Greenbone

Handbuch

Greenbone Cloud Service

Greenbone

Greenbone AG
Neumarkt 12
49074 Osnabrück
Deutschland
https://www.greenbone.net

Status: 6. März 2024

Dies ist das Handbuch für den Greenbone Cloud Service.
Der Greenbone Cloud Service wird fortlaufend weiterentwickelt. Dieses Handbuch bemüht sich, immer die aktuellste Version zu dokumentieren. Dennoch kann es sein, dass neueste Funktionen noch nicht im Handbuch berücksichtigt sind.
Sollten Sie Anmerkungen oder Fehlerkorrekturen zu diesem Handbuch haben, kontaktieren Sie bitte den Greenbone Enterprise Support (https://www.greenbone.net/technischer-support/).

Inhaltsverzeichnis

KAPITEL 1

Einführung

Schwachstellenmanagement

In der IT-Sicherheit bildet das Zusammentreffen von drei Grundelementen die Angriffsfläche einer IT-Infrastruktur.

1. Angreifende mit ausreichend Erfahrung, Ausrüstung und Geld, um den Angriff auszuführen.
2. Zugriff auf die IT-Infrastruktur.
3. Schwachstellen in IT-Systemen, verursacht durch Fehler in den Anwendungen und Betriebssystemen oder inkorrekte Konfigurationen.

Falls diese drei Elemente zusammentreffen, ist ein erfolgreicher Angriff auf die IT-Infrastruktur wahrscheinlich. Das dritte Element kann beeinflusst werden, da 999 von 1.000 erfolgreich ausgenutzten Schwachstellen seit mehr als einem Jahr bekannt sind.

Das Schwachstellenmanagement ist ein Kernelement der modernen IT-Compliance. Die IT-Compliance beschreibt die Einhaltung gesetzlicher, unternehmensweiter und vertraglicher Regeln und Vereinbarungen bezüglich der IT-Infrastruktur. Sie betrifft hauptsächlich die Sicherheit, Verfügbarkeit, Speicherung und Vertraulichkeit von Informationen. Unternehmen und Behörden müssen in diesem Bereich viele gesetzliche Pflichten erfüllen.

Die Kontrolle und Verbesserung der IT-Sicherheit ist ein kontinuierlicher Prozess, welcher mindestens aus den folgenden Schritten besteht:

- Feststellen des aktuellen Zustands
- Verbessern des momentanen Zustands
- Überprüfen der ergriffenen Maßnahmen

Greenbone Cloud Service

Der Greenbone Cloud Service bietet einen einfach nutzbaren, hochwertigen Dienst für das Schwachstellenmanagement. Er prüft die IT-Infrastruktur auf Sicherheitslücken und liefern einen Bericht, der alle gefundenen Schwachstellen sortiert nach Schweregrad enthält.

Dazu bieten der Greenbone Cloud Service die Möglichkeit, den Bedarf an zu scannenden IP-Adressen ganz individuell festzulegen. Kommerzielle und öffentliche Einrichtungen jeder Größe können den Greenbone Cloud Service selbstständig nutzen, um sich mit ihren besonderen Sicherheitsanforderungen zu befassen.

Benutzer loggen sich mit ihren Zugangsdaten ein und haben die Möglichkeit ortsunabhängig mit dem Greenbone Cloud Service zu arbeiten. Dabei können sowohl öffentliche IP-Dienste (WWW-Server, E-Mail-Server, etc.) als auch interne Netzwerke gescannt werden. Die Pakete sind als Abonnements strukturiert und können auf monatlicher Basis gekündigt oder bearbeitet werden.

Der Greenbone Cloud Service erreicht dies durch unterschiedliche Sichtweisen von Angreifenden:

Extern
: Der Greenbone Cloud Service kann einen externen Angriff simulieren, um veraltete oder falsch konfigurierte Firewalls zu entdecken.

Demilitarisierte Zone (DMZ)
: Der Greenbone Cloud Service identifiziert tatsächliche Schwachstellen, welche von Angreifenden, die die Firewall überwunden haben, ausgenutzt werden können.

Intern
: Der Greenbone Cloud Service ist zusätzlich in der Lage, Schwachstellen, die ausgenutzt werden können (z. B. durch Social Engineering oder Computerwürmer), zu entdecken. Aufgrund der möglichen Auswirkungen solcher Attacken ist diese Perspektive für die Sicherheit von IT-Infrastrukturen besonders wichtig.

Für DMZ und interne Scans kann zwischen authentifizierten und nicht-authentifizierten Scans unterschieden werden. Wenn ein authentifizierter Scan durchgeführt wird, nutzt der Greenbone Cloud Service Anmeldedaten und kann Schwachstellen in Anwendungen, die nicht als Dienst laufen, aber ein hohes Risiko mit sich bringen, entdecken. Dies beinhaltet Webbrowser, Office-Anwendungen und PDF-Viewer. Für die Vor- und Nachteile von authentifizierten Scans siehe Kapitel *6.3.1* (Seite 47).

Aufgrund dessen, dass jeden Tag neue Schwachstellen entdeckt werden, sind regelmäßige Systemupdates und -tests nötig. Der Greenbone Enterprise Feed stellt sicher, dass der Greenbone Cloud Service immer mit den neuesten Tests versorgt ist und die neuesten Schwachstellen zuverlässig feststellen kann. Greenbone analysiert CVE-Nachrichten und -Sicherheitsmitteilungen[1] von Anbietern und entwickelt täglich neue Schwachstellentests.

Wenn ein Schwachstellenscan mit dem Greenbone Cloud Service durchgeführt wird, erhalten die zuständigen Fachleute eine Liste aller Schwachstellen, die auf dem Zielsystem identifiziert wurden. Für die Auswahl der Beseitigungsmaßnahmen wird eine Priorisierung benötigt. Die wichtigsten Maßnahmen sind die, die das System gegen kritische Risiken schützen und die entsprechenden Sicherheitslücken eliminieren.

Der Greenbone Cloud Service nutzt das Common Vulnerability Scoring System (CVSS). CVSS ist ein Industriestandard für die Klassifizierung und Bewertung von Schwachstellen. Es unterstützt bei der Prioritätensetzung von Beseitigungsmaßnahmen.

Grundsätzlich gibt es zwei Möglichkeiten zum Behandeln von Schwachstellen:

- Eliminieren der Schwachstelle durch Updaten der Software, Entfernen der fehlerhaften Komponente oder Verändern der Konfiguration.
- Implementieren einer Regel in einer Firewall oder einem Intrusion-Prevention-Systeme (Virtual Patching).

  Virtual Patching ist die scheinbare Eliminierung einer Schwachstelle durch eine ausgleichende Maßnahme. Die wirkliche Schwachstelle existiert weiterhin und Angreifende können die Schwachstelle ausnutzen, falls die Maßnahme versagt oder ein alternativer Ansatz genutzt wird.

Eine tatsächliche Korrektur oder ein Update der betroffenen Software ist dem Virtual Patching immer vorzuziehen.

Der Greenbone Cloud Service unterstützt auch das Prüfen implementierter Beseitigungsmaßnahmen. Mit seiner Hilfe können zuständige Fachleute den aktuellen Status der IT-Sicherheit dokumentieren, Änderungen erkennen und diese Änderungen in Berichten erfassen.

[1] Das Common Vulnerability and Exposures (CVE) Projekt ist ein herstellerunabhängiges Forum für die Identifikation und Veröffentlichung neuer Schwachstellen.

KAPITEL 2

Vor der ersten Anwendung lesen

Der Greenbone Cloud Service nutzt einen vollständigen Schwachstellenscanner. Obwohl der Schwachstellenscanner so konzipiert wurde, dass alle negativen Auswirkungen auf die Netzwerkumgebung minimal sind, muss er während des Scans mit dem untersuchten Zielsystem interagieren und kommunizieren. Dazu gehören Analysen über verschiedene Protokolle (z. B. HTTP, FTP) bei allen betroffenen Diensten zur Diensterkennung.

Bemerkung: Es ist die grundlegende Aufgabe des Greenbone Cloud Service andernfalls unentdeckte Schwachstellen zu finden und zu identifizieren. Bis zu einem gewissen Ausmaß muss sich der Scanner wie tatsächliche Angreifende verhalten.

Obwohl die standardmäßigen und empfohlenen Einstellungen die Auswirkungen des Schwachstellenscanners auf die Netzwerkumgebung auf ein Minimum beschränken, sind unerwünschte Nebeneffekte möglich. Durch die Einstellungen des Scanners können diese Nebeneffekte kontrolliert und verbessert werden.

Bemerkung: Die folgenden Nebeneffekte sollten zur Kenntnis genommen werden:

- Auf dem Zielsystem können Protokoll- und Warnmeldungen können angezeigt werden.
- Auf Netzwerkgeräten, Überwachungslösungen, Firewalls und Intrusion-Detection-/Intrusion-Prevention-Systemen können Protokoll- und Warnmeldungen angezeigt werden.
- Firewall-Regeln und andere Intrusion-Prevention-Maßnahmen können ausgelöst werden.
- Scans können die Latenzzeit auf dem Ziel und/oder dem gescannten Netzwerk erhöhen. In extremen Fällen kann dies zu Situationen führen, die einem Denial-of-Service-Angriff (DoS) ähneln.
- In anfälligen oder unsicheren Anwendungen können durch den Scan Fehler ausgelöst werden. Diese können weitere Fehler oder Abstürze verusachen.
- Eingebettete Systeme und Elemente der operativen Technologien mit schwachen Netzwerk-Stacks sind besonders anfällig für mögliche Abstürze oder sogar beschädigte Geräte.
- Logins (z. B. über SSH oder FTP) werden zu Banner-Grabbing-Zwecken gegen die Zielsysteme durchgeführt.
- Scans können dazu führen, dass Benutzerkonten durch das Testen standardmäßiger Benutzername-Passwort-Kombinationen gesperrt werden.

Da das oben beschriebene Verhalten beim Schwachstellenscanning erwartet, gewünscht oder sogar erforderlich ist, sollte(n) die IP-Adresse(n) des Scanners auf dem betroffenen System in die Liste der zulässigen Verbindungen aufgenommen werden. Informationen zur Erstellung einer solchen Liste finden sich in der Dokumentation oder beim Support des jeweiligen Systems/Diensts.

Das Auslösen von Fehlern, Abstürzen oder Sperrungen mit den Standardeinstellungen bedeutet, dass Angreifende dasselbe zu einer ungewissen Zeit und zu einem ungewissen Ausmaß tun kann. Das Finden von Schwachstellen, bevor sie von Angreifenden gefunden werden, ist der Schlüssel zur Widerstandsfähigkeit.

Obwohl die Nebeneffekte sehr selten auftreten, wenn standardmäßige und empfohlene Einstellungen genutzt werden, erlaubt der Schwachstellenscanner die Konfiguration von invasivem Verhalten, welches die Wahrscheinlichkeit der genannten Effekte erhöht.

Bemerkung: Die oben genannten Gegebenheiten sollten berücksichtigt und die benötigte Autorisierung sollte verifiziert werden, bevor der Greenbone Cloud Service zum Scannen des Zielsystems genutzt wird.

KAPITEL 3

Leitfaden zur Benutzung des Greenbone Cloud Service

Die folgenden Schritte sind wesentlich in der Benutzung des Greenbone Greenbone Cloud Service:

- Einen Benutzeraccount zum Einloggen erstellen → Kapitel *4.1* (Seite 12)
- Einen Abonnement-Plan wählen → Kapitel *5.5* (Seite 22)
- Einen Scan durchführen → Kapitel *6* (Seite 27)
- Einen authentifizierten Scan durchführen → Kapitel *6.3* (Seite 46)
- Einen Bericht lesen und nutzen → Kapitel *7.1* (Seite 77)

KAPITEL 4

Die Plattform kennenlernen und darauf zugreifen

4.1 Einen Benutzeraccount erstellen

Um den Greenbone Cloud Service nutzen zu können, muss ein Benutzeraccount erstellt werden.

- Wenn Self-Service nicht aktiviert ist (= Managed-Service), muss der vMSP die Benutzeraccounts erstellen.
- Wenn Self-Service aktiviert ist, können Benutzer ihre eigenen Accounts wie im Folgenden beschrieben erstellen. Trotzdem kann auch der vMSP die Benutzeraccounts erstellen.
- Der erstellte Benutzeraccount ist ein Hauptbenutzeraccount.
- Der Hauptbenutzer kann andere Benutzer in sein Team einladen (siehe Kapitel *5.4* (Seite 21)).

Bemerkung: Standardmäßig sind alle neu erstellten Accounts kostenlose Probeaccounts, die später in kostenpflichtige Accounts umgewandelt werden können (siehe Kapitel *5.5* (Seite 22)).

Ein neuer Benutzeraccount kann wie folgt erstellt werden:

1. Webbrowser öffnen.
2. URL des Greenbone Cloud Service eingeben.
3. Auf *Registrieren* klicken.
4. E-Mail-Adresse für den Account in das Eingabefeld *E-Mail-Adresse* eingeben.
5. Passwort für den Account in das Eingabefeld *Neues Passwort* eingeben und im Eingabefeld *Neues Passwort wiederholen* wiederholen.
6. Checkboxen für die Zustimmung zu den Nutzungsbedingungen und der Datenschutzerklärung aktivieren.
7. Auf *Kostenlos testen* klicken.

   Bemerkung: Zur Auswahl eines Abonnements siehe Kapitel *5.5* (Seite 22).

4.2 In die Plattform einloggen

Auf den Greenbone Cloud Service kann wie folgt zugegriffen werden:

1. Webbrowser öffnen.
2. URL des Greenbone Cloud Service eingeben.

   Tipp: Die Sprache der Plattform kann in der rechten oder linken oberen Ecke gewählt werden.

3. Mit der E-Mail-Adresse und dem Passwort des Greenbone-Cloud-Service-Accounts einloggen (siehe Kapitel *4.1* (Seite 12)).

   → Die Seite *Scan Verwaltung* wird angezeigt.

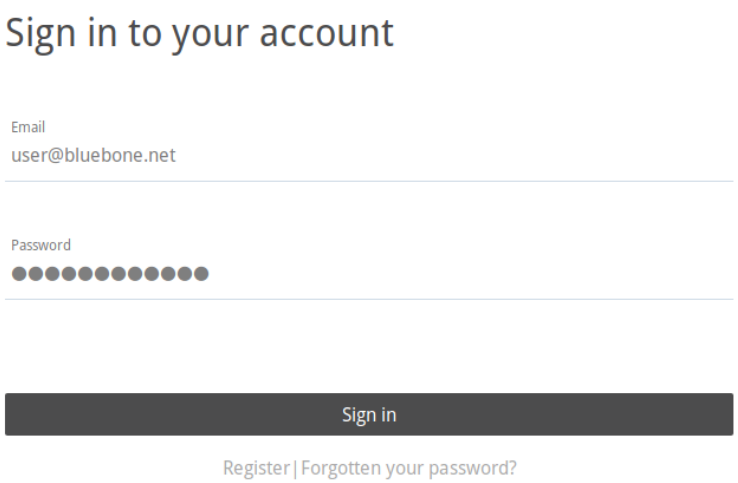

Abb. 4.1: In die Plattform einloggen

Bemerkung: Falls das Passwort vergessen wurde, kann auf *Passwort vergessen?* geklickt werden, um einen Link zum Zurücksetzen anzufordern.

4.3 Struktur der Plattform

4.3.1 Listenseiten

Listenseiten zeigen einen Überblick über alle Objekte einer Art (siehe Abb.4.2). Sie sind für Scans, Scanaufgaben, Ziele, Anmeldedaten, Zeitpläne und Gateways verfügbar.

Eine Listenseite kann geöffnet werden, indem die gewünschte Seite im Menüpanel gewählt wird, z. B. öffnet das Wählen von *Ziele* in der Kategorie *Scan-Konfiguration* im Menüpanel die Listenseite *Ziele*.

Die Liste der Objekte (siehe Abb.4.2/5) stellt Informationen wie den Namen, den Status, den Typ oder mögliche Aktionen für einzelne Objekte bereit (siehe Abb.4.2/2). Die in der Tabelle gezeigten Informationen hängen vom Objekttyp ab.

1 – Nach dem Namen eines bestimmten Objekts suchen.

2 – Aktionen für einzelne Objekte, abhängig vom Seiteninhalt.

3 – Zwischen Seiten wechseln.

4 – Anzahl der Objekte, die auf einer Seite dargestellt werden, wählen.

5 – Liste aller vorhandenen Objekte des gewählten Objekttyps.

6 – Ein neues Objekt des gewählten Objekttyps erstellen.

Abb. 4.2: Aufbau von Listenseiten

Die Listeninhalte können nach einer gewählten Spalte sortiert werden, indem auf den Spaltentitel geklickt wird. Der Inhalt kann auf- oder absteigend sortiert werden:

- ↑ im Spaltentitel zeigt, dass die Objekte aufsteigend sortiert sind.
- ↓ im Spaltentitel zeigt, dass die Objekte absteigend sortiert sind.

4.3.2 Detail-Overlays

Für manche Objekte kann ein Overlay geöffnet werden, das detaillierte Informationen enthält, z. B. werden durch Klicken auf einen Zeitplannamen in der Liste der Scanaufgaben (siehe Abb.4.3) Informationen über den genutzten Zeitplan angezeigt.

Bemerkung: Falls ein Overlay verfügbar ist, ist der Name des Objekts unterstrichen.

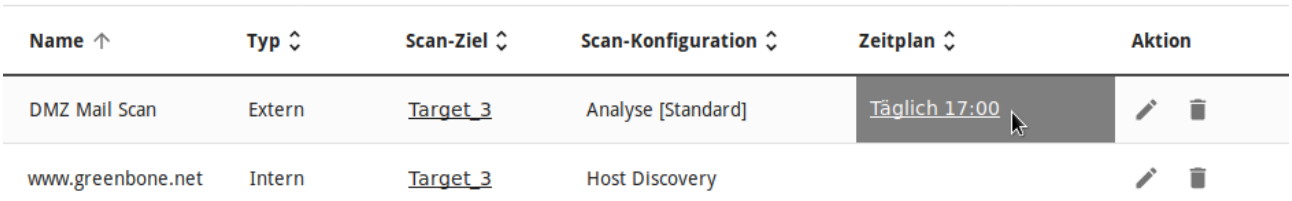

Abb. 4.3: Öffnen des Overlays

4.4 Support erhalten

Der Menüpunkt *Hilfe* bietet folgende Hilfestellungen und Informationen:

Übersicht
: Erklärung der Grundbegriffe der Greenbone Cloud Service.

Anleitung
: Umfassendes Anwendungshandbuch mit Schritt-für-Schritt-Anleitungen für alle Aktivitäten im Zusammenhang mit der Plattform.

Rechtliche Informationen
: Allgemeine Nutzungsbedingungen und Datenschutzbestimmungen des Greenbone Cloud Service.

KAPITEL 5

Die Benutzer-, Team- und Accounteinstellungen konfigurieren

Alle Benutzer des Greenbone Cloud Service können ihre eigenen Einstellungen für Scans und die Plattform verwalten.

5.1 Die Sprache ändern

Die Sprache der Plattform kann in der rechten oberen Ecke geändert werden.

Bemerkung: Alternativ kann die Sprache beim Einloggen gewählt werden (siehe Kapitel *4.2* (Seite 13)).

5.2 Benachrichtigungen einrichten

Benutzer können Zusammenfassungen aller durchgeführten Scans oder Benachrichtigungen mit Berichten erhalten, wenn Scans abgeschlossen sind.

Scan-Zusammenfassungen

Benachrichtigungen mit Scan-Zusammenfassungen können wie folgt eingerichtet werden:

1. *Benachrichtigungen* (Kategorie *Benutzer Einstellungen*) im Menüpanel wählen.
2. Zeitabstand wählen, in dem Benachrichtigungen erhalten werden sollen (siehe Abb.5.1).

   Bemerkung: Die Einstellung ist für jedes Zeitintervall vordefiniert.

   Es können mehrere Intervalle gleichzeitig ausgewählt werden.

   Wenn kein Intervall ausgewählt ist, sind die Scan-Zusammenfassungen deaktiviert.

   → Die Auswahl wird sofort angewendet. Die Benachrichtigungen werden an die E-Mail-Adresse gesendet, die zum Einloggen genutzt wird.

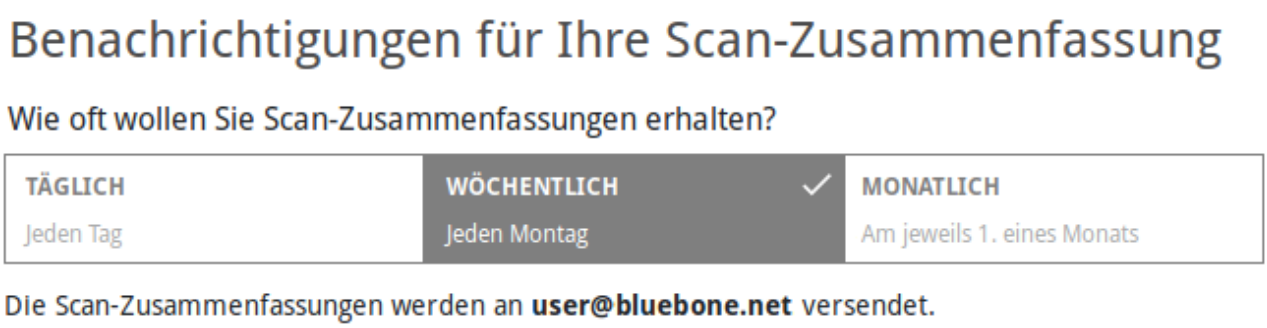

Abb. 5.1: Einrichten von Scan-Zusammenfassungen

Abgeschlossene Scans

Benachrichtigungen für abgeschlossene Scans können wie folgt eingerichtet werden:

1. *Benachrichtigungen* (Kategorie *Benutzer Einstellungen*) im Menüpanel wählen.
2. Kanal wählen, auf dem die Benachrichtigung erhalten werden soll und, falls nötig, weitere Details bereitstellen (siehe Abb.5.2).

   Bemerkung: Es können mehrere Kanäle gleichzeitig ausgewählt werden.

3. Minimalen Schweregrad wählen, den ein Bericht benötigt, damit eine Benachrichtigung gesendet wird.

   → Die Auswahl wird sofort angewendet.

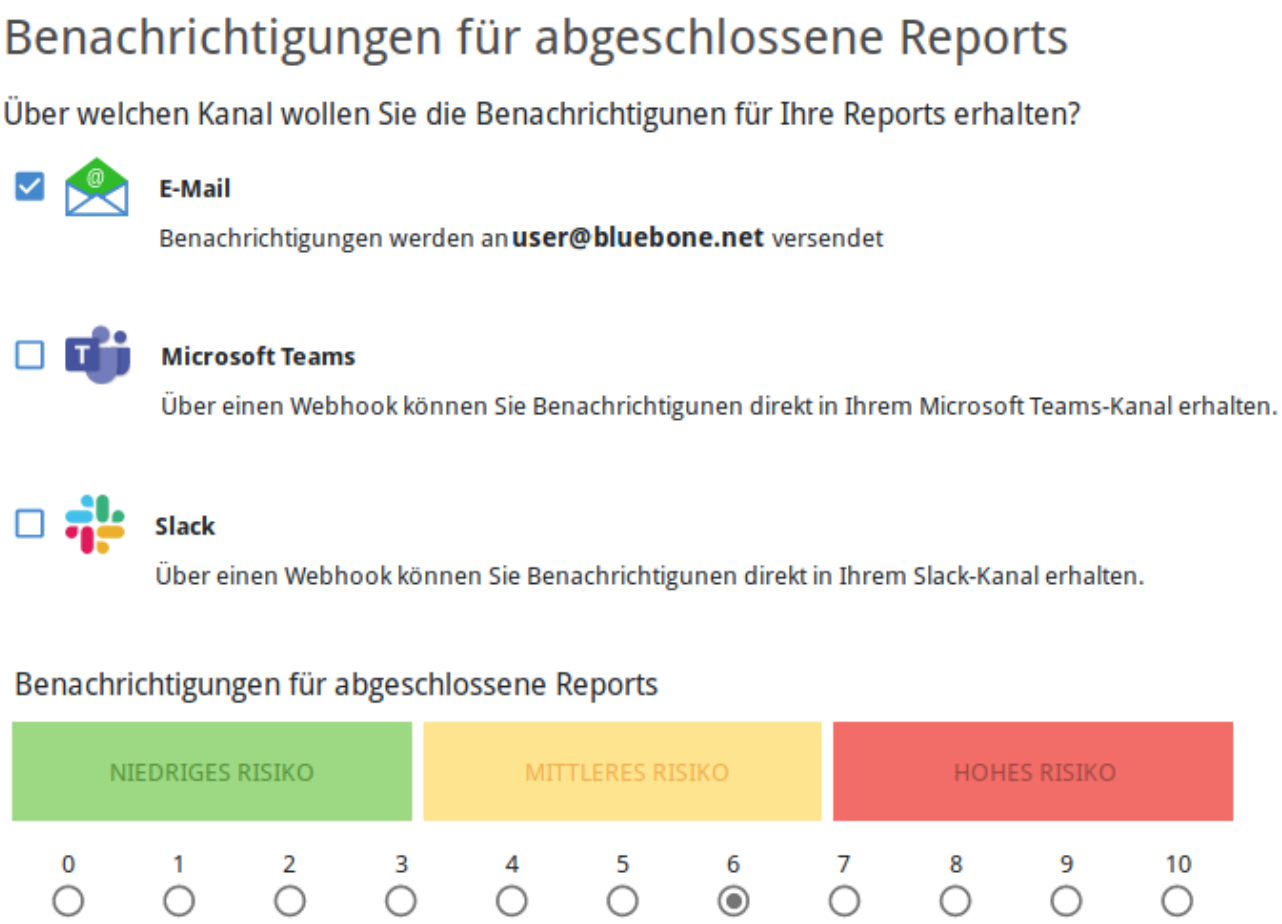

Abb. 5.2: Einrichten von Benachrichtigungen für abgeschlossene Scans

5.3 Die Sicherheitseinstellungen ändern

5.3.1 Das Benutzerpasswort ändern

Das Passwort, das zum Einloggen genutzt wird, kann wie folgt geändert werden:

1. *Sicherheit* (Kategorie *Benutzer Einstellungen*) im Menüpanel wählen.
2. Aktuelles Passwort in das Eingabefeld *Passwort* eingeben.
3. Neues Passwort in das Eingabefeld *Neues Passwort* eingeben.
4. Passwort im Eingabefeld *Passwort bestätigen* wiederholen.
5. Auf *Speichern* klicken.

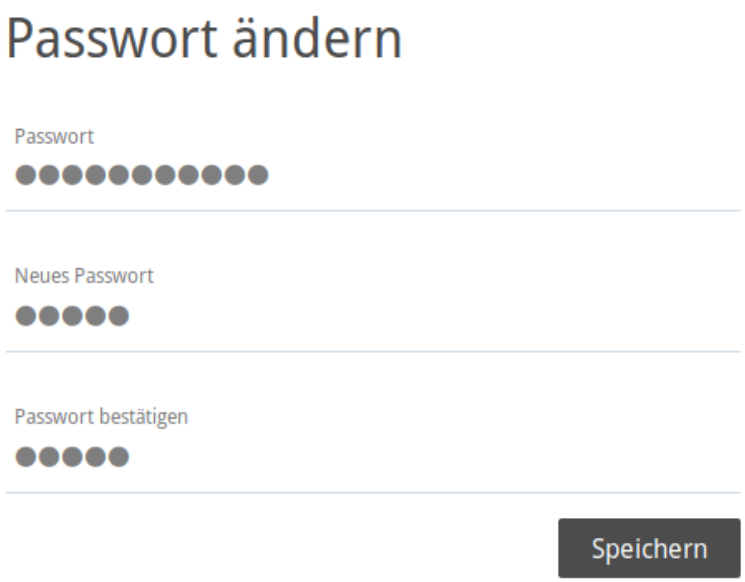

Abb. 5.3: Ändern des Benutzerpassworts

5.3.2 Eine Zwei-Faktor-Authentifizierung einrichten

Um das Einloggen sicherer zu machen, kann eine Zwei-Faktor-Authentifizierung wie folgt eingerichtet werden:

1. Eine der folgenden Apps für Smartphones herunterladen:
   - *FreeOTP* (verfügbar für Android)
   - *Google Authenticator* (verfügbar für Android und iOS)
2. Initiales Setup der App abschließen.
3. *Sicherheit* (Kategorie *Benutzer Einstellungen*) im Menüpanel wählen.
4. QR-Code, der im Abschnitt *Zwei-Faktor-Authentifizierung* angezeigt wird, scannen (siehe Abb.5.4).
5. Einmalkennwort, das von der Authentifikator-App geliefert wird, in das Eingabefeld *Einmalkennwort* eingeben.
6. Auf *Speichern* klicken.

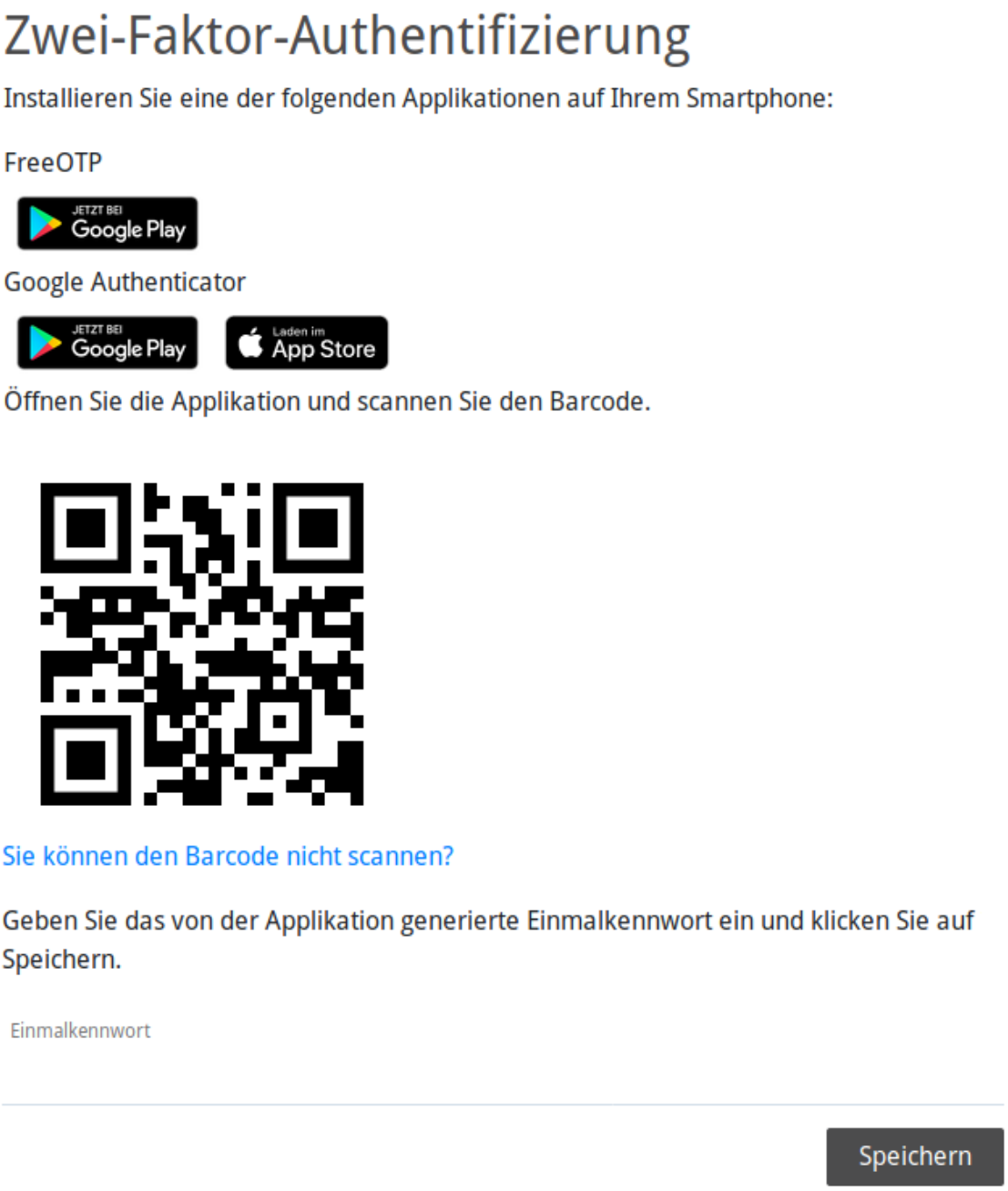

Abb. 5.4: Einrichten einer Zwei-Faktor-Authentifizierung

5.4 Teams erstellen und verwalten

Ein Hauptbenutzer, dessen Konto entweder von einem vMSP oder vom Benutzer selbst erstellt wurde (siehe Kapitel *4.1* (Seite 12)), kann andere Benutzer in sein Team einladen. Alle Benutzer eines Teams arbeiten mit den gleichen Rechten und nutzen das Abonnement des Hauptbenutzers.

5.4.1 Benutzer zu einem Team hinzufügen

1. *Team* (Kategorie *Team Einstellungen*) im Menüpanel wählen.
2. *Einladungen* wählen.
3. Auf *+ Neue Einladung erstellen* klicken.
4. E-Mail-Adresse eines Benutzers, der eingeladen werden soll, eingeben.
5. Auf *Einladung senden* klicken.

   → Eingeladene Benutzer erhalten eine E-Mail, können einen Account erstellen und dem Team beitreten.

   Beigetretene Benutzer werden angezeigt, wenn *Mitglieder* ausgewählt ist.

