Zentrum der
Brandenburgischen
Hochschulen für
Digitale Transformation

Zentraler Dienst Schwachstellenscan

ZDT-Jahrestagung 2025

Präsentator: Ahmed Mehmedovic

06. November 2025

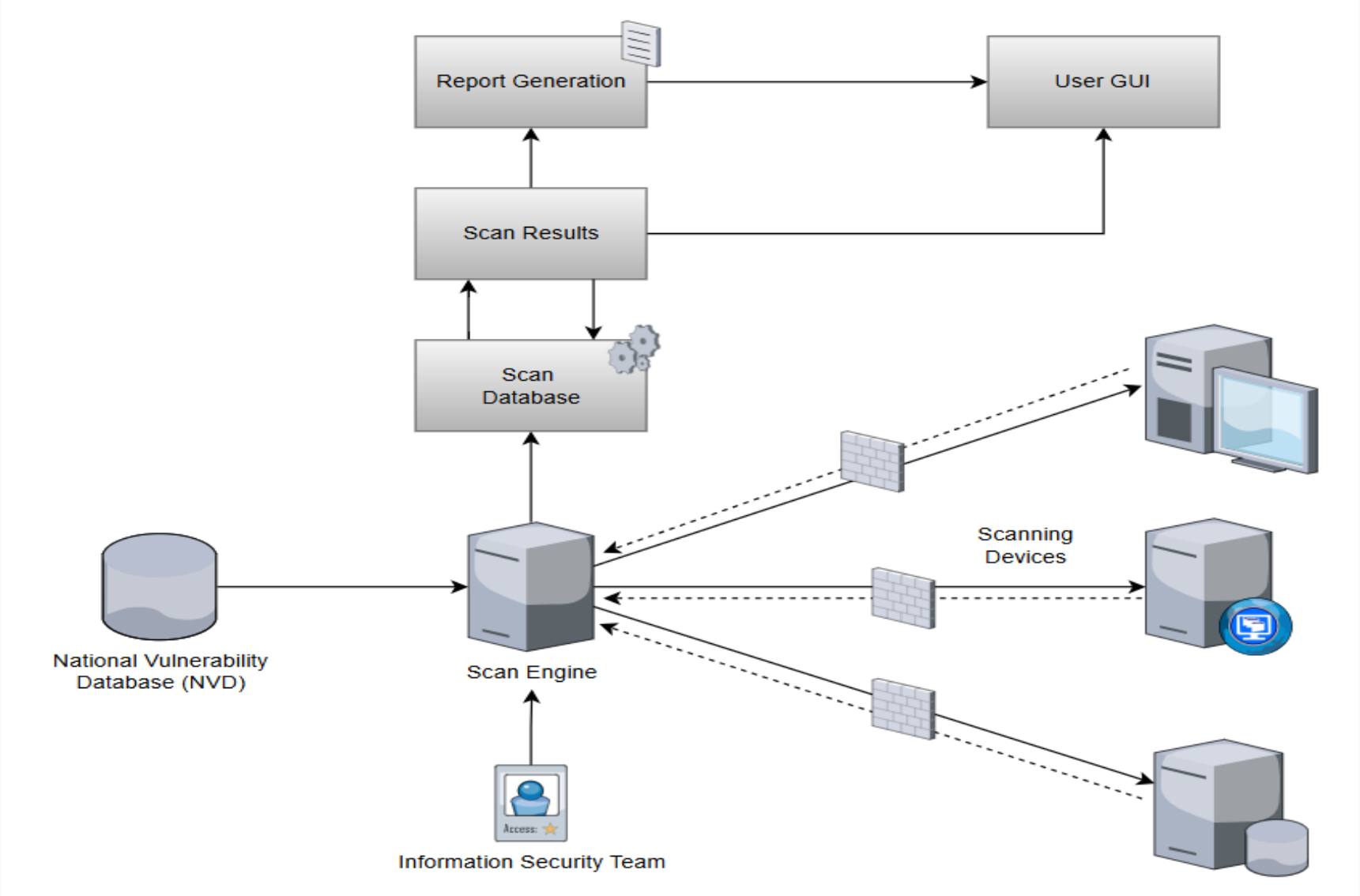
Technische
Hochschule
Wildau
Technical University
of Applied Sciences
WILDAU

Agenda

1. Was ist ein Schwachstellenscan?
2. Technische Umsetzung
3. Architektur: Master–Sensor-Prinzip
4. Installation & Komponenten
5. Schwachstellentests-Portal
6. Credit-System
7. Scanablauf
8. Erste Schritte für Admins
9. Projektzeitplan
10. Perspektive & Weiterentwicklung

Was ist ein Schwachstellenscan?

