicht höhere Marktposition, da Crowdstrike mit ihrer Lösung noch nicht so lange auf dem Markt ist und daher weniger etabliert ist. Greenbone ist hingegen bereits sehr lange am Markt und wird direkt vom BSI empfohlen. Allerdings konnte Greenbone für Schnelligkeit und Kundenorientierung keine Punkte vergeben werden, da die Open Source Lösung des Anbieters keinen Support beinhaltet.

3.7.3 Auswertung

Crowdstrike bietet mit Falcon Spotlight für die Systeme, auf denen der Agent installiert werden kann, die beste Lösung, welche im Vergleich zu InsightVM deutlich günstiger ist. Der Fokus bei der Beseitigung der Schwachstellen liegt auf genau diesen Systemen, da sie als ein höheres Risiko angesehen werden. OpenVAS bietet für die übrigen Geräte eine gute Lösung, welche den Anforderungen gerecht wird. Mit InsightVM hätte das Unternehmen zwar beides in einer Lösung, jedoch kann hierfür aufgrund des sehr großen Kostenunterschiedes bei der Lizensierung von 3500 Assets und der Qualität der Lösung keine Empfehlung ausgesprochen werden.

Empfehlung: Falcon Spotlight zusammen mit OpenVAS einsetzen.

3.8 Wirtschaftlichkeitsbetrachtung

Um die Wirtschaftlichkeit des Projektes zu beurteilen, wurde ermittelt, wie hoch der Schaden für das Unternehmen bei einem erfolgreichen Ransomware[10] Angriff wäre. Dazu wurde mit einer durchschnittlichen Ausfallzeit des Betriebs von 23 Tagen bei einem Ransomware Angriff gerechnet.

Art	Summe	Einheit
Gesamtumsatz	XXXXXXX €	Jahr
Umsatz pro Tag	XXXXXXX €	Tag
Ausfallzeit Ransomware Angriff (Durchschnitt)	23	Tage
Verlust gesamt	**XXXXXXXX €**	

Tabelle 8 - Wirtschaftlicher Schaden bei Ransomware Angriff

[10] Siehe Glossar: Ransomware

Position	Anzahl	Einheit	Einzel	Gesamtkosten
Personalkosten (Auszubildender 3. Lehrjahr)	40	Stunden	50,00 €	2.000,00 €
Kosten Softwarelizenzen	750	Lizenzen	XXXXXXX €	XXXXXXX €
Kosten Support	1	Support	XXXXXXX €	XXXXXXX €
Serverkosten	1	Server	XXXXXXX €	XXXXXXX €
Gesamt				**XXXXXXX €**

Tabelle 9 – Projektkosten für Falcon Spotlight & OpenVAS

Verglichen mit den Kosten von gerundet etwa XXXXXXX Euro bei einem erfolgreichen Ransomware Angriff auf das Unternehmen mit einer Dauer von 23 Tagen, ist die Investition von XXXXXXX Euro für das erste Jahr gerechtfertigt.

3.9 Vorstellung der Angebote und Entscheidung

Die gesammelten Erkenntnisse aus der Testphase und dem Angebotsvergleich wurden dem Projektleiter und dem Leiter der IT-Abteilung in einem Meeting vorgestellt. Dabei wurde die Empfehlung für die Lizensierung der 750 Geräte mit Falcon Spotlight und der Einsatz von OpenVAS für alle übrigen Geräte ausgesprochen. Die vorgeschlagene Lösung überzeugte die Verantwortlichen. Da für den zeitnah auslaufenden Vertrag der Endpoint Protection Lösung von Crowdstrike eine Vertragsverlängerung bevorstand, sollte in diesem Zusammenhang die Lizensierung von Falcon Spotlight ausgehandelt werden.

Somit war die Kaufentscheidung für Falcon Spotlight für 750 Geräte getroffen. OpenVAS sollte nun schrittweise auf alle Agent-Less[11] Geräte ausgeweitet werden. Dabei sollte für den Rahmen des Projektes zunächst die Konfiguration des Hauptstandorts Aldrup abgeschlossen werden.

Vertragsverhandlungen

Die Verhandlungen für die Vertragsverlängerung von Falcon Complete, für die Endpoint Protection, zusammen mit der Erweiterung um Falcon Spotlight wurden in Zusammenarbeit mit der IT-Leitung durchgeführt. Letztlich wurde dort eine Einigung erzielt und die Vertragsverlängerung zusammen mit Falcon Spotlight für ein weiteres Jahr abgeschlossen.

4. Implementierungsphase

4.1 Installation und Konfiguration

4.1.1 Falcon Spotlight

Da Falcon Spotlight als Software as a Service (SaaS) von Crowdstrike in einer Amazon Cloud bereitgestellt wird, musste wie bereits für die Testphase keine Installation auf eigenen Systemen durchgeführt werden. Die Installation der Agenten war wie erwähnt bereits für alle unterstützten Geräte abgeschlossen und muss zukünftig nur auf neuen Geräten durchgeführt werden. Für Windows Clients gibt es ein über Windows Deployment Services (WDS) bereitgestelltes Installationsimage, welche die Installation des Falcon Agenten beinhaltet. Um die Agenten mit unserem Konto in der Cloud zu verknüpfen, muss bei der Installation ein Schlüssel eingetragen werden. Auch dies ist im WDS-Image bereits enthalten. Für die manuelle Installation des Agenten, zum Beispiel für Serverbetriebssysteme, wurde eine Installationsanleitung geschrieben.

[11] Siehe Glossar: Agent-Less

4.1.2 OpenVAS

Der für die Testphase bereitgestellte Server für OpenVAS konnte für den Produktivbetrieb weiterverwendet werden. In der Testphase wurde das System mit insgesamt 300 Zielgeräten getestet. Aufgrund einer deutlich größeren Geräteanzahl in der Produktivumgebung, mussten die Ressourcen des Servers jedoch hochskaliert werden. Bevor die Änderungen an der virtuellen Maschine vorgenommen wurden, wurde mittels dem Hypervisor vSphere ein Snapshot[12] der VM erstellt. Falls bei den vorgenommen Einstellungen Fehler entstehen, können diese damit im Notfall rückgängig gemacht werden.

4.1.2.1 Festplattenspeicher erweitern

Entscheidend war vor allem der Festplattenspeicher, da die Dateigröße sowie die Anzahl der gespeicherten Berichte, welche automatisch nach jedem Scan erstellt werden und die Daten über die gefundenen Schwachstellen enthalten, deutlich zunehmen würde. Zunächst wurde der VM in den Einstellungen auf dem Hypervisor mehr Festplattenspeicher zugewiesen. Anschließend musste noch die entsprechende Partition auf dem Linux Server erweitert werden.

4.1.2.2 Ziele definieren

Für den Hauptstandort Aldrup wurde für jedes VLAN ein Scan Ziel mit dem entsprechenden IP-Adressbereich erstellt. Diese wurden einheitlich in folgendem Format benannt. „VLAN-ID + Name des VLANS“. Diese Schreibweise für den Namen der Ziele wurde als Standard auch in der Anwenderdokumentation vorgegeben.

Name ▲	Hosts	IPs	Portliste	Anmeldedaten
10 - Computer	192.0.2.0-192.0.4.255	768	All TCP and UDP	SMB:DomainAdmin

Abbildung 1 - Beispiel Zielnetzwerk OpenVAS

4.1.2.3 Schnelligkeit der Scans

Die Schnelligkeit der Scans wird hauptsächlich durch den Arbeitsspeicher der virtuellen Maschine beeinflusst, da jeder Scan eine bestimmte Menge an RAM für die Dauer des Scans in Anspruch nimmt. Bislang wurden gleichzeitig maximal 20 Hosts gescannt, wobei jeweils maximal 4 NVTs gleichzeitig durchgeführt wurden. Dabei können die Scans für ein Subnetzwerk mit der Größe von 254 Hosts bis zu einen Tag dauern. Der Scan eines einzelnen Gerätes dauert etwa 30 Minuten. Da man nicht auf einen schnelleren Abschluss der Scans angewiesen ist, wurde beschlossen den Arbeitsspeicher zunächst bei 8GB zu belassen. Sollte sich diese Anforderung in Zukunft ändern, können nachträglich jederzeit kurzfristige Änderungen vorgenommen werden.