Bemerkung: Die Einladung läuft nach 24 Stunden ab.

Falls ein Benutzer die E-Mail nicht erhält oder die Einladungsfrist abgelaufen ist, kann die E-Mail durch Klicken auf ↻ in der Spalte *Aktionen* erneut gesendet werden.

5.4.2 Teammitglieder (de)aktivieren

Das Löschen einzelner Benutzer oder des Hauptbenutzers eines Teams ist nicht möglich. Benutzer können nur deaktiviert werden.

Bemerkung: Nur der Hauptbenutzer kann andere Benutzer (de)aktivieren.

Ein Benutzer kann wie folgt aktiviert oder deaktiviert werden:

1. *Team* (Kategorie *Team Einstellungen*) im Menüpanel wählen.
2. Auf den Slider in der Spalte *Status* klicken.

   → Die Änderung wird sofort angewendet.

   Ein deaktivierter Benutzer kann sich nicht mehr einloggen.

5.4.3 Den Hauptbenutzer ändern

Der Hauptbenutzer eines Teams, d. h. der Account, dessen Abonnement genutzt wird, kann geändert werden, beispielsweise wenn der betreffende Mitarbeiter das Unternehmen verlässt.

Der neue Hauptbenutzer muss ein aktiver Benutzer sein, deaktivierte Benutzer können nicht als Hauptbenutzer festgelegt werden (siehe Kapitel *5.4.2* (Seite 21)).

Bemerkung: Nur der Hauptbenutzer kann den Hauptbenutzer ändern.

Alternativ kann der vMSP kontaktiert werden, um den Hauptbenutzer zu ändern.

Der Hauptbenutzer kann wie folgt geändert werden:

1. *Team* (Kategorie *Team Einstellungen*) im Menüpanel wählen.

   Bemerkung: Der aktuelle Hauptbenutzer wird durch vor der E-Mail-Adresse angegeben.

2. In der Zeile des Benutzers, der der Hauptbenutzer sein soll, in der Spalte *Aktion* auf klicken.

   → Es wird eine Nachricht angezeigt, um die Änderung zu bestätigen.

3. Auf *Ok* klicken.

5.4.4 Den Account löschen

Das Löschen einzelner Benutzer oder des Hauptbenutzers eines Teams ist nicht möglich, diese können lediglich deaktiviert werden (siehe Kapitel *5.4.2* (Seite 21)). Das Löschen eines Accounts bewirkt Folgendes:

- Der Hauptbenutzer sowie alle anderen Benutzer des Teams werden gelöscht.
- Der Hauptbenutzer sowie alle anderen Benutzer können sich nicht mehr anmelden und den Greenbone Cloud Service nutzen.
- Alle Benutzer-, Team- und Kundendaten werden dauerhaft gelöscht.
- Alle Ziele und Berichte werden gelöscht.
- Aktive Abonnements laufen am Ende des aktuellen Abrechnungszeitraums aus.

Bemerkung: Nur der Hauptbenutzer kann einen Account löschen.

Alternativ kann der vMSP kontaktiert werden, um den Account zu löschen.

1. *Team* (Kategorie *Team Einstellungen*) im Menüpanel wählen.
2. Im Abschnitt *Account Löschen* auf *Account Löschen* klicken.

   → Es wird eine Nachricht angezeigt, um die Löschung zu bestätigen.

3. Auf *Ok* klicken.

   → Es wird eine E-Mail mit einem Link zur Bestätigung der Löschung an die E-Mail-Adresse des Hauptnutzers gesendet.

5.5 Das Abonnement konfigurieren

Das aktuelle Abonnement wird durch Wählen von *Abonnement* (Kategorie *Team Einstellungen*) im Menüpanel angezeigt (siehe Abb.5.5).

Bemerkung: Im Falle eines Managed-Service-Accounts ist es nicht möglich, das Abonnement selbst zu ändern oder zu kündigen. In diesem Fall muss der vMSP kontaktiert werden.

5.5.1 Ändern des Abonnementumfangs

Der Wechsel zu einem weniger umfangreichen Abonnement ist nur zum Ende des aktuellen Buchungsmonats möglich.

Das Upgrade zu einem umfangreicheren Abonnement ist sofort möglich.

Das Abonnement kann wie folgt geändert werden:

1. *Abonnement* (Kategorie *Team Einstellungen*) im Menüpanel wählen.
2. Auf *Upgrade* klicken.
3. Gewünschte Gesamtzahl der IP-Adressen (Summe aus externen und internen) in das Eingabefeld *Total IP's* eingeben (siehe Abb.5.5).
4. Schieberegler verschieben, um die Gesamtzahl zwischen internen und externen IP-Adressen wie gewünscht zu verteilen.

   → Die Zusammensetzung des Preises wird in der Übersicht angezeigt.

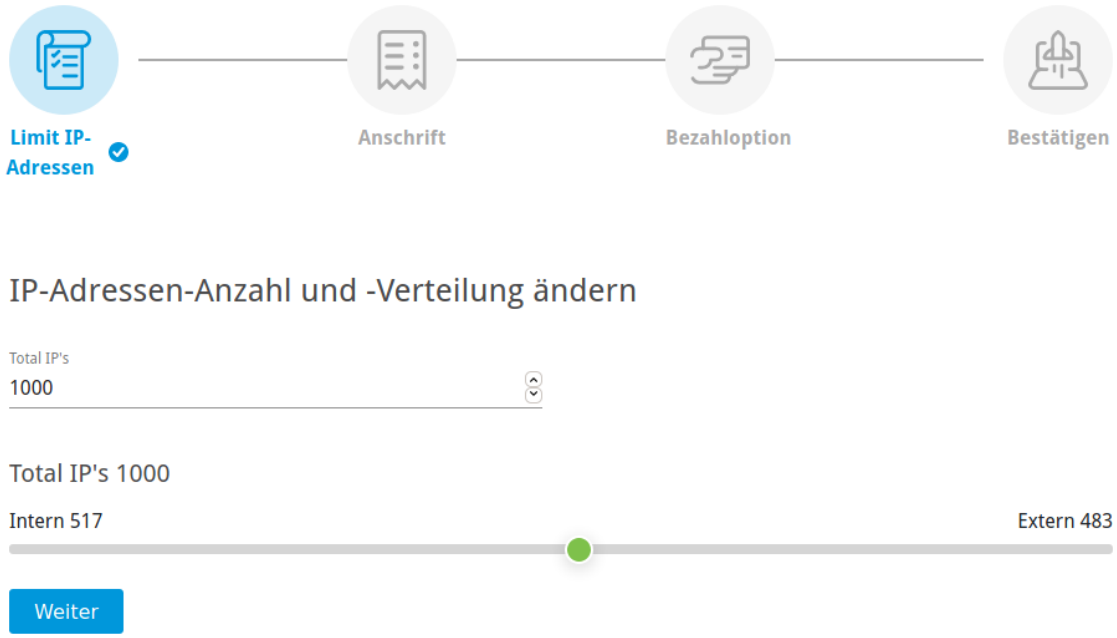

Abb. 5.5: Ändern des Abonnements

5. Auf *Weiter* klicken.
6. Kontaktdaten in die entsprechenden Eingabefelder eingeben.

   Tipp: Eine abweichende Rechnungsadresse kann genutzt werden, siehe Schritt 8.

7. Umsatzsteuer-Identifikationsnummer (USt-IdNr.) in das Eingabefeld eingeben.
8. Optional: Checkbox *Alternative Rechnungsadresse verwenden* aktivieren und Daten in die entsprechenden Eingabefelder eingeben.
9. Auf *Weiter* klicken.
10. Radiobutton der gewünschten Zahlungsmethode auswählen. Falls nötig, weitere Zahlungsdetails angeben, z. B. Kreditkarteninformationen.

11. Auf *Weiter* klicken.

    → Die Bestellübersicht wird angezeigt (siehe Abb.5.6).

12. Optional: Checkbox *Direkt upgraden* aktivieren, falls das neue Abonnement sofort genutzt werden soll.

13. Auf *Jetzt kaufen* klicken.

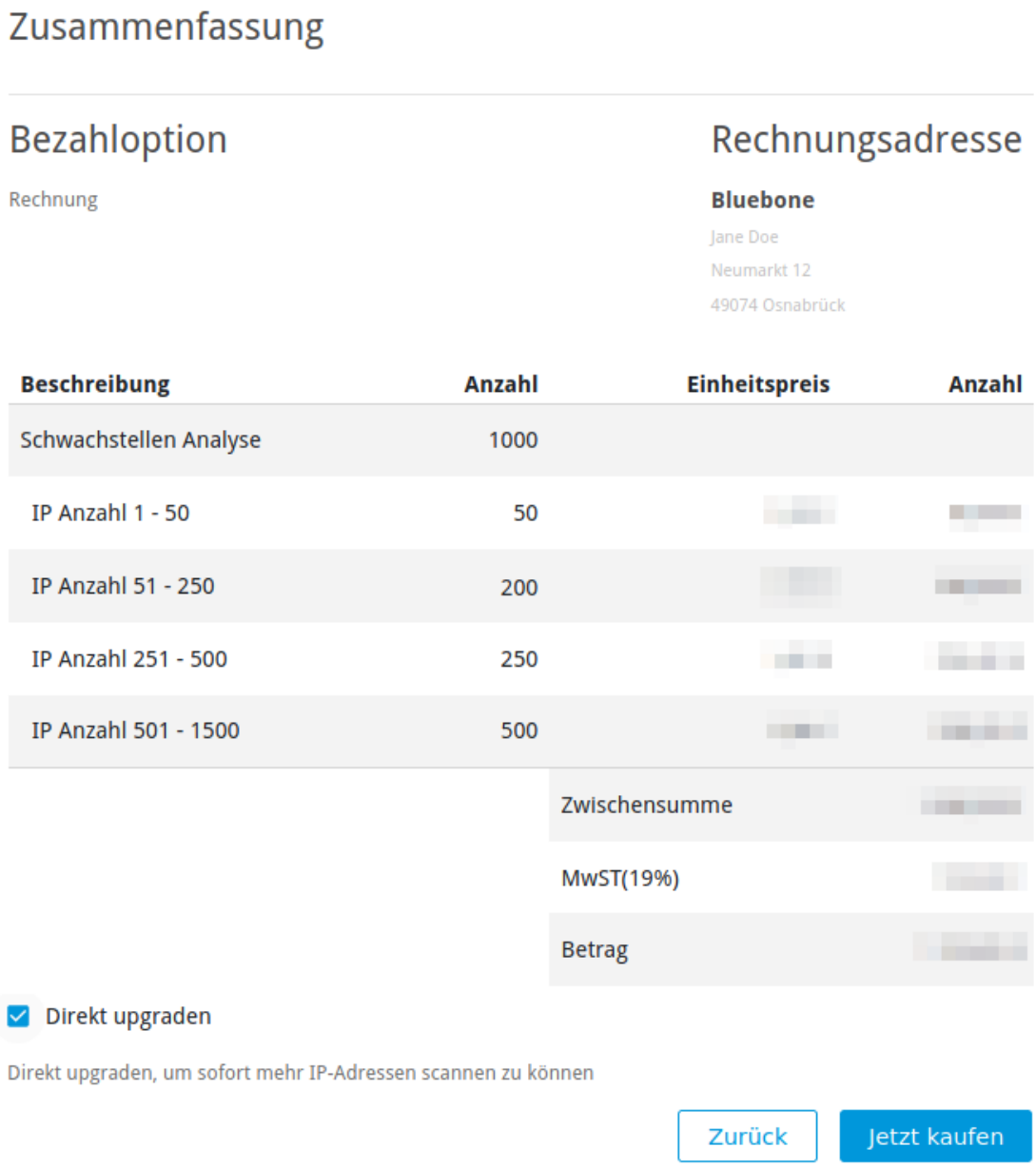

Abb. 5.6: Bestätigen des Abonnements

5.5.2 Beenden des Abonnements

Ein aktives Abonnement kann wie folgt beendet werden:

1. *Abrechnung* (Kategorie *Team Einstellungen*) im Menüpanel wählen.
2. Auf *Abonnement beenden* klicken.

5.6 Die Rechnungsdaten ändern

Die Kundendaten können wie folgt geändert werden:

1. *Abrechnung* (Kategorie *Team Einstellungen*) im Menüpanel wählen.
2. Daten im Abschnitt *Firmenadresse* in die entsprechenden Eingabefelder eingeben (siehe Abb.5.7).
3. Auf *Speichern* klicken.

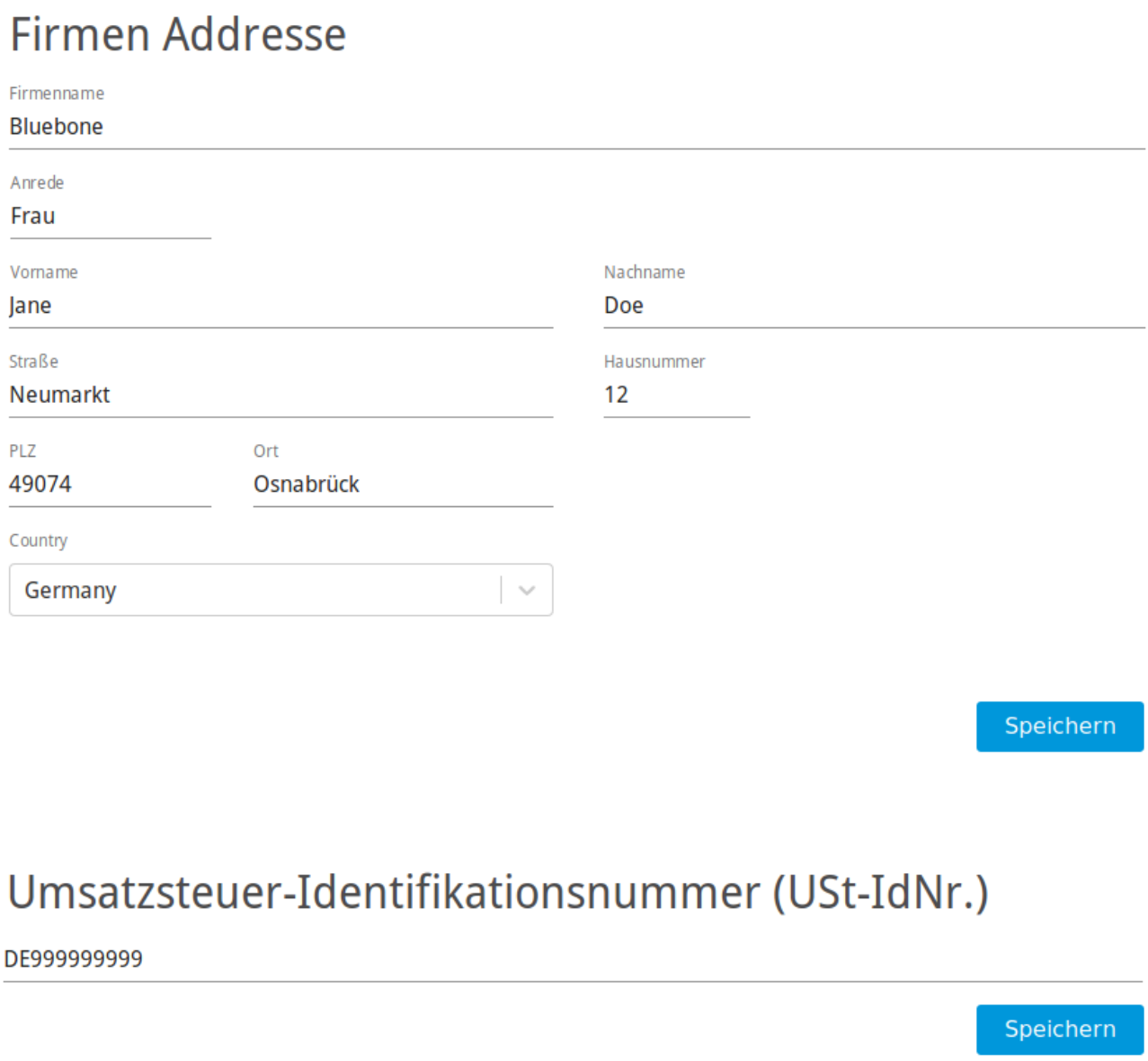

Abb. 5.7: Ändern der Rechnungsdaten

Die Umsatzsteuer-Identifikationsnummer (USt-IdNr.) kann wie folgt hinzugefügt oder geändert werden:

1. *Abrechnung* (Kategorie *Team Einstellungen*) im Menüpanel wählen.
2. USt-IdNr. im Abschnitt *Umsatzsteuer-Identifikationsnummer (USt-IdNr.)* in das entsprechende Eingabefeld eingeben (siehe Abb.5.7).
3. Auf *Speichern* klicken.

5.7 Rechnungen herunterladen

Bemerkung: Das Herunterladen von Rechnungen ist nur für Self-Service-Accounts und per Kreditkarte bezahlte Abonnements möglich.

Alle Rechnungen aktueller und früherer Abonnements können heruntergeladen werden, indem im Menüpanel *Rechnungen* (Kategorie *Team Einstellungen*) gewählt und in der Zeile der jeweiligen Rechnung auf PDF geklickt wird.

5.8 Die Managed-Security-Einstellungen ändern

Im Falle eines Managed-Service-Accounts kann dem vMSP Zugriff auf einige Berichtdaten oder Vollzugriff gewährt werden („Managed Security“).

1. *Managed Security* (Kategorie *Team Einstellungen*) im Menüpanel wählen.
2. Auf den Slider für *Report Access* klicken, um dem vMSP Zugriff auf Berichte zu erteilen.

   Dazu gehört der Zugriff auf den Schweregrad der Berichte und Aufgaben der letzten zwei Wochen und die Anzahl der Ergebnisse für *Hoch*, *Mittel*, *Niedrig* und *Log*.

   oder/und
3. Auf den Slider für *Vollzugriff* klicken, um dem vMSP Vollzugriff auf Einstellungen und Berichte zu erteilen.

KAPITEL 6

Ein System scannen

6.1 Den Aufgaben-Wizard für einen ersten Scan nutzen

Der Aufgaben-Wizard kann einen Scan mit minimalem Input vom Benutzer konfigurieren und starten.

1. *Scanverwaltung* im Menüpanel wählen.
2. Auf *+ Neue Scan-Aufgabe mit Wizard vorbereiten* klicken.

   → Eine Information wird angezeigt.
3. Auf *Los geht's!* klicken.

   Bemerkung: Falls die Nachricht nicht wieder angezeigt werden soll, Checkbox *Nicht wieder anzeigen* aktivieren, bevor auf *Los geht's!* geklickt wird.
4. Namen für die Aufgabe in das Eingabefeld *Aufgabenname* eingeben (siehe Abb.6.1).
5. Optional: Beschreibung für die Aufgabe in das Eingabefeld *Beschreibung (optional)* eingeben.
6. Scan-Konfiguration wählen.

   Bemerkung: Die Scan-Konfiguration *Analyse [Standard]* wird empfohlen.
7. Auf *Speichern und weiter* klicken.

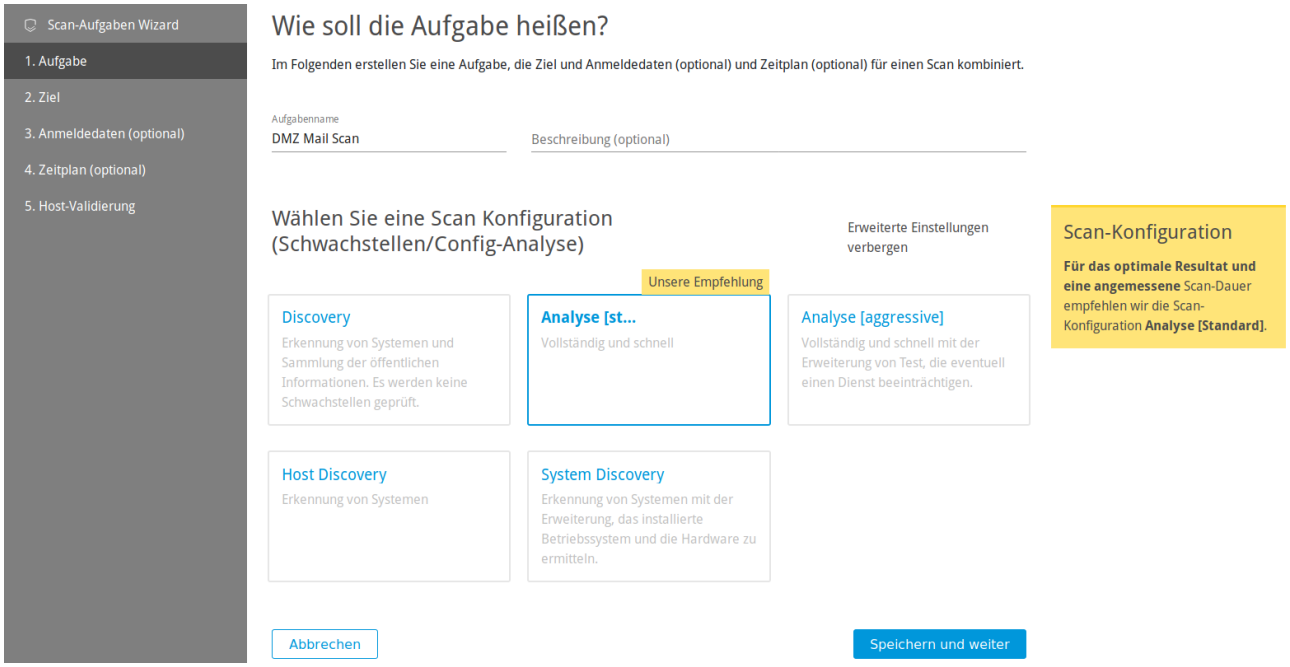

Abb. 6.1: Verwenden des Wizards

Bemerkung: Wenn der Wizard genutzt wird, können nur externe Ziele gescannt werden.

8. Bereits vorhandenes Ziel aus der Liste wählen.

   oder

8. Auf *+ Neues Ziel erstellen* klicken, um ein neues Ziel zu erstellen.

   Tipp: Für die Informationen, die in die Eingabefelder eingegeben werden müssen, siehe Kapitel *6.2.1* (Seite 31).

9. Auf *Speichern und weiter* klicken.
10. Optional: bereits vorhandene Anmeldedaten für den Microsoft-Windows-Login, SSH oder VMware ESXi aus der Liste wählen.

    oder

10. Optional: auf *+ Neue Anmeldedaten anlegen* klicken, um neue Anmeldedaten zu erstellen.

    Tipp: Für die Informationen, die in die Eingabefelder eingegeben werden müssen, siehe Kapitel *6.3.2.1* (Seite 49).

11. Auf *Speichern und weiter* klicken.
12. Optional: bereits vorhandenen Zeitplan aus der Liste wählen.

    oder

12. Optional: auf *+ Neuen Zeitplan erstellen* klicken, um einen neuen Zeitplan zu erstellen.

Tipp: Für die Informationen, die in die Eingabefelder eingegeben werden müssen, siehe Kapitel *6.4.1* (Seite 64).

13. Auf *Speichern und weiter* klicken.

Bemerkung: Falls ein externes Ziel gewählt wurde und der/die Host(s) noch nicht validiert wurde(n), wird *Host-Validierung anfragen* für den/die Host(s) angezeigt (siehe Abb.6.2).

Abb. 6.2: Host(s) noch nicht validiert

14. Auf *Host-Validierung anfragen* klicken, um die Host-Validierung durchzuführen.

    → Die Kontakte für den/die konfigurierten Host(s) werden von RIPE NCC eingeholt. Für weitere Informationen siehe Kapitel *6.2.2* (Seite 35).

    Wenn dieser Prozess abgeschlossen ist, zeigt ein Overlay die gefundenen Kontakte (siehe Abb.6.3).

Bemerkung: Falls kein Kontakt gefunden wurde, müssen die Hosts manuell vom Security-Team des vMSP überprüft werden.

15. Kontaktperson aus der Liste wählen.

    oder

15. Checkbox *Manuelle Prüfung durch das Security-Team.* aktivieren.
16. Auf *Host-Validierung anfragen* klicken.

    → Eine E-Mail wird an die Kontaktperson oder das Security-Team gesendet. Der Status der Host-Validierung wird auf der Seite *Ziele* angezeigt.

17. Auf *Scan vorbereiten* klicken.

    → Die Seite *Scanverwaltung* wird geöffnet. Die neue Aufgabe hat den Status *Neu und verfügbar*.

18. In der Zeile der erstellten Aufgabe auf ⊙ klicken.

Für den Status einer Aufgabe siehe Kapitel *6.7* (Seite 70).

Tipp: Sobald die Aufgabe gestartet wurde, kann der Bericht angezeigt werden, indem für die entsprechende Aufgabe auf der Seite *Scan Verwaltung* auf 🗎 geklickt wird.

Für das Lesen, Verwalten und Herunterladen von Berichten siehe Kapitel *7* (Seite 77).

Sobald sich der Status auf *Abgeschlossen* ändert, ist der gesamte Bericht verfügbar. Zu jeder Zeit können Zwischenergebnisse angesehen werden (siehe Kapitel *7.1* (Seite 77)).

Bemerkung: Die Fertigstellung des Scans kann einige Zeit in Anspruch nehmen. Die Seite aktualisiert automatisch, falls neue Daten verfügbar sind.

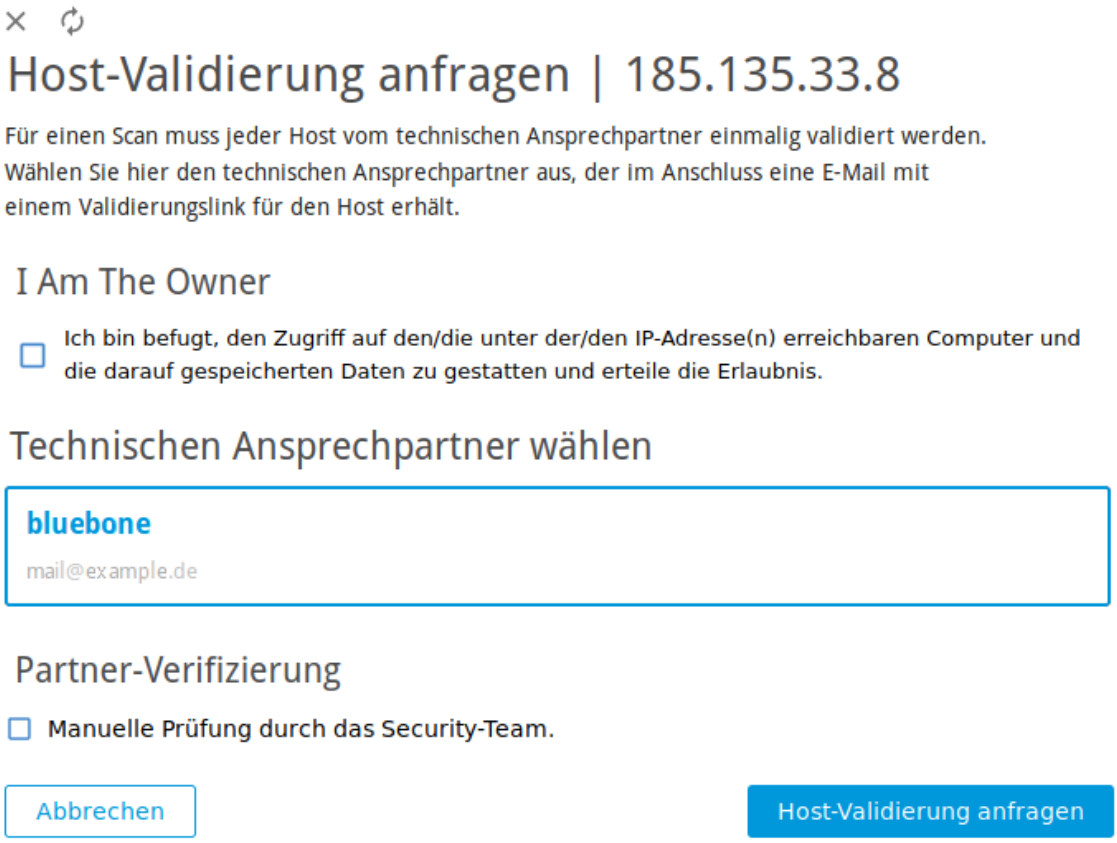

Abb. 6.3: Auswählen eines Kontakts für die Host-Validierung

6.2 Einen einfachen Scan manuell konfigurieren

Im Allgemeinen kann der Greenbone Cloud Service zwei unterschiedliche Vorgehensweisen nutzen, um ein Ziel zu scannen:

- Einfacher Scan
- Authentifizierter Scan mithilfe lokaler Sicherheitskontrollen (siehe Kapitel *6.3* (Seite 46))

Die folgenden Schritte müssen ausgeführt werden, um einen einfachen Scan zu konfigurieren:

- Erstellen eines Ziels (siehe Kapitel *6.2.1* (Seite 31))
- Validieren des/der Host(s) (siehe Kapitel *6.2.2* (Seite 35)) oder Erstellen eines Gateways (siehe Kapitel *6.2.3* (Seite 39))
- Erstellen einer Aufgabe (siehe Kapitel *6.2.4* (Seite 44))
- Starten der Aufgabe (siehe Kapitel *6.2.5* (Seite 46))

6.2.1 Ein Ziel erstellen

Der erste Schritt ist es, ein externes oder internes Scanziel zu erstellen.

6.2.1.1 Ein externes Ziel erstellen

1. *Ziele* (Kategorie *Scan-Konfiguration*) im Menüpanel wählen.
2. Auf *Externe Ziele* klicken.
3. Neues Ziel durch Klicken auf *+ Neues externes Ziel erstellen* erstellen.

4. Zielmodus durch Klicken auf *IP-Adresse* oder *Hostname* wählen. Er legt fest, in welcher Form das Ziel angegeben wird.

   Bemerkung: Der Zielmodus kann nach dem erstmaligen Erstellen des Ziels nicht mehr geändert werden.

   Ein gemischter Zielmodus ist nicht möglich.

5. Ziel definieren (siehe Abb.6.4).
6. Auf *Ziel erstellen* klicken.

   Bemerkung: Eine Host-Validierung ist zum Scannen eines externen Ziels notwendig (siehe Kapitel *6.2.2* (Seite 35)).

Die folgenden Informationen können eingegeben werden:

Zielname
Der Name kann frei gewählt werden. Falls möglich, sollte ein aussagekräftiger Name gewählt werden.

Beschreibung (optional)
Der optionale Kommentar erlaubt es, Hintergrundinformationen festzulegen. Diese erleichtern später das Verständnis des konfigurierten Ziel.

Zu scannende Hosts (für Zielmodus *IP-Adresse*)
Manuelle Eingabe der Hosts, die gescannt werden sollen, getrennt durch Kommas.

Bemerkung: Die IP-Adresse oder der Hostname wird benötigt. In beiden Fällen ist es nötig, dass sich der Greenbone Cloud Service mit dem System verbinden kann. Falls der Hostname verwendet wird, muss der Greenbone Cloud Service in der Lage sein, den Namen aufzuschlüsseln.

Für die Eingabe sind die folgenden Optionen möglich:

- Einzelne IPv4-Adresse, z. B. 192.168.15.5
- Domainname, z. B. example.com
- IPv4-Adressbereich, z. B. 192.168.15.5-192.168.15.27
- IPv4-Adressbereich in CIDR-Schreibweise, z. B. 192.168.15.0/24
- Einzelne IPv6-Adresse, z. B. fe80::222:64ff:fe76:4cea
- IPv6-Adressbereich in CIDR-Schreibweise, z. B. fe80::222:64ff:fe76:4cea/120

Mehrere Optionen können gemischt werden.

Vom Scan ausgeschlossene Hosts (für Zielmodus *IP-Adresse*)
Manuelle Eingabe der Hosts, die vom Scan ausgeschlossen werden sollen, getrennt durch Kommas.

Es gelten die gleichen Vorgaben wie für *Zu scannende Hosts*.

Zu scannende Hostnamen (für Zielmodus *Hostname*)
Manuelle Eingabe der Hosts, die gescannt werden sollen, getrennt durch Kommas.

Bemerkung: Der Hostname wird benötigt. Es ist nötig, dass sich der Greenbone Cloud Service mit dem System verbinden kann. Der Greenbone Cloud Service muss außerdem in der Lage sein, den Namen aufzuschlüsseln.