Technische Umsetzung eines Schwachstellenscans



Architektur: Master–Sensor-Prinzip

Zentrale Steuerung:
Der Greenbone Master an der TH Wildau verwaltet alle Sensoren und Scanaufträge zentral.

Verteilte Sensoren:
Jede Hochschule betreibt einen eigenen Greenbone Sensor, der lokal in den internen Netzen scannt.

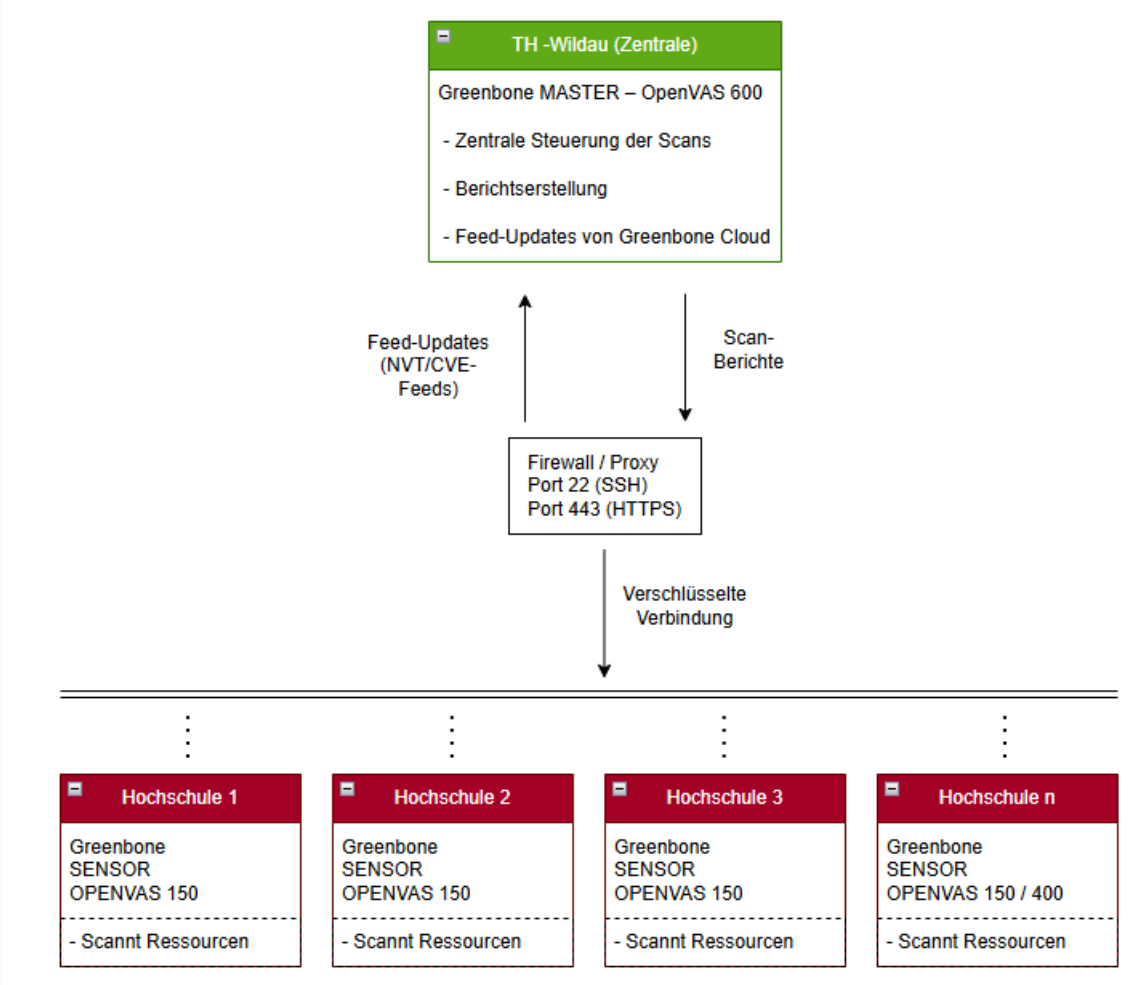
Datenfluss:

- Master verteilt Scan-Jobs → Sensor
- Sensor führt Scan durch → sendet Ergebnisse zurück
- Kommunikation ausschließlich verschlüsselt (SSH / HTTPS)

Feed-Updates:
Master erhält regelmäßig aktuelle NVT- und CVE-Daten aus dem Greenbone Feed und verteilt sie an Sensoren.

Zielsetzung:

- Einheitliche Scan-Standards über alle Hochschulen
- Minimierte Netzbelastung durch lokale Scans
- Zentrale Auswertung und Berichtserstellung



Was wird installiert?

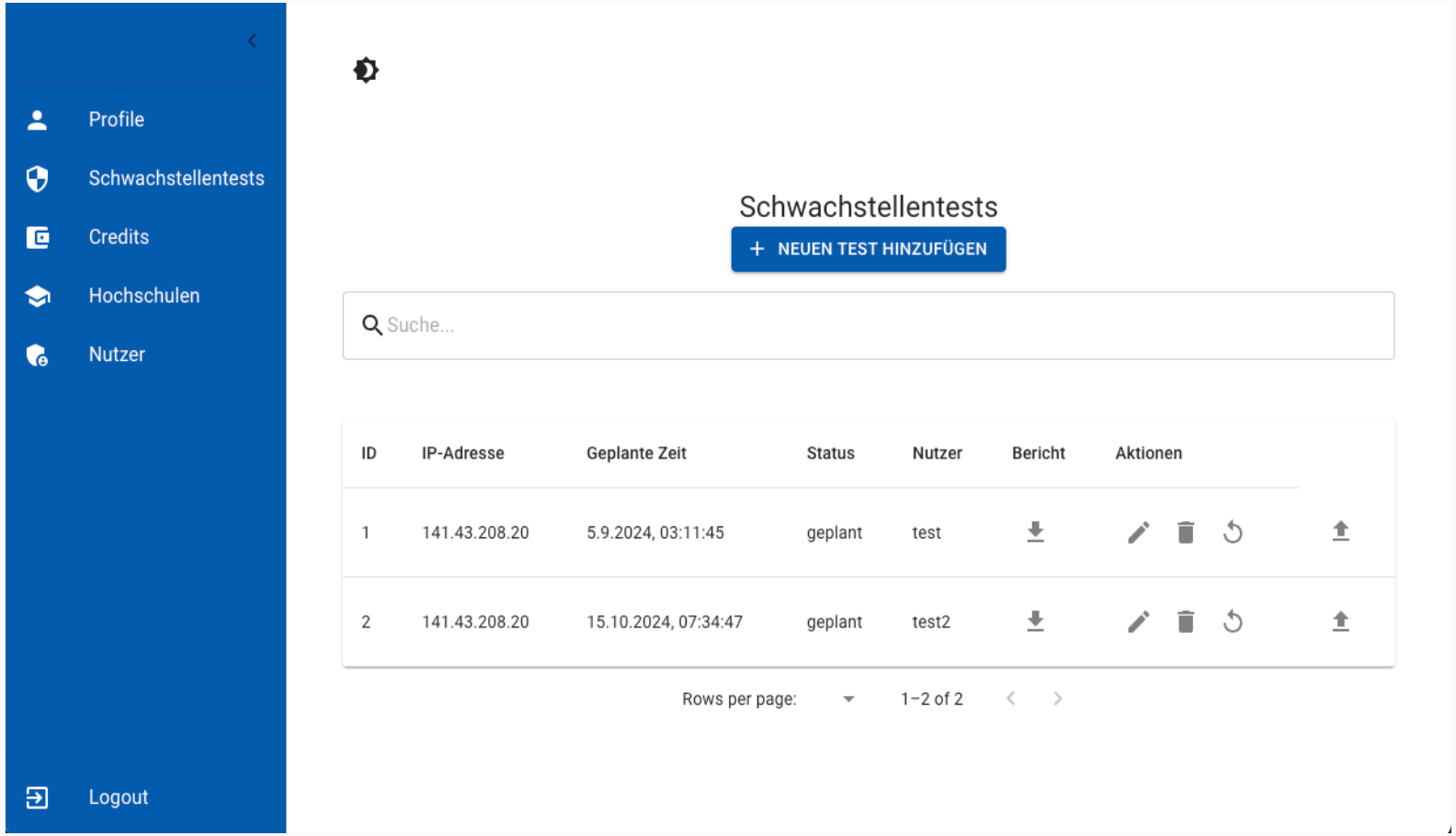
Standort	Komponente	Aufgabe	Bemerkung
TH –Wildau (Zentrale)	Greenbone Master (OpenVAS 600)	Steuerung aller Scans, Berichtsmanagement, Feed-Updates	Dedizierter Server
Hochschule 1 –7	Greenbone Sensor (OpenVAS 150 o. 400)	Lokale Durchführung der Scans, Rückmeldung an Master	Sensor in eigenem Netzsegment
Greenbone Feed Server (extern)	-	Bereitstellung aktuller Schwachstellendaten	Verbindung nur vom Master
Administrationszugang (intern)	Web-UI (HTTPS)	Konfiguration, Auswertung, Task-Management	Zugriff über zentrale Benutzerverwaltung