4.1.2.4 Häufigkeit der Scans

Für die Scans auf nicht als kritisch eingestufte Ziele wurden automatisierte Scans eingestellt, welche am Anfang des Monats ausgeführt werden. Die Scans auf kritische Ziele im Produktionsbereich und die dazugehörige Infrastruktur wurden nicht automatisiert und werden nur manuell nach Absprache außerhalb der Produktionszeiten durchgeführt.

4.1.2.4 Automatisierungen der Feed-Daten

Die Aktualisierung der Feeds muss manuell über einen Befehl im CLI durchgeführt werden. Die Aktualität der Schwachstellendaten ist von großer Bedeutung. Um diesen sich immer wiederholenden Prozess zu vereinfachen beziehungsweise zu automatisieren, wurde ein Cron-Job[13] erstellt. Dieser startet jeden Montag um 03:00 Uhr ein Bash-Skript, welches die erforderlichen Befehle enthält.

[12] Siehe Glossar A.8 Snapshot
[13] Siehe Glossar A.9 Cronjob

```
#!/bin/bash
# Befehl zum Ziehen der Docker-Abbilder
docker-compose -f greenbone-community-container/docker-compose.yml -p greenbone-
community-edition pull notus-data vulnerability-tests scap-data dfn-cert-data
cert-bund-data report-formats data-objects
# Befehl zum Starten der Docker-Container im Hintergrund
docker-compose -f greenbone-community-container/docker-compose.yml -p greenbone-
community-edition up -d notus-data vulnerability-tests scap-data dfn-cert-data
cert-bund-data report-formats data-objects
```

Abbildung 2 - Batch-Skript Feed Aktualisierung

```
0 3 * * 1 /tmp/home/adminvas/updatefeed.sh
```

Abbildung 3 - Cronjob Eintrag

4.2 Backup Strategie

Der über den ESXi Host bereitgestellte Server für OpenVAS ist automatisch in die bestehende Backup Strategie von Agrarfrost implementiert. Dadurch wird jede Woche ein Vollbackup aller Server erstellt. Zwischen den Vollbackups werden Differentielle Backups gefahren.

4.3 Richtlinie für Umgang mit Schwachstellen

Um die Sicherheit der IT-Systeme kontinuierlich zu verbessern, wurde für den Umgang mit gefunden Schwachstellen eine Richtlinie aufgestellt. In dieser ist für die Kritikalität der Hosts und Schwachstellen eine Zeit vorgegeben, in welcher die Schwachstellen behoben werden müssen.

Netzwerkposition / Kritikalität	Internes Netzwerk	DMZ
Kritisch	X Tage	X Tage
Hoch	X Tage	X Tage
Mittel	X Tage	X Tage
Niedrig	X Tage	X Tage

Tabelle 10 - Richtlinie zur Behebung von Schwachstellen

Für Systeme in der DMZ gelten strengere Richtlinien, da diese über das Internet und somit einfacher für Angreifer erreichbar sind. Diese Systeme gilt es besonders zu schützen.

Die automatisierte Bewertung der Schwachstellen nach Kritikalität sollte vor der Behebung einer Schwachstelle kritisch geprüft und eventuell manuell korrigiert werden.

4.4 Anwenderdokumentation

Die eingeführten Lösungen werden nur innerhalb der IT-Abteilung genutzt. Um die Mitarbeiter im Umgang mit der Software zu schulen, wurde für Falcon Spotlight und OpenVAS jeweils eine Anwenderdokumentation in der internen Wissensdatenbank bereitgestellt (siehe Anhang).

Für die Administration der Docker Container von OpenVAS wurde eine Dokumentation für Administratoren bereitgestellt (siehe Anhang).

5. Projektabschluss

5.1 Vorstellung der Projektergebnisse

Die Ergebnisse des Projektes wurden der IT-Abteilung vorgestellt. Dies erfolgte mithilfe einer Präsentation, in der die wichtigsten Kennzahlen und Informationen dargestellt wurden.

5.2 Vergleich Projektantrag

Zur ersten Zeitplanung aus dem Projektantrag sind während des Projektes Unterschiede entstanden[14]. Zum einen nahm die Erstellung des Sollkonzeptes mehr Zeit in Anspruch als ursprünglich geplant. Einen größeren Unterschied gab es allerdings bei der benötigten Zeit zwischen Installation der Testversionen und der Installation in der Implementierungsphase. Dies lag vor allem daran, dass die Installation und Konfiguration von OpenVAS für die Testphase viel Zeit in Anspruch nahm. Für die Implementierungsphase entfiel der Schritt der Installation, da der Server für OpenVAS weiterverwendet werden konnte. In der Implementierungsphase nahm die Anpassung von OpenVAS an die Anforderungen mehr Zeit in Anspruch.

5.3 Fazit

Mit den Lösungen Falcon Spotlight und OpenVAS wurde im Unternehmen erfolgreich eine Schwachstellenmanagement-Lösung implementiert, wodurch das Unternehmen eine Übersicht über die bestehenden Schwachstellen der IT-Systemen erhalten hat. Die beiden Lösungen ergänzen sich, um auf allen IT-Systemen Schwachstellen zu identifizieren, einzuordnen und Remediations zu liefern und erfüllen somit alle zuvor definierten Anforderungen. In Zukunft wird das Unternehmen kontinuierlich an der Beseitigung der Schwachstellen Arbeiten und somit die Sicherheit der Systeme verbessern. Im Hinblick auf die kommende NIS2-Richtlinie der EU erfüllt das Unternehmen nun die rechtlichen Anforderungen und kann einen Schwachstellenmanagement-Prozess nachweisen.

[14] Siehe Tabelle Zeitvergleich

6. Anhang

6.1 Anwenderdokumentation OpenVAS

OpenVAS

Open Vulnerability Assessment Scanner

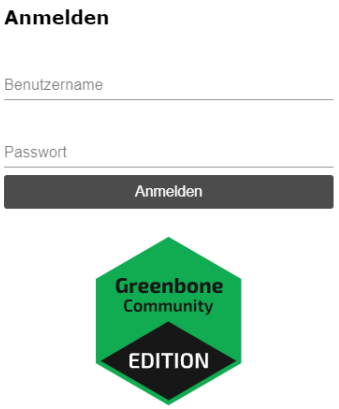
Dokumentation für Anwender

Diese Dokumentation dient der Bedienung von OpenVAS. OpenVAS wird als Schwachstellenmanagement Lösung für alle Geräte eingesetzt, auf denen der Crowdstrike Falcon Agent nicht installiert ist / installiert werden kann.

Aus Sicherheitsgründen wurden IP-Adressen und Schwachstelleninformationen für die Dokumentation zensiert und die IP-Adresse des Servers durch die Adresse 192.0.2.100 getauscht

1 Webinterface aufrufen

http://192.0.2.100:9392/



Die Anmeldung findet über einen Benutzer statt, welcher im Passwortmanager hinterlegt ist (Name: OpenVAS Anmeldung)

2 Navigation

Die Navigation im Webinterface erfolgt über eine Navigationsleiste am oberen Bildschirmrand, welche die Oberpunkte der Navigation darstellt. Bewegen Sie den Mauszeiger über diese Punkte um die untergeordneten Menüpunkte zu sehen.

3 Dashboard Erklärung

Auf der Startseite befindet sich das Dashboard. Dort werden aktuelle Daten in Form von Diagrammen und Tabellen veranschaulicht dargestellt.

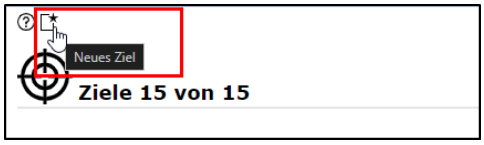
Über das markierte Symbol [1] können weitere Dashboard Ansichten hinzugefügt werden. Per Drag & Drop können die Ansichten verschoben und gelöscht werden.