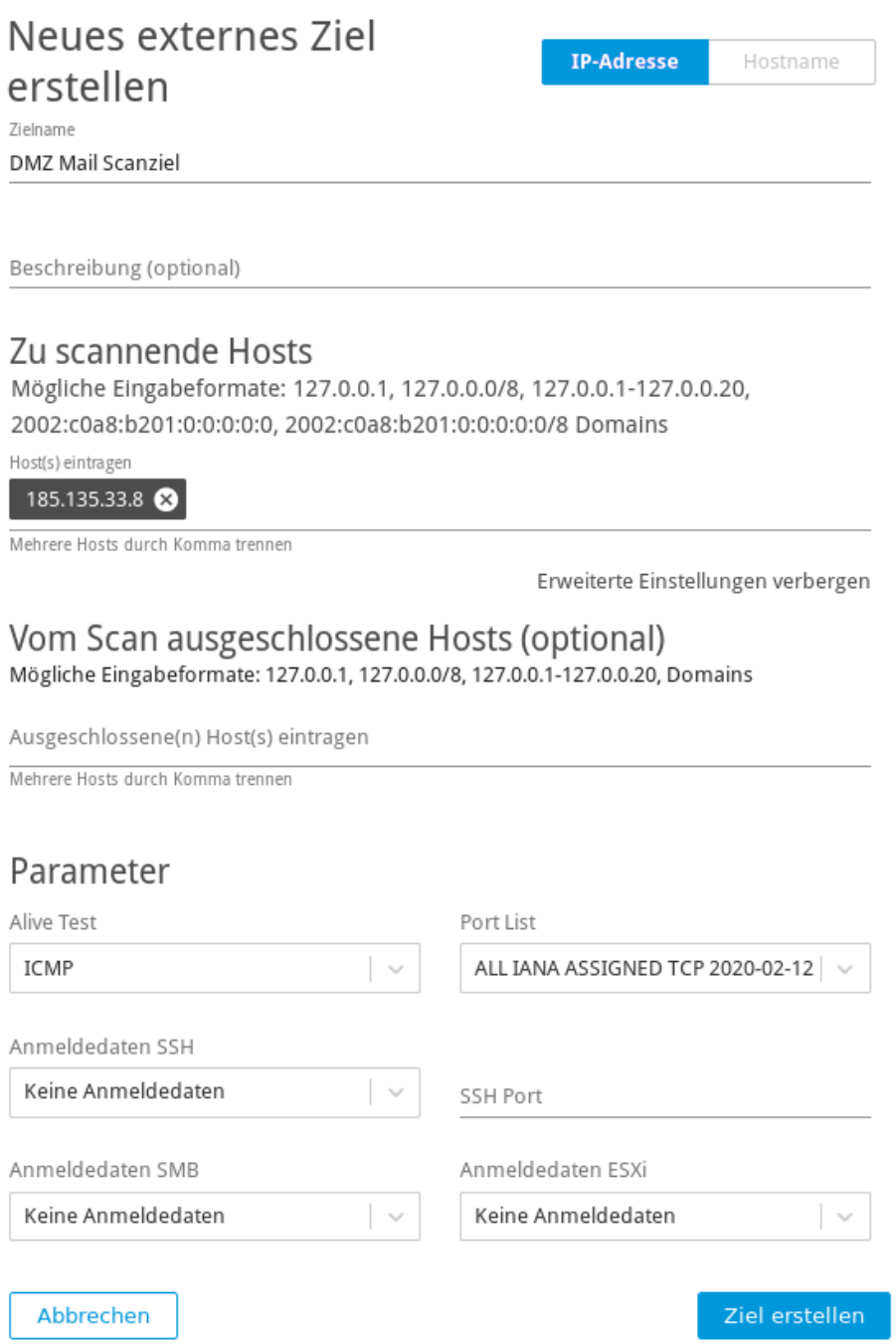

Abb. 6.4: Erstellen eines neuen Ziels

Alive Test
Diese Option legt die Methode fest, mit der geprüft wird, ob ein Ziel erreichbar ist. Die Möglichkeiten sind:

- TCP ack service
- ICMP
- Consider alive
- TCP syn service

Portliste
Portliste, die für den Scan genutzt wird (siehe Kapitel *6.9* (Seite 74)).

Anmeldedaten SSH
Auswahl eines Benutzers, der sich in das Zielsystem einloggen kann, falls dieses ein Linux- oder Unix-System ist. Dies ermöglicht einen authentifizierten Scan mit lokalen Sicherheitskontrollen (siehe Kapitel *6.3* (Seite 46)).

Anmeldedaten SMB
Auswahl eines Benutzers, der sich in das Zielsystem einloggen kann, falls dieses ein Microsoft-Windows-System ist. Dies ermöglicht einen authentifizierten Scan mit lokalen Sicherheitskontrollen (siehe Kapitel *6.3* (Seite 46)).

Anmeldedaten ESXi
Auswahl eines Benutzers, der sich in das Zielsystem einloggen kann, falls dieses ein VMware-ESXi-System ist. Dies ermöglicht einen authentifizierten Scan mit lokalen Sicherheitskontrollen (siehe Kapitel *6.3* (Seite 46)).

6.2.1.2 Ein internes Ziel erstellen

1. *Ziele* (Kategorie *Scan-Konfiguration*) im Menüpanel wählen.
2. Auf *Interne Ziele* klicken.
3. Neues Ziel durch Klicken auf *+ Neues internes Ziel erstellen* erstellen.
4. Ziel definieren.
5. Auf *Ziel erstellen* klicken.

Bemerkung: Ein Gateway muss zum Scannen eines internen Ziels genutzt werden (siehe Kapitel *6.2.3* (Seite 39)).

Die folgenden Informationen können eingegeben werden:

Zielname
Der Name kann frei gewählt werden. Falls möglich, sollte ein aussagekräftiger Name gewählt werden.

Beschreibung (optional)
Der optionale Kommentar erlaubt es, Hintergrundinformationen festzulegen. Diese erleichtern später das Verständnis des konfigurierten Ziel.

Zu scannende Hosts
Manuelle Eingabe der Hosts, die gescannt werden sollen, getrennt durch Kommas.

Bemerkung: Die IP-Adresse oder der Hostname wird benötigt. In beiden Fällen ist es nötig, dass sich der Greenbone Cloud Service mit dem System verbinden kann. Falls der Hostname verwendet wird, muss der Greenbone Cloud Service in der Lage sein, den Namen aufzuschlüsseln.

Für die Eingabe sind die folgenden Optionen möglich:

- Einzelne IPv4-Adresse, z. B. 192.168.15.5
- Domainname, z. B. example.com
- IPv4-Adressbereich, z. B. 192.168.15.5-192.168.15.27
- IPv4-Adressbereich in CIDR-Schreibweise, z. B. 192.168.15.0/24

Mehrere Optionen können gemischt werden.

Vom Scan ausgeschlossene Hosts (optional)
Manuelle Eingabe der Hosts, die vom Scan ausgeschlossen werden sollen, getrennt durch Kommas.

Es gelten die gleichen Vorgaben wie für *Zu scannende Hosts*.

Alive Test
Diese Option legt die Methode fest, mit der geprüft wird, ob ein Ziel erreichbar ist. Die Möglichkeiten sind:

- TCP ack service
- ICMP
- Consider alive
- TCP syn service

Portliste
Portliste, die für den Scan genutzt wird (siehe Kapitel *6.9* (Seite 74)).

Anmeldedaten SSH
Auswahl eines Benutzers, der sich in das Zielsystem einloggen kann, falls dieses ein Linux- oder Unix-System ist. Dies ermöglicht einen authentifizierten Scan mit lokalen Sicherheitskontrollen (siehe Kapitel *6.3* (Seite 46)).

Anmeldedaten SMB
Auswahl eines Benutzers, der sich in das Zielsystem einloggen kann, falls dieses ein Microsoft-Windows-System ist. Dies ermöglicht einen authentifizierten Scan mit lokalen Sicherheitskontrollen (siehe Kapitel *6.3* (Seite 46)).

Anmeldedaten ESXi
Auswahl eines Benutzers, der sich in das Zielsystem einloggen kann, falls dieses ein VMware-ESXi-System ist. Dies ermöglicht einen authentifizierten Scan mit lokalen Sicherheitskontrollen (siehe Kapitel *6.3* (Seite 46)).

6.2.2 Für externe Ziele: Hosts validieren

Falls ein externes Ziel erstellt wird, müssen die festgelegten Hosts validiert werden. Das Scannen von Zielen ohne Host-Validierung ist nicht möglich.

Ein Host kann durch die folgenden Personen validiert werden:

- Durch die Benutzer selbst, wenn sie den/die Host(s) besitzen
- Durch die für den/die Host(s) verantwortliche Person
- Durch das Security-Team des vMSP

6.2.2.1 Validierung durch den Benutzer als Besitzer

Der Host kann durch den Benutzer validiert werden.

Bemerkung: Der Nutzer muss bestätigen, dass er berechtigt ist, den Zugriff auf den/die unter der/den IP-Adresse(n) erreichbaren Computer und die darauf gespeicherten Daten zuzulassen. Mit dieser Zustimmung übernimmt der Nutzer die Verantwortung für die auf dem/den entsprechenden Computer(n) durchgeführten Schwachstellenscans sowie für alle Auswirkungen und Folgen, die sich aus den Scans ergeben können. Etwaige Beschwerden oder Anfragen Dritter werden von Greenbone direkt an den Nutzer weitergeleitet und Greenbone wird diese Beschwerden oder Anfragen weder weiter bearbeiten noch Unterstützung leisten.

---

1. *Ziele* (Kategorie *Scan-Konfiguration*) im Menüpanel wählen.
2. Auf *Externe Ziele* klicken.

   → Falls die Validierung noch nicht abgeschlossen wurde, wird Verification pending in der Spalte *Verifiziert* angezeigt.
3. In der Zeile des Ziels auf klicken.
4. Auf *Host-Validierung anfragen* klicken (siehe Abb.6.5).

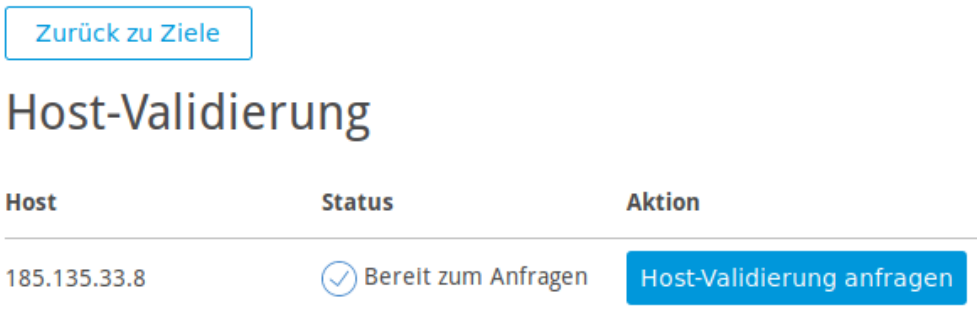

Abb. 6.5: Anfragen der Host-Validierung

5. Checkbox *I Am The Owner* aktivieren (siehe Abb.6.6).
6. Auf *Host validieren* klicken.

   → Wenn die Hosts validiert wurden, wird Host entries verified in der Spalte *Verifiziert* auf der Seite *Ziele* angezeigt.

6.2.2.2 Validierung durch die Kontaktperson oder durch das Security-Team des vMSP

Falls vorhanden, wird die verantwortliche Kontaktperson von RIPE NCC[2] bezogen. RIPE NCC ist die Regional Internet Registry (RIR) für Europa, den Nahen Osten und Teile Zentralasiens und übernimmt die Zuweisung und Registrierung von IP-Adressbereichen.

Falls kein Kontakt gefunden wird, müssen die Hosts manuell vom Security-Team des vMSP überprüft werden.

1. *Ziele* (Kategorie *Scan-Konfiguration*) im Menüpanel wählen.
2. Auf *Externe Ziele* klicken.

   → Falls die Validierung noch nicht abgeschlossen wurde, wird Verification pending in der Spalte *Verifiziert* angezeigt.

[2] https://www.ripe.net/

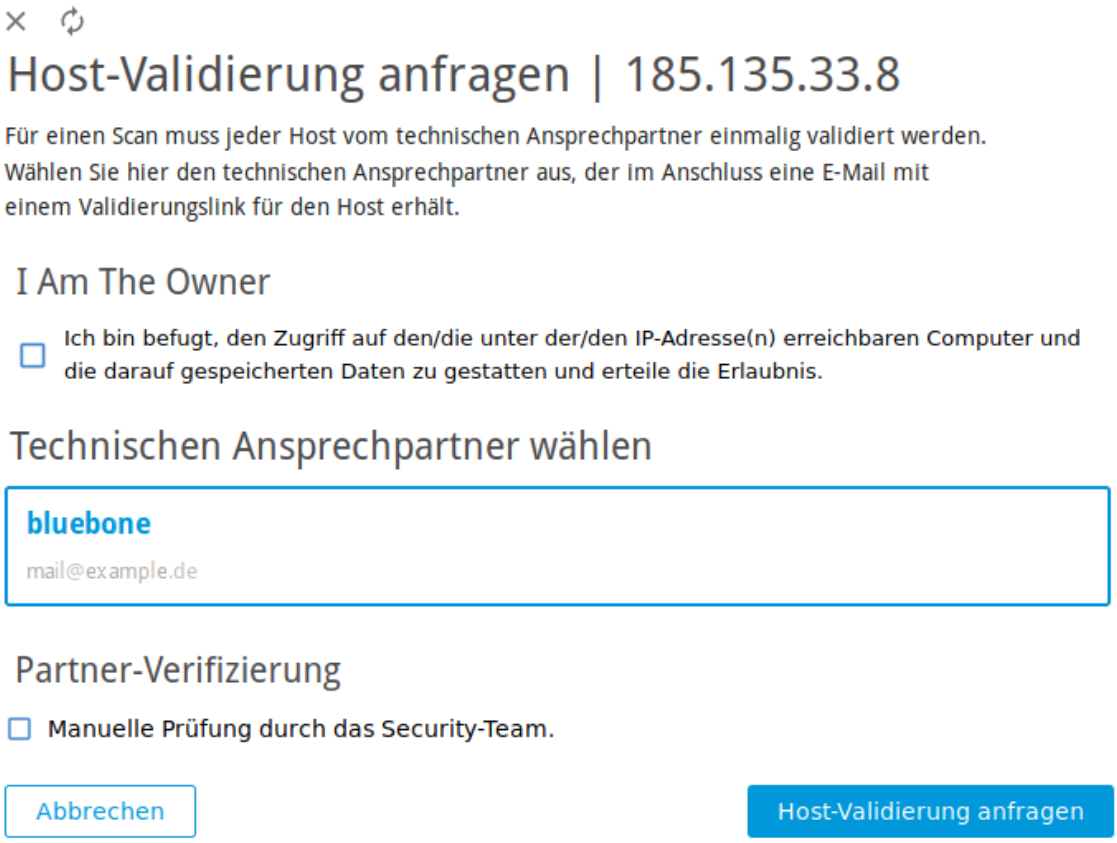

Abb. 6.6: Auswählen eines Kontakts für die Host-Validierung

3. In der Zeile des Ziels auf klicken.
4. Auf *Host-Validierung anfragen* klicken (siehe Abb.6.5).

   → Die Kontakte für den konfigurierten Host werden von RIPE NCC gesammelt.

   Wenn dieser Prozess abgeschlossen ist, zeigt ein Overlay den gefundenen Kontakt (siehe Abb.6.6).
5. Kontaktperson aus der Liste wählen.

   oder
5. Falls keine Kontaktperson gefunden wurde, Checkbox *Manuelle Prüfung durch das Security-Team.* aktivieren.
6. Auf *Host-Validierung anfragen* klicken.

   → Eine E-Mail wird an die Kontaktperson oder das Security-Team gesendet.

Bemerkung: Durch Klicken auf *Kontaktauswahl zurücksetzen* wird der gewählte Kontakt verworfen.

Falls die Hosts validiert wurden, wird Host entries verified in der Spalte *Verifiziert* auf der Seite *Ziele* angezeigt.

Falls die Host-Validierung abgelehnt wurde, wird Verification rejected in der Spalte *Verifiziert* auf der Seite *Ziele* angezeigt.

6.2.3 Für interne Ziele: Ein Gateway erstellen

Falls ein internes Ziel im Kunden-Netzwerk gescannt werden soll, muss ein Gateway genutzt werden.

Ressourcen

Das Gateway benötigt mindestens die folgenden Ressourcen:

- 1 virtuelle CPU
- 512 MB RAM
- 8 GB Festplatte

Unterstütze Hypervisoren

Die folgenden Hypervisoren werden offiziell für den Einsatz eines Gateways unterstützt:

- Microsoft Hyper-V, Version 5.0 oder höher
- VMware vSphere Hypervisor (ESXi), Version 6.0 oder höher

Bemerkung: Je nach verwendeter virtueller Umgebung müssen die unter *Konfiguration für Umgebung* beschriebenen Einstellungen vorgenommen werden (siehe Abb.6.7).

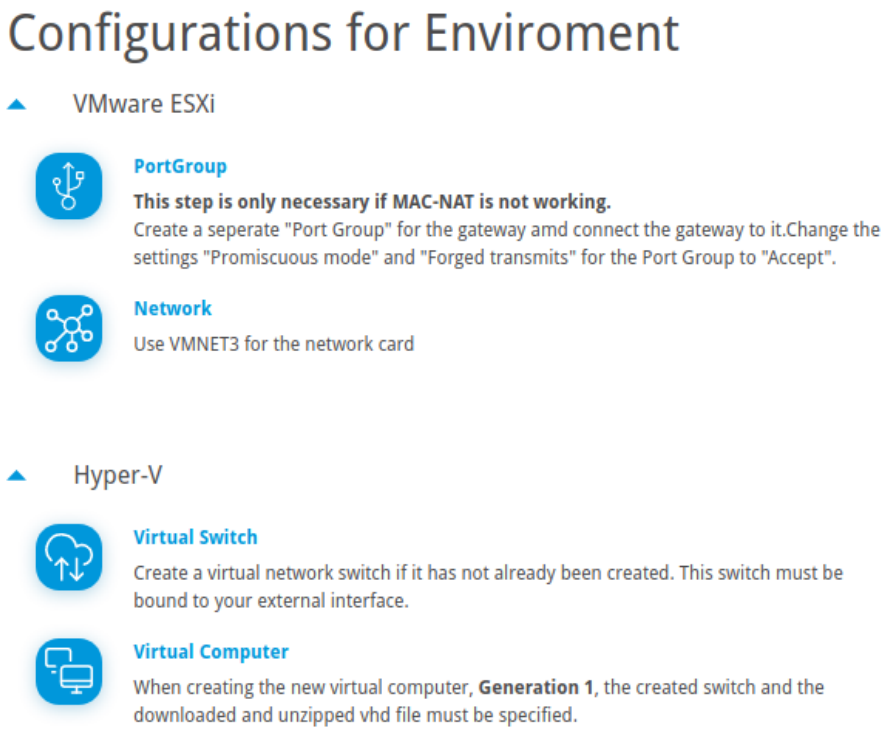

Abb. 6.7: Erweiterte Einstellungen der virtuellen Umgebung

Ein Gateway kann wie folgt erstellt werden:

1. *Gateways* (Kategorie *Scan-Konfiguration*) im Menüpanel wählen.
2. Gewünschte virtuelle Umgebung in der Drop-down-Liste *Download* wählen und auf klicken.
3. Gateway in die virtuelle Umgebung importieren.
4. Gateway in der virtuellen Umgebung starten.

5. Nachdem der Boot-Vorgang abgeschlossen ist, wird eine Eingabeaufforderung angezeigt. Die Standarddaten für den Login sind:
   - Anmeldename: `admin`
   - Passwort: `admin`

   → Das Gateway-Administrationsmenü wird geöffnet.
6. *Gateway configuration* wählen und `Enter` drücken.
7. *Set web password* wählen und `Enter` drücken.
8. Passwort zweimal eingeben und `Tab` drücken (siehe Abb.6.8).

Bemerkung: Das Passwort muss die folgenden Kriterien erfüllen:
- Mindestens 8 Zeichen
- Enthält Klein- und Großbuchstaben
- Enthält mindestens ein Sonderzeichen
- Enthält mindestens eine Zahl

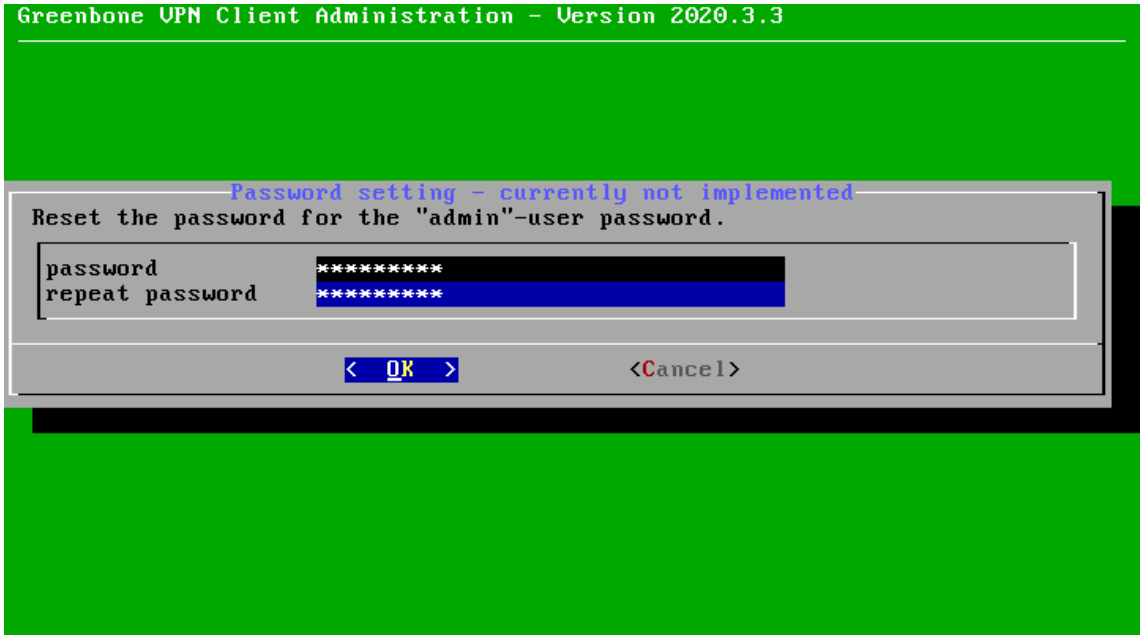

Abb. 6.8: Passwort für die Gateway-Web-Oberfläche einrichten

9. `Enter` drücken.
10. *Save changes* wählen und `Enter` drücken.

    → Es wird eine Nachricht angezeigt, dass das Gateway erfolgreich konfiguriert wurde.
11. `Enter` drücken, um die Nachricht zu schließen.
12. *Netzwork configuration* wählen und `Enter` drücken.

Bemerkung: Für alle Konfigurationsoptionen siehe Kapitel *6.6.2* (Seite 68).

13. Angezeigte IP-Adresse des Gateways notieren (siehe Abb.6.9). Sie wird für den Zugriff auf die Gateway-Web-Oberfläche benötigt.

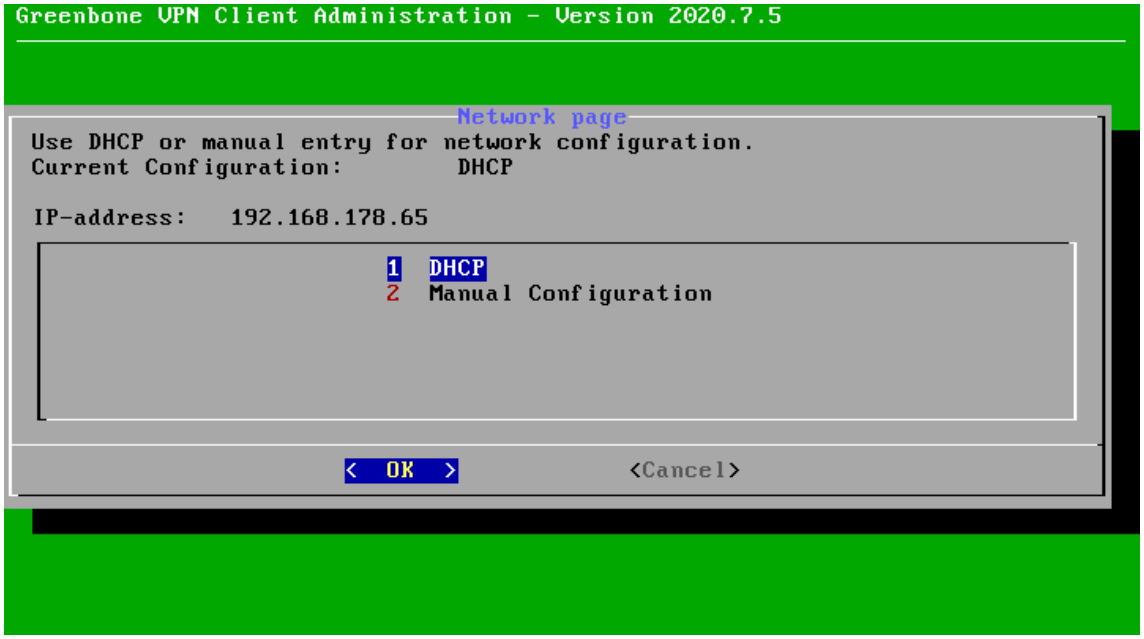

Abb. 6.9: IP-Adresse des Gateways

14. Auf der Plattform auf *+ Neues Gateway erstellen* klicken.

15. Textliche Beschreibung des Gateway-Standorts in das Eingabefeld *Standort* eingeben (siehe Abb.6.10).

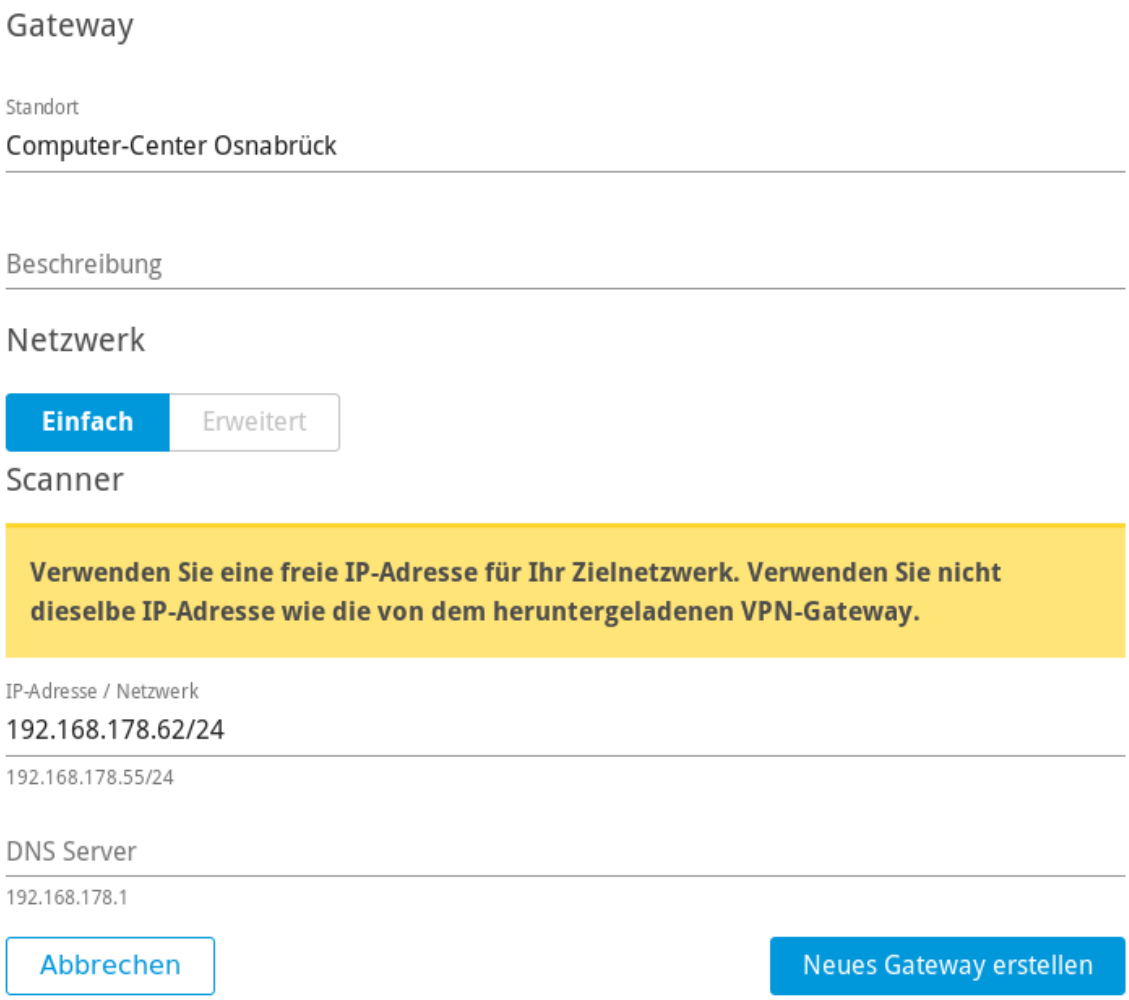

Abb. 6.10: Erstellen eines neuen Gateways

16. Optional: Beschreibung für das Gateway in das Eingabefeld *Beschreibung* eingeben.
17. Freie IP-Adresse aus dem Netzwerk, das gescannt werden soll, inklusive der Präfixlänge in das Eingabefeld *IP-Adresse/Netzwerk* eingeben.

Bemerkung: Die eingegebene IP-Adresse muss sich von der IP-Adresse des Gateways unterscheiden.

---

18. IP-Adresse eines DNS-Servers, der sich im Zielnetzwerk befindet, in das Eingabefeld *DNS Server* eingeben.

Bemerkung: Standardmäßig ist MAC-NAT aktiviert.

---

19. Falls MAC-NAT nicht funktioniert, auf *Erweitert* klicken und die Checkbox *MAC-NAT nutzen* deaktivieren.

Bemerkung: Wenn VMware ESXi die verwendete virtuelle Umgebung ist, müssen die Einstellungen konfiguriert werden, die auf der Seite *Gateways* unter *Konfiguration für Umgebung* angezeigt werden.

Bemerkung: Wenn ein Netzwerk gescannt werden soll, in dem sich der Scanner nicht befindet, kann das Netzwerk-Routing verwendet werden.

20. Auf *+ Netzwerk hinzufügen* klicken.
21. Route durch Eingabe des Netzwerks und des im Netzwerk befindlichen Gateways in die jeweiligen Eingabefelder definieren.
22. Metrikinformation in das Eingabefeld *Metrik* eingeben.

    Die Metrik ist wichtig, wenn es mehrere Routen für dasselbe Zielnetzwerk gibt. In diesem Fall ist die beste Route diejenige mit dem kleinsten Metrikwert.
23. Auf *Speichern* klicken.

    → Die Route wird in der Tabelle angezeigt.
24. Auf *Neues Gateway erstellen* klicken.

    → Das Gateway wird erstellt und auf der Seite *Gateways* angezeigt.

Das Gateway registrieren

Das Gateway muss entweder über die Gateway-Web-Oberfläche oder über das Gateway-Administrationsmenü (CLI) registriert werden.

Die Registrierung via Gateway-Web-Oberfläche wird wie folgt durchgeführt:

1. In der Zeile des Gateways auf ✎ klicken.
2. *WEB* wählen.
3. Auf *In die Zwischenablage kopieren* klicken, um den API-Schlüssel zu kopieren.
4. Webbrowser öffnen und folgende URL eingeben: `https://<ip>`. `<ip>` durch die IP-Adresse des Gateways ersetzen (siehe Schritt 13).
5. Mit dem Benutzernamen `admin` und dem Passwort, das in den Schritten 6 – 9 festgelegt wurde, einloggen.
6. *Settings* im Menüpanel wählen.
7. API-Schlüssel in das Eingabefeld *API-Key* einfügen.
8. Auf *Speichern* klicken.

   → Auf der Seite *Gateways* auf der Plattform wird in der Spalte *Status CONNECTED* angezeigt (siehe Abb.6.11).

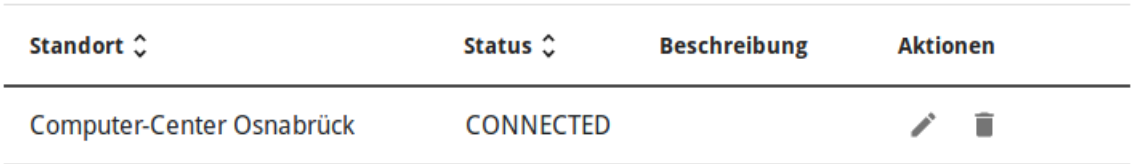

Abb. 6.11: Verbinden des Gateways

Die Registrierung via Gateway-Administrationsmenü (CLI) wird wie folgt durchgeführt:

1. In der Zeile des Gateways auf ✎ klicken.
2. *CLI* wählen.
3. URL und Token notieren.

4. In der CLI *Gateway configuration* wählen und `Enter` drücken.
5. *Enter connection token (Optional)* wählen und `Enter` drücken.
6. URL und Token in die entsprechenden Eingabefelder eingeben (siehe Abb.6.12).

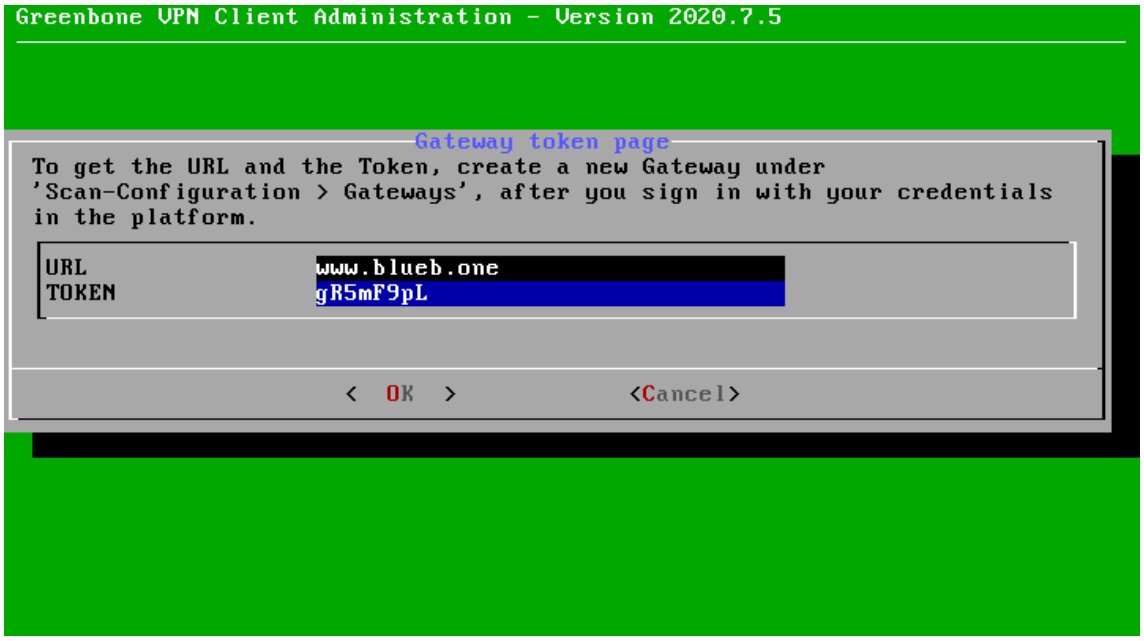

Abb. 6.12: Verbinden des Gateways

7. `Tab` und `Enter` drücken.