Technische Eckpunkte

- Betrieb auf Linux-Basis (Debian)
- Kommunikation ausschließlich verschlüsselt (SSH, HTTPS)
- Automatische Feed-Synchronisation über den Master
- Updates und Wartung zentral durchgeführt

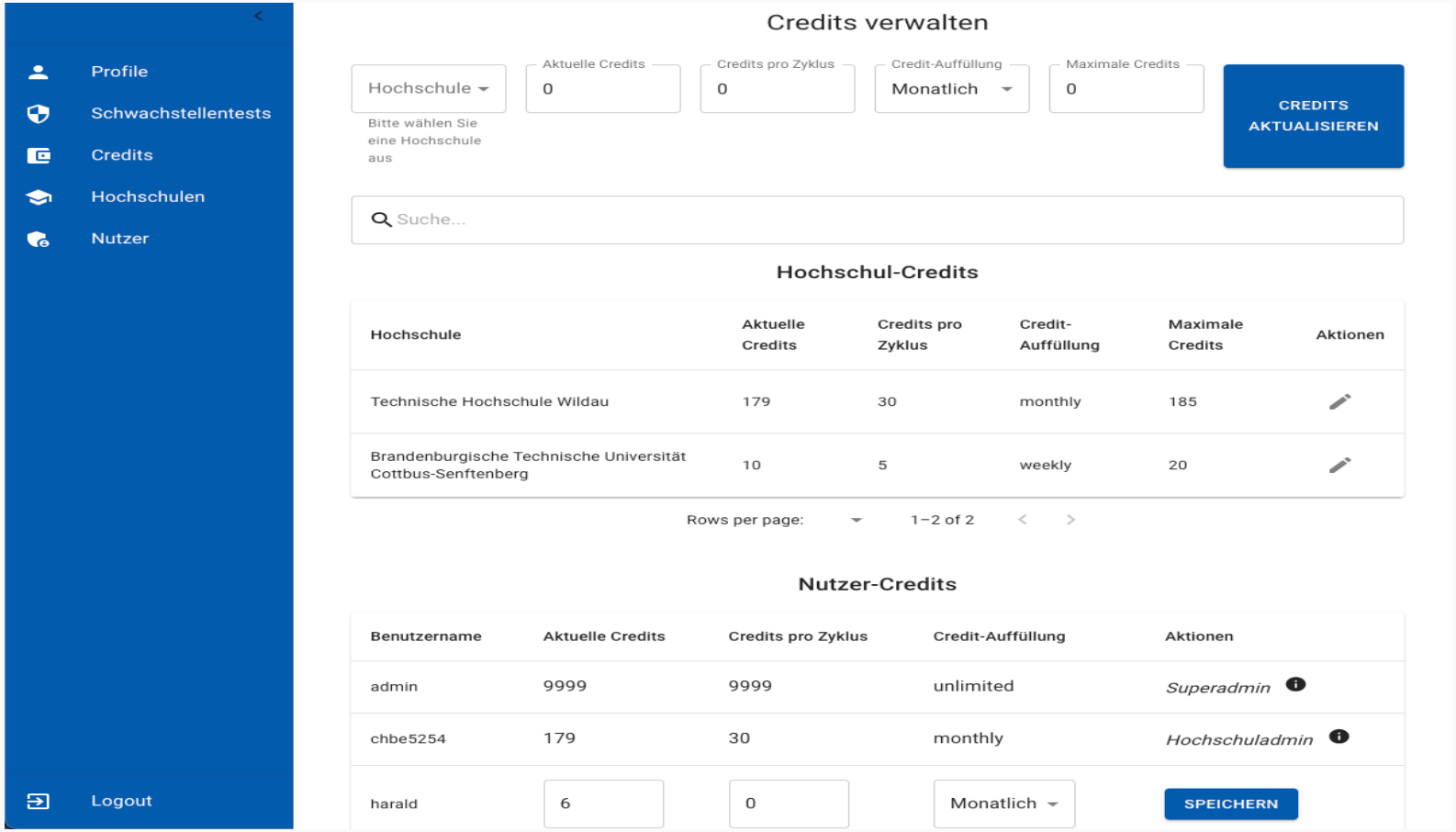
Schwachstellentests-Portal (Übersicht)