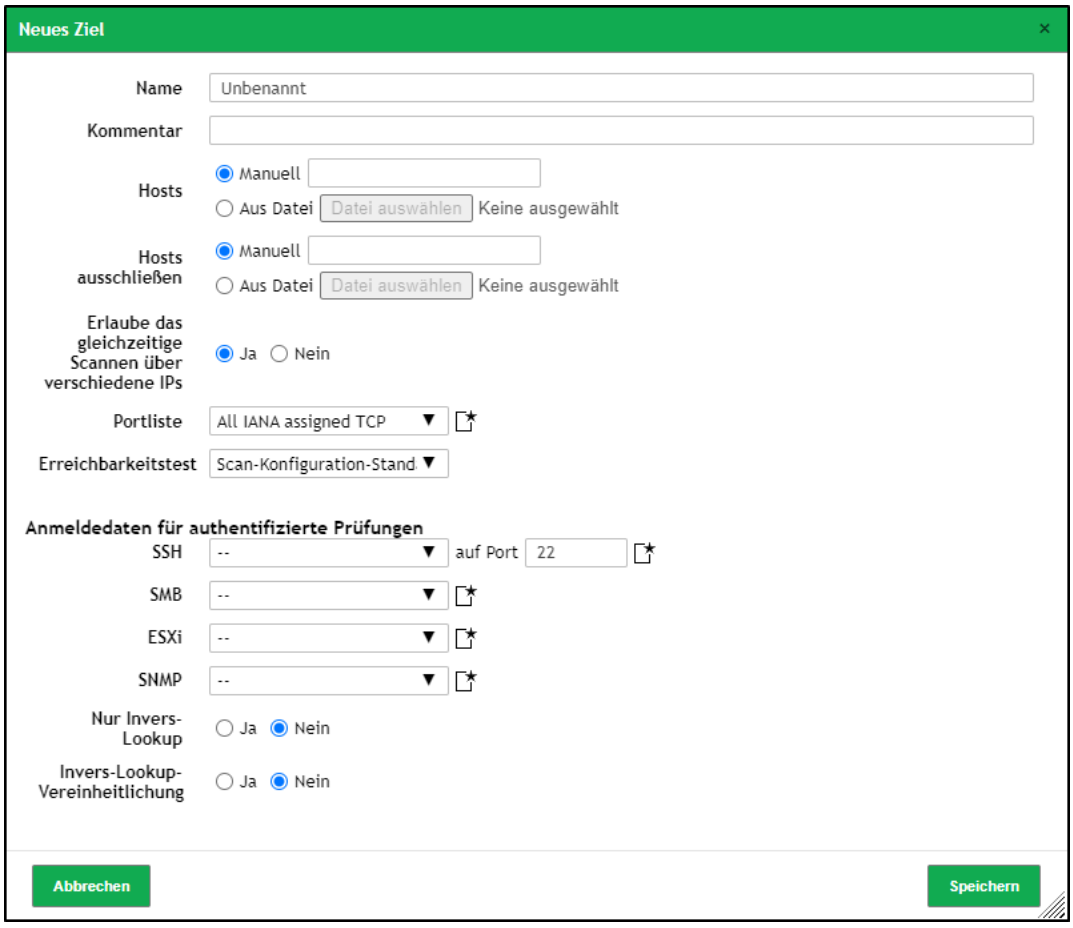
4 Ziele

Um die Ziele zu verwalten, navigieren sie zum Menüpunkt *Konfiguration* > *Ziele*

4.1 Ziel erstellen

Um ein neues Ziel zu definieren, klicken Sie zunächst auf dieses Symbol





Dort können Sie nun das Ziel benennen, einen Zielbereich in Form von IP-Adressen angeben, bestimmte Zieladressen ausschließen und weitere Einstellungen vornehmen. Die Portliste bestimmt, welche Ports auf Schwachstellen untersucht werden. Um genauere Scans durchzuführen, wählen Sie dort die entsprechenden Anmeldedaten z.B. für Windows Hosts aus. Für die genauere Konfiguration dieser Einstellungen sehen Sie in der Anleitung unter Anmeldedaten und Portlisten nach.

4.1.1 Schreibweise IP-Adressen

Für die Angabe der IP-Adressen bei den Zielen sowie den Hosts, welche ausgeschlossen werden sollen, gibt es drei Schreibweisen.

Einzelne IP-Adressen durch Kommata getrennt (192.0.2.1,192.0.2.2…)

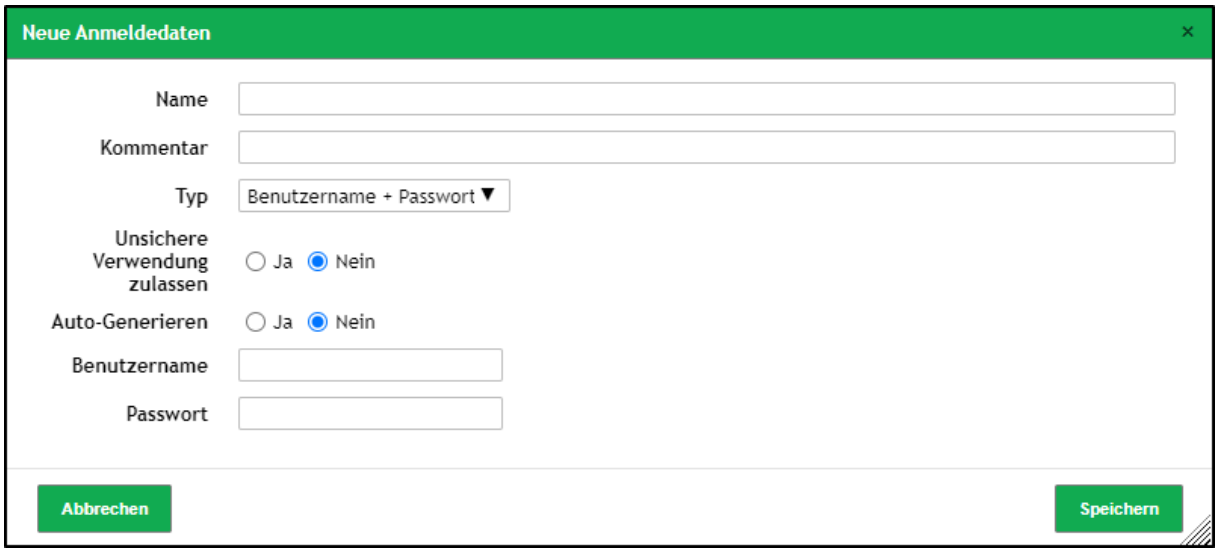
CIDR-Schreibweise (192.0.2.0/24)

IP-Range angeben (192.0.2.0-192.0.4.255 oder 192.0.2.0-255)

5 Anmeldedaten

Damit OpenVAS authentifizierte Scans auf die Zielsysteme durchführen kann, müssen die Anmeldedaten zuvor erstellt werden. Die Verwaltung der Anmeldedaten erfolgt über den Menüpunkt *Konfiguration > Anmeldedaten*

5.1 Neue Anmeldedaten erstellen



Vergeben Sie einen eindeutigen Namen für die Anmeldedaten (z.B. Domainbenutzername)

Tragen Sie den Benutzernamen + Kennwort in die Felder ein

5.1.1 Schreibweise Anmeldedaten

SMB: Domainname\Benutzername (z.B. example.de\admin)

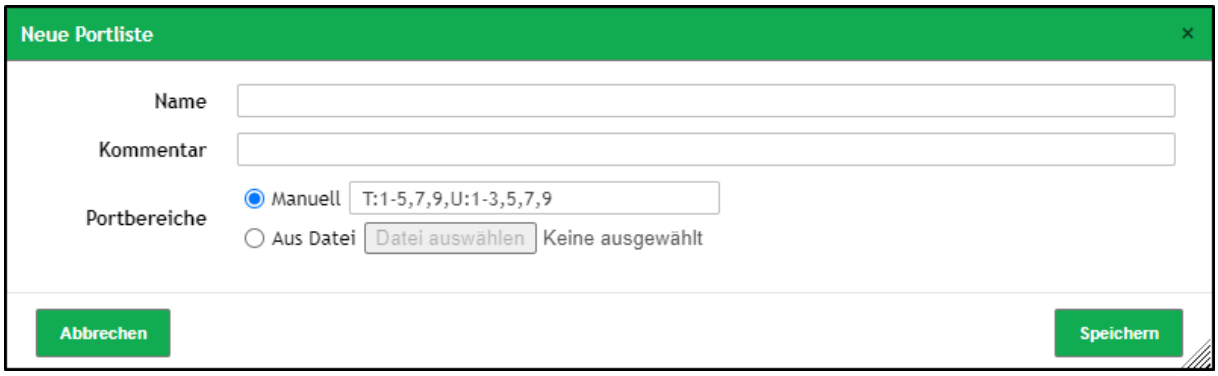
Andere Methoden: Benutzername + Kennwort

6 Portlisten

OpenVAS liefert vordefinierte Portlisten. Diese Listen geben an, welche Ports alle gescannt werden. Die Portliste „All TCP and UDP“ scannt alle TCP und UDP-Ports von 1-65535. Je größer der Portbereich, desto mehr Zeit nehmen die Scans in Anspruch.