   → Auf der Seite *Gateways* auf der Plattform wird in der Spalte *Status CONNECTED* angezeigt (siehe Abb.6.11).

6.2.4 Eine Aufgabe erstellen

Der nächste Schritt ist das Erstellen einer Aufgabe.

Der Greenbone Cloud Service steuert die Ausführung von Scans mithilfe von Aufgaben. Diese Aufgaben können regelmäßig wiederholt oder zu bestimmten Zeiten ausgeführt werden (siehe Kapitel *6.4* (Seite 64)).

Eine Aufgabe kann wie folgt erstellt werden:

1. *Scan-Konfiguration* im Menüpanel wählen.
2. Neue Aufgabe durch Klicken auf *+ Neue Aufgabe erstellen* erstellen.
3. Aufgabe definieren (siehe Abb.6.13).
4. Auf *Scan-Aufgabe erstellen* klicken.

   → Die Aufgabe wird erstellt und auf der Seite *Scanverwaltung* angezeigt.

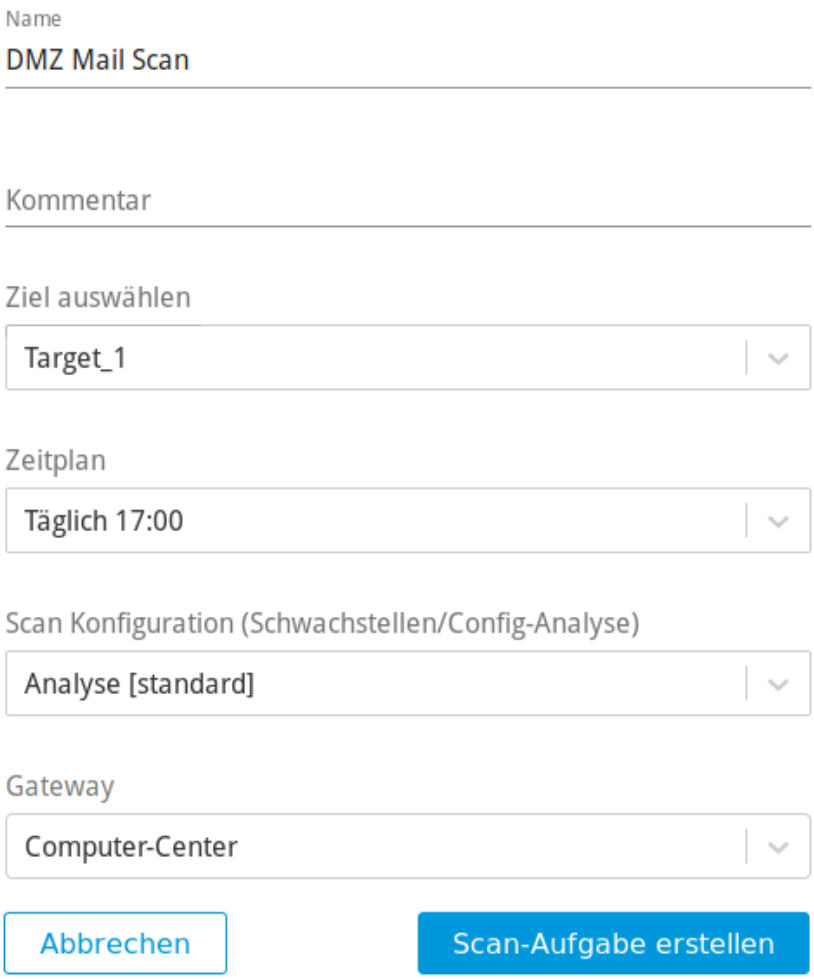

Abb. 6.13: Erstellen einer neuen Aufgabe

Die folgenden Informationen können eingegeben werden:

Name
Der Name kann frei gewählt werden. Falls möglich, sollte ein aussagekräftiger Name gewählt werden.

Kommentar
Der optionale Kommentar erlaubt es, Hintergrundinformationen festzuhalten. Diese erleichtern später das Verständnis der konfigurierten Aufgabe.

Ziel auswählen
Zuvor konfiguriertes Ziel aus der Drop-down-Liste wählen (siehe Kapitel *6.2.1* (Seite 31)).

Zeitplan
Zuvor konfigurierten Zeitplan aus der Drop-down-Liste wählen (siehe Kapitel *6.4* (Seite 64)). Die Aufgabe kann einmalig oder wiederholt zu einer festgelegten Zeit, z. B. jeden Montagmorgen um 6:00, durchgeführt werden.

Das Wählen eines Zeitplans ist optional. Falls kein Zeitplan genutzt werden soll, *Keinen Zeitplan verwenden* wählen.

Scan-Konfiguration
Die Scan-Konfiguration gibt an, welche Schwachstellentests während eines Scans durchgeführt werden.

Der Greenbone Cloud Service bietet verschiedene vordefinierte Scan-Konfigurationen (siehe Kapitel *6.8* (Seite 73)).

Die folgende Option ist nur sichtbar, falls ein interes Ziel gewählt wurde:

Gateway
Zuvor konfiguriertes Gateway aus der Drop-down-Liste wählen (siehe Kapitel *6.2.3* (Seite 39)).

6.2.5 Die Aufgabe starten

Scanverwaltung im Menüpanel wählen. In der Zeile der gewünschten Aufgabe auf ⊙ klicken.

→ Der Scan wird ausgeführt. Für den Status einer Aufgabe siehe Kapitel *6.7* (Seite 70).

Tipp: Sobald eine Aufgabe gestartet wurde, kann der Bericht der Aufgabe durch Klicken auf 🗎 dargestellt werden. Für das Lesen, Verwalten und Herunterladen von Berichten siehe Kapitel *7* (Seite 77).

Sobald sich der Status auf *Abgeschlossen* ändert, ist der gesamte Bericht verfügbar. Zu jeder Zeit können Zwischenergebnisse angesehen werden (siehe Kapitel *7.1* (Seite 77)).

Bemerkung: Die Fertigstellung des Scans kann einige Zeit in Anspruch nehmen. Die Seite aktualisiert automatisch, falls neue Daten verfügbar sind.

6.3 Einen authentifizierten Scan mit lokalen Sicherheitskontrollen konfigurieren

Ein authentifizierter Scan kann mehr Details über Schwachstellen auf dem gescannten System bereitstellen. Während eines authentifizierten Scans wird das Ziel sowohl von außen über das Netzwerk als auch von innen mithilfe eines gültigen Benutzerlogins gescannt.

Während eines authentifizierten Scans loggt sich der Greenbone Cloud Service in das Zielsystem ein, um lokale Sicherheitskontrollen durchzuführen. Der Scan benötigt die vorherige Erstellung von Anmeldedaten. Diese

Anmeldedaten werden für die Authentifizierung auf unterschiedlichen Diensten auf dem Zielsystem genutzt. Unter manchen Umständen können die Ergebnisse durch die Berechtigungen des Benutzers eingeschränkt werden.

Die VTs in den entsprechenden VT-Familien (lokale Sicherheitskontrollen) werden nur ausgeführt, falls sich der Greenbone Cloud Service in das Zielsystem einloggen konnten. Die VTs der lokalen Sicherheitskontrollen im resultierenden Scan sind minimalinvasiv.

Der Greenbone Cloud Service bestimmt nur die Risikostufe, aber nimmt keine Änderungen am Zielsystem vor. Trotzdem wird der Login des Greenbone Cloud Service wahrscheinlich in den Protokollen des Zielsystems vermerkt.

Der Greenbone Cloud Service kann unterschiedliche Anmeldedaten, basierend auf den Eigenschaften des Ziels, nutzen. Die wichtigsten sind:

- **SMB**
  Auf Microsoft-Windows-Systemen kann der Greenbone Cloud Service das Patchlevel und lokal installierte Software wie Adobe Acrobat Reader oder die Java-Suite prüfen.
- **SSH**
  Dieser Zugang wird für das Prüfen des Patchlevels von Unix- und Linuxsystemen genutzt.
- **ESXi**
  Dieser Zugang wird für das lokale Prüfen von VMware-ESXi-Servern genutzt.

6.3.1 Vorteile und Nachteile authentifizierter Scans

Der Umfang und Erfolg der Prüfroutinen für authentifizierte Scans hängen stark von den Berechtigungen des genutzten Benutzeraccounts ab.

Auf Linux-Systemen ist ein unprivilegierter Benutzer ausreichend und kann auf die meisten relevanten Informationen zugreifen, während ein unprivilegierter Benutzer auf Microsoft-Windows-Systemen sehr eingeschränkt ist und ein administrativer Benutzer mehr Ergebnisse liefert. Ein unprivilegierter Benutzer hat keinen Zugriff auf die Microsoft-Windows-Registrierungsdatenbank („Registrierung“) und den Microsoft-Windows-Systemorder `\windows`, welcher Informationen zu Updates und Patchlevels enthält.

Lokale Sicherheitskontrollen sind die schonendste Methode, um nach Schwachstellendetails zu suchen. Während Remote-Sicherheitsheitskontrollen ebenfalls versuchen, möglichst nicht-invasiv zu sein, verursachen sie einige Auswirkungen.

Einfach gesagt ähnelt ein authentifizierter Scan einem Whitebox-Ansatz. Der Greenbone Cloud Service hat Zugriff auf frühere Informationen und kann von innen auf das Ziel zugreifen. Insbesondere sind die Registrierung, Softwareversionen und Patchlevels zugänglich.

Ein Remotescan ähnelt einem Blackbox-Ansatz. Der Greenbone Cloud Service nutzt die gleichen Techniken und Protokolle wie ein potenzielle Angreifende, um von außen auf das Ziel zuzugreifen. Die einzigen verfügbaren Informationen werden vom Greenbone Cloud Service selbst gesammelt. Während einer Prüfung kann der Greenbone Cloud Service Fehlfunktionen auslösen, um Informationen über die genutzte Software zu erhalten, z. B. kann der Scanner eine fehlerhafte Anfrage an einen Dienst senden, um eine Antwort auszulösen, die weitere Informationen über das eingesetzte Produkt enthält.

Während eines Remotescans mit der Scan-Konfiguration *Analyse [Standard]* sind alle Remoteprüfungen sicher. Die genutzten VTs haben möglicherweise einige invasive Komponenten, aber keiner der genutzten VTs versucht, einen Defekt oder eine Fehlfunktion auf dem Ziel auszulösen (siehe Beispiel unten). Alle VTs mit sehr invasiven Komponenten oder solche, die einen Denial of Service (DoS) auslösen, werden automatisch von der Prüfung ausgeschlossen.

Beispiel für einen invasiven VT

Ein Beispiel für einen invasiven, aber sicheren VT ist der Heartbleed-VT. Er wird sogar ausgeführt, wenn VTs, die Schaden am Host-System anrichten können, deaktiviert sind, da der VT keine negativen Auswirkungen auf das Ziel hat.

Der VT ist trotzdem invasiv, da er die Speicherlecks des Ziels prüft. Falls das Ziel angreifbar ist, wird tatsächlicher Speicher des Ziels geleaked. Der Greenbone Cloud Service bewertet die geleakten Informationen nicht. Die Informationen werden umgehend gelöscht.

6.3.2 Anmeldedaten nutzen

Anmeldedaten für lokale Sicherheitsprüfungen werden benötigt, um VTs das Einloggen in ein Zielsystem zu ermöglichen, z. B. um das Vorhandensein aller Sicherheitspatches des Herstellers lokal zu prüfen.

6.3.2.1 Anmeldedaten erstellen

Neue Anmeldedaten können wie folgt erstellt werden:

1. *Anmeldedaten* (Kategorie *Scan-Konfiguration*) im Menüpanel wählen.
2. Neue Anmeldedaten durch Klicken auf *+ Neue Anmeldedaten erstellen* erstellen.
3. Anmeldedaten definieren (siehe Abb.6.14).

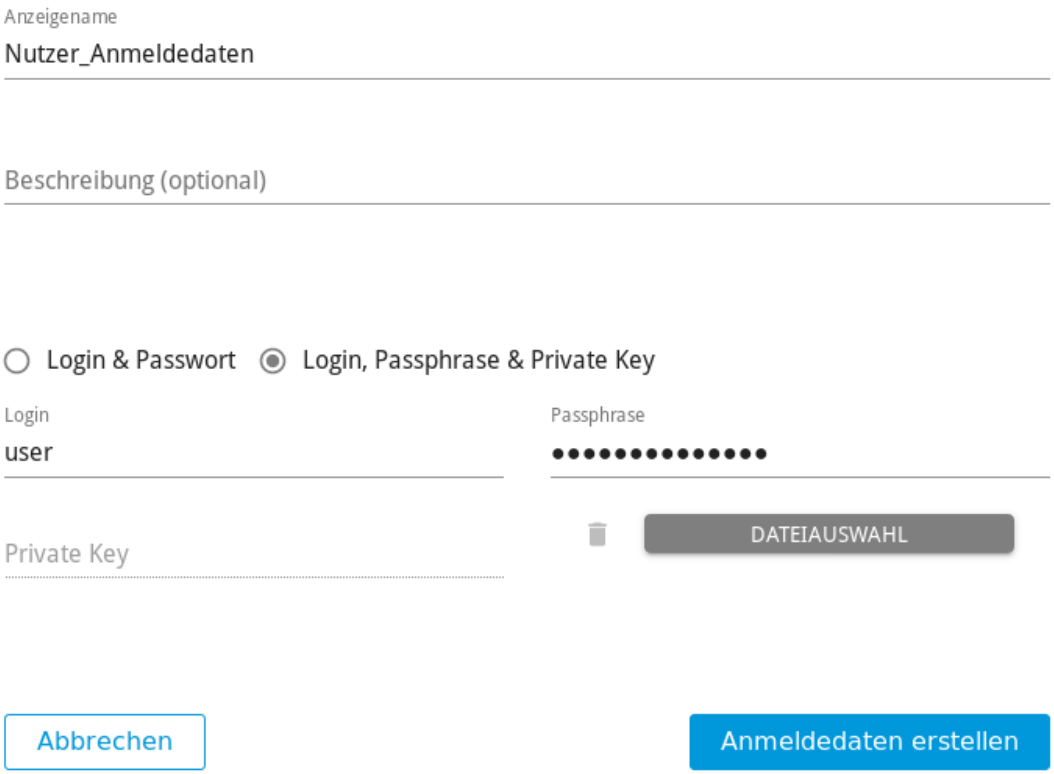

Abb. 6.14: Erstellen neuer Anmeldedaten

4. Auf *Anmeldedaten erstellen* klicken.

Die folgenden Details der Anmeldedaten können festgelegt werden:

Bemerkung: Falls die Details deutsche Umlaute enthalten, funktioniert der Login nicht. Die Umlaute müssen wie folgt ersetzt werden:

- „ß“ → „ss“
- „ä“ → „a“
- „ö“ → „o“
- „ü“ → „u“

Anzeigenamen
Festlegung des Namens. Der Name kann frei gewählt werden.

Beschreibung (optional)
Ein optionaler Kommentar kann zusätzliche Informationen enthalten.

Login & Passwort/Login, Passphrase & Private Key
Wahl des Anmeldedatentyps.

Abhängig vom gewählten Typen werden weitere Optionen angezeigt:

Login & Passwort

- **Login**
  Festlegung des Loginnamens, der vom Greenbone Cloud Service genutzt wird, um sich auf dem gescannten Zielsystem zu authentifizieren.
- **Passwort**
  Festlegung des Passworts, das vom Greenbone Cloud Service genutzt wird, um sich auf dem gescannten Zielsystem zu authentifizieren.

Login, Passphrase & Private Key

- **Login**
  Festlegung des Loginnamens, der vom Greenbone Cloud Service genutzt wird, um sich auf dem gescannten Zielsystem zu authentifizieren.
- **Passphrase**
  Festlegung der Passphrase des privaten SSH-Schlüssels.
- **Private Key**
  Privaten SSH-Schlüssel durch Klicken auf *DATEIAUSWAHL* hochladen.

  Eine hochgeladene Datei kann durch Klicken auf gelöscht werden.

6.3.2.2 Anmeldedaten verwalten

Alle vorhandenen Anmeldedaten können angezeigt werden, indem *Anmeldedaten* im Menüpanel gewählt wird.

Für alle Anmeldedaten werden die folgenden Informationen angezeigt:

Name
Name der Anmeldedaten.

Anmeldename
Benutzername für die Anmeldedaten.

Kommentar
Optionale zusätzliche Informationen über die Anmeldedaten.

Für alle Anmeldedaten sind die folgenden Aktionen verfügbar:

- Die Anmeldedaten bearbeiten.
- Die Anmeldedaten löschen. Nur Anmeldedaten, die aktuell nicht genutzt werden, können gelöscht werden.

6.3.3 Anforderungen auf Zielsystemen mit Microsoft Windows

6.3.3.1 Allgemeine Hinweise zur Konfiguration

- Der Dienst der Remote-Registrierung muss gestartet werden, um auf die Registrierung zuzugreifen.

  Dies wird erreicht, indem das automatischte Starten des Diensts eingestellt wird. Falls ein automatischer Start nicht bevorzugt wird, kann ein manueller Start konfiguriert werden. In diesem Fall wird der Dienst, während das System vom Greenbone Cloud Service gescannt wird, gestartet und anschließend wieder deaktiviert. Um dieses Verhalten sicherzustellen, muss der folgende Punkt über LocalAccountTokenFilterPolicy beachtet werden.

- Es ist notwendig, dass für alle gescannten Systeme der Datei- und Druckerzugriff aktiviert ist. Falls Microsoft Windows XP genutzt wird, muss die Einstellung *Use Simple File Sharing* deaktiviert sein.

- Für einzelne Systeme, die nicht mit einer Domäne verbunden sind, muss der folgende Registrierungsschlüssel festgelegt werden:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\
DWORD: LocalAccountTokenFilterPolicy = 1
```

- Auf Systemen mit Domänen-Controller muss der genutzte Benutzeraccount Mitglied der Gruppe *Domain Administrators* sein, um die bestmöglichen Ergebnisse zu erhalten. Wegen des Berechtigungskonzepts ist es nicht möglich, alle Schwachstellen zu erkennen, wenn der *Local Administrator* oder die von der Domain zugewiesenen Administratoren genutzt werden. Alternativ können die Anweisungen in Kapitel *6.3.3.2* (Seite 52) befolgt werden.

- Sollte ein *Local Administrator* gewählt werden – was ausdrücklich nicht empfohlen wird – ist es auch notwendig, den folgenden Registrierungsschlüssel festzulegen:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\
DWORD: LocalAccountTokenFilterPolicy = 1
```

- Generiertes Installationspaket für Anmeldedaten: Das Installationsprogramm stellt den Remote-Registrierungsdienst auf automatisches Starten ein. Falls das Installationsprogramm auf einem Domänen-Controller ausgeführt wird, wird der Benutzeraccount der Gruppe *BUILTIN/Administratoren* (`SID S-1-5-32-544`) zugeordnet.

- Auf der Microsoft-Windows-Firewall muss eine Ausnahmeregel für den Greenbone Cloud Service erstellt werden. Zusätzlich muss auf XP-Systemen der Dienst *File and Printer Sharing* auf *enabled* eingestellt sein.

- Generiertes Installationspaket für Anmeldedaten: Während der Installation bietet das Installationsprogramm einen Dialog, um die IP-Adresse des Greenbone Cloud Service einzugeben. Wenn die Eingabe bestätigt wird, wird eine Regel für die Firewall konfiguriert. Der Dienst *File and Printer Sharing* wird in den Regeln der Firewall aktiviert.

6.3.3.2 Einen Domänenaccount für authentifizierte Scans konfigurieren

Für authentifizierte Scans von Microsoft-Windows-Zielsystemen wird die Nutzung eines Domänenaccounts mit einer Domänenrichtlinie, die lokale Administratorprivilegien erteilt, empfohlen. Dies hat mehrere Vorteile:

- Eine Domänenrichtlinie muss nur einmal erstellt werden und kann dann für unterschiedliche Benutzer angewendet oder widerrufen werden.
- Das lokale Bearbeiten der Registrierung von Microsoft Windows ist nicht länger nötig. Die Benutzerverwaltung ist somit zentralisiert, was auf lange Sicht Zeit spart und mögliche Konfigurationsfehler reduziert.
- Aus Sicht der Schwachstellenbewertung ermöglicht nur ein Domänenaccount die Erkennung domänenzugehöriger Scanergebnisse. Diese Ergebnisse fehlen, falls ein ein lokaler Benutzeraccount genutzt wird.
- Es gibt auch einige Sicherheitsvorteile beim Nutzen eines Domänenaccounts mit einer Domänenrichtlinie, die von Greenbone Networks emfohlen wird: Der zugehörige Benutzer kann sich möglicherweise nicht lokal oder über die Remotedesktopverbindung einloggen, was etwaige Angriffsvektoren begrenzt. Zusätzlich werden die Anmeldedaten via Kerberos geschützt, während bei einem Passwort eines lokalen Benutzers ein höheres Risiko des Ausnutzens besteht.

Um einen Domänenaccount für hostbasierte Remote-Audits auf einem Microsoft-Windows-Ziel zu nutzen, muss die folgende Konfiguration unter Windows XP Professional, Windows Vista, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows 7, Windows 8, Windows 8.1 oder Windows 10 geschehen. Das System muss auch Teil der Domäne sein.

Eine Sicherheitsgruppe erstellen

1. In einen Domänen-Controller einloggen und *Active Directory Users and Computers* öffnen.
2. *Aktion* > *Neu* > *Gruppe* in der Menüleiste wählen.
3. `Greenbone Local Scan` in das Eingabefeld *Name* eingeben.
4. *Global* für *Gruppenbereich* und *Sicherheit für Gruppentyp* wählen.
5. Account, der unter Microsoft Windows für die lokalen authentifizierten Scans vom Greenbone Cloud Service genutzt wird, zur Gruppe hinzufügen.
6. Auf *OK* klicken.

Eine Gruppenrichtlinie (engl. Group Policy Object, GPO) erstellen

1. Im linken Panel die Konsole *Gruppenrichtlinienverwaltung* öffnen.
2. Auf *Gruppenrichtlinienobjekte* rechtsklicken und *Neu* wählen.
3. `Greenbone Local SecRights` in das Eingabefeld *Name* eingeben (siehe Abb.6.15).
4. Auf *OK* klicken.

Konfigurieren der Richtlinie

1. Auf die Richtlinie *Greenbone Local SecRights* klicken und *Bearbeiten...* wählen.
2. *Computerkonfiguration* > *Richtlinien* > *Windows-Einstellungen* > *Sicherheitseinstellungen* im linken Panel wählen.
3. Auf *Eingeschränkte Gruppen* klicken und *Gruppe hinzufügen* wählen.
4. Auf *Durchsuchen...* klicken und `Greenbone Local Scan` in das Eingabefeld eingeben (siehe Abb.6.16).
5. Auf *Namen überprüfen* klicken.
6. Zweimal auf *OK* klicken, um die offenen Fenster zu schließen.
7. Bei *Diese Gruppe ist Mitglied von* auf *Hinzufügen...* klicken.

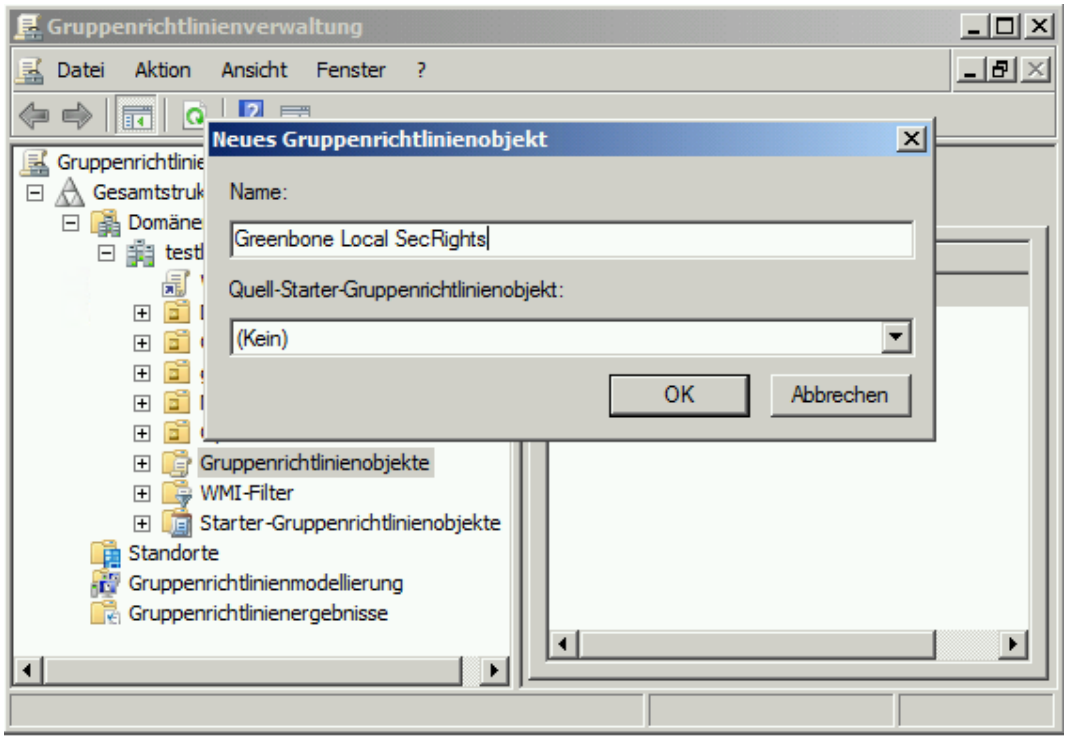

Abb. 6.15: Erstellen einer neuen Microsoft-Windows-Gruppenrichtlinie für Scans durch Greenbone

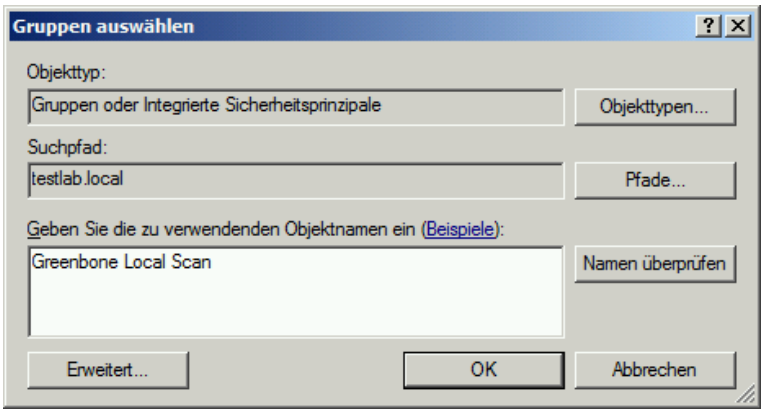

Abb. 6.16: Prüfen der Microsoft-Windows-Gruppennamen

8. `Administrators` in das Eingabefeld *Gruppe* eingeben (siehe Abb.6.17) und zweimal auf *OK* klicken, um die offenen Fenster zu schließen.

Bemerkung: Auf nicht-englischsprachigen Systemen den entsprechenden Namen der lokalen Administratorengruppe eingeben.

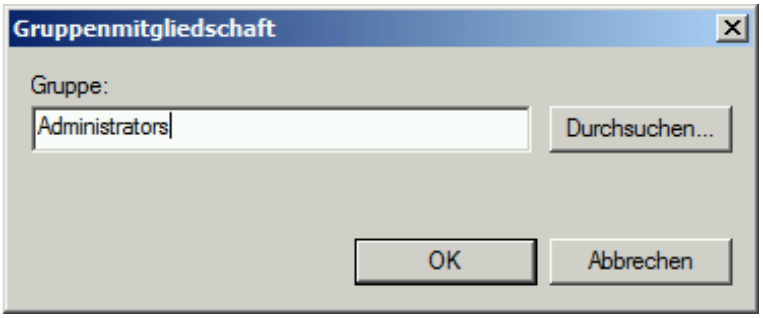

Abb. 6.17: Hinzufügen einer Gruppenmitgliedschaft

Konfigurieren der Richtlinie, sodass der Gruppe Greenbone Local Scan das lokale Einloggen in das System verweigert wird

1. Auf die Richtlinie *Greenbone Local SecRights* klicken und *Bearbeiten...* wählen.
2. *Computerkonfiguration > Richtlinien > Windows-Einstellungen > Sicherheitseinstellungen > Lokale Richtlinien > Zuweisen von Benutzerrechten* im linken Panel wählen.
3. Im rechten Panel auf *Lokal anmelden verweigern* doppelklicken.
4. Checkbox *Diese Richtlinieneinstellungen definieren* aktivieren und auf *Benutzer oder Gruppe hinzufügen* klicken.
5. Auf *Durchsuchen...* klicken und `Greenbone Local Scan` in das Eingabefeld eingeben (siehe Abb.6.18).
6. Auf *Namen überprüfen* klicken.
7. Dreimal auf *OK* klicken, um die offenen Fenster zu schließen.

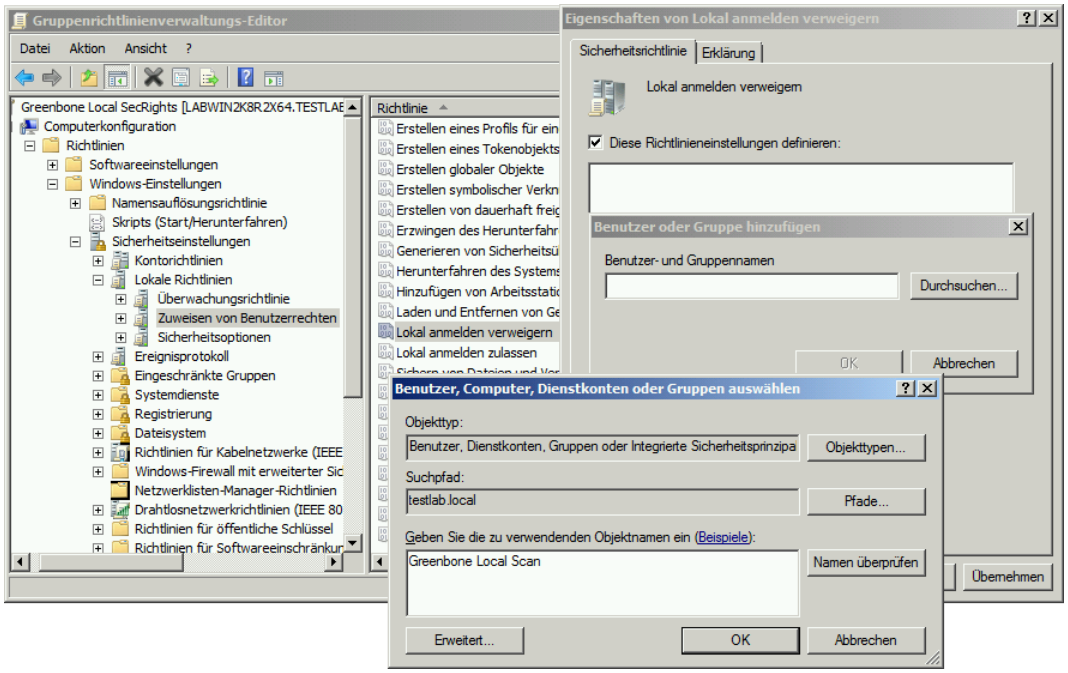

Abb. 6.18: Bearbeiten der Richtlinie

Konfigurieren der Richtlinie, sodass der Gruppe Greenbone Local Scan das remote Einloggen in das System verweigert wird

1. Auf die Richtlinie *Greenbone Local SecRights* klicken und *Bearbeiten...* wählen.
2. *Computerkonfiguration > Richtlinien > Windows-Einstellungen > Sicherheitseinstellungen > Lokale Richtlinien > Zuweisen von Benutzerrechten* im linken Panel wählen.
3. Im rechten Panel auf *Anmelden über Remotedesktopdienst verweigern* doppelklicken.
4. Checkbox *Diese Richtlinieneinstellungen definieren* aktivieren und auf *Benutzer oder Gruppe hinzufügen* klicken.
5. Auf *Durchsuchen...* klicken und `Greenbone Local Scan` in das Eingabefeld eingeben (siehe Abb.6.19).
6. Auf *Namen überprüfen* klicken.
7. Dreimal auf *OK* klicken, um die offenen Fenster zu schließen.