- Eigenständige Verwaltung von Scans durch Hochschulen
- Übersicht über geplante, laufende und abgeschlossene Tests
- Direkter Zugriff auf Berichte und Scan-Historie
- Zentrale Benutzerverwaltung und Rechtekonzept
- Transparente Nachvollziehbarkeit aller Aktivitäten

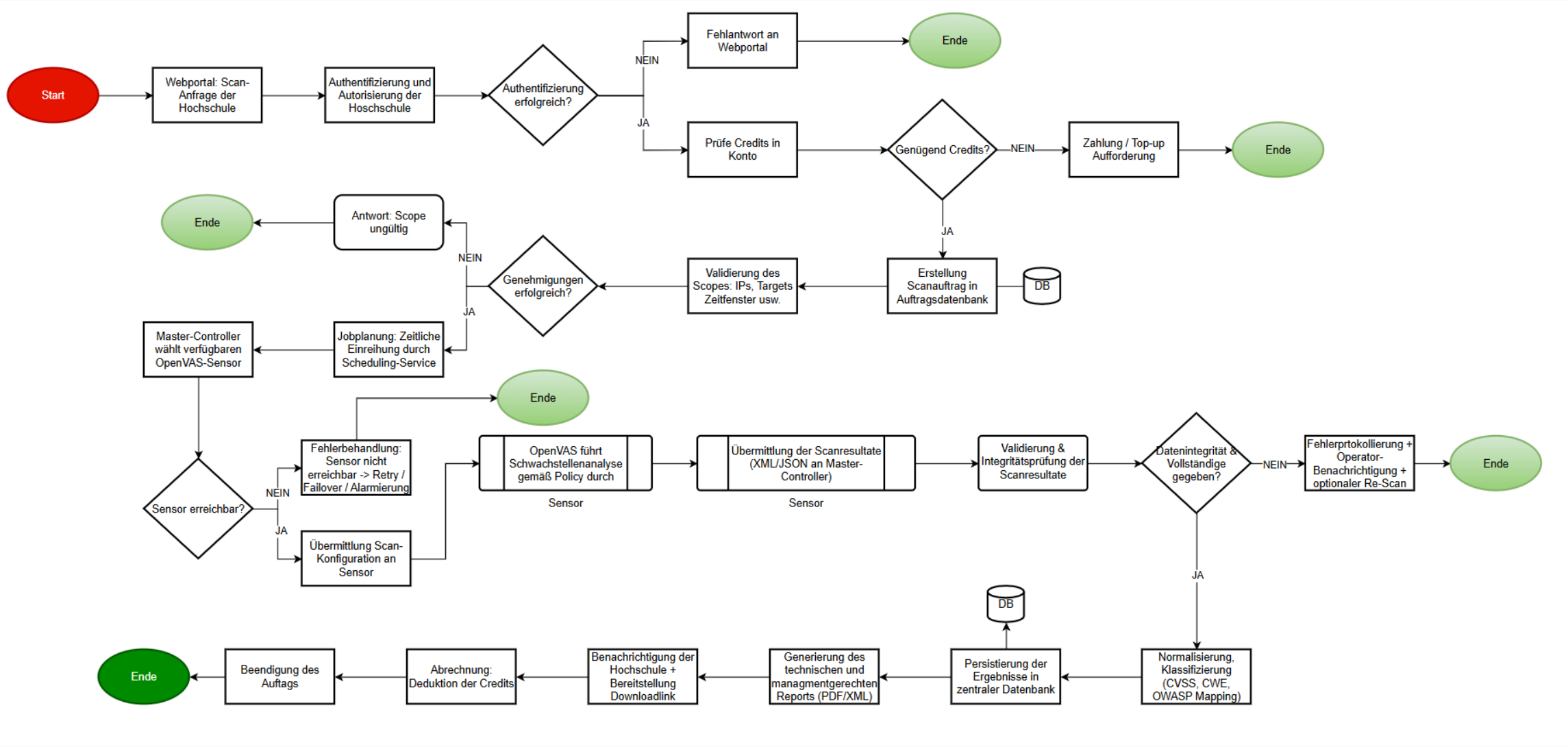


Credit-System (Ressourcensteuerung)

- Steuerung der verfügbaren Scan-Kapazitäten
- Credits pro Hochschule und Nutzer
- Automatische Auffüllung nach Zyklus (monatlich, wöchentlich etc.)
- Priorisierung und Fairness zwischen Hochschulen
- Transparente Übersicht im Admin-Portal



Scanablauf


Start
Webportal: Scan-Anfrage der Hochschule
Authentifizierung und Autorisierung der Hoschschule
Authentifizierung erfolgreich?
NEIN
Fehlantwort an Webportal
Ende
JA
Prüfe Credits in Konto
Genügend Credits?
NEIN
Zahlung / Top-up Aufforderung
Ende
JA
Erstellung Scanauftrag in Auftragsdatenbank
DB
Validierung des Scopes: IPs, Targets Zeitfenster usw.
Genehmigungen erfolgreich?
NEIN
Antwort: Scope ungültig
Ende
JA
Jobplanung: Zeitliche Einreihung durch Scheduling-Service
Master-Controller wählt verfügbaren OpenVAS-Sensor