Um die Portlisten zu verwalten, navigieren Sie zum Menüpunkt *Konfiguration > Portlisten*

5.1 Neue Portliste erstellen



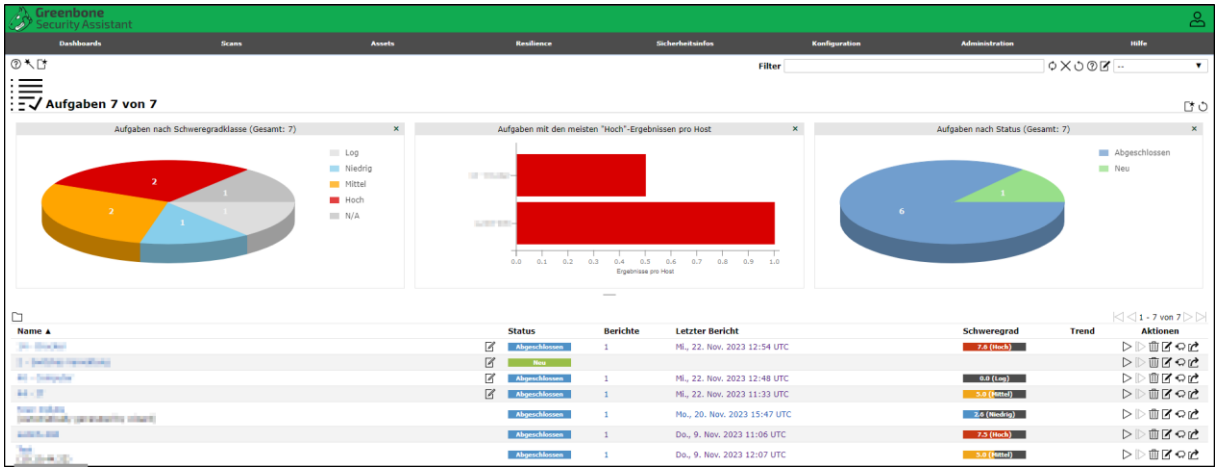
Vergeben sie einen eindeutigen Namen

Portbereich angeben:
T:1-x für TCP-Ports
U:1-x für UDP-Ports

7 Scans

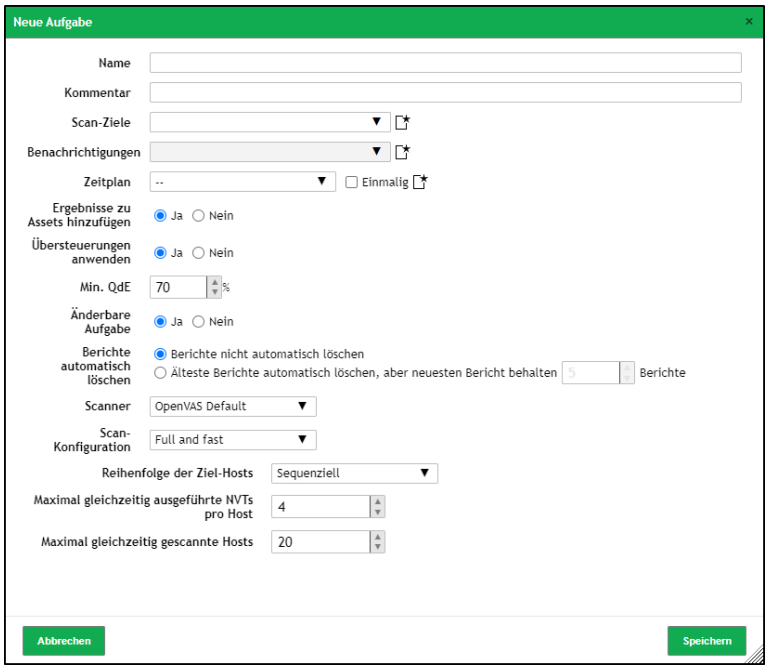
Um einen Scan auf ein Ziel durchzuführen, muss zuvor eine Aufgabe erstellt werden. Navigieren Sie hierzu zum Menüpunkt *Scans* > *Aufgaben*

7.1 Übersicht Aufgaben



Die Startseite der Scan Aufgaben liefert einen Überblick über den Status der aktuellen Scan Aufgaben und über die Ergebnisse der Abgeschlossenen Scans.

7.1 Aufgabe erstellen

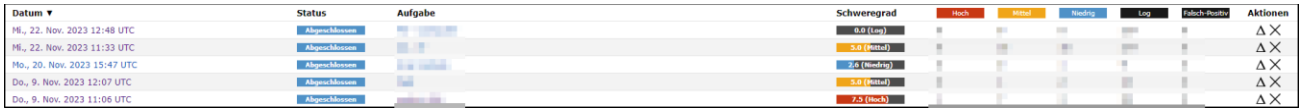


Hier können Sie das Ziel, welches Sie scannen möchten, Auswählen und den Scan konfigurieren. Sie können die Genauigkeit der Scans einstellen und wie viele Hosts gleichzeitig gescannt werden sollen. Dies beeinfluss die Schnelligkeit der Scans. Stellen sie bei Bedarf Benachrichtigungen und einen Zeitplan für die automatisierte Ausführung ein.

8 Berichte

8.1 Berichte auswerten

Die Berichte über abgeschlossene Scans lassen sich zum einen Über einen klick auf den abgeschlossenen Aufgabenstatus einer Aufgabe oder alternativ über den Menüpunkt *Scans* > *Berichte* aufrufen.



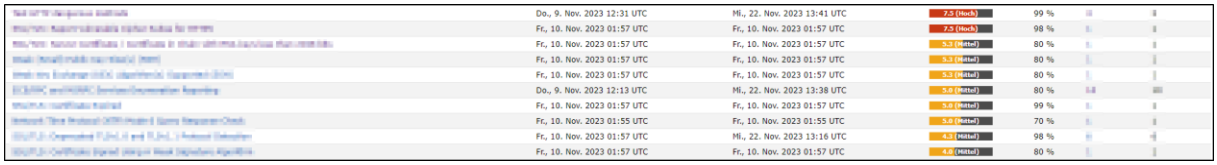
In den Berichten lassen sich folgende Daten zu den Zielen finden.

- Gefundene Schwachstellen, nach Schweregrad sortiert
- Erreichbare Ziele (Hosts)
- Erreichbare Ports
- Anwendungen auf den Systemen
- Betriebssysteme
- Liste der CVEs
- Bereits geschlossene CVEs für die Ziel-Hosts
- TLS-Zertifikate
- Fehlermeldungen (Welche Systeme/ Ports nicht erreichbar sind)
- Um einen Bericht zu öffnen, klicken Sie auf das im obigen Beispiel rot markierte Datum.

9 Schwachstellen

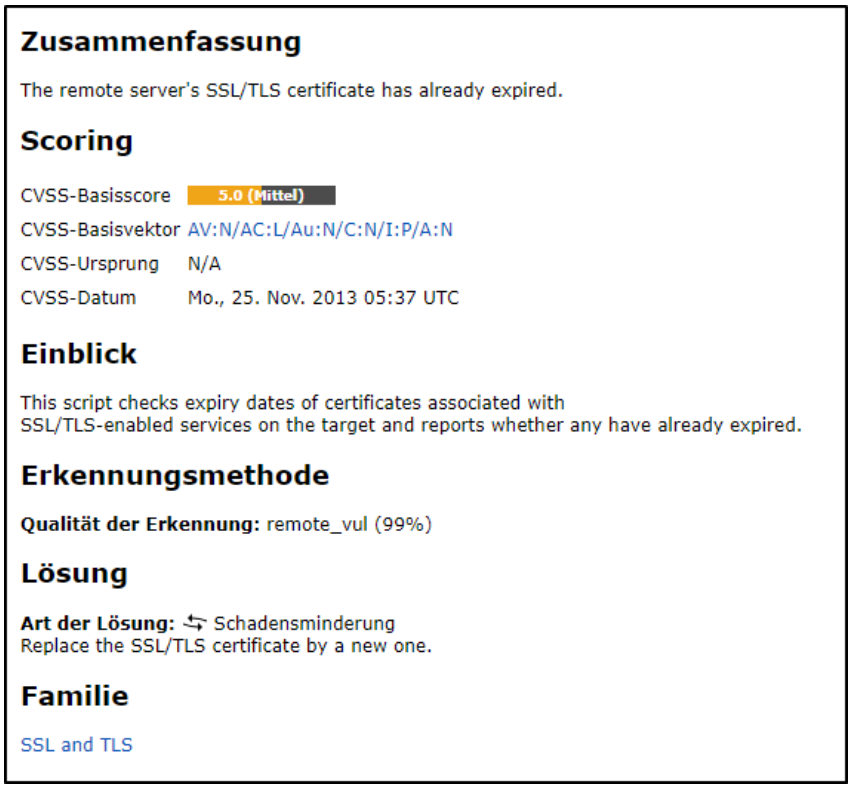
Der Menüpunkt Schwachstellen liefert eine Liste aller gefunden Schwachstellen, welche nach dem Schweregrad absteigend sortiert ist. Somit sind die kritischen Schwachstellen immer an oberster Stelle.