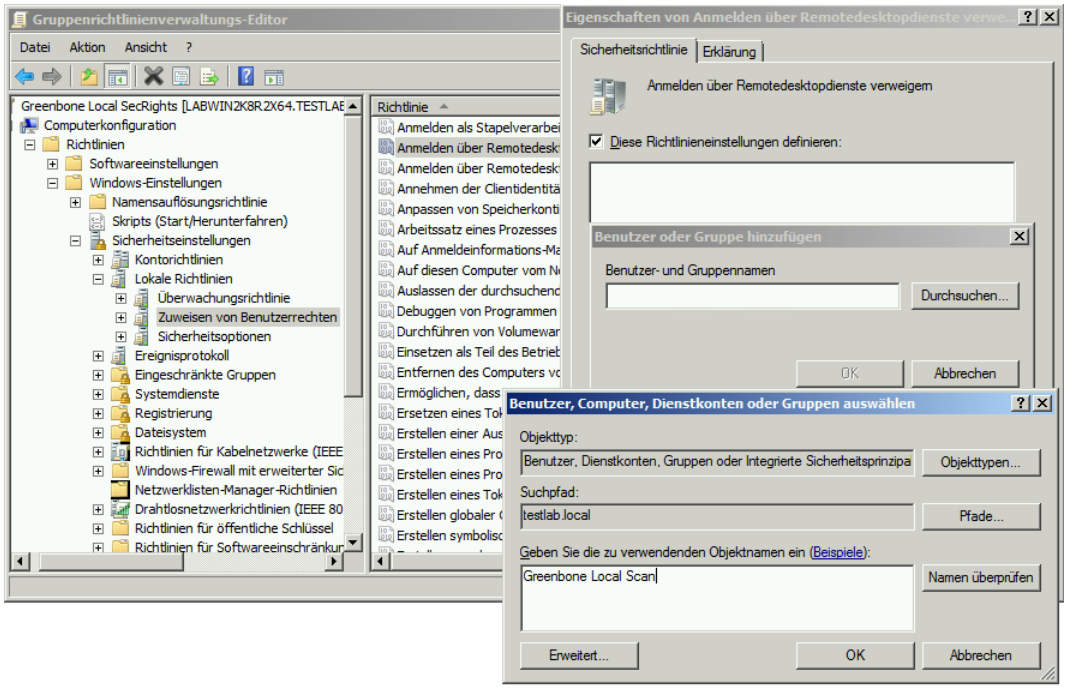

Abb. 6.19: Bearbeiten der Richtlinie

Konfigurieren der Richtlinie, sodass die Gruppe Greenbone Local Scan auf der Registrierung nur Leserechte hat

---

Wichtig: Diese Einstellung ist auch nach Entfernen der Gruppenrichtlinie vorhanden („tattooing GPO“).

Dies ändert grundlegende Privilegien, welche nicht einfach durch Entfernen der Gruppenrichtlinie rückgängig gemacht werden können.

Es muss geprüft werden, ob die Einstellungen mit der Umgebung kompatibel sind.

Bemerkung: Die folgenden Schritte sind optional.

---

1. Im linken Panel auf *Registrierung* klicken und *Schlüssel hinzufügen. . .* wählen.
2. *USERS* wählen und auf *OK* klicken (siehe Abb.6.20).
3. Auf *Erweitert* und *Hinzufügen* klicken.
4. `Greenbone Local Scan` in das Eingabefeld eingeben und auf *OK* klicken (siehe Abb.6.21).
5. *Dieses Objekt und untergeordnete Objekte* in der Drop-down-Liste *Übernehmen für* wählen.
6. Alle Checkboxen für *Zulassen* deaktivieren und Checkboxen *Wert festlegen*, *Unterschlüssel erstellen*, *Link erstellen*, *Löschen*, *Berechtigungen ändern* und *Besitz übernehmen* für *Verweigern* aktivieren (siehe Abb.6.22).
7. Zweimal auf *OK* klicken und Warnung durch Klicken auf *Ja* bestätigen.
8. Auf *OK* klicken.
9. Radiobuttons *Diesen Schlüssel konfigurieren* und *Vererbbare Berechtigungen an alle Unterschlüssel verteilen* wählen und auf *OK* klicken (siehe Abb.6.23).
10. Schritte 2 bis 9 für *MACHINE* und *CLASSES_ROOT* wiederholen.

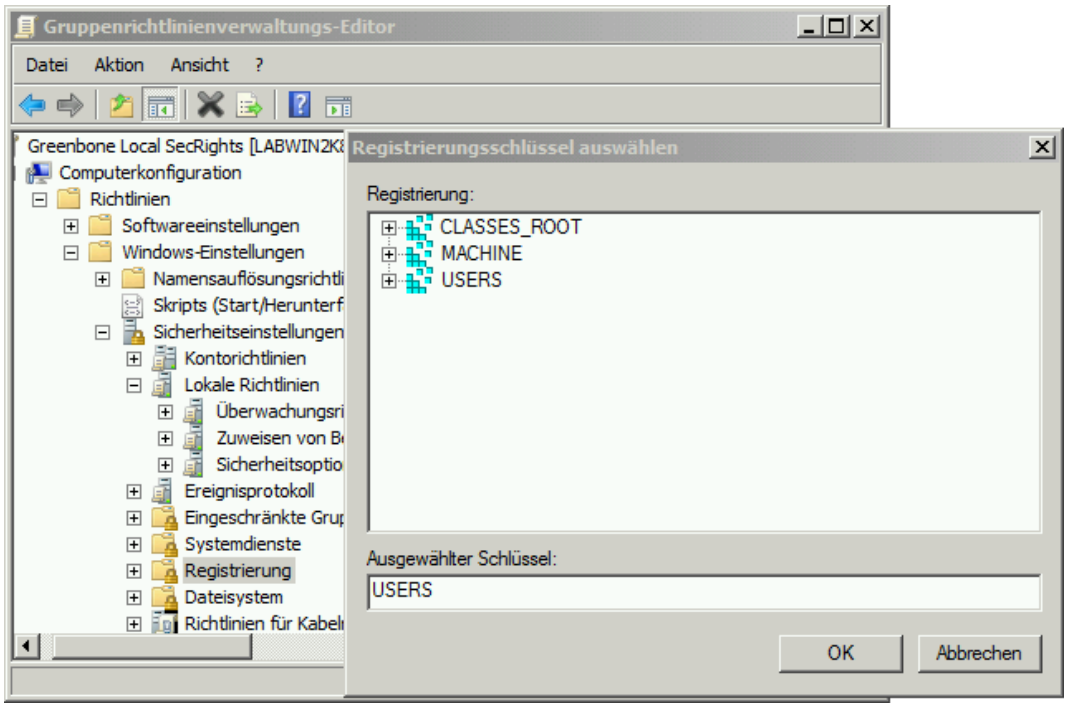

Abb. 6.20: Wählen des Registrierungsschlüssels

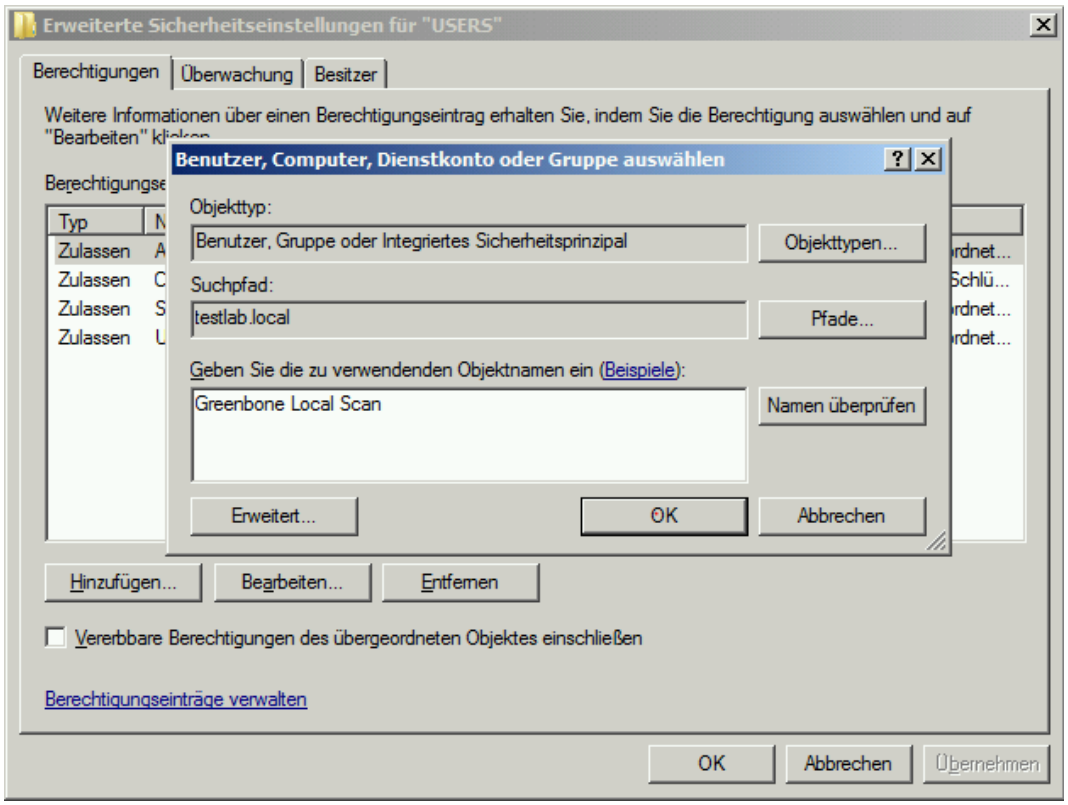

Abb. 6.21: Wählen der Gruppe *Greenbone Local Scan*

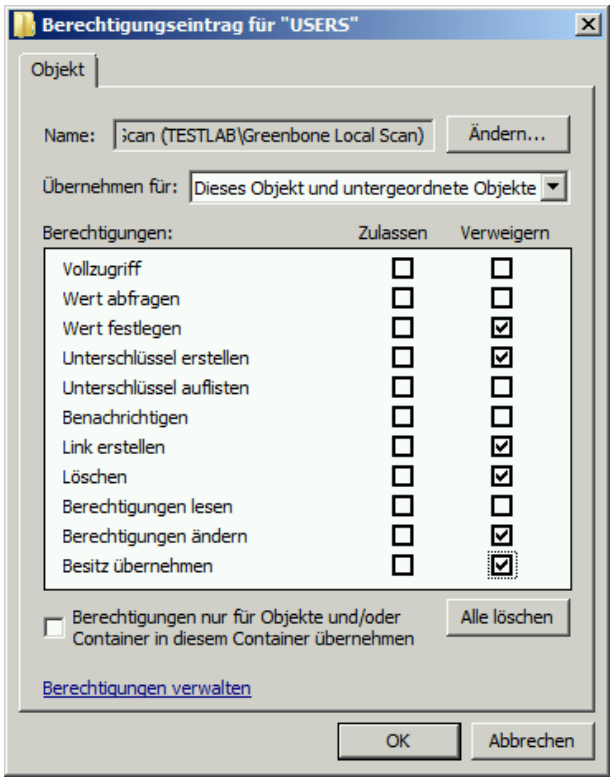

Abb. 6.22: Verweigern der Bearbeitung der Registrierung

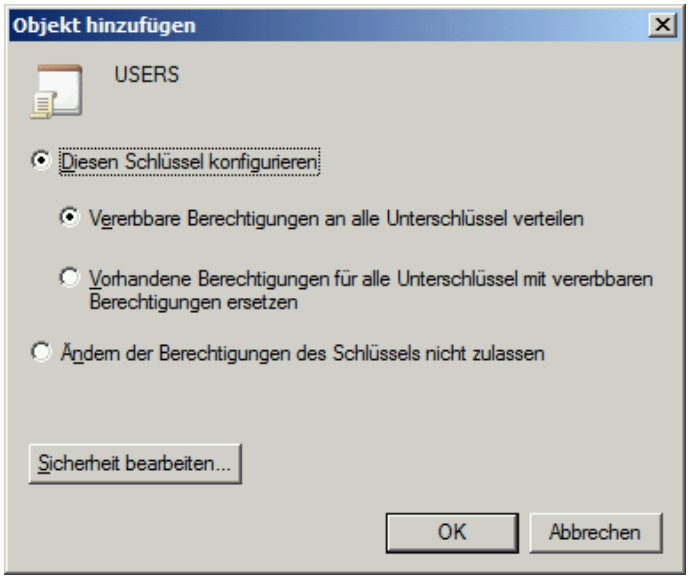

Abb. 6.23: Rekursivmachen der Berechtigungen

Die Gruppenrichtlinie verbinden

1. Im rechten Panel auf die Domäne rechtsklicken und *Vorhandenes Gruppenrichtlinienobjekt verknüpfen* wählen.
2. *Greenbone Local SecRights* im Abschnitt *Gruppenrichtlinienobjekte* wählen und auf *OK* klicken (siehe Abb.6.24).

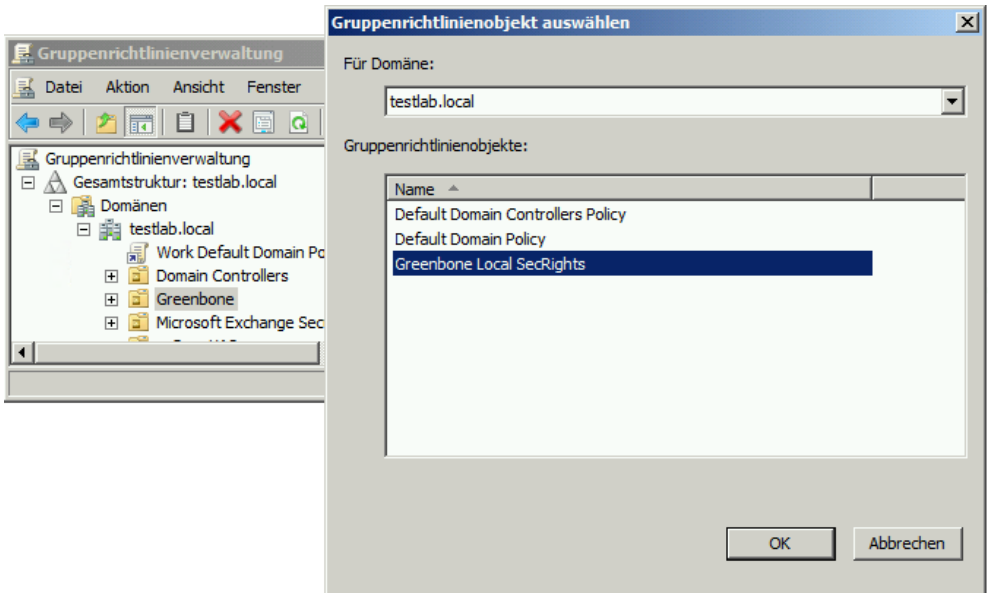

Abb. 6.24: Verbinden der Richtlinie

6.3.3.3 Einschränkungen

Da Schreibrechte auf der Registrierung und dem Systemlaufwerk entfernt wurden, funktionieren die beiden folgenden Tests nicht mehr:

- **`Leave information on scanned Windows hosts` OID 1.3.6.1.4.1.25623.1.0.96171**
  Falls gewünscht, erstellt dieser Test Informationen über den Start und das Ende eines Scans unter HKLM\Software\VulScanInfo. Da HKLM die Schreibrechte verweigert werden, ist dies nicht länger möglich. Falls der Test ausgeführt werden soll, muss das Gruppenrichtlinienobjekt entsprechend angepasst werden.
- **`Windows file Checksums` OID 1.3.6.1.4.1.25623.1.0.96180**
  Falls gewünscht, speichert dieser Test das Tool ReHash unter C:\Windows\system32 (auf 32-Bit-Systemen) oder C:\Windows\SysWOW64 (auf 64-Bit-Systemen). Da die Schreibrechte verweigert werden, ist dies nicht länger möglich. Falls der Test durchgeführt werden soll, muss das Tool separat gespeichert werden oder die Gruppenrichtlinie entsprechend angepasst werden.

6.3.3.4 Scannen ohne Domänenadministrator und lokale Administratorberechtigungen

Es ist möglich, eine Gruppenrichtlinie zu erstellen, in der der Benutzer keine lokalen Administratorberechtigungen hat. Allerdings ist der Aufwand, die entsprechenden Leserechte zu jedem Zweig und Ordner der Registrierung hinzuzufügen, sehr hoch. Leider ist das Vererben von Berechtigungen für viele Ordner und Zweige deaktiviert. Außerdem können diese Änderungen zwar durch die Gruppenrichtlinie festgelegt, aber nicht wieder entfernt werden („tattooing GPO“). Bestimmte Berechtigungen könnten überschrieben werden, sodass zusätzliche Probleme auftreten.

Das Erstellen einer Gruppenrichtlinie, in der der Benutzer keinerlei Administratorberechtigungen hat, ist aus technischer und administrativer Sicht nicht sinnvoll.

6.3.4 Anforderungen auf Zielsystemen mit Linux/Unix

- Für einen authentifizierten Scan auf Linux- oder Unix-Systemen ist in der Regel ein einfacher Benutzerzugang ausreichend. Der Login erfolgt dabei über SSH. Die Authentifizierung erfolgt entweder über auf dem Greenbone Cloud Service hinterlegte Passwörter oder über einen SSH-Schlüssel.
- Es muss sichergestellt werden, dass die Authentifizierung mit dem öffentlichen Schlüssel nicht durch den SSH-Daemon verhindert wird. Die Zeile `PubkeyAuthentication no` darf nicht vorhanden sein.
- Vorhandene SSH-Schlüssel können auch genutzt werden. SSH-Schlüssel können mit OpenSSH mithilfe des Befehls `ssh-keygen` auf Linux oder `puttygen.exe` beim Nutzen von PuTTY auf Microsoft Windows generiert werden. Die Formate Ed25519 oder RSA werden empfohlen. Alle SSH-Schlüssel müssen RFC 4716[3] entsprechen.
- Für Scans, die das Prüfen von Richtlinien beinhalten, sind möglicherweise root-Berechtigungen oder die Mitgliedschaft in bestimmten Gruppe (oft `wheel`) nötig. Aus Sicherheitsgründen sind einige Konfigurationsdateien nur von Super-Benutzern oder Mitgliedern bestimmter Gruppen lesbar.

[3] https://datatracker.ietf.org/doc/html/rfc4716

6.3.5 Anforderungen auf Zielsystemen mit ESXi

Bemerkung: Wenn eine vCenter Server Appliance (VCSA) zur Steuerung von ESXi-Hosts verwendet wird und User auf der VCSA erstellt werden, sind sie nur auf der VCSA und nicht auf den ESXi-Hosts bekannt.

Scan-User müssen auf jedem ESXi-Host, der gescannt wird, erstellt werden.

Standardmäßig sind lokale ESXi-User auf Rollen ohne Schreibrechte beschränkt. Es muss entweder ein administrativer Account oder eine Read-only-Rolle mit Berechtigung für globale Einstellungen genutzt werden.

Eine Read-only-Rolle mit Berechtigung für globale Einstellungen kann wie folgt eingerichtet werden:

1. Web-Oberfläche der VMware ESXi-Instanz öffnen und einloggen.
2. *Host* > *Verwalten* in der Spalte *Navigator* links wählen.
3. Register *Sicherheit und Benutzer* wählen.
4. *Rollen* im linken Menüpanel wählen (siehe Abb.6.25).

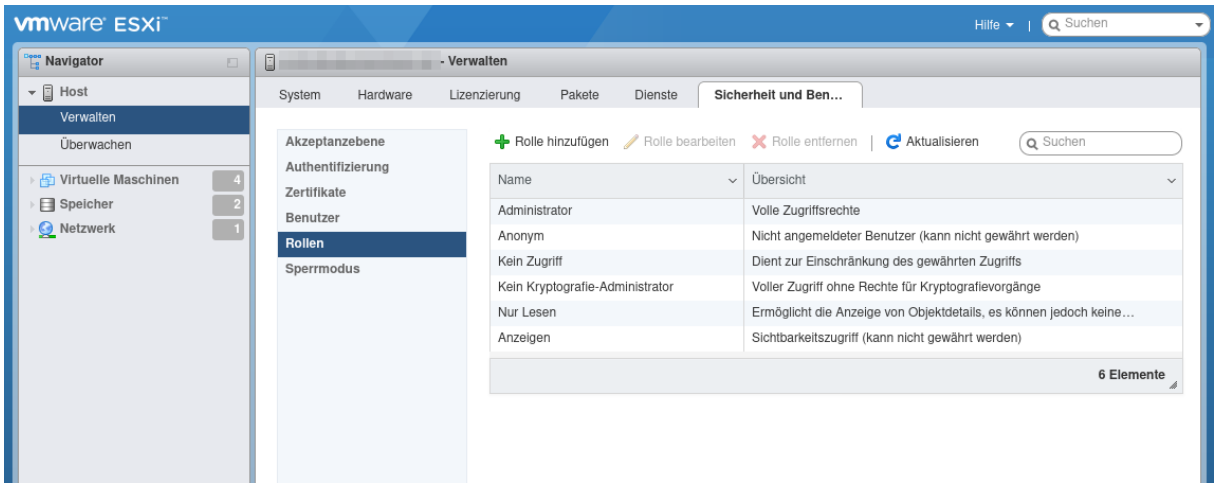

Abb. 6.25: Anzeigen der Rollen

5. Auf *Rolle hinzufügen* klicken.
6. Namen für die Rolle in das Eingabefeld *Rollenname* eingeben.
7. Checkbox *System* aktivieren.
8. Auf *Global* klicken und Checkbox *Settings* aktivieren (siehe Abb.6.26).
9. Auf *Hinzufügen* klicken.
10. In der Spalte *Navigator* links auf *Host* rechtsklicken und *Berechtigungen* wählen.
11. Scan-Useraccount, der vom Greenbone Cloud Service genutzt wird, wählen.
12. Auf *Rolle zuweisen* klicken.
13. Zuvor erstellte Rolle in der Drop-down-Liste wählen (siehe Abb.6.27).
14. Auf *Rolle zuweisen* klicken.
15. Auf *Schließen* klicken.

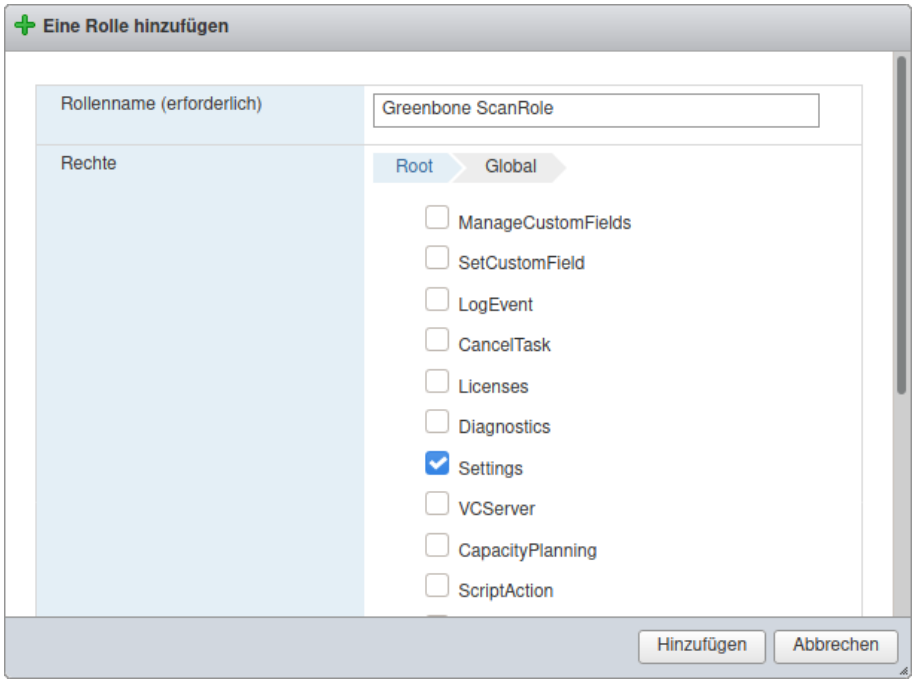

Abb. 6.26: Erstellen einer Rolle

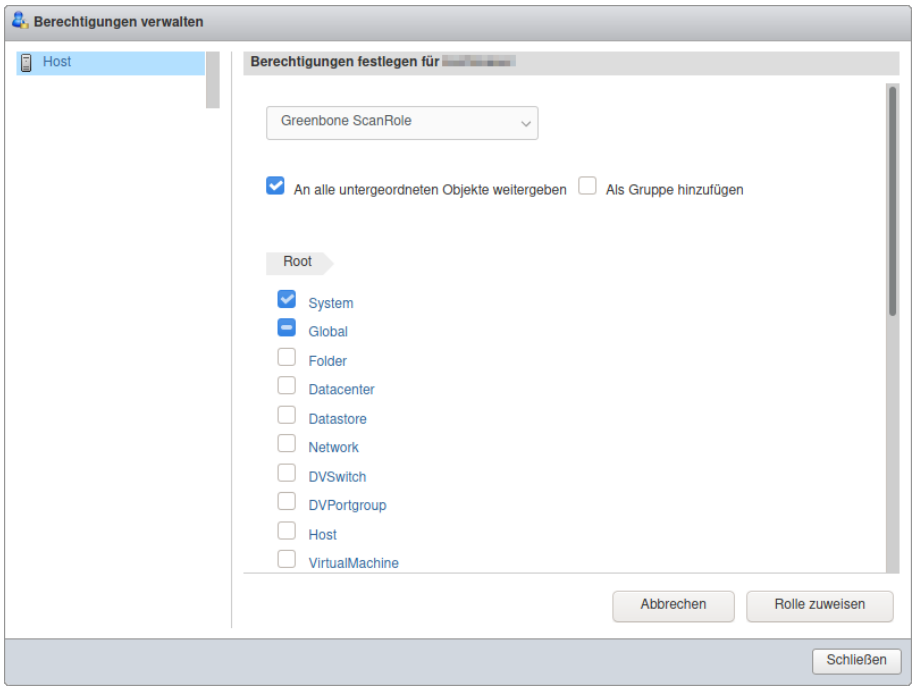

Abb. 6.27: Zuweisen der Rolle an den Scan-Benutzer

6.3.6 Anforderungen auf Zielsystemen mit Cisco OS

Der Greenbone Cloud Service kann auch Netzwerkkomponenten wie Router und Switches auf Schwachstellen prüfen. Während die üblichen Netzwerkdienste über das Netzwerk gefunden und geprüft werden, können einige Schwachstellen durch einen authentifizierten Scan entdeckt werden.

Der Greenbone Cloud Service benötigt aktuell nur den Befehl `show version`, um die aktuelle Version der Firmware des Geräts zu erhalten.

Um einen weniger privilegierten Benutzer einzurichten, der nur diesen Befehl ausführen darf, sind verschiedene Ansätze möglich. Das folgende Beispiel nutzt die rollenbasierte Zugriffskontrollenfunktionalität.

Tipp: Bevor eines der folgenden Beispiele genutzt wird, muss sichergestellt werden, dass alle Nebeneffekte der Konfiguration verstanden werden. Falls sie ohne Verifizierung genutzt wird, beschränkt das System möglicherweise weitere Logins über SSH oder die Konsole.

Um die rollenbasierte Zugriffskontrolle zu nutzen, müssen AAA und Views aktiviert werden:

```
> enable
# configure terminal
(config)# aaa new-model
(config)# exit
> enable view
# configure terminal
```

Der folgende Befehl erstellt eine eingeschränkte Sicht, die nur den Befehl `show version` beinhaltet. Das gelieferte Passwort `view-pw` ist nicht kritisch:

```
(config)# parser view gcs-view
(config-view)# secret 0 view-pw
(config-view)# commands exec include show version
(config-view)# exit
```

Nun wird der Benutzer `gcs-user` mit dem Passwort `gcs-pw` erstellt und mit der Sicht `gcs-view` verknüpft:

```
(config)# username gcs-user view gcs-view password 0 gcs-pw
(config)# aaa authorization console
(config)# aaa authorization exec default local
```

Falls SSH noch nicht aktiviert ist, erledigt dies der folgende Befehl. Der entsprechende Hostname und die entsprechende Domäne müssen genutzt werden:

```
(config)# hostname switch
(config)# ip domain-name greenbone.net
(config)# crypto key generate rsa general-keys modulus 2048
```

SSH-Logins mithilfe des folgenden Befehls aktivieren:

```
(config)# line vty 0 4
(config-line)# transport input ssh
(config-line)# Crtl-Z
```

Die Anmeldedaten des Benutzers müssen auf den GCS eingegebene werden. *Anmeldedaten* (Kategorie *Scan-Konfiguration* im Menüpanel wählen und den entsprechenden Benutzer erstellen (siehe Kapitel *6.3.2* (Seite 49)).

Anmeldedaten mit dem Ziel verbinden, damit sie als SSH-Anmeldedaten genutzt werden können.

6.4 Einen geplanten Scan ausführen

Für ein durchgehendes Schwachstellenmanagement ist das manuelle Ausführen von Aufgaben umständlich. Der Greenbone Cloud Service unterstützt zur Automatisierung die Zeitplanung von Aufgaben und bezeichnen automatische Scans zu festgelegten Zeiten als Zeitpläne. Sie können einmalig oder wiederholt ausgeführt werden.

6.4.1 Einen Zeitplan erstellen

Ein neuer Zeitplan kann wie folgt erstellt werden:

1. *Zeitpläne* (Kategorie *Scan-Konfiguration*) im Menüpanel wählen.
2. Neuen Zeitplan durch Klicken auf *+ Neuen Zeitplan erstellen* erstellen.
3. Zeitplan definieren (siehe Abb.6.28).

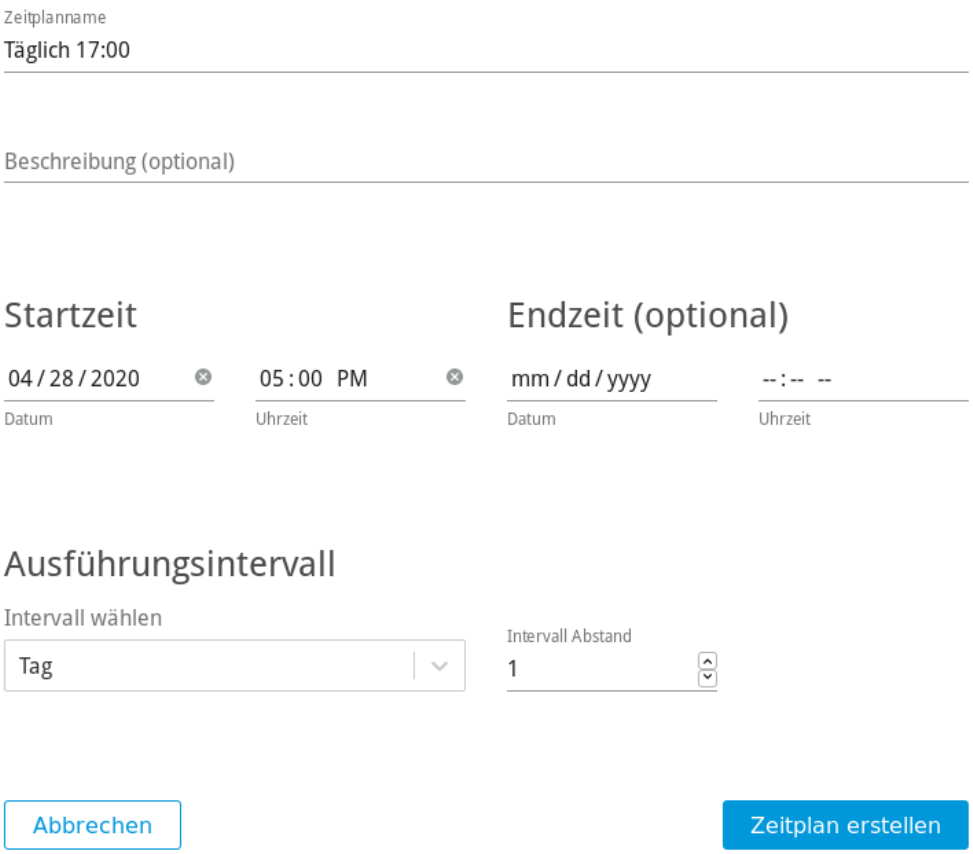

Abb. 6.28: Erstellen eines neuen Zeitplans

4. Auf *Zeitplan erstellen* klicken.

   → Der Zeitplan wird erstellt und kann beim Erstellen einer neuen Aufgabe gewählt werden (siehe Kapitel *6.2.4* (Seite 44)).

Die folgenden Details des Zeitplans können festgelegt werden:

Zeitplanname
Festlegung des Namens. Der Name kann frei gewählt werden.

Beschreibung (optional)
Ein optionaler Kommentar kann zusätzliche Informationen enthalten.

Startzeit
Festlegen des Datums und der Uhrzeit für den Start des ersten Scans.

Endzeit (optional)
Festlegen des Datums und der Uhrzeit für das Ende des ersten Scans.

Wenn keine Endzeit festgelegt wird, läuft der Scan auf unbestimmte Zeit, bis er abgeschlossen ist.

Ausführungsintervall
Festlegen der Wiederholungsrate der Aufgabe. Es kann zwischen *Täglich*, *Wöchentlich* und *Monatlich* gewählt werden. Zusätzlich wird der Abstand zwischen den Intervallen festgelegt.

Beispiel: eine geplante Aufgabe mit einem Intervall *Wöchentlich* und einem Intervallabstand von *2* wird alle zwei Wochen ausgeführt.

6.4.2 Zeitpläne verwalten

Alle vorhandenen Zeitpläne können angezeigt werden, indem *Zeitpläne* (Kategorie *Scan-Konfiguration*) im Menüpanel gewählt wird.

Für alle Zeitpläne werden die folgenden Informationen angezeigt:

Name
Name des Zeitplans.

Kommentar
Optionale Beschreibung des Zeitplans.

Startzeit
Startzeit der ersten Ausführung der Aufgabe.

Endzeit
Optionale Endzeit der ersten Ausführung der Aufgabe.

Intervalltyp
Zeitabstand zwischen zwei Ausführungen der Aufgabe.