Sensor erreichbar?
NEIN
Fehlerbehandlung: Sensor nicht erreichbar -> Retry / Failover / Alarmierung
Ende
JA
Übermittlung Scan-Konfiguration an Sensor
OpenVAS führt Schwachstellenanalyse gemäß Policy durch
Sensor
Übermittlung der Scanresultate (XML/JSON an Master-Controller)
Sensor
Validierung & Integritätsprüfung der Scanresultate
Datenintegrität & Vollständige gegeben?
NEIN
Fehlerprtokollierung + Operator-Benachrichtigung + optionaler Re-Scan
Ende
JA
Normalisierung, Klassifizierung (CVSS, CWE, OWASP Mapping)
Persistierung der Ergebnisse in zentraler Datenbank
DB
Generierung des technischen und managmentgerechten Reports (PDF/XML)
Benachrichtigung der Hochschule + Bereitstellung Downloadlink
Abrechnung: Deduktion der Credits
Beendigung des Auftags
Ende

Erste Schritte für Admins

STEP 1

Firewall-Freigaben prüfen

- Freigabe für Kommunikation Sensor ↔ Master
- Ports: 22 (SSH) und 443 (HTTPS)

STEP 2

Ansprechpartner bestätigen

- Benennung lokaler IT-Ansprechpersonen

STEP 3

Verbindung zum Master testen

- Rückmeldung an zentrales Team, dass Sensor erreichbar ist

STEP 4

Scanbereiche definieren