Navigation: *Scans* > *Schwachstellen*



Um weitere Informationen zu einer Schwachstelle zu erhalten, klicken Sie auf den Namen der Schwachstelle.

Hier ist beispielhaft die Übersicht zu einer Schwachstelle welche auf ein ausgelaufenes SSL/TLS-Zertifikat hindeutet.



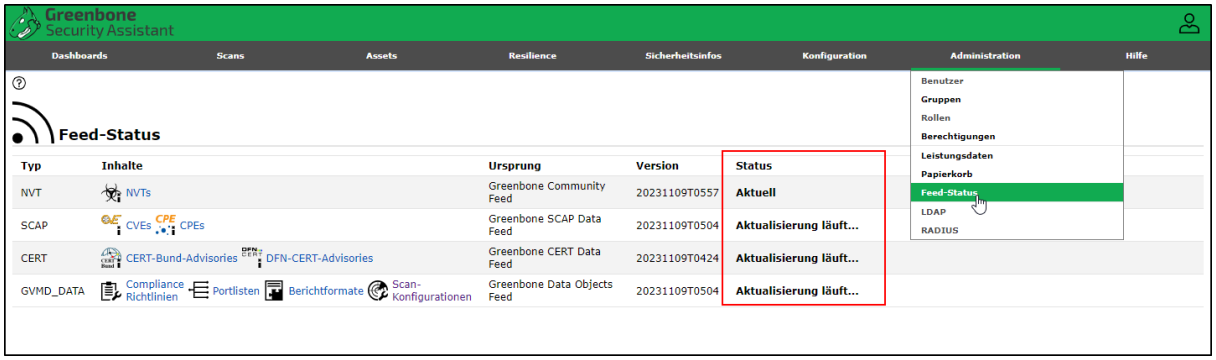
9.1 Remediations

In dieser Übersicht befindet sich auch die Remediation / Lösung der Schwachstelle. Um die Schwachstelle zu beseitigen, führen Sie die Lösungsmethode durch.

9.2 Feed Status kontrollieren

Feeds sind die Daten zu allen bekannten Schwachstellen, Vulnerability Tests, Portlisten, Scan-Konfigurationen, Berichtsformaten und Compliance Richtlinien, welche von Greenbone zur Verfügung gestellt werden.

Um zu kontrollieren, ob diese aktuell sind, navigieren zu *Administration* > *Feed-Status.*



Die Feeds werden wöchentlich automatisiert aktualisiert.

6.2 Anwenderdokumentation Falcon Spotlight

Info: Aus Sicherheitsgründen wurden IP-Adressen, Schwachstellen-IDs und sonstige Daten zu den Systemen des Unternehmens für die Dokumentation zensiert.

Falcon Spotlight ist eine Webanwendung, welche im Unternehmen eingesetzt wird, um Schwachstellen auf den folgenden Systemen zu erkennen und zu managen.

- Windows-Systeme
- Linux-Systeme
- macOS-Systeme

Die Webanwendung ist unter folgendem Link aufzurufen:
XXXXXXXXXXXX

1 Anmeldung

Für die Anmeldung wird ihnen von Informationssicherheitsbeauftragten ein Konto erstellt. Die Anmeldung erfolgt über ihre E-Mail-Adresse des Firmenkontos mit einem von ihnen selbst definierten Kennwort. Zusätzlich findet eine Zwei-Faktor-Authentifizierung in der „Microsoft Authenticator“ App statt.

2 Dashboard Ansicht

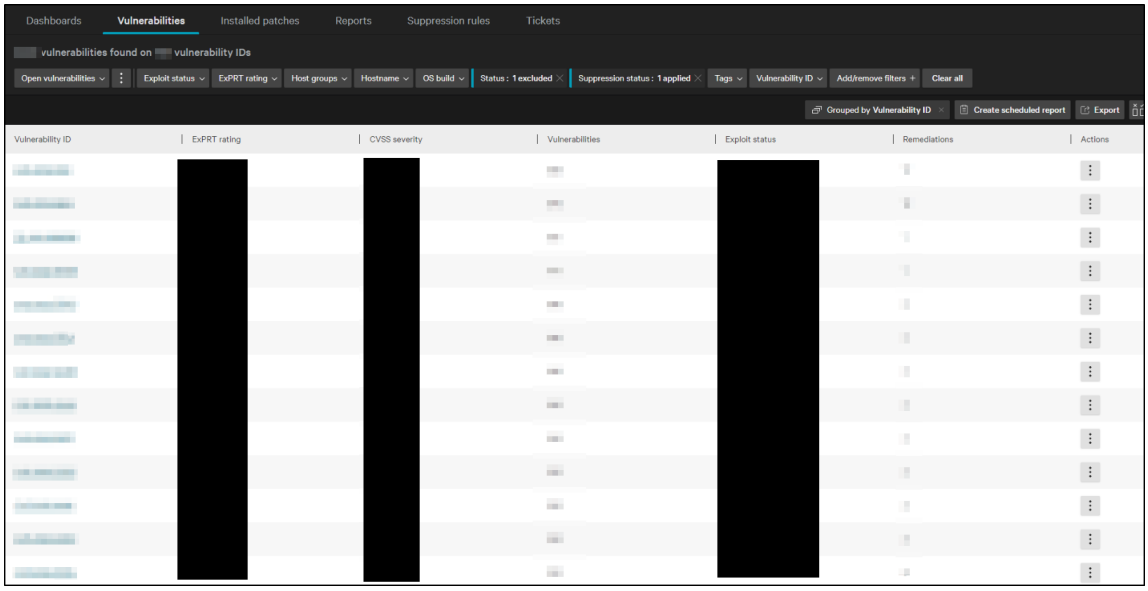
Auf der Startseite befinden sich Dashboards, welche die aktuellen Daten zu offenen Schwachstellen, Anzahl der betroffenen Hosts und Remediations darstellen.

3 Navigation

Die Navigation im Webinterface erfolgt über eine Navigationsleiste am oberen Rand.

4 Schwachstellen

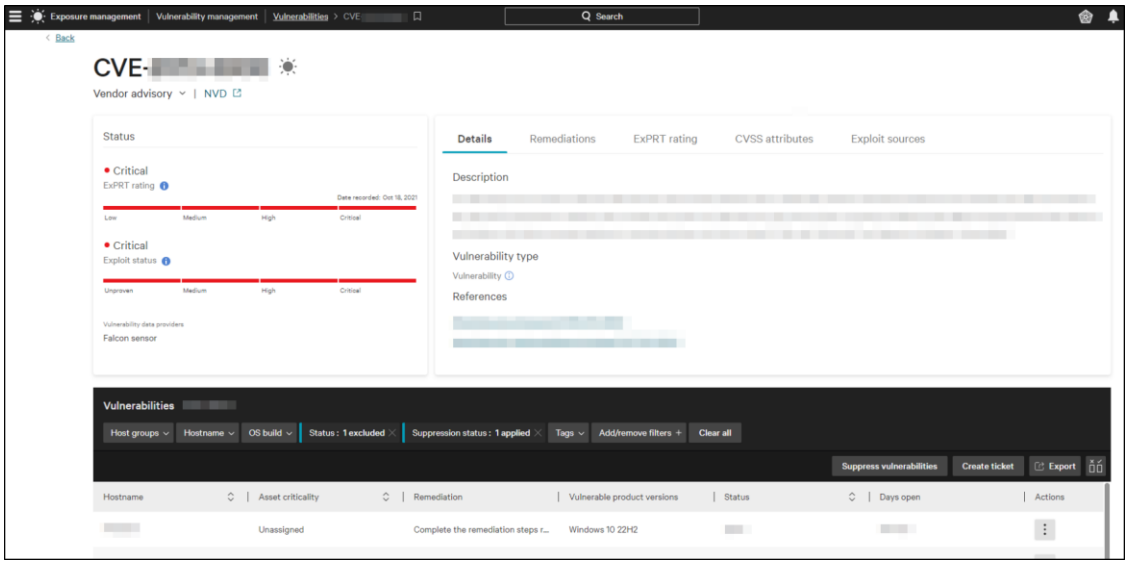
Um eine Übersicht über die gefundenen Schwachstellen zu erhalten, navigieren sie zum Reiter *Vulnerabilitys*



Dort erhalten Sie standardmäßig eine Liste mit den Schwachstellen, welche nach der Anzahl der betroffenen Systeme absteigend sortiert ist. Über Gruppierungen und Filter können sie in dieser Liste nach bestimmen Systemen oder Schwachstellen suchen.