Intervallabstand
Abstand zwischen den Intervallen.

Für alle Zeitpläne sind die folgenden Aktionen verfügbar:

- Den Zeitplan bearbeiten.
- Den Zeitplan löschen. Nur Zeitpläne, die aktuell nicht genutzt werden, können gelöscht werden.

6.5 Ziele verwalten

Alle vorhandenen Ziele können angezeigt werden, indem *Ziele* (Kategorie *Scan-Konfiguration*) im Menüpanel gewählt wird.

Interne Ziele

Für alle internen Ziele werden die folgenden Informationen angezeigt:

Name
: Name des Ziels.

Portliste
: Portliste, die genutzt wird, falls das Ziel für einen Scan genutzt wird (siehe Kapitel *6.2.4* (Seite 44)).

IP-Adressen
: Anzahl gescannter Hosts.

Für alle Ziele sind die folgenden Aktionen verfügbar:

- Ein Overlay mit detaillierten Informationen über das Ziel öffnen.
- Das Ziel bearbeiten.
- Das Ziel löschen. Nur Ziele, die aktuell nicht genutzt werden, können gelöscht werden.

Durch Klicken auf wird ein Overlay geöffnet (siehe Abb.6.29), das die folgenden Informationen enthält:

Zielname
Name des Ziels.

Zu scannende Hosts
Hosts, die gescannt werden, falls das Ziel für einen Scan genutzt wird (siehe Kapitel *6.2.4* (Seite 44)).

Portliste
Portliste, die genutzt wird, falls das Ziel für einen Scan genutzt wird (siehe Kapitel *6.2.4* (Seite 44)).

Anmeldedaten
Anmeldedaten, die für das Ziel konfiguriert wurden.

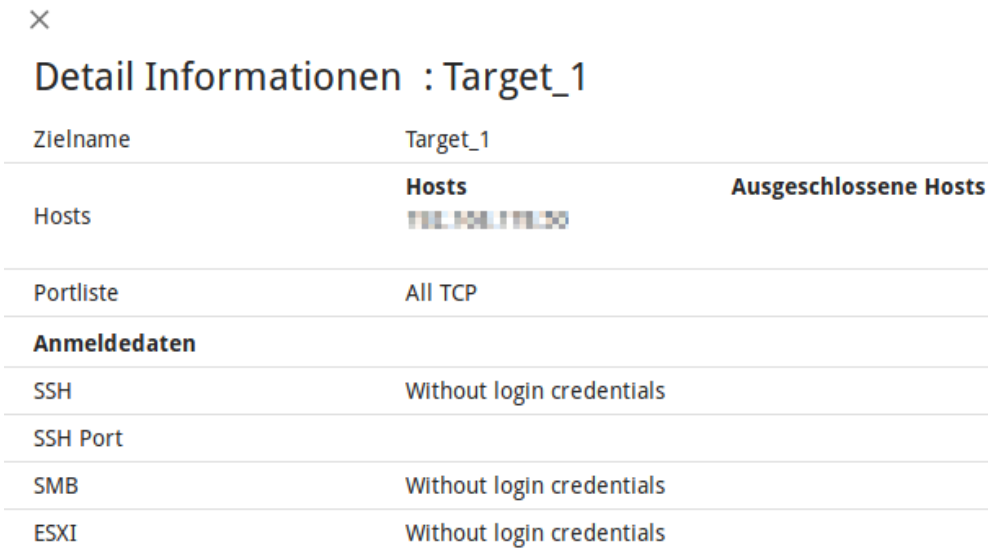

Abb. 6.29: Overlay mit Informationen über das Ziel

Externe Ziele

Für alle externen Ziele werden die folgenden Informationen angezeigt:

Name
Name des Ziels.

Portliste
Portliste, die genutzt wird, falls das Ziel für einen Scan genutzt wird (siehe Kapitel *6.2.4* (Seite 44)).

Verifiziert
Status der Validierung der konfigurierten Hosts.

IP-Adressen
Anzahl gescannter Hosts.

Für alle Ziele sind die folgenden Aktionen verfügbar:

- Ein Overlay mit detaillierten Informationen über das Ziel öffnen.
- Das Ziel bearbeiten.
- Das Ziel löschen. Nur Ziele, die aktuell nicht genutzt werden, können gelöscht werden.
- Ausstehende Host-Validierungen anzeigen.

Durch Klicken auf wird ein Overlay geöffnet (siehe Abb.6.29), das die folgenden Informationen enthält:

Zielname
Name des Ziels.

Zu scannende Hosts
Hosts, die gescannt werden, falls das Ziel für einen Scan genutzt wird (siehe Kapitel *6.2.4* (Seite 44)).

Portliste
Portliste, die genutzt wird, falls das Ziel für einen Scan genutzt wird (siehe Kapitel *6.2.4* (Seite 44)).

Anmeldedaten
Anmeldedaten, die für das Ziel konfiguriert wurden.

6.6 Gateways verwalten

6.6.1 Seite *Gateways*

Alle vorhandenen Gateways können angezeigt werden, indem *Gateways* (Kategorie *Scanverwaltung*) im Menüpanel gewählt wird.

Für alle Gateways werden die folgenden Informationen angezeigt:

Standort
Textliche Beschreibung des Standorts des Gateways.

Status
Status der Verbindung mit dem Scanner.

Beschreibung (optional)
Optionale Beschreibung des Gateways.

Für alle Gateways sind die folgenden Aktionen verfügbar:

- Das Gateway bearbeiten.
- Das Gateway löschen.

6.6.2 Gateway-Administrationsmenü (CLI)

Bemerkung: Das Gateway kann in Microsoft Hyper-V oder VMware ESXi importiert werden.

Netzwerkeinstellungen des Gateways werden mithilfe des Gateway-Administrationsmenüs verwaltet:

1. Gateway in der virtuellen Umgebung starten.
2. Nachdem der Boot-Vorgang abgeschlossen ist, in das Gateway-Administrationsmenü einloggen. Die Standarddaten für den Login sind:
   - Anmeldename: `admin`
   - Passwort: `admin`

   → Aktionen für das Gateway werden angezeigt (siehe Abb.6.30).

Die folgenden Aktionen sind verfügbar:

Network configuration
Netzwerk des Gateways durch Nutzung von DHCP oder durch manuelles Eingeben von IP-Adresse, Netzmaske, DNS und Gateway einrichten.

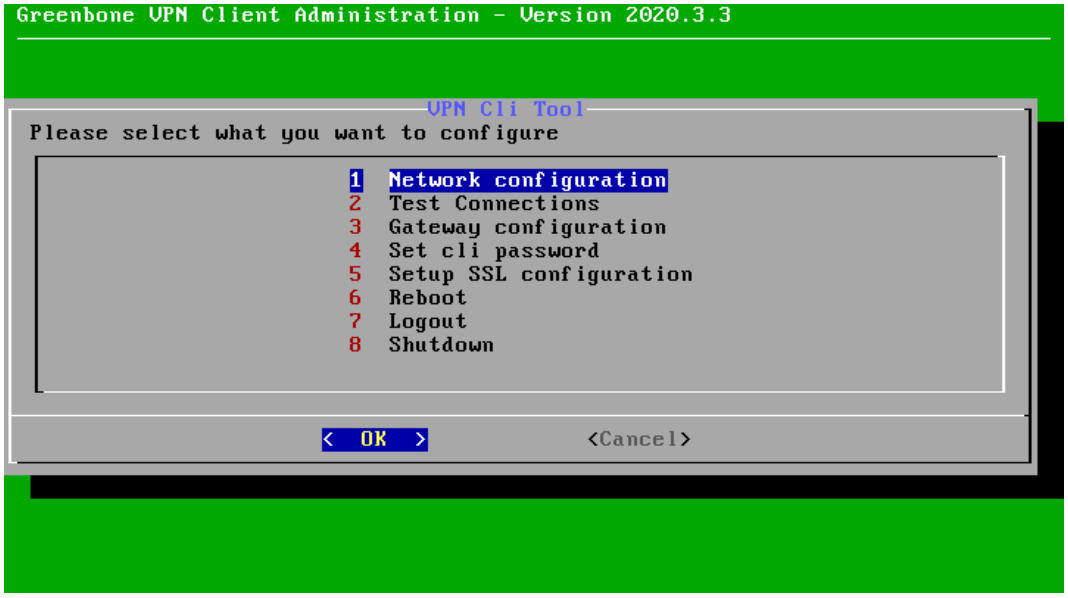

Abb. 6.30: Verwalten eines Gateways

Test connections
Prüfen, ob alle Gateway-Verbindungen wie vorgesehen funktionieren.

Gateway configuration
Passwort für die Gateway-Web-Oberfläche festlegen und das Gateway registrieren.

Set cli password
Passwort für das Gateway-Administrationsmenü (CLI) festlegen.

Setup SSL configuration
Ein neues SSL-Zertifikat einrichten.

Reboot
Das Gateway rebooten.

Logout
Aus dem Gateway-Administrationsmenü ausloggen.

Shutdown
Das Gateway herunterfahren.

6.6.3 Gateway-Web-Oberfläche

1. Webbrowser öffnen und folgende URL eingeben: `https://<ip>`. `<ip>` durch die IP-Adresse des Gateways ersetzen.

   Tipp: Die IP-Adresse kann im Gateway-Administrationsmenü angezeigt werden, indem *Network configuration* gewählt und `Enter` gedrückt wird (siehe Kapitel *6.6.2* (Seite 68)).

2. Mit dem Benutzernamen `admin` und dem Passwort, das im Gateway-Administrationsmenü festgelegt wurde, einloggen (siehe Kapitel *6.6.2* (Seite 68)).
3. Status und Ports des Gateways durch Klicken auf *Overview* im Menüpanel anzeigen.

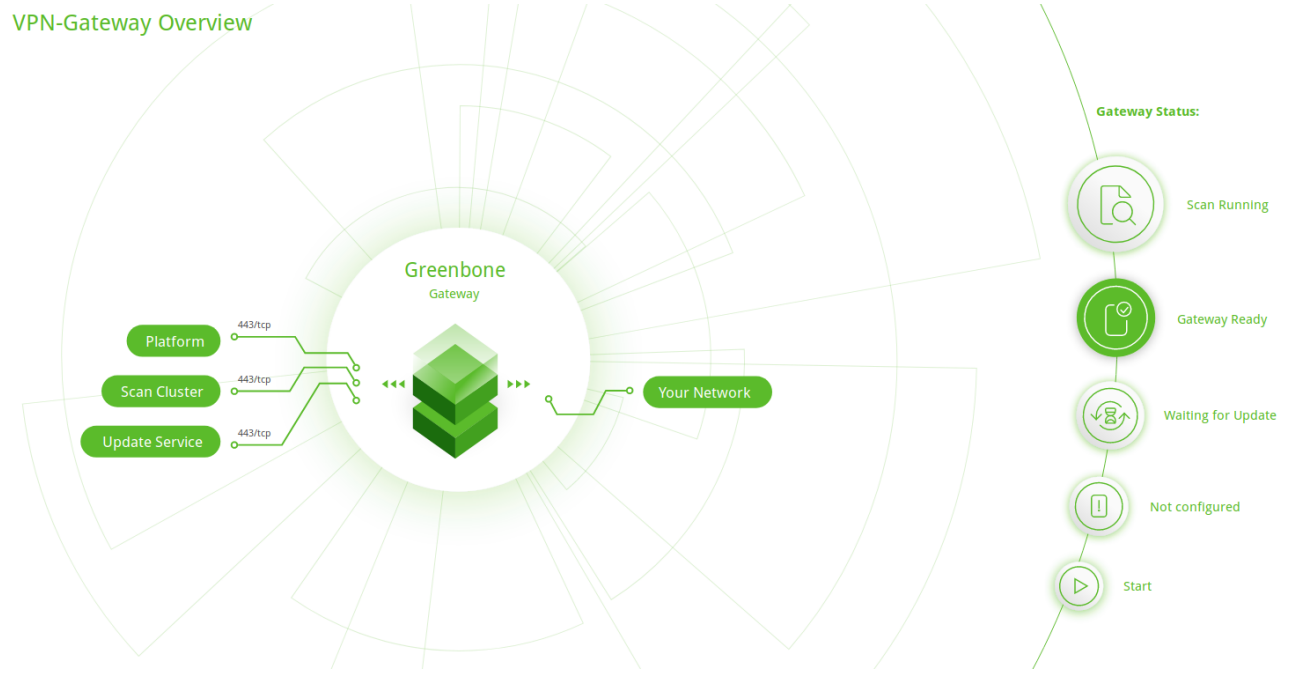

Abb. 6.31: Gateway-Übersicht

4. *Settings* im Menüpanel wählen.

   → Die folgenden Aktionen sind verfügbar:

   - Einrichten des API-Schlüssels des Gateways (siehe Kapitel *6.2.3* (Seite 39)).
   - Einrichten des Passworts zum Einloggen in die Gateway-Web-Oberfläche.
   - Aktivieren/Deaktivieren der Fehlerberichterstattung.

6.7 Aufgaben verwalten

Alle vorhandenen Aufgaben können auf den Seiten *Scanverwaltung* und *Scan-Konfiguration* angezeigt und verwaltet werden.

6.7.1 Seite *Scanverwaltung*

Scanverwaltung im Menüpanel wählen.

Für alle Aufgaben werden die folgenden Informationen angezeigt:

Neuesten Bericht des Scans öffnen. Für das Lesen, Verwalten und Herunterladen von Berichten siehe Kapitel *7* (Seite 77).

Aufgabe
: Name der Aufgabe.

  Durch Klicken auf den Namen einer Aufgabe wird ein Overlay mit Details geöffnet.

Status
: Aktueller Status der Aufgabe. Die folgenden Statusbalken sind möglich:

Verfügbar Die Aufgabe wurde noch nicht ausgeführt, seitdem sie erstellt wurde.

Export angefordert Der Export der Aufgabe auf die Scanmaschine wurde angefragt.

Exportiert Die Aufgabe wurde erfolgreich auf die Scanmaschine exportiert.

Export fehlgeschlagen Der Export der Aufgabe auf die Scanmaschine ist fehlgeschlagen.

Scan angefordert Die Aufgabe wurde gerade gestartet. Der Greenbone Cloud Service bereitet den Scan vor.

Laufend Die Aufgabe wird gerade ausgeführt. Die Spalte *Fortschritt* liefert weitere Details.

Löschen angefordert Die Aufgabe wurde gelöscht. Der tatsächliche Löschvorgang kann einige Zeit in Anspruch nehmen, da Berichte ebenfalls gelöscht werden müssen.

Stop angefordert Die Aufgabe wurde vor Kurzem aufgefordert, zu stoppen. Die Scanmaschine hat noch nicht auf die Anfrage reagiert.

Gestoppt Die Aufgabe wurde gestoppt. Der neueste Bericht ist möglicherweise noch nicht vollständig. Andere Gründe für diesen Status können der Reboot der Scanmaschine oder ein Stromausfall sein. Nach dem Neustart des Scanners wird die Aufgabe automatisch fortgesetzt.

Abgeschlossen Die Aufgabe wurde erfolgreich abgeschlossen.

Interner Fehler Ein Fehler ist aufgetreten und die Aufgabe wurde unterbrochen. Der neueste Bericht ist möglicherweise noch nicht vollständig oder fehlt komplett.

Fortschritt

Wenn der Scan gestartet wurde, werden weiterführende Informationen über den Scanstatus angezeigt.

Ein Prozentwert zeigt die Fertigstellung des Scans basierend auf der Anzahl an VTs, die auf den gewählten Hosts ausgeführt werden. Aus diesem Grund hängt der Wert nicht zwingend mit der bereits verstrichenen Zeit zusammen.

Reports

Anzahl der Berichte für die Aufgabe. Durch Klicken auf die Anzahl wird ein Überblick über alle Berichte geöffnet.

Letzter Scan

Datum und Zeit des letztens Scans der Aufgabe.

Ziel

Scanziel, das untersucht wird, wenn die Aufgabe ausgeführt wird.

Durch Klicken auf den Namen eines Ziels wird ein Overlay mit Details geöffnet.

Executive PDF

Durch Klicken auf ⤓ kann der „Executive Report“ heruntergeladen werden. Er enthält allgemeine Informationen über den Scan und Listen von Hosts sortiert nach Schweregrad.

Technical PDF

Durch Klicken auf ⤓ kann der „Technical Report“ heruntergeladen werden. Er enthält allgemeine Informationen über den Scan sowie Informationen über die gescannten Hosts und Details für jede erkannte Schwachstelle.

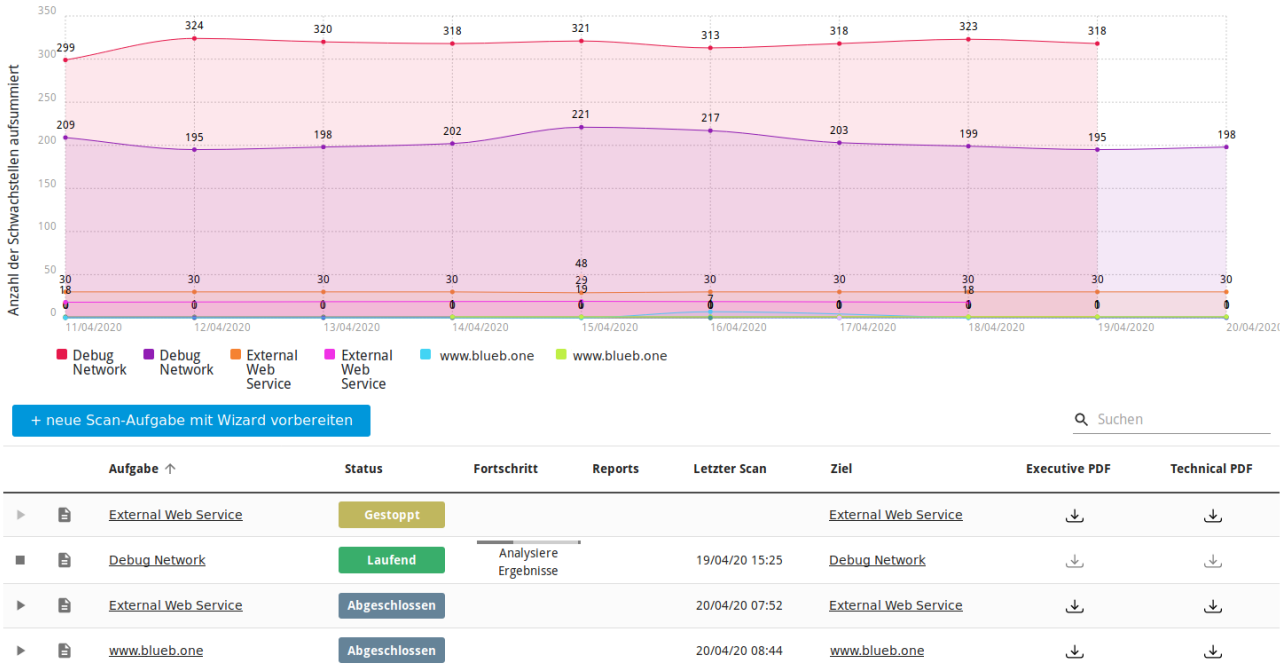

Abb. 6.32: Seite *Scanverwaltung*

6.7.2 Seite *Scan-Konfiguration*

Scan-Konfiguration im Menüpanel wählen.

Für alle Aufgaben werden die folgenden Informationen angezeigt:

Name
: Name der Aufgabe.

Typ
: Typ des Ziels: intern oder extern.

Scanziel
: Scanziel, das untersucht wird, wenn die Aufgabe ausgeführt wird.

  Durch Klicken auf den Namen eines Ziels wird ein Overlay geöffnet, das detaillierte Informationen enthält.

Scan-Konfiguration
: Scan-Konfiguration, die für die Aufgabe genutzt wird.

Zeitplan
: Zeitplan für diese Aufgabe (siehe Kapitel *6.4* (Seite 64)).

  Durch Klicken auf den Namen eines Zeitplans wird ein Overlay geöffnet, das detaillierte Informationen enthält.

Für alle Ziele sind die folgenden Aktionen verfügbar:

- Das Ziel bearbeiten.
- Das Ziel löschen. Nur Ziele, die aktuell nicht genutzt werden, können gelöscht werden.

6.8 Scan-Konfigurationen

Die Scan-Konfiguration gibt an, welche Schwachstellentests während eines Scans durchgeführt werden. Der Greenbone Cloud Service bietet verschiedene vordefinierte Scan-Konfigurationen.

Die folgenden Scan-Konfigurationen sind standardmäßig verfügbar:

Discovery
: Diese Scan-Konfiguration nutzt nur VTs, die Informationen über das Zielsystem sammeln. Dabei werden keine Schwachstellen erkannt.

  Zu den gesammelten Informationen gehören unter anderem Informationen über offene Ports, genutzte Hardware, Firewalls, genutzte Dienste, installierte Software und Zertifikate. Das System wird komplett inventarisiert.

  Die VT-Familien sind dynamisch, das heißt neue VTs der gewählten VT-Familien werden automatisch hinzugefügt und berücksichtigt.

Host Discovery
: Diese Scan-Konfiguration wird nur zum Erkennen der Zielsysteme genutzt. Dabei werden keine Schwachstellen erkannt.

  Es wird der Portscanner *Ping Host* genutzt, welcher erkennt, ob ein Host erreichbar ist.

  Die VT-Familien sind dynamisch, das heißt neue VTs der gewählten VT-Familien werden automatisch hinzugefügt und berücksichtigt.

System Discovery
: Diese Scan-Konfiguration wird nur zum Erkennen der Zielsysteme, der Betriebssysteme und der verwendeten Hardware genutzt. Dabei werden keine Schwachstellen erkannt.

  Es werden die Portscanner *Ping Host* und *Nmap* genutzt, welche erkennen, ob ein Host erreichbar ist.

  Die VT-Familien sind dynamisch, das heißt neue VTs der gewählten VT-Familien werden automatisch hinzugefügt und berücksichtigt.

Analyse [Standard]
: Für viele Umgebungen ist das für den Anfang eine der besten Optionen.

  Diese Scan-Konfiguration basiert auf den Informationen, die in einem vorherigen Portscan gesammelt wurden und nutzt fast alle VTs. Nur VTs, die das Zielsystem nicht beschädigen, werden genutzt. VTs sind bestmöglich optimiert, um die Anzahl von Falsch-Positiv-Meldungen besonders niedrig zu halten. Die anderen Konfigurationen bieten nur in seltenen Fällen einen Mehrwert, verbunden mit einem höheren Aufwand.

  Die VT-Familien sind dynamisch, das heißt neue VTs der gewählten VT-Familien werden automatisch hinzugefügt und berücksichtigt.

Analyse [Aggressiv]
: Diese Scan-Konfiguration erweitert die Scan-Konfiguration *Analyse [Standard]* um VTs, die Dienst- oder Systemstörungen oder sogar Abstürze hervorrufen könnten.

  Die VT-Familien sind dynamisch, das heißt neue VTs der gewählten VT-Familien werden automatisch hinzugefügt und berücksichtigt.

  Diese Scan-Konfiguration ist je nach Umgebungsbedingungen möglicherweise nicht immer absolut zuverlässig, was sich in einer erhöhten Falsch-positiv-Rate zeigen kann. Die Eingrenzung der vermuteten falsch-positiven Sonderfälle kann eine manuelle Analyse erfordern.

Analyse [standard] without Brute force attacks and Default Accounts
: Für viele Umgebungen ist das für den Anfang eine der besten Optionen.

Diese Scan-Konfiguration basiert auf den Informationen, die in einem vorherigen Portscan gesammelt wurden und nutzt fast alle VTs. Nur VTs, die das Zielsystem nicht beschädigen, werden genutzt. VTs sind bestmöglich optimiert, um die Anzahl von Falsch-Positiv-Meldungen besonders niedrig zu halten.

Die VT-Familien sind dynamisch, das heißt neue VTs der gewählten VT-Familien werden automatisch hinzugefügt und berücksichtigt.

Exchange ZeroDay CVE-2021-26855
Diese Scan-Konfiguration prüft auf die CVE-2021-26855, die im Zusammenhang mit dem Microsoft Exchange Server steht. CVE-2021-26855 ist eine Server-Side-Request-Forgery-Schwachstelle (SSRF-Schwachstelle) in Exchange, welche es Angreifenden erlaubt, HTTP-Anfragen zu senden und sich beim Exchange-Server zu authentifizieren.

Log4j Zero Day CVE-2021-44228
Diese Scan-Konfiguration prüft auf die CVE-2021-44228 in der Protokollierungsbibliothek Log4j. Die in CVE-2021-44228 aufgeführte Schwachstelle könnte eine Remote-Codeausführung ermöglichen.

6.9 Portlisten

Die Portliste, die für ein Ziel konfiguriert wurde, hat einen großen Einfluss auf die Dauer des Erreichbarkeitstests und des Schwachstellenscans dieses Ziels.

Ports sind die Verbindungspunkte der Netzwerkkommunikation. Jeder Port eines Systems verbindet sich mit dem Port eines anderen Systems.

Transmission Control Protocol (TCP) Ports

- 65535 TCP-Ports für jedes System
- Datenübertragung zwischen zwei TCP-Ports geschieht in beide Richtungen.
- Der Scan von TCP-Ports wird normalerweise schnell und einfach durchgeführt.

User Datagram Protocol (UDP) Ports

- 65535 UDP-Ports für jedes System
- Datenübertragung zwischen zwei UDP-Ports geschieht nur in eine Richtung.
- Der Empfang von Daten, die über UDP übertragen werden, wird nicht zwingend bestätigt, sodass das Prüfen von UDP-Ports normalerweise länger dauert.

Port 0 bis 1023 sind privilegierte oder Systemports und können nicht von Benutzeranwendungen geöffnet werden[6].

Die Internet Assigned Numbers Authority (IANA)[4] weist Standardprotokollen Ports zu, z. B. Port 80 zu „http“ oder Port 443 zu „https“. Über 5000 Ports sind registriert.

Das Scannen aller Ports dauert in vielen Fällen zu lang und viele Ports werden normalerweise nicht genutzt. Um dieses Problem zu beheben, können Portlisten genutzt werden.

Alle Ports aller per Internet zugänglichen Systeme wurden untersucht und Listen der meist genutzten Ports wurden erstellt. Diese spiegeln nicht unbedingt die IANA-Liste wider, da es keine Pflicht ist, für einen bestimmten Diensttyp einen entsprechenden Port zu registrieren. Nmap[5], ein Open-Source-Portscanner und der OpenVAS-Scanner nutzen standardmäßig unterschiedliche Listen und prüfen nicht alle Ports.

Für die meisten Scans ist es oft ausreichend die Ports zu scannen, die bei IANA registriert sind.

Die folgenden Portlisten sind auf dem Greenbone Cloud Service vordefiniert:

[6] Unter Unix-ähnlichen Systemen ist der Zugriff auf diese privilegierten Ports nur für privilegierte Benutzer (d. h. root) erlaubt. Ports ab 1024 sind auch für nicht-privilegierte Benutzer verfügbar.

[4] https://www.iana.org/

[5] https://nmap.org/

- All IANA assigned TCP 2012-02-10: Alle TCP-Ports, die von IANA am 10. Februar 2012 zugewiesen waren
- All privileged TCP
- All privileged TCP and UDP
- All TCP
- OpenVAS Default: Die TCP-Ports, die vom OpenVAS-Scanner beim Übergeben der standardmäßigen Portbereichpräferenz, gescannt werden
- All IANA assigned TCP and UDP 2012-02-10: Alle TCP- und UDP-Ports, die von IANA am 10. Februar 2012 zugewiesen waren
- All TCP and Nmap 5.51 top 100 UDP: Alle TCP-Ports und die 100 meistgenutzten UDP-Ports gemäß Nmap 5.51
- All TCP and Nmap 5.51 top 1000 UDP: Alle TCP-Ports und die 1000 meistgenutzten UDP-Ports gemäß Nmap 5.51
- Nmap 5.51 top 2000 TCP and top 100 UDP: Die 2000 meistgenutzten TCP-Ports und die 100 meistgenutzten UDP-Ports gemäß Nmap 5.51
- Web services

6.10 Benachrichtigungen nutzen

Der Benutzer kann Zusammenfassungen der konfigurierten Scans oder Benachrichtigungen für fertiggestellte Scans erhalten (siehe Kapitel *5.2* (Seite 16)).

6.11 Hindernisse beim Scannen

Es gibt eine Reihe typischer Probleme, welche während eines Scans mit den Standardwerte des Greenbone Cloud Service auftreten können. Während die Standardwerte für die meisten Umgebungen und Kunden passend sind, benötigen sie abhängig von der tatsächlichen Umgebung und der Konfiguration der gescannten Hosts möglicherweise etwas Optimierung.

6.11.1 Hosts nicht gefunden

Während eines typischen Scans (entweder *Discovery* oder *Analyse [Standard]*) nutzen die GCS standardmäßig zuerst den Pingbefehl, um die Verfügbarkeit der konfigurierten Ziele zu prüfen. Falls ein Ziel nicht auf die Pinganfrage antwortet, wird es als unerreichbar angenommen und nicht vom Portscanner oder einem VT gescannt.

In den meisten LAN-Umgebungen stellt dies kein Problem dar, da alle Geräte auf eine Pinganfrage antworten. Allerdings unterdrücken (lokale) Firewalls oder andere Konfigurationen manchmal die Pingantwort. Falls dies passiert, wird das Ziel nicht gescannt und ist nicht in den Ergebnissen und im Bericht enthalten.

Um dieses Problem zu beseitigen, müssen sowohl die Konfiguration des Ziels als auch die Scan-Konfiguration die Einstellung des Erreichbarkeitstest unterstützen (siehe Kapitel *6.2.1* (Seite 31)).

Falls das Ziel nicht auf die Pinganfrage reagiert, könnte ein TCP-Ping getestet werden.

6.11.2 Lang andauernde Scans

Wenn mithilfe des Pingbefehls erkannt wurde, dass das Ziel erreichbar ist, nutzt der Scanner einen Portscanner, um das Ziel zu scannen. Standardmäßig wird eine TCP-Portliste mit ungefähr 5000 Ports genutzt. Falls das Ziel durch eine (lokale) Firewalls geschützt wird, die die meisten dieser Pakete weglässt, muss der Portscan auf das Timeout jedes einzelnen Ports warten. Falls die Hosts durch (lokale) Firewalls geschützt werden, müssen die Portlisten oder die Firewalls angepasst werden. Falls die Firewall die Anfrage nicht fallen lässt, aber sie ablehnt, muss der Portscanner nicht auf das Timeout warten. Dies gilt insbesondere dann, wenn UDP-Ports im Scan enthalten sind.

KAPITEL 7

Berichte und Schwachstellenmanagement

Die Scanergebnisse werden in einem Bericht zusammengefasst. Berichte können in unterschiedlichen Formaten angezeigt und heruntergeladen werden.

Der Greenbone Cloud Service speichert nicht nur den letzten Bericht, sondern alle Berichte aller jemals gelaufenen Scans. Dies ermöglicht den Zugriff auf vergangene Informationen. Die Berichte enthalten erkannte Schwachstellen und Informationen über den Scan.

Nach dem Starten eines Scans kann der Bericht der bis dahin gefundenen Ergebnisse angesehen werden. Wenn der Scan abgeschlossen ist, ändert sich der Status zu *Abgeschlossen* und keine weiteren Ergebnisse werden hinzugefügt.

7.1 Einen Bericht lesen

Ein Überblick über alle vorhandenen Berichte einer Aufgabe kann angezeigt werden, indem *Scanverwaltung* im Menüpanel gewählt und auf die Anzahl der Berichte in der Spalte *Reports* geklickt wird (siehe Abb.7.1).

Die folgenden Informationen werden angezeigt:

Datum
: Datum und Zeit der Berichterstellung.

  Unfertige Scans sind mit ⚠ markiert.

Schweregrad
: Höchster Schweregrad, der auf dem Ziel gefunden wurde.

Kritisch/Mittel/Niedrig/Log
: Anzahl der gefundenen Schwachstelle für jede Schweregradklasse.

🗎
: Alle Ergebnisse für den entsprechenden Bericht anzeigen.

Executive PDF
: Durch Klicken auf ⭳ kann der „Executive Report“ heruntergeladen werden. Er enthält allgemeine Informationen über den Scan und Listen von Hosts sortiert nach Schweregrad.

Technical PDF

Durch Klicken auf kann der „Technical Report“ heruntergeladen werden. Er enthält allgemeine Informationen über den Scan sowie Informationen über die gescannten Hosts und Details für jede erkannte Schwachstelle.