4.1 Schwachstellen untersuchen

Um nähere Informationen zu Schwachstellen und die dazugehörigen Remediations zu erhalten, klicken Sie auf den Namen der Schwachstelle.



Im Rechten Feld können Sie über die Reiter zwischen mehreren Informationen wechseln.

- Details
- Remediations
- ExPRT Rating
- CVSS attributes
- Exploit Status

Darunter erhalten Sie eine Liste aller Hosts, die von der Schwachstelle betroffen sind.

5 Remediations

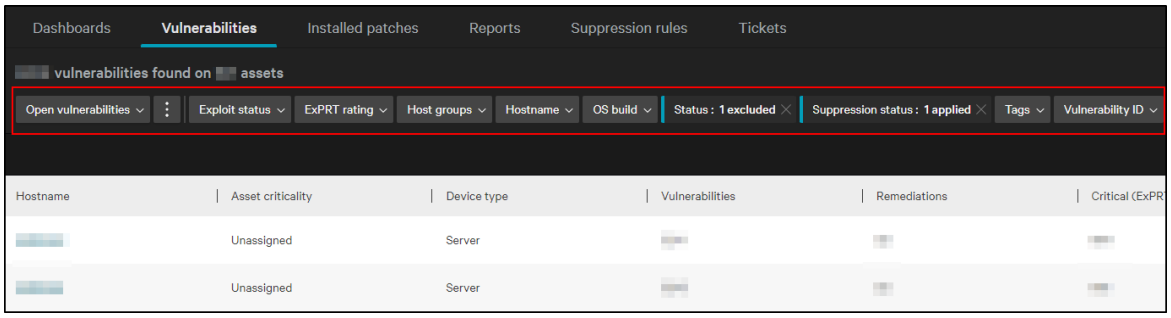
Remediations sind Anleitungen, wie bestimme Schwachstellen geschlossen werden können. Dabei kann das Durchführen einer Remediation mehrere Schwachstellen schließen. In der Dashboard Ansicht ist eine Liste der Remediations, welche am meisten Schwachstellen schließen.

Um eine Liste aller Remediations zu erhalten, navigieren Sie zum Reiter *Remediations.*

6 Filter anwenden

Auf alle Listen zu Schwachstellen, Remediations, Hosts… können Filter angewendet werden.

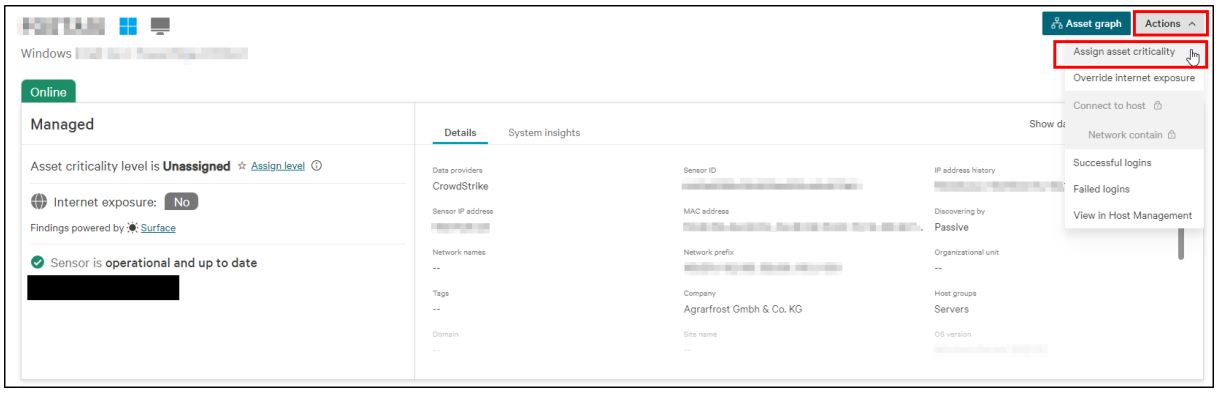
Diese befinden sich oberhalb der Liste. Dort können Sie zu bestimmen Kategorien über ein Drop Down Menü Filter vornehmen und weitere Filter hinzufügen.

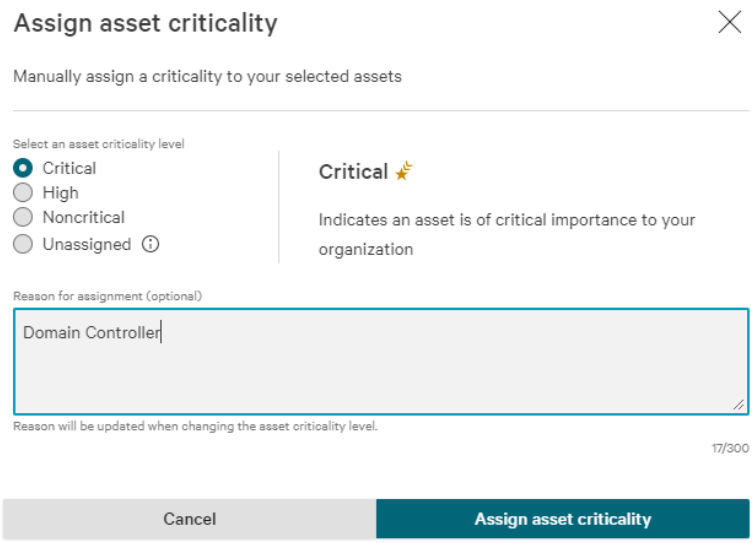


7 Bewertung von Hosts nach Kritikalität

Den Hosts kann eine Kritikalität zugewiesen werden. Dies ist hilfreich um Schwachstellen, welche kritische Systeme betreffen zu identifizieren.

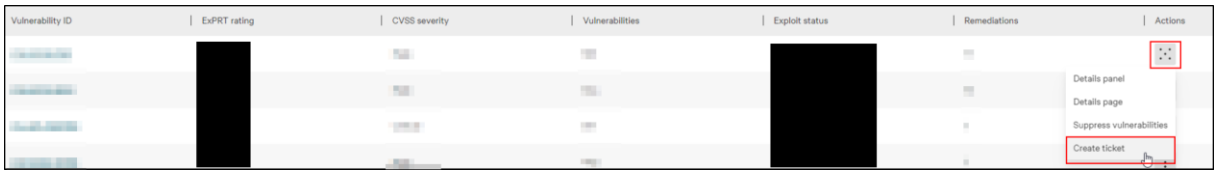
Rufen sie den Hosts aus der Liste der Hosts auf.





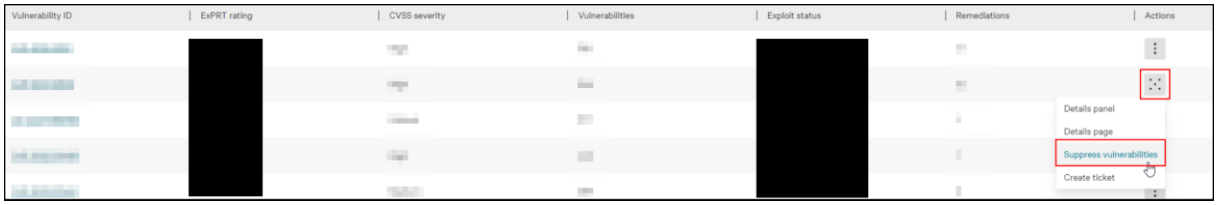
8 Ticket erstellen

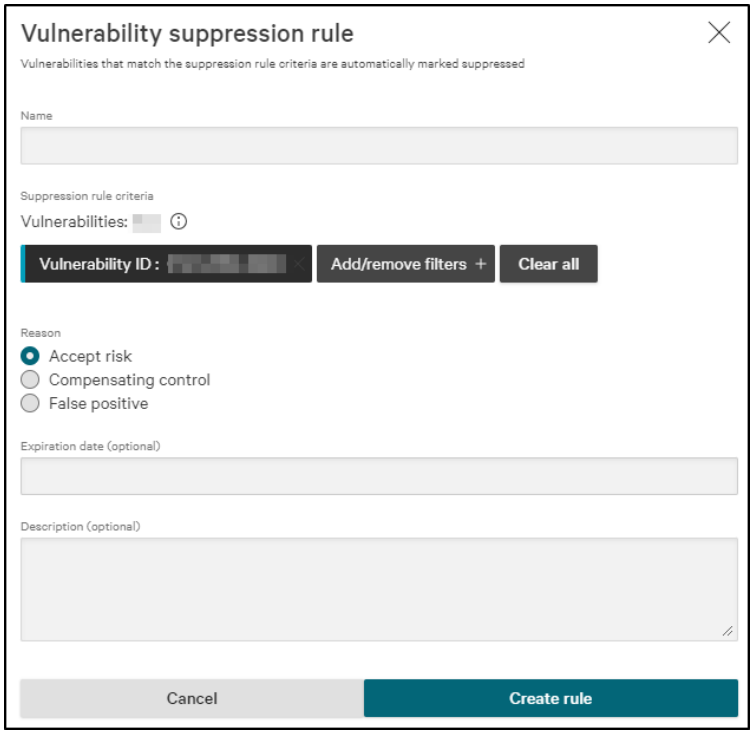
Sie können Tickets erstellen um bestimmen Anwendern die Behebung eine Schwachstelle zuzuweisen.



9 Schwachstelle unterdrücken

Falls eine Schwachstelle nicht behoben werden kann, oder in der eigenen Infrastruktur keine Bedeutung hat, kann sie unterdrückt werden. Somit wird sie in den Listen nicht mehr angezeigt.





6.3 Admindokumentation OpenVAS-Server

Info: Die IP-Adressen und Hostnamen wurden zu Dokumentationszwecken geändert.

Basic Infos

FQDN:	openvas.example.de
Betriebssystem:	Linux Debian 12
Benutzername:	adminvas
Kennwort:	(im Passwortmanager)

Netzwerkkonfiguration (statisch)

IP-Adresse:	192.0.2.100
Default-Gateway:	192.0.2.1
DNS-Server:	192.0.2.40
VLAN:	101 – Server

Funktion

Server für Schwachstellenscanner der über das Netzwerk auf netzwerkfähigen Geräten nach Schwachstellen sucht, diese Bewertet und Lösungsvorschläge anzeigt.

Anwendungen & Dienste

- Docker
  - Greenbone-Community-Edition
- SSH-Server
- Apache Webserver
- Gnome
- ufw

Docker Container

Befehl, um Status der Container zu prüfen:

```
Docker ps
```

```
CONTAINER ID   IMAGE                                COMMAND                  CREATED         STATUS         PORTS                    NAMES
3be13da9aaae   greenbone/gsa:stable                 "/usr/local/bin/entr…"   9 minutes ago   Up 9 minutes   0.0.0.0:9392->80/tcp     greenbone-community-edition-gsa-1
ab156390901b   greenbone/gvmd:stable                "/usr/local/bin/entr…"   9 minutes ago   Up 9 minutes                            greenbone-community-edition-gvmd-1
99ec2664e61c   greenbone/ospd-openvas:stable        "/usr/bin/tini -- /u…"   9 minutes ago   Up 9 minutes                            greenbone-community-edition-ospd-openvas-1
d60c419f875e   greenbone/notus-scanner:stable       "/usr/local/bin/entr…"   9 minutes ago   Up 9 minutes                            greenbone-community-edition-notus-scanner-1
f3f51d56a373   greenbone/redis-server               "/bin/sh -c 'rm -f /…"   9 minutes ago   Up 9 minutes                            greenbone-community-edition-redis-server-1
946d03a9cb72   greenbone/pg-gvm:stable              "/usr/local/bin/entr…"   9 minutes ago   Up 9 minutes                            greenbone-community-edition-pg-gvm-1
a664cbc529e0   greenbone/mqtt-broker                "/bin/sh -c 'mosquit…"   9 minutes ago   Up 9 minutes                            greenbone-community-edition-mqtt-broker-1
```

Verfügbarkeit von Updates prüfen:

docker compose -f docker-compose.yml -p greenbone-community-edition pull

Container manuell starten:

docker compose -f docker-compose.yml -p greenbone-community-edition up -d

Feed Status aktualisieren:
Für die Aktualisierung der Feeds wurde ein Bash-Skript im Verzeichnis des Benutzers adminvas erstellt. Ein Cron Job, führt das Skript jeden Montag um 03:00Uhr aus.

Feeds manuell aktualisieren
sudo ./updatefeed.sh

6.4 Angebot Crowdstrike – Falcon Spotlight

[redacted]

[redacted]

Firma
Agrarfrost GmbH & Co. KG
Herr Marcel Plate
Aldrup 3
27793 Wildeshausen

Kunden-Angebot

Datum
Ihre Kunden-Nr.
Ihre E-Mail-Adresse
Angebots-Nr.
Angebot gültig bis
Vertrieb

Innendienst

[redacted]

Crowdstrike Falcon Complete V3

Sehr geehrter Herr Plate,

wir bedanken uns für Ihr Interesse an unserem Lösungsangebot. Auf der Grundlage der bereits geführten Gespräche und der uns vorliegenden Informationen unterbreiten wir Ihnen das folgende Angebot.

Pos	Bezeichnung	Menge	ME	Einzelpreis	Gesamtpreis
	Laufzeit 12 Monate				
1	Falcon Complete with Threat Graph Standard on EU Cloud - Tier 1	750,000	Stk	[redacted] €	[redacted] €
2	Insight - Bundled	750,000	Stk	€	€
3	Prevent - Bundled	750,000	Stk	€	€
4	Discover - Bundled	750,000	Stk	€	€
5	Falcon Complete Subscription (Up to 299)	750,000	Stk	€	€
6	Overwatch - Bundled	750,000	Stk	€	€
7	Threat Graph Standard on EU Cloud	750,000	Stk	€	€
8	Falcon Complete: Complimentary CID	1,000	Stk	€	€
9	University LMS Subscription Customer Acc	6,000	Stk	€	€
10	Express Support	1,000	Stk	€	€
	Addon Spotlight Application				
	****** Alternativ zu vorherstehender Position ******				
11	Falcon Spotlight Application - Tier 1	750,000	Stk	€	*
	****** Alternativ zu vorherstehender Position ******				
12	Express Support	1,000	Stk	€	*
	Summe Falcon Spotlight: 17.777,94				
	Addon Exposure Management				
13	Falcon Exposure Management Upgrade	750,000	Stk	€	€
14	Express Support	1,000	Stk	€	€

6.5 Angebot Rapid7 – InsightVM 750 Assets

[redacted]
Agrarfrost GmbH
Herr Schröder
Aldrup 3
27793 Wildeshausen

Angebot

[redacted]

Bitte bei allen Rückfragen angeben !

Lieferanschrift:
Agrarfrost GmbH
Aldrup 3
27793 Wildeshausen

Versandart	digitale Lieferung
Lieferbedingung	Frei Haus

[redacted]

Sehr geehrter Herr Schröder,

wir bedanken uns für Ihr Interesse an unseren Produkten und übersenden Ihnen anbei unser Angebot.

Pos.	Artikelnr. / Bezeichnung	Menge ME	Einzelpreis	Gesamtpreis SC
1	R7-IVM-SUB Rapid7 InsightVM Additional Year for existing InsightVM Subscription rate based on customer's total asset count Laufzeit: 1 Jahre	750Stk	[redacted]	[redacted]
Optional, nicht in der Summe enthalten :				
2	R7-IVM-SUB Rapid7 InsightVM Additional 3 Year for existing InsightVM Subscription rate based on customer's total asset count Laufzeit: 3 Jahre	750Stk		
3	R7-IVMESS-SUB Rapid7 External Scanning Service Stk enthält 1 Stk	1Stk		
4	R7-PSIVMDEP3D Rapid7 3-Day - Vulnerability Management Setup and Quick Product Feature Overview	1Stk		
5	R7-PSIVMTRN-OE Rapid7 Certified Administrator Training 2-Day Training Class for one (1) student InsightVM	1Stk		
			Zwischensumme EUR	[redacted] SC

6.6 Angebot Rapid7 - InsightVM 3500 Assets

[redacted]

[redacted]
Agrarfrost GmbH
Herr Schröder
Aldrup 3
27793 Wildeshausen

Angebot

[redacted]

Bitte bei allen Rückfragen angeben !