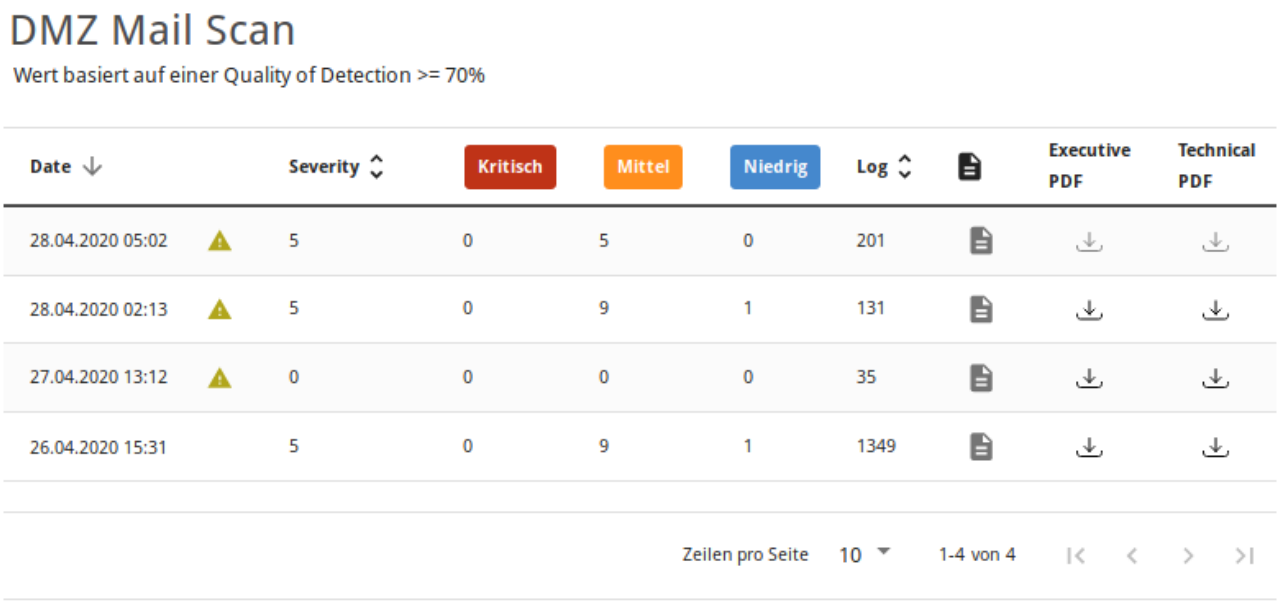

Abb. 7.1: Zusammenfassung aller Berichte eines Scans

7.1.1 Einen Bericht interpretieren

Um die Ergebnisse zu interpretieren, müssen die folgenden Informationen beachtet werden:

- **Mehrere Ergebnisse können dieselbe Ursache haben.**
  Falls ein besonders altes Softwarepaket installiert ist, existieren oft mehrere Schwachstellen. Jede dieser Schwachstellen wird von einem anderen VT geprüft und löst eine Benachrichtigung aus. Die Installation eines aktuellen Pakets entfernt viele Schwachstellen auf einmal.
- **Kritisch** Kritisch **und Mittel** Mittel
  Ergebnisse der Schweregrade *Kritisch* und *Mittel* sind am wichtigsten und sollten priorisiert behandelt werden. Bevor Ergebnisse mittleren Schweregrads behandelt werden, sollten Ergebnisse kritischen Schweregrads thematisiert werden. Nur in außergewöhnlichen Fällen sollte von diesem Ansatz abgewichen werden, z. B. falls bekannt ist, dass die Ergebnisse mit kritischem Schweregrad weniger beachtet werden müssen, da der Dienst durch die Firewall nicht erreichbar ist.
- **Niedrig** Niedrig **und Log** Log
  Ergebnisse mit dem Schweregrad *Niedrig* und *Log* sind hauptsächlich für das Detailverständnis hilfreich. Diese Ergebnisse werden standardmäßig ausgefiltert, können jedoch interessante Informationen enthalten. Ihr Berücksichtigen erhöht die Sicherheit des Netzwerks und der Systeme. Oftmals ist für ihr Verständnis eine tiefergehende Kenntnis der Anwendung nötig. Typisch für ein Ergebnis mit dem Schweregrad *Log* ist, dass ein Dienst ein Banner mit seinem Namen und seiner Versionsnummer nutzt. Dies kann für Angreifende hilfreich sein, falls diese Versionsnummer eine bekannte Schwachstelle besitzt.

  Bemerkung: VTs, die durch ein Timeout beendet werden, bevor ein Ergebnis vorliegt, werden mit dem Schweregrad *Niedrig* und einer Qualität der Erkennung (QdE) von 0 angegeben (siehe Kapitel

7.1.2 (Seite 80)). Weitere Informationen zu diesem Fehler befinden sich in den Details solcher Ergebnisse.

7.1.2 Konzept der Qualität der Erkennung

Die Qualität der Erkennung (QdE) ist ein Wert zwischen 0 % und 100 % und beschreibt die Zuverlässigkeit der ausgeführten Schwachstellen- oder Produkterkennung.

Obwohl der QdE-Bereich es erlaubt, die Qualität detailgenau darzustellen, nutzen die meisten Prüfroutinen eine Standardmethodik. Deshalb werden den QdE-Werten QdE-Typen zugewiesen. Die aktuelle Typenliste wird möglicherweise mit der Zeit erweitert.

Bemerkung:

- Die QdE eines „Erkennungs“-Ergebnisses ist höher als die eines tatsächlichen „Schwachstellen“-Ergebnisses, da sie die Qualität der Produkterkennung selbst widerspiegelt – die zuverlässig ist – und nicht die Qualität der zugehörigen Schwachstellentests, die aus verschiedenen Gründen unzuverlässig sein können (siehe Tabelle).
- Es wird immer die niedrigste verfügbare QdE verwendet, beispielsweise im Falle mehrerer Erkennungsmethoden (remote oder lokal/authentifiziert).

QdE	QdE-Typ	Beschreibung
100 %	exploit	Die Erkennung erfolgte durch die Ausnutzung einer Sicherheitslücke und ist daher vollständig bestätigt.
99 %	remote_vul	Aktive Prüfung auf dem Zielsystem (Codeausführung, Traversal-Angriff, SQL-Einschleusung etc.), bei welcher die Antwort eindeutig das Vorhandensein der Schwachstelle zeigt.
98 %	remote_app	Aktive Prüfung auf dem Zielsystem (Codeausführung, Traversal-Angriff, SQL-Einschleusung etc.), bei welcher die Antwort eindeutig das Vorhandensein der gefährdeten Anwendung zeigt.
97 %	package	Authentifizierte paketbasierte Prüfungen für Linux(oide) Systeme.
97 %	registry	Authentifizierte Prüfungen auf Basis der Registry von Microsoft Windows.
95 %	remote_active	Aktive Prüfung auf dem Zielsystem (Codeausführung, Traversal-Angriff, SQL-Einschleusung etc.), bei welcher die Antwort das wahrscheinliche Vorhandensein der gefährdeten Anwendung oder der Schwachstelle zeigt. „Wahrscheinlich“ bedeutet, dass die Erkennung nur in seltenen Fällen inkorrekt ist.
80 %	remote_banner	Prüfung von Anwendungsbannern auf dem Zielsystem, die den Patch-Status als Information anbieten. Zum Beispiel ist dies für viele proprietäre Produkte der Fall.
80 %	executable_version	Authentifizierte Versionsprüfung über eine ausführbare Datei für Linux(oide) und Microsoft Windows Systeme, bei denen Anwendungen den Patch-Status in der Version anbieten.
75 %		Wenn Ergebnisse ohne QdE-Informationen verarbeitet werden, wird ihnen dieser Wert zugewiesen.
70 %	remote_analysis	Prüfungen auf dem Zielsystem, die einige Analysen durchführen, jedoch je nach Umgebungsbedingungen nicht immer vollständig zuverlässig sind. Die Eingrenzung von vermuteten falsch-positiven oder falsch-negativen Sonderfällen kann eine Analyse durch den Nutzer erfordern.
50 %	remote_probe	Prüfung auf dem Zielsystem, bei welcher zwischenliegende Systeme wie Firewalls die korrekte Erkennung vortäuschen können, sodass nicht eindeutig ist, ob die Anwendung selbst geantwortet hat. Zum Beispiel kann dies für Verbindungen ohne TLS geschehen.

QdE	QdE-Typ	Beschreibung
30 %	remote_banner_unreliable	Prüfung von Anwendungsbannern des Zielsystems, die den Patch-Status nicht als Information anbieten. Zum Beispiel ist dies für viele Open-Source-Produkte aufgrund von Backport-Patches der Fall.
30 %	executable_version_unreliable	Authentifizierte Versionsprüfung über eine ausführbare Datei für Linux(oide) Systeme, bei denen Anwendungen den Patch-Status nicht in der Version anbieten.
1 %	general_note	Allgemeine Notiz zu einer potentiellen Schwachstelle ohne konkrete Erkennung einer vorhandenen Anwendung.
0 %	timeout	Der Test war nicht in der Lage, ein Ergebnis zu ermitteln, bevor er durch ein Timeout beendet wurde.

Standardmäßig werden nur Ergebnisse angezeigt, die durch VTs mit einer QdE von 70 % oder höher erkannt wurden. Ergebnisse, die von einem Test mit einer niedrigeren QdE erkannt werden, sind anfällig für Falsch-Positiv-Ergebnisse. Der Filter kann angepasst werden, sodass auch Ergebnisse mit niedrigerer QdE angezeigt werden (siehe Kapitel *7.3* (Seite 88)).

Bemerkung: Wenn der Standardfilter geändert wird, um Ergebnisse anzuzeigen, die von einem Test mit einer niedrigen QoD erkannt wurden, liegt es in der eigenen Verantwortung, festzustellen, ob es sich um ein Falsch-Positiv-Ergebnis handelt.

7.2 Ergebnisse eines Berichts

Ein Bericht kann geöffnet werden, indem in der Berichtübersicht für den gewünschten Bericht auf geklickt wird (siehe Abb.7.1).

Tipp: Der neueste Bericht eines Scans kann angezeigt werden, indem *Scanverwaltung* im Menüpanel gewählt und in der Zeile des Scans auf geklickt wird.

Der Name, das Datum und die Zeit eines Scans sowie der höchste gefundene Schweregrad werden im oberen Bereich dargestellt.

Die folgenden Register sind verfügbar:

- Dashboard
- Kachelübersicht
- Tabellenübersicht

7.2.1 Dashboard

Das Dashboard stellt einen zusammenfassenden Überblick über die gefundenen Schwachstellen, ihre Schweregrade und ihre möglichen Lösungen bereit.

Die folgenden Informationen werden angezeigt:

- Gesamtzahl erkannter Schwachstellen
- Anzahl erkannter Schwachstellen für jeden Lösungstyp
- Anzahl erkannter Schwachstellen für jedes Schweregradlevel
- Die beiden Lösungen mit der höchsten Behebungsquote
- Risikolevel (höchster gefundener Schweregrad)
- Top 10 Hosts mit der Anzahl gefundener Schwachstellen und Verteilung der Schweregrade (sortiert nach Anzahl der Schwachstellen oder nach Schweregrad)

7.2.2 Kachelübersicht

Die Kachelübersicht zeigt alle gefundenen Schwachstellen sortiert vom höchsten zum niedrigsten Schweregrad.

Die Ergebnisse können gefiltert werden, indem auf *Filter +* geklickt wird (siehe Kapitel *7.3* (Seite 88)).

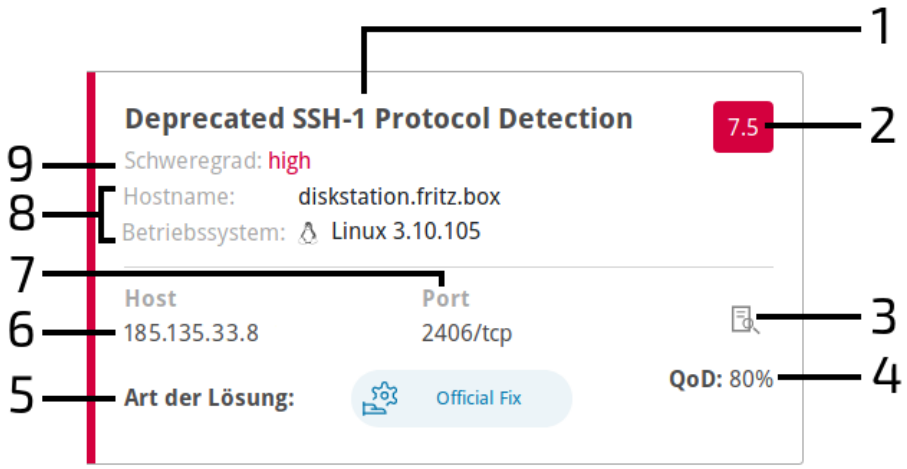

Abb. 7.2: Ergebnis eines Scans

Für jedes Ergebnis werden die folgenden Informationen angezeigt:

1 – Name der gefundenen Schwachstelle.

2 – Schweregrad der Schwachstelle.

3 – Overlay mit Details der Schwachstelle öffnen.

4 – QoD ist kurz für „Quality of Detection“ (engl. für „Qualität der Erkennung“) und zeigt, wie verlässlich die Erkennung einer Schwachstelle ist (siehe Kapitel *7.1.2* (Seite 80)).

5 – Lösung für die gefundene Schwachstelle. Die folgenden Lösungen sind möglich:

- Offizielle Lösung: eine offizielle Herstellerlösung ist verfügbar. Sofern nicht anders vermerkt, wird angenommen, dass die Lösung die Schwachstelle komplett beseitigt.

- Temporäre Lösung: eine Problemumgehung (Informationen über Konfigurationen oder bestimmte Einsatzszenarien, die die Gefährdung durch die Schwachstelle verringern) ist verfügbar, um die Schwachstelle temporär zu beseitigen.

  Es können keine, eine oder mehrere Problemumgehungen verfügbar sein.

  Dies ist normalerweise die „erste Verteidigungslinie“ gegen neue Schwachstellen, bevor eine Risikominderung oder offizielle Lösung entdeckt oder ausgegeben wurde.
- Risikominderung: es sind Informationen über Konfigurationen oder Einsatzszenarien verfügbar, die das Risiko der Schwachstelle reduzieren, was die Schwachstelle auf dem betroffenden Produkt allerdings nicht entfernt.
- Keine Lösung verfügbar: es gibt keine Lösung für die Schwachstelle und es wird auch zukünftig keine geben.

  Dies ist oft der Fall, wenn ein Produkt verwaist ist, nicht länger gewartet wird oder andersweitig überholt ist.
- Lösung wird gesucht: es ist momentan keine Lösung verfügbar, um die Schwachstelle zu beseitigen, möglicherweise gibt es aber in der Zukunft eine.

6 – Host, für den das Ergebnis gefunden wurde.

7 – Genutzte Portnummer und genutzter Protokolltyp zum Erkennen der Schwachstelle auf dem Host.

8 – Hostname und Betriebssystem des Hosts, für den das Ergebnis gefunden wurde.

9 – Schweregrad der Schwachstelle.

7.2.3 Tabellenübersicht

Die Tabellenübersicht zeigt die Ergebnisse des Scans in Form von unterschiedlichen Tabellen.

Es gibt drei unterschiedliche Tabellen, die gewählt werden können (siehe Abb.7.3):

- Übersicht: alle gefundenen Ergebnisse
- Host: Ergebnisse nach Host gruppiert
- Schwachstelle: Ergebnisse nach Schwachstelle gruppiert

Die Ergebnisse können gefiltert werden, indem auf *Filter +* geklickt wird (siehe Kapitel *7.3* (Seite 88)).

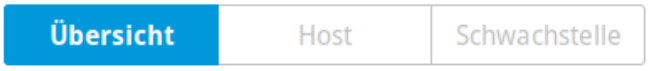

Abb. 7.3: Unterschiedliche Tabellen in der Tabellenübersicht

7.2.3.1 „Übersicht“-Tabelle

Für jedes Ergebnis werden die folgenden Informationen angezeigt:

Name
: Name der entsprechenden Schwachstelle.

Schweregrad
: Schweregrad der entsprechenden Schwachstelle. Er wird in der Farbe des entsprechenden Schweregradlevels angezeigt, um die Analyse der Ergebnisse zu unterstützen.

Host
: Host, für den die Schwachstelle gefunden wurde.

Port
Genutzte Portnummer und genutzter Protokolltyp zum Erkennen des Ergebnisses auf dem Host .

Lösung
Lösung für die entsprechende Schwachstelle. Die folgenden Lösungen sind möglich:

- Offizielle Lösung: eine offizielle Herstellerlösung ist verfügbar. Sofern nicht anders vermerkt, wird angenommen, dass die Lösung die Schwachstelle komplett beseitigt.
- Temporäre Lösung: eine Problemumgehung (Informationen über Konfigurationen oder bestimmte Einsatzszenarien, die die Gefährdung durch die Schwachstelle verringern) ist verfügbar, um die Schwachstelle temporär zu beseitigen.

  Es können keine, eine oder mehrere Problemumgehungen verfügbar sein.

  Dies ist normalerweise die „erste Verteidigungslinie“ gegen neue Schwachstellen, bevor eine Risikominderung oder offizielle Lösung entdeckt oder ausgegeben wurde.
- Risikominderung: es sind Informationen über Konfigurationen oder Einsatzszenarien verfügbar, die das Risiko der Schwachstelle reduzieren, was die Schwachstelle auf dem betroffenden Produkt allerdings nicht entfernt.
- Keine Lösung verfügbar: es gibt keine Lösung für die Schwachstelle und es wird auch zukünftig keine geben.

  Dies ist oft der Fall, wenn ein Produkt verwaist ist, nicht länger gewartet wird oder andersweitig überholt ist.
- Lösung wird gesucht: es ist momentan keine Lösung verfügbar, um die Schwachstelle zu beseitigen, möglicherweise gibt es aber in der Zukunft eine.

QdE
QoD ist kurz für „Quality of Detection“ (engl. für „Qualität der Erkennung“) und zeigt, wie verlässlich die Erkennung einer Schwachstelle ist (siehe Kapitel *7.1.2* (Seite 80)).

Standardmäßig werden nur Ergebnisse angezeigt, die durch VTs mit einer QoD von 70 % oder höher erkannt wurden. Die Möglichkeit von Falschmeldungen ist dadurch geringer. Der Filter kann angepasst werden, sodass auch Ergebnisse mit niedrigerer QoD angezeigt werden (siehe Kapitel *7.3* (Seite 88)).

Details
Durch Klicken auf wird ein Overlay mit Details der Schwachstelle geöffnet.

7.2.3.2 „Host“-Tabelle

Für jeden Host werden die folgenden Informationen angezeigt:

Name
IP-Adresse des Hosts.

Schweregrad
Höchster Schweregrad, der auf dem Host gefunden wurde.

Hoch/Mittel/Niedrig
Anzahl der gefundenen Schwachstelle für jeden Schweregrad.

Durch Klicken auf eine Zahl werden die Top 20 Schwachstellen für den gewählten Schweregrad, die auf dem entsprechenden Host gefunden wurden, angezeigt.

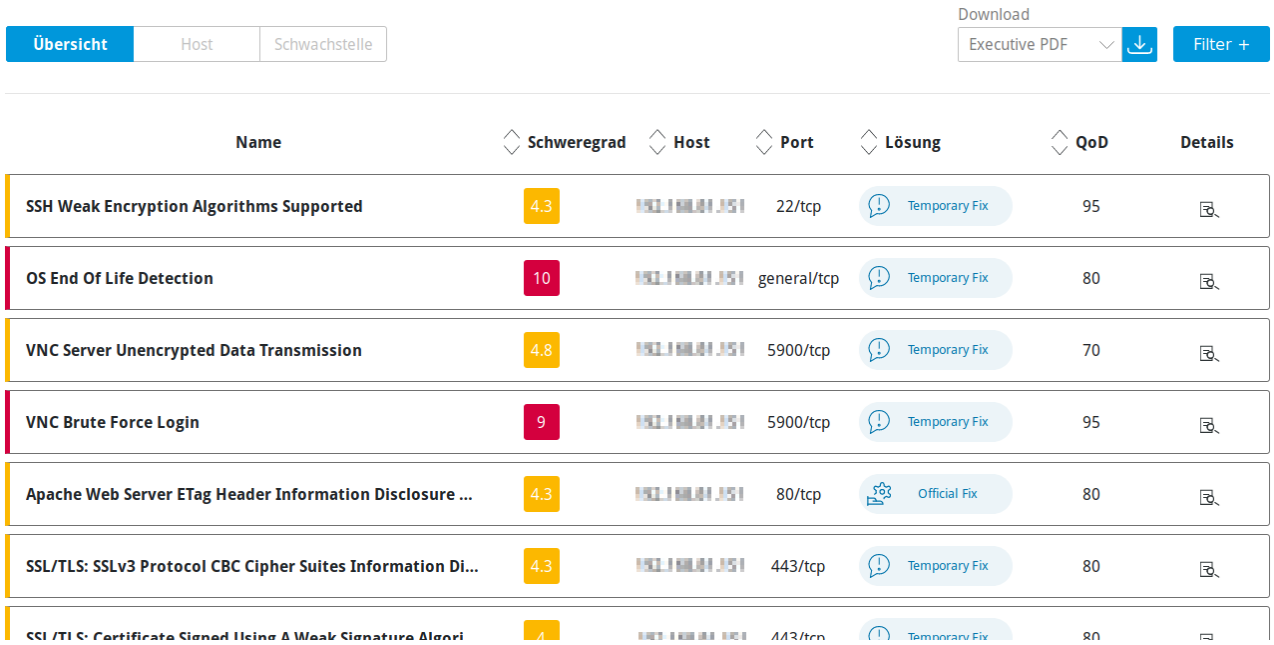

Abb. 7.4: „Übersicht“-Tabelle

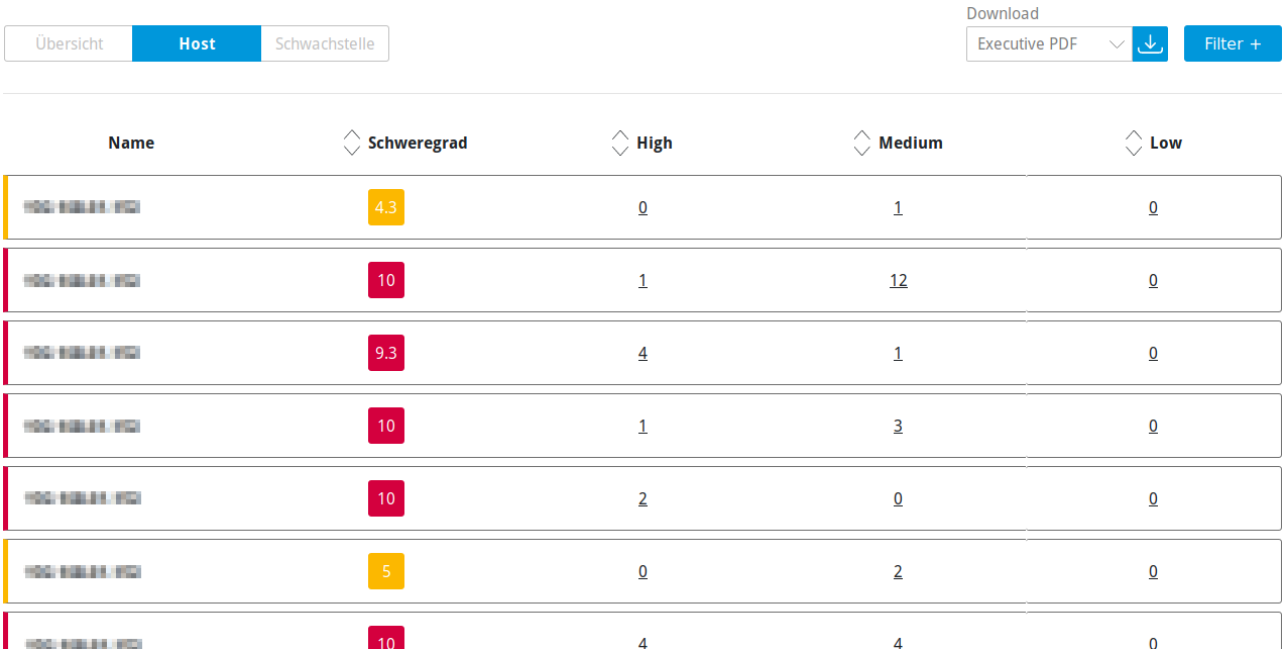

Abb. 7.5: „Host“-Tabelle

7.2.3.3 „Schwachstelle“-Tabelle

Für jede Schwachstelle werden die folgenden Informationen angezeigt:

Name
Name der Schwachstelle.

Schweregrad
Schweregrad der Schwachstelle. Er wird in der Farbe des entsprechenden Schweregradlevels angezeigt, um die Analyse der Ergebnisse zu unterstützen.

Host
Anzahl der Hosts, auf denen die Schwachstelle gefunden wurde.

Durch Klicken auf eine Zahl werden die Top 20 Hosts, auf denen die Schwachstelle gefunden wurde, zusammen mit zusätzlichen Details angezeigt.

Port
Anzahl der Ports, mit denen die Schwachstelle gefunden wurde.

Durch Klicken auf eine Zahl werden die Top 20 Ports, mit denen die Schwachstelle gefunden wurde, zusammen mit zusätzlichen Details angezeigt.

Lösung
Lösung für die entsprechende Schwachstelle. Die folgenden Lösungen sind möglich:

- Offizielle Lösung: eine offizielle Herstellerlösung ist verfügbar. Sofern nicht anders vermerkt, wird angenommen, dass die Lösung die Schwachstelle komplett beseitigt.
- Temporäre Lösung: eine Problemumgehung (Informationen über Konfigurationen oder bestimmte Einsatzszenarien, die die Gefährdung durch die Schwachstelle verringern) ist verfügbar, um die Schwachstelle temporär zu beseitigen.

  Es können keine, eine oder mehrere Problemumgehungen verfügbar sein.

  Dies ist normalerweise die „erste Verteidigungslinie“ gegen neue Schwachstellen, bevor eine Risikominderung oder offizielle Lösung entdeckt oder ausgegeben wurde.
- Risikominderung: es sind Informationen über Konfigurationen oder Einsatzszenarien verfügbar, die das Risiko der Schwachstelle reduzieren, was die Schwachstelle auf dem betroffenden Produkt allerdings nicht entfernt.
- Keine Lösung verfügbar: es gibt keine Lösung für die Schwachstelle und es wird auch zukünftig keine geben.

  Dies ist oft der Fall, wenn ein Produkt verwaist ist, nicht länger gewartet wird oder andersweitig überholt ist.
- Lösung wird gesucht: es ist momentan keine Lösung verfügbar, um die Schwachstelle zu beseitigen, möglicherweise gibt es aber in der Zukunft eine.

QdE
QoD ist kurz für „Quality of Detection“ (engl. für „Qualität der Erkennung“) und zeigt, wie verlässlich die Erkennung einer Schwachstelle ist (siehe Kapitel *7.1.2* (Seite 80)).

Standardmäßig werden nur Ergebnisse angezeigt, die durch VTs mit einer QoD von 70 % oder höher erkannt wurden. Die Möglichkeit von Falschmeldungen ist dadurch geringer. Der Filter kann angepasst werden, sodass auch Ergebnisse mit niedrigerer QoD angezeigt werden (siehe Kapitel *7.3* (Seite 88)).

Details
Durch Klicken auf  wird ein Overlay mit Details der Schwachstelle geöffnet.

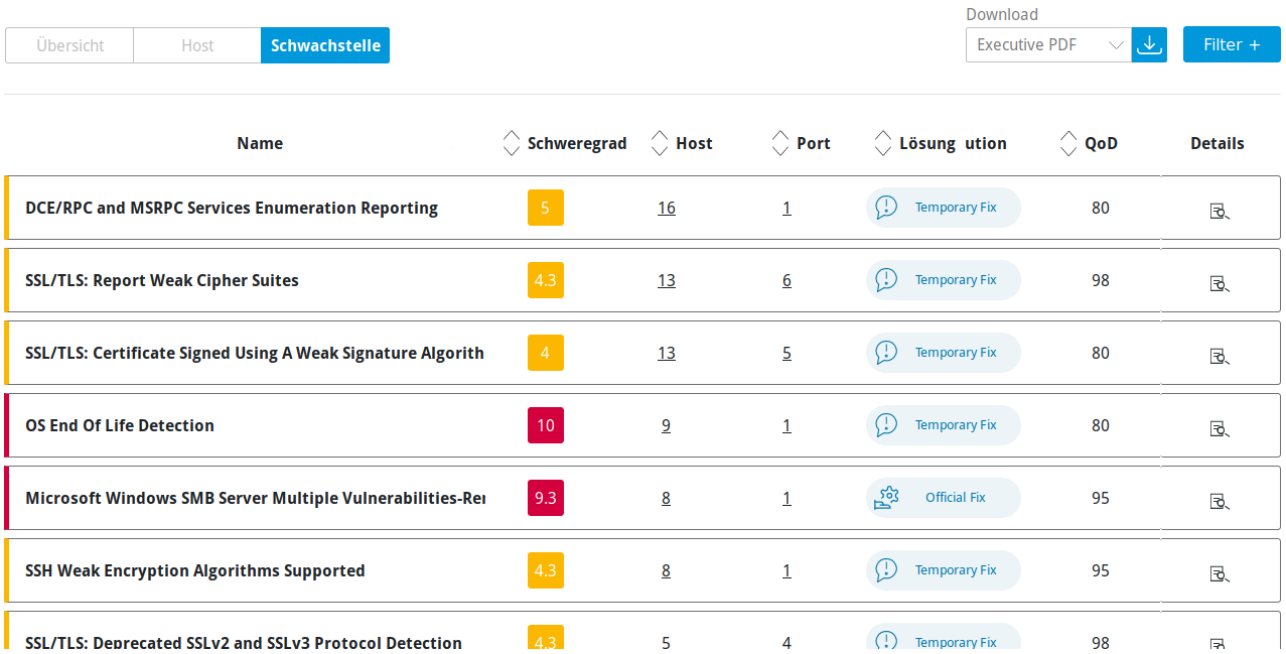

Abb. 7.6: „Schwachstelle“-Tabelle

7.3 Einen Bericht filtern

Da ein Bericht oft viele Ergebnisse enthält, können sowohl der gesamte als auch gefilterte Ergebnisse angezeigt werden.

Die Kachel- oder die Tabellenübersicht eines Berichts (siehe Kapitel *7.2* (Seite 82)) kann wie folgt gefiltert werden:

1. *Scanverwaltung* im Menüpanel wählen.
2. Auf die Gesamtanzahl der Berichte in der Spalte *Berichte* klicken.

   → Der Überblick über alle Berichte einer Aufgabe wird geöffnet.
3. In der Zeile des gewünschten Berichts auf klicken.
4. Register *Kachelübersicht* oder *Tabellenübersicht* wählen.
5. Auf *Filter +* klicken.
6. Für *Quality Of Detection Range (QoD)* und *Schweregrad* die minimalen und maximalen Werte mithilfe der Schieberegler einstellen (siehe Abb.7.7).
7. Für *Lösung* die Buttons der gewünschten Lösungstypen wählen.

   Tipp: Die gewählten Lösungstypen werden durch eine Umrandung hervorgehoben.
8. Für *Port*, *Host*, *Hostname* und *Betriebssystem* die Ports, Hosts, Hostnamen und Betriebssysteme, für die die gefundenen Ergebnisse angezeigt werden sollen, in den Drop-down-Listen wählen.
9. Auf *Anwenden* klicken.

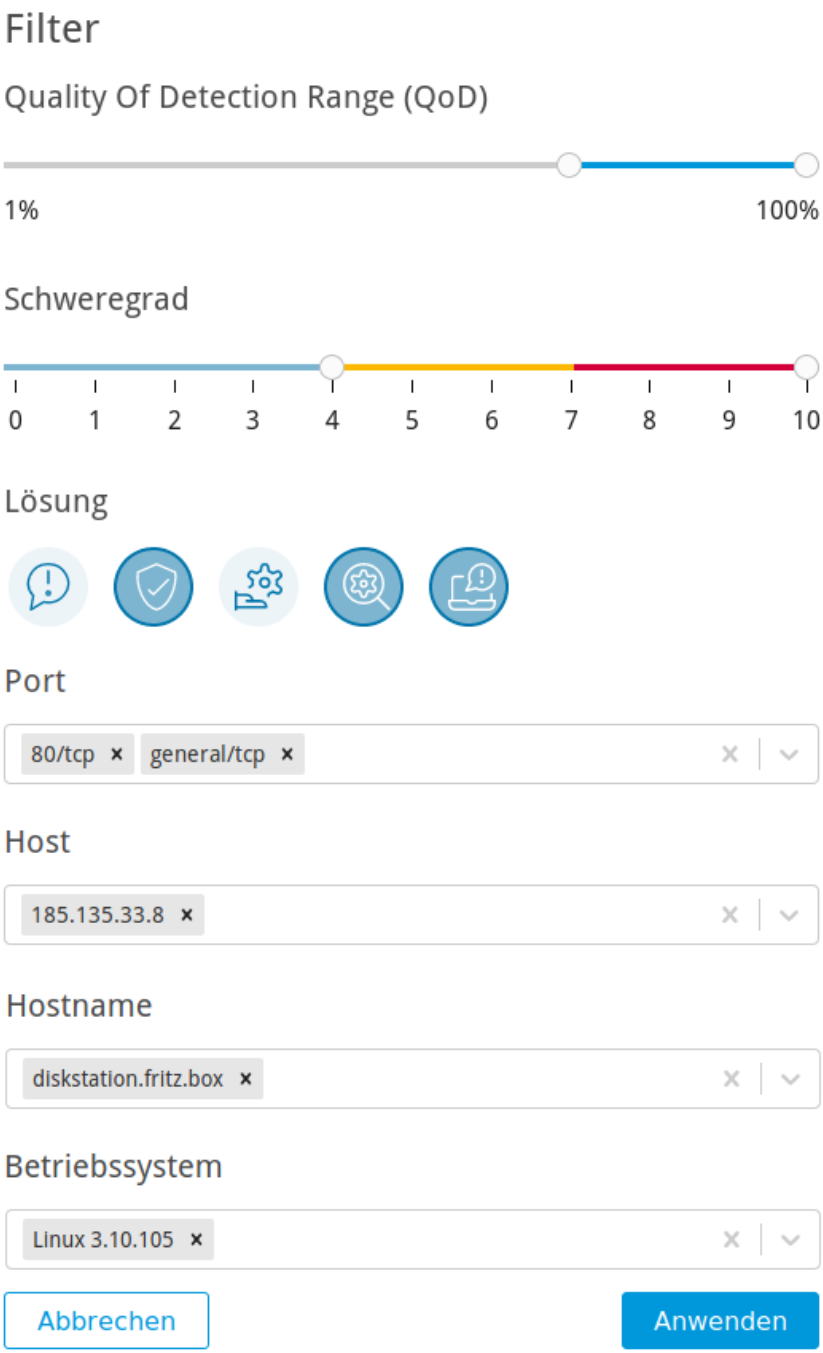

Abb. 7.7: Anpassen des Filters für den Bericht

7.4 Einen Bericht exportieren

Ein Bericht kann in unterschiedlichen Formaten exportiert werden:

Executive Report (PDF oder JSON)
Dieser Bericht enthält allgemeine Informationen über den Scan und Listen von Hosts sortiert nach Schweregrad.