Versandart	digitale Lieferung
Lieferbedingung	Frei Haus

[redacted]

Sehr geehrter Herr Schröder,

wir bedanken uns für Ihr Interesse an unseren Produkten und übersenden Ihnen anbei unser Angebot.

Pos.	Artikelnr. / Bezeichnung	Menge ME	Einzelpreis	Gesamtpreis SC
1	R7-IVM-SUB Rapid7 InsightVM Additional Year for existing InsightVM Subscription rate based on customer's total asset count Laufzeit: 1 Jahre	3500Stk	[redacted]	[redacted]
	Optional, nicht in der Summe enthalten :			
2	R7-IVM-SUB Rapid7 InsightVM Additional 3 Year for existing InsightVM Subscription rate based on customer's total asset count Laufzeit: 3 Jahre	3500Stk		
3	R7-IVMESS-SUB Rapid7 External Scanning Service Stk enthält 1 Stk	1Stk		
4	R7-PSIVMDEP3D Rapid7 3-Day - Vulnerability Management Setup and Quick Product Feature Overview	1Stk		
5	R7-PSIVMTRN-OE Rapid7 Certified Administrator Training 2-Day Training Class for one (1) student InsightVM	1Stk		
			Zwischensumme EUR	[redacted] SC
	zzgl. MwSt. mit Steuercode 101	19,00	% von [redacted]	
			Endsumme EUR	

6.7 Herleitung Serverkosten auf Dell Hypervisor

Abschreibungskosten Server-Landschaft			
Geräte	**Anschaffungskosten**	**Abschreibung pro Jahr**	**Pro Server**
Dell Hardware	XXX.XXX €	XX.XXX €	XXX €
Backup Server	XX.XXX €	X.XXX €	XX €
Summe (jährlich pro Server			XXX €

Tabelle 11 - Herleitung Abschreibungskosten pro Server

Um die Kosten eines einzelnen Servers pro Jahr zu berechnen, wurde zunächst die Abschreibung der gesamten Virtualisierungsumgebung auf 5 Jahre betrachtet. Anschließend wurde dies durch die Anzahl an Server (164) geteilt. Hinzu kommen die Kosten für das Backup-System, wobei ebenfalls von einer Abschreibung von 5 Jahren ausgegangen ist.

6.8 Herleitung Wartungskosten

Wartungskosten Serverlandschaft (jährlich)			
Anzahl Server	**VMWare Wartung**	**ArcServe Wartung**	**Bandlaufwerke Hardware**
140	XX.XXX €	X.XXX €	X.XXX €
1	XX €	XX €	XX €
Summe (jährlich pro Server			XX €

Tabelle 12 - Herleitung Wartungskosten pro Server

Zeitplanung - Abschlussprojekt	SOLL-Stunden	IST-Stunden	Differenz
Planungsphase	6	7	1
Projektumfang	1	1	0
Ist-Analyse	1	1	0
Anforderungen / Soll-Konzept	1	2	1
Anbietersuche	2	2	0
Auswahl an Testprodukten	1	1	0
Angebots und Testphase	10	12	2
Kontaktaufnahme mit Anbietern	1	1	0
Installation und Konfiguration der Testversionen	3	6	3
Auswertung der Testphase	2	2	0
Kostenrechnung und Angebotsvergleich	2	2	0
Lösungsvorschläge entwickeln und vorstellen	2	1	-1
Implementierungsphase	21	18,5	-2,5
Installation und Konfiguration	7	6	-1
Funktionstest bei ausgewählten Systemen	3	4	1
Finale Ausbreitung der Software	3	2	-1
Konfiguration der Schwachstellenberichte	2	2	0
Einweisen der Administratoren	2	1	-1
Systemdokumentation	2	1,5	-0,5
Anwenderdokumentation	2	2	0
Projektabschluss	3	2,5	-0,5
Abschlussbericht über erkannte Schwachstellen	1	1	0
Vorstellung vor der Geschäftsleitung	1	0,5	-0,5
Bewertung des Projekts	1	1	0
Gesamt	40	40	0

Tabelle 13 - Zeitplanung Vergleich

Tabellenverzeichnis

Abbildungsverzeichnis

Glossar

Legacy System (dt. Altsytem)
Bei Legacy Systemen handelt es sich um veraltete Computersoftware und Hardware, welche immer noch eingesetzt werden
(vgl. https://www.talend.com/de/resources/was-ist-ein-legacy-system)

Asset Management
Asset Management für IT-Systeme bezieht sich auf die systematische Dokumentation, Verwaltung und Überwachung von IT-Ressourcen eines Unternehmens
(vgl. https://www.atlassian.com/de/itsm/it-asset-management)

Mobile Device Management (MDM)
Unter Mobile Device Management versteht man eine Software, mit der Unternehmen ihre mobilen Geräte wie Smartphones und Tablets zentralisiert konfigurieren, überwachen, verwalten und sichern können. (vgl. https://de.wikipedia.org/wiki/Mobile-Device-Management)

CVE
CVE steht für Common Vulnerabilitys and Exposures. Dabei handelt es sich um ein standardisiertes Verfahren für die Benennung von bekannten IT-Sicherheitslücken. Einer bekannten Sicherheitslücke wird eine bestimme Nummer zugewiesen, wodurch sie eindeutig identifizierbar ist. (vgl. https://de.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures)

Open Source
Open Source bezieht sich auf Software, deren Quellcode öffentlich zugänglich ist, was es Benutzern erlaubt, die Software frei zu nutzen, zu modifizieren und zu verbreiten.
(vgl. https://de.wikipedia.org/wiki/Open_Source)

Active-Scanning
Beim Active-Scanning Ansatz, warden die Zielgeräte aktiv über das Netzwerk gescannt.

Repository-Server
Server, von dem die benötigten Pakete für Anwendungen bereitgestellt werden.

Container
Container sind leichtgewichtige, portable Softwareeinheiten, die Anwendungen in isolierten Umgebungen kapseln, um diese unabhängig von einem Betriebssystem auszuführen. Dazu wird eine Docker Umgebung auf dem System benötigt. Ein Beispiel dafür ist die im Projekt verwendete Docker Umgebung.

Snapshot
Ein Snapshot ist eine Momentaufnahme einer virtuellen Maschine, in der der aktuelle Zustand der virtuellen Maschine einschließlich Speicherdaten. Dies ermöglicht es zu einem bestimmen Zustand einer VM zurückzukehren.

Agent-Less
Als Agent-Less Gräte werden die Geräte bezeichnet, auf denen der Agent von Crowdstrike nicht installiert ist.

Cronjob
Ein Cronjob ist eine geplante Aufgabe in Unix basierten Betriebssystemen. Damit können Skripte, Befehle und Programme zu definierten Zeiten automatisch und wiederkehrend ausgeführt werden

Quellen

Alle Links wurden am 05.12.2023 noch einmal aufgerufen und auf Aktualität geprüft.

Webseite Agrarfrost
https://www.agrarfrost.de/

Beitrag über NIS2-EU-Richtlinie von Haufe
https://www.haufe.de/compliance/recht-politik/nis-2-richtlinie-muss-bis-oktober-2024-umgesetzt-werden_230132_606072.html

Schwachstellenscanner im Test

https://www.gartner.com/reviews/market/vulnerability-assessment

BSI-Empfehlung für OpenVAS

BSI - Open Vulnerability Assessment System (bund.de)

OpenVAS Docker Container Installationsanleitung

https://greenbone.github.io/docs/latest/22.4/container/index.html

Anforderungen an Scans OpenVAS

https://docs.greenbone.net/GSM-Manual/gos-21.04/de/performance.html

Rapid7 InsightVM Systemanforderungen

https://docs.rapid7.com/insightvm/system-requirements/

Bedienungsanleitung OpenVAS

https://docs.greenbone.net/GSM-Manual/gos-21.04/de

Cronjob Informationen

https://www.sysadminslife.com/linux/cronjob-unter-debian-und-ubuntu-erstellen/

Ausfallszeit Ransomware Angriff

https://www.storage-insider.de/wie-sich-lange-ausfallzeiten-bei-ransomware-attacken-verhindern-lassen-a-b6d9ee772e950d679262ea206dd56242/#:~:text=Die%20durchschnittliche%20Ausfallzeit%20nach%20einem,Betriebsunterbrechungen%20geht%2C%20ist%20Timing%20alles.