Technical Report (PDF oder JSON)
Dieser Bericht enthält allgemeine Informationen über den Scan sowie über die gescannten Hosts und Details zu jeder gefundenen Schwachstelle.

XML

Ein Bericht kann wie folgt exportiert werden:

1. *Scanverwaltung* im Menüpanel wählen.
2. Auf die Gesamtanzahl der Berichte in der Spalte *Berichte* klicken.

   → Der Überblick über alle Berichte eines Scans wird geöffnet.
3. In der Zeile des gewünschten Berichts für *Executive PDF* oder *Technical PDF* auf klicken.
4. Auf *OK* klicken, um den Bericht zu speichern.

   oder

1. *Scanverwaltung* im Menüpanel wählen.
2. Auf die Gesamtanzahl der Berichte in der Spalte *Berichte* klicken.

   → Der Überblick über alle Berichte eines Scans wird geöffnet.
3. In der Zeile des gewünschten Berichts auf klicken.
4. Register *Kachelübersicht* oder *Tabellenübersicht* wählen.
5. Gewünschtes Berichtformat in der Drop-down-Liste *Download* wählen (siehe Abb.7.8).
6. Auf den Slider *Anonymized* klicken, falls IP-Adressen im heruntergeladenen Bericht anonymisiert werden sollen.

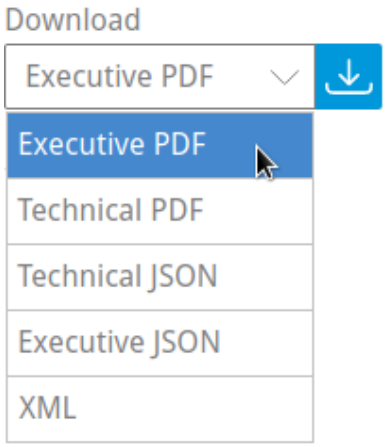

Abb. 7.8: Exportieren eines Berichts

7. Auf klicken.
8. Auf *OK* klicken, um den Bericht zu speichern.

7.5 Benachrichtigungen für Berichte

Benachrichtigungen können regelmäßig als Scan-Zusammenfassungen oder wenn ein Bericht fertiggestellt ist gesendet werden (siehe Kapitel *5.2* (Seite 16)).

KAPITEL 8

Häufig gestellte Fragen

8.1 Welche Firewall-Zugriffsregeln sind für die Kommunikation zwischen dem Greenbone Scan Cluster (GSC) und dem VPN-Gateway erforderlich?

Das Gateway nutzt die folgenden ausgehenden Verbindungen:

- 443/tcp ausgehend zum GSC (45.135.106.140)
- 443/tcp ausgehend zum Greenbone Cloud Service (195.252.156.97)
- 443/tcp ausgehend zum Updatedienst (gpublic.azurecr.io)

8.2 Welche Firewall-Zugriffsregeln sind für die Kommunikation zwischen dem Greenbone Scan Cluster (GSC) und externen Zielen erforderlich?

Der Greenbone Scan Cluster (GSC) verwendet den IP-Adressbereich 45.135.106.0/25 für den Scanverkehr zu externen Zielen. Die verwendeten Ports werden entsprechend der beim Erstellen des Ziels konfigurierten Portliste ausgewählt (siehe Kapitel *6.2.1* (Seite 31) und *6.9* (Seite 74)).

8.3 Welche Technologie wird für die VPN-Verbindung genutzt?

Ein SSH-Schicht-2-basiertes VPN wird für die VPN-Verbindung genutzt.

8.4 Was muss getan werden, falls MAC-NAT nicht funktioniert?

Mit der Gateway-Version 1.5.1 oder höher treten in der Regel keine Probleme auf.

Falls MAC-NAT nicht funktioniert, muss die Checkbox *MAC-NAT nutzen* beim Erstellen eines Gateways deaktiviert und die folgenden Einstellungen in VMware ESXi oder Oracle VirtualBox vorgenommen werden:

In VMWare ESXi:

- Separate *Portgruppe* für das Gateway erstellen und das Gateway damit verbinden.
- Einstellungen *Promiscuous-Modus* und *Gefälschte Übertragungen* für die Portgruppe auf *Akzeptieren* setzen.

In Oracle VirtualBox:

- In den Netzwerk-Einstellungen *Erweitert* öffnen und die Einstellung *Promiscuous Mode* auf *erlauben für alle VMs und den Host* setzen.

8.5 Was passiert mit dem Nutzeraccount, wenn das Abonnement endet?

Wenn das Abonnement endet, kann der Nutzer sich weiterhin einloggen und alle fertiggestellten Berichte ansehen. Das Starten neuer Scans ist nicht mehr möglich.

Falls der Account nicht mehr genutzt wird, wird er nach einiger Zeit gelöscht. Der Nutzer wird zuvor darüber informiert.

8.6 Warum ist der Scanprozess so langsam?

Die Geschwindigkeit eines Scans hängt von vielen Faktoren ab. Ein möglicher Grund ist das zeitintensive Scannen von ungenutzten IP-Adressen.

Um dies zu vermeiden, sollte vor dem eigentlichen Scan ein „Discovery“-Scan ausgeführt werden. Dieser Scan erkennt für jede IP-Adresse, ob diese aktiv ist oder nicht. Inaktive IP-Adressen werden während des eigentlichen Scans nicht untersucht. Firewalls und andere Systeme können solch eine erfolgreiche Feststellung verhindern.

Zusätzlich wird die Dauer eines Scans hauptsächlich durch die Netzwerkkonfiguration und die Anzahl der zu prüfenden Ports bestimmt. Der Dienst hinter jedem Port, der abgefragt wird, reagiert mit mindestens einem Log-Eintrag. Andere Kriterien sind die Abwehrmechanismen, die durch vollständige Portscans ausgelöst werden und Gegenmaßnahmen oder Benachrichtigungen einleiten. Selbst bei gewöhnlichen Scans können Firewalls simulieren, dass alle 65535 Ports aktiv sind und somit den Scan mit sogenannten Time-outs ausbremsen. In Situationen, in denen Portdrosselung auftritt, kann das Scannen aller TCP- und UDP-Ports eines einzelnen Systems bis zu 24 Stunden oder länger dauern. Da einige Gegenmaßnahmen die Dauer eines Scans erhöhen können, kann eine Drosselung vermieden werden, indem die Konfiguration des Abwehrsystems geändert wird. Bei Verdachtsfällen einer Kompromittierung oder höchsten Sicherheitsansprüchen ist ein vollständiger Scan unerlässlich.

8.7 Warum unterscheiden sich die Ergebnisse für dasselbe Ziel bei mehreren aufeinanderfolgenden Scans?

Die Ergebnisse aufeinanderfolgender Scans können aus folgenden Gründen voneinander abweichen:

- Es gab einen Verbindungsverlust über unzuverlässige Netzwerkverbindungen (zwischen dem Scanner-Host und dem Ziel).
- Die Netzwerkverbindung oder die Ausrüstung (zwischen dem Scanner-Host und dem Ziel) war überlastet.
- Ein überlasteter Zielhost und/oder -dienst hat aufgehört zu reagieren.
- „Fragile“ Protokolle (z. B. das Remote Desktop Protocol) reagieren nicht immer wie erwartet.
- Eine frühere Prüf-/Angriffsanfrage hat dazu geführt, dass der Dienst für eine kurze Zeit nicht reagiert hat.

Obwohl der Scanner versucht, das Auftreten solcher Situationen durch interne Wiederholungsroutinen zu reduzieren, können sie nicht vollständig ausgeschlossen werden.

8.8 Warum erscheint ein VNC-Dialog auf dem gescannten Zielsystem?

Beim Prüfen des Ports 5900 oder beim Konfigurieren eines VNC-Ports, erscheint ein Fenster zum Erlauben der Verbindung auf dem gescannten System. Dies wurde für UltraVNC Version 1.0.2 beobachtet.

Lösung: Port 5900 oder andere konfigurierte VNC-Ports von der Zielspezifikation ausschließen. Alternativ könnte ein Upgrade auf eine neuere Version von UltraVNC hilfreich sein (UltraVNC 1.0.9.6.1 nutzt lediglich Sprechblasen zum Informieren von Benutzern).

8.9 Warum löst der Scan Alarme bei anderen Sicherheitstools aus?

Bei vielen Schwachstellenprüfungen wird das Verhalten eines echten Angriffs simuliert. Zwar findet kein tatsächlicher Angriff statt, aber einige Sicherheitstools könnten einen Alarm ausgeben.

Ein bekanntes Beispiel ist:

Symantec meldet einen Angriff bezüglich CVE-2009-3103, falls der VT *Microsoft Windows SMB2 ‚_Smb2ValidateProviderCallback()‘ Remote Code Execution Vulnerability* (1.3.6.1.4.1.25623.1.0.100283) ausgeführt wird. Dieser VT wird nur ausgeführt, falls VTs, die Schaden am Hostsystem anrichten könnten, durch die Scan-Konfiguration aktiviert sind. Andernfalls kann das Zielsystem betroffen sein.

KAPITEL 9

Glossar

Dieser Abschnitt definiert relevante Begriffe die immer wieder im gesamten System verwendet werden.

9.1 CERT-Bund-Advisory

Der CERT-Bund[7], das Computer Emergency Response Team des Bundesamts für Sicherheit in der Informationstechnik (BSI), ist ein zentraler Kontaktpunkt für vorbeugende und reaktionsfähige Maßnahmen, die sicherheitsbezogene Computervorfälle betreffen.

Mit der Intention, Schäden zu vermeiden und potentielle Verluste einzugrenzen, umfasst die Arbeit des CERT-Bunds das Folgende:

- Erstellen und Veröffentlichen von Empfehlungen für vorbeugende Maßnahmen
- Aufzeigen von Schwachstellen in Hardware- und Softwareprodukten
- Vorschlagen von Maßnahmen, die bekannte Schwachstellen behandeln
- Unterstützen von Einrichtungen des öffentlichen Rechts beim Reagieren auf IT-Sicherheitsvorfälle
- Vorschlagen unterschiedlicher Schadensminderungsmaßnahmen

Zusätzlich betreibt CERT-Bund das Nationale IT-Lagezentrum[8].

Die Dienste des CERT-Bunds sind hauptsächlich für Bundesbehörden verfügbar und beinhalten das Folgende:

- 24-Stunden-Rufbereitschaft in Zusammenarbeit mit dem IT Situation Centre
- Analyse eingehender Vorfallberichte
- Erstellen von Empfehlungen, die von Vorfällen abgeleitet wurden
- Unterstützung von Bundesbehörden während IT-Sicherheitsvorfällen
- Betreiben eines Warn- und Informationsdiensts
- Aktives Benachrichtigen der Bundesverwaltung im Falle drohender Gefahr

[7] https://www.cert-bund.de/
[8] https://www.bsi.bund.de/DE/Themen/KRITIS/Aktivitaeten/IT-Lagezentrum/lagezentrum_node.html

CERT-Bund bietet einen Warn- und Informationsdienst (WID) an. Momentan stellt dieser Dienst die CERT-Bund-Advisories bereit. Dieser Informationsdienst ist nur für Bundesbehörden als nichtöffentliche Liste verfügbar. Die Advisories beschreiben aktuelle Informationen über sicherheitskritische Vorfälle in Computersystemen und detaillierte Maßnahmen zum Beseitigen von Sicherheitsrisiken.

9.2 CPE

Die Common Platform Enumeration (CPE)[9] ist CVE nachempfunden. Sie ist gegliedertes Benennungsschema für Anwendungen, Betriebssysteme und Hardwaredevices.

CPE wurde von MITRE[10] eingeführt und wird von NIST als Teil der National Vulnerability Database (NVD)[11] gewartet. NIST wartet bereits seit mehreren Jahren das offizielle CPE-Wörterbuch und die CPE-Spezifikationen. CPE basiert auf der allgemeinen Syntax des Uniform Resource Identifiers (URI) und enthält ein formales Namensformat, eine Sprache zum Beschreiben komplexer Plattformen, eine Methode zum Vergleichen von Namen mit einem System und ein Beschreibungsformat, um Texte und Tests an einen Namen zu binden.

Ein CPE-Name beginnt mit „cpe:/“, gefolgt von bis zu sieben Komponenten, die durch Doppelpunkte getrennt sind (siehe Abb.9.1):

- Part („h“ für Hardware, „o“ für Betriebssystem oder „a“ für Anwendung)
- Vendor
- Product
- Version
- Update
- Edition
- Language

Beispiel: cpe:/o:linux:kernel:2.6.0

CPE besteht aus den folgenden Komponenten:

- **Naming**
  Die Naming-Spezifikation beschreibt die logische Struktur von sogenannten well-formed names (WFNs), ihre Verbindung zu URIs und formatierten Zeichenketten sowie ihre Umwandlung.
- **Name Matching**
  Die Name-Matching-Spezifikation beschreibt die Methoden, um WFNs mit anderen zu vergleichen. Dies ermöglicht die Überprüfung, ob sich einige oder alle WFNs auf das gleiche Produkt beziehen.
- **Dictionary**
  Das Wörterbuch ist ein Verzeichnis von CPE-Namen und -Metadaten. Jeder Name definiert eine einzelne Klasse von IT-Produkten. Die Dictionary-Spezifikation beschreibt die Prozesse zum Nutzen des Wörterbuchs, z. B. das Suchen nach einem bestimmten Namen oder nach Einträgen, die zu einer allgemeineren Klasse gehören.
- **Applicability Language**
  Die Applicability-Language-Spezifikation beschreibt die Erstellung komplexer, logischer Ausdrücke mithilfe von WFNs. Diese Anwendbarkeitsangaben können zum Taggen von Checklisten, Richtlinien oder anderen Dokumenten und damit für die Beschreibung, für welche Produkte die Dokumente relevant sind, genutzt werden.

[9] https://csrc.nist.gov/projects/security-content-automation-protocol/specifications/cpe
[10] https://www.mitre.org/
[11] https://nvd.nist.gov/

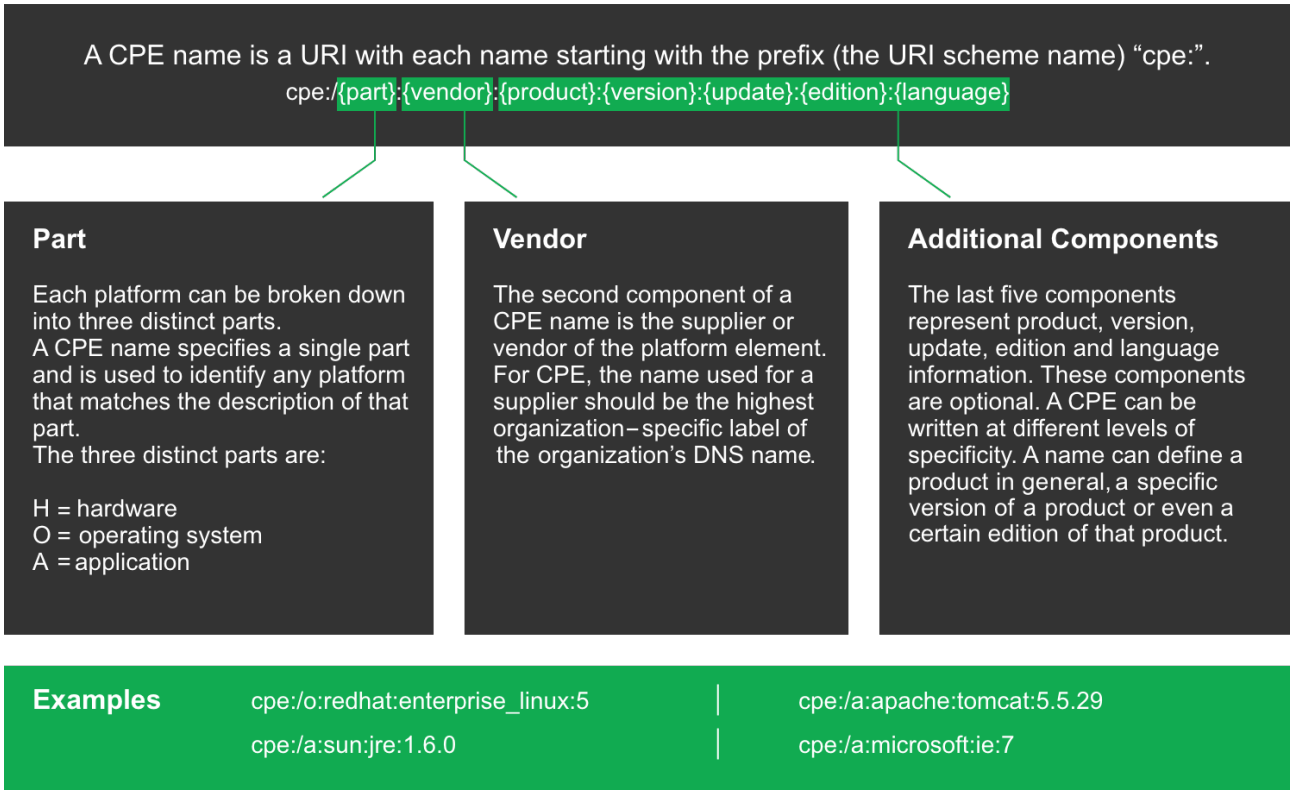

Abb. 9.1: Namensstruktur eines CPE-Namens

9.3 CVE

In der Vergangenheit entdeckten und meldeten unterschiedliche Organisationen Schwachstellen zur gleichen Zeit und benannten diese mit unterschiedlichen Namen. Dies führte dazu, dass die gleiche Schwachstelle von mehreren Scannern unter unterschiedlichen Namen gemeldet wurde, was die Kommunikation und den Vergleich der Ergebnisse erschwerte.

Um das zu beheben, gründete MITRE[12] das Common Vulnerabilities and Exposure (CVE) Projekt[13]. Jeder Schwachstelle wird eine eindeutige Kennzeichnung zugeordnet, die aus dem Veröffentlichungsjahr und einer einfachen Nummer besteht. Diese Kennzeichnung dient als zentrale Referenz.

Die CVE-Datenbank von MITRE ist keine Schwachstellendatenbank. CVE wurde entwickelt, um die Schwachstellendatenbank mit anderen Systemen zu verbinden und den Vergleich von Sicherheitswerkzeugen und -diensten zu ermöglichen.

Die CVE-Datenbank enthält keine detaillierten, technischen Informationen oder Informationen bezüglich der Risiken, Auswirkungen oder Beseitigung einer Schwachstelle. Eine CVE enthält nur die Kennzeichnungsnummer mit dem Status, einer kurzen Beschreibung und Referenzen zu Berichten und Advisories.

Die National Vulnerability Database (NVD)[14] bezieht sich auf die CVE-Datenbank und ergänzt den Inhalt mit Informationen bezüglich der Beseitigung, des Schweregrads, der möglichen Auswirkung und der betroffenen Produkte einer Schwachstelle. Greenbone bezieht sich auf die CVE-Datenbank der NVD.

[12] https://www.mitre.org/
[13] https://cve.mitre.org/
[14] https://nvd.nist.gov/

9.4 CVSS

Um die Deutung von Schwachstellen zu unterstützen, wurde das Common Vulnerability Scoring System (CVSS) entwickelt. CVSS ist ein Industriestandard zum Beschreiben des Schweregrads eines Sicherheitsrisikos in Computersystemen.

Sicherheitsrisiken werden mithilfe unterschiedlicher Kritierien bewertet und verglichen. Dies ermöglicht das Erstellen einer Prioritätenliste von Gegenmaßnahmen.

CVSS wurde von der CVSS Special Interest Group (CVSS-SIG)[15] des Forum of Incident Response and Security Teams[16] (FIRST) entwickelt. Die aktuelle CVSS-Scoreversion ist 3.1.

Der CVSS-Score in Version 2 unterstützt Base-Score-Metrics, Temporal-Score-Metrics und Environmental-Score-Metrics.

Base-Score-Metrics
: Base-Score-Metrics prüfen die Nutzbarkeit einer Schwachstelle und ihre Auswirkung auf das Zielsystem. Zugang, Komplexität und Anforderungen der Authentifizierung werden eingestuft. Zusätzlich bewerten die Maße, ob die Vertraulichkeit, Integrität oder Verfügbarkeit gefährdet ist.

Temporal-Score-Metrics
: Temporal-Score-Metrics prüfen, ob ein vollständiger Beispielcode existiert, der Anbieter einen Patch anbietet und die Schwachstelle bestätigt. Der Score ändert sich stark im Laufe der Zeit.

Environmental-Score-Metrics
: Environmental-Score-Metrics beschreiben den Effekt einer Schwachstelle innerhalb einer Organisation. Sie berücksichtigen Schaden, Verteilung der Ziele, Vertraulichkeit, Integrität und Verfügbarkeit. Die Beurteilung hängt stark von der Umgebung, in der das gefährdete Produkt genutzt wird, ab.

9.5 DFN-CERT-Advisory

Während die einzelnen VTs, CVEs, CPEs und OVAL-Definitionen vorrangig erstellt wurden, um von Computersystemen verarbeitet zu werden, veröffentlicht DFN-CERT[17] regelmäßig neue Advisories.

DFN-CERT ist für hunderte Universitäten und Forschungsinstitute, die mit dem Deutschen Forschungsnetz (DFN)[18] verbunden sind, verantwortlich. Zusätzlich stellt er entscheidende Sicherheitsdienste für die Regierung und die Industrie bereit.

Ein Advisory beschreibt besonders kritische Risiken, die eine schnelle Reaktion erfordern. Der DFN-CERT-Advisory-Dienst enthält die Kategorisierung, Verteilung und Bewertung von Advisorythemen durch verschiedene Softwarehersteller und -händler.

9.6 Greenbone Enterprise Feed

Der Inhalt des Greenbone Enterprise Feeds, der die Schwachstellentests (VTs) zum Scannen bereitstellt, kann in Greenbones SecInfo-Portal[19] eingesehen werden.

[15] https://www.first.org/cvss/
[16] https://www.first.org/
[17] https://www.dfn-cert.de/
[18] https://www.dfn.de/
[19] https://www.greenbone.net/secinfo-portal/

9.7 Host

Ein Host ist ein einzelnes System, das mit einem Computernetzwerk verbunden ist und gescannt werden kann. Ein oder mehrere Hosts bilden die Basis eines Scanziels.

Hosts in Scanzielen und Scanberichten können mithilfe ihrer Netzwerkadresse, entweder eine IP-Adresse oder ein Hostname, identifiziert werden.

9.8 Vulnerability Test (VT)

Ein Vulnerability Test (VT) ist eine Routine, die ein Zielsystem auf das Vorhandensein von konkreten bekannten und potentiellen Sicherheitsproblemen untersucht. VTs enthalten Informationen über das Entwicklungsdatum, die betroffenen Systeme, die Auswirkungen von Schwachstellen und die Beseitigung.

9.9 OVAL-Definition

Die Open Vulnerability and Assessment Language (OVAL)[20] ist ein Projekt von MITRE[21] und wird vom Centre of Internet Security (CIS) gepflegt.

OVAL ist eine Sprache zum Beschreiben von Schwachstellen, Konfigurationseinstellungen (Compliance), Patches und Anwendungen (Bestand).

Die XML-basierten Definitionen erlauben die einfache Verarbeitung durch automatisierte Systeme und beschreiben die Erkennung einzelner Systeme und Schwachstellen.

9.10 Portliste

Eine Portliste ist eine Liste von Ports. Jedes Ziel wird mit einer Portliste verbunden. Diese bestimmt, welche Ports während eines Scans des Ziel untersucht werden.

9.11 Qualität der Erkennung (QdE)

Die Qualität der Erkennung (QdE) ist ein Wert zwischen 0 % und 100 % und beschreibt die Zuverlässigkeit der ausgeführten Schwachstellen- oder Produkterkennung.

Obwohl der QdE-Bereich es erlaubt, die Qualität detailgenau darzustellen, nutzen die meisten Prüfroutinen eine Standardvorgehensweise. Deshalb werden den QdE-Werten QdE-Typen zugewiesen. Die aktuelle Typenliste wird möglicherweise mit der Zeit erweitert.

[20] https://oval.cisecurity.org/
[21] https://www.mitre.org/

QdE in %	QoD-Typ	Beschreibung
100	exploit	Die Erkennung erfolgte durch die Ausnutzung einer Sicherheitslücke und ist daher vollständig bestätigt.
99	remote_vul	Aktive Prüfung auf dem Zielsystem (Codeausführung, Traversal-Angriff, SQL-Einschleusung etc.), bei welcher die Antwort eindeutig das Vorhandensein der Schwachstelle zeigt.
98	remote_app	Aktive Prüfung auf dem Zielsystem (Codeausführung, Traversal-Angriff, SQL-Einschleusung etc.), bei welcher die Antwort eindeutig das Vorhandensein der gefährdeten Anwendung zeigt.
97	package	Authentifizierte paketbasierte Prüfungen für Linux(oide) Systeme.
97	registry	Authentifizierte Prüfungen auf Basis der Registry von Microsoft Windows.
95	remote_active	Aktive Prüfung auf dem Zielsystem (Codeausführung, Traversal-Angriff, SQL-Einschleusung etc.), bei welcher die Antwort das wahrscheinliche Vorhandensein der gefährdeten Anwendung oder der Schwachstelle zeigt. „Wahrscheinlich“ bedeutet, dass die Erkennung nur in seltenen Fällen inkorrekt ist.
80	remote_banner	Prüfung von Anwendungsbannern auf dem Zielsystem, die den Patch-Status als Information anbieten. Zum Beispiel ist dies für viele proprietäre Produkte der Fall.
80	executable_version	Authentifizierte Versionsprüfung über eine ausführbare Datei für Linux(oide) und Microsoft Windows Systeme, bei denen Anwendungen den Patch-Status in der Version anbieten.
75		Während der Systemmigration wurde dieser Wert jedem Ergebnis zugeordnet, das vor der Einführung von QdE gewonnen wurde. Trotzdem haben einige VTs möglicherweise aus anderem Grund diesen Wert.
70	remote_analysis	Prüfung auf dem Zielsystem, bei welcher Analysen durchführt werden, die nicht vollständig zuverlässig sind.
50	remote_probe	Prüfung auf dem Zielsystem, bei welcher zwischenliegende Systeme wie Firewalls die korrekte Erkennung vortäuschen können, sodass nicht eindeutig ist, ob die Anwendung selbst geantwortet hat. Zum Beispiel kann dies für Verbindungen ohne TLS geschehen.
30	remote_banner_unreliable	Prüfung von Anwendungsbannern des Zielsystems, die den Patch-Status nicht als Information anbieten. Zum Beispiel ist dies für viele Open-Source-Produkte aufgrund von Backport-Patches der Fall.
30	executable_version_unreliable	Authentifizierte Versionsprüfung über eine ausführbare Datei für Linux(oide) Systeme, bei denen Anwendungen den Patch-Status nicht in der Version anbieten.
1	general_note	Allgemeine Notiz zu einer potentiellen Schwachstelle ohne konkrete Erkennung einer vorhandenen Anwendung.

9.12 Bericht

Ein Bericht ist das Ergebnis eines Scans und enthält eine Zusammenfassung dessen, was die ausgewählten VTs für jeden der Zielhosts erkannt haben.

Ein Bericht ist immer mit einer Aufgabe verknüpft. Die Scan-Konfiguration, die den Umfang des Berichts festlegt, ist Teil der verknüpften Aufgabe und kann nicht verändert werden. Daher ist für jeden Bericht sichergestellt, dass die ausführende Konfiguration erhalten bleibt und verfügbar ist.

9.13 Ergebnis

Ein einzelnes Ergebnis, das vom Scanner als Teil des Berichts erzeugt wurde, z. B. eine Schwachstellenwarnung oder eine Log-Nachricht.

9.14 Scan

Ein Scan ist eine Aufgabe, die ausgeführt wird. Für jede Aufgabe kann jeweils nur ein Scan aktiv sein. Das Ergebnis ist ein Scanbericht.

Die Status aller aktiven Scans sind auf der Seite *Scanverwaltung* sichtbar.

Wenn ein Scan ausgeführt wird, wird der Fortschritt als Prozentangabe der Gesamtanzahl aller auszuführenden Tests angezeigt. Die Dauer eines Scans wird aus der Anzahl von Zielen und der Komplexität der Scan-Konfiguration bestimmt und reicht von wenigen Minuten bis zu einigen Stunden oder sogar Tagen.

Die Seite *Scanverwaltung* bietet die Möglichkeit, einen Scan zu stoppen.

9.15 Scanner

Ein Scanner ist ein OpenVAS-Scanner-Daemon oder ein kompatibler OSP-Daemon, auf dem der Scan läuft.

9.16 Scan-Konfiguration

Eine Scan-Konfiguration deckt die Auswahl an VTs sowie genereller und spezieller Parameter für den Scanserver und für einige der VTs ab.

Die Scan-Konfiguration beinhaltet nicht die Auswahl der Ziele.

9.17 Zeitplan

Ein Zeitplan legt fest, zu welcher Zeit eine Aufgabe automatisch starten soll, nach welcher Zeitspanne die Aufgabe automatisch wiederholt werden soll und welche maximale Laufzeit eine Aufgaben haben darf.

9.18 Schweregrad

Der Schweregrad ist ein Wert zwischen 0.0 (kein Schweregrad) und 10.0 (höchster Schweregrad) und zeigt auch die Schweregradklasse (*Log*, *Niedrig*, *Mittel* oder *Kritisch*).

Dieses Konzept basiert auf CVSS, aber wird auch in Fällen angewendet, in denen kein vollständiger CVSS-Basisvektor verfügbar ist. Beispielsweise werden beliebige Werte in diesem Bereich für Übersteuerungen angewendet und von OSP-Scannern genutzt, ohne dass es eine Vektordefinition gibt.

Der Vergleich, die Gewichtung und die Priorisierung aller Scanergebnisse oder VTs ist möglich, da das Schwachstellenkonzepts konsequent über das ganze System hinweg angewendet wird. Jedem neuen VT wird ein vollständiger CVSS-Vektor zugewiesen, selbst wenn CVE keinen zur Verfügung stellt und jedem Ergebnis von OSP-Scannern wird ein entsprechender Schweregrad zugeordnet, selbst wenn der Scanner ein anderes Schweregradschema nutzt.

Die Schweregradklassen *Log*, *Niedrig*, *Mittel* und *Kritisch* werden als Unterbereiche des Hauptbereichs 0.0 – 10.0 definiert.

Scanergebnissen, die gefunden werden, wird ein Schweregrad zugewiesen. Der Schweregrad des zugehörigen VTs ändert sich möglicherweise mit der Zeit.

9.19 Lösungstyp

Diese Information zeigt mögliche Lösungen für die Beseitigung einer Schwachstelle.

Temporäre Lösung
: Eine Problemumgehung (Informationen über Konfigurationen oder bestimmte Einsatzszenarien, die die Belastung durch die Schwachstelle vermeiden) ist verfügbar, um die Schwachstelle temporär zu beseitigen. Es können keine, eine oder mehrere Problemumgehungen verfügbar sein. Dies ist normalerweise die „erste Verteidigungslinie“ gegen neue Schwachstellen, bevor eine Risikominderung oder offizielle Lösung entdeckt oder ausgegeben wurde.

Risikominderung
: Es sind Informationen über Konfigurationen oder Einsatzszenarien verfügbar, die das Risiko der Schwachstelle reduzieren, was die Schwachstelle auf dem betroffenden Produkt allerdings nicht entfernt.

Offizielle Lösung
: Eine offizielle Herstellerlösung ist verfügbar. Sofern nicht anders vermerkt, wird angenommen, dass die Lösung die Schwachstelle komplett beseitigt.

Lösung wird gesucht
: Es ist momentan keine Lösung verfügbar, um die Schwachstelle zu beseitigen, möglicherweise gibt es aber zukünftig eine.

Keine Lösung verfügbar
: Es gibt keine Lösung für die Schwachstelle und es wird auch zukünftig keine geben. Dies ist oft der Fall, wenn ein Produkt verwaist ist, nicht länger gewartet wird oder andersweitig überholt ist.

9.20 Ziel

Ein Ziel definiert ein Set aus Systemen (Hosts), das gescannt wird. Die Systeme werden entweder durch ihre IP-Adresse, durch ihre Hostnamen oder mithilfe einer CIDR-Netzwerkschreibweise gekennzeichnet.

9.21 Aufgabe

Eine Aufgabe wird zunächst duch ein Ziel und eine Scan-Konfiguration gebildet. Das Ausführen der Aufgabe leitet den Scan ein. Jeder Scan erzeugt einen Bericht. Als Ergebnis sammelt eine Aufgabe eine Reihe von Berichten.

Das Ziel und die Scan-Konfiguration einer Aufgabe sind statisch. Deshalb beschreibt eine Folge von Berichten die Änderung des Sicherheitsstatus mit der Zeit.

Stichwortverzeichnis

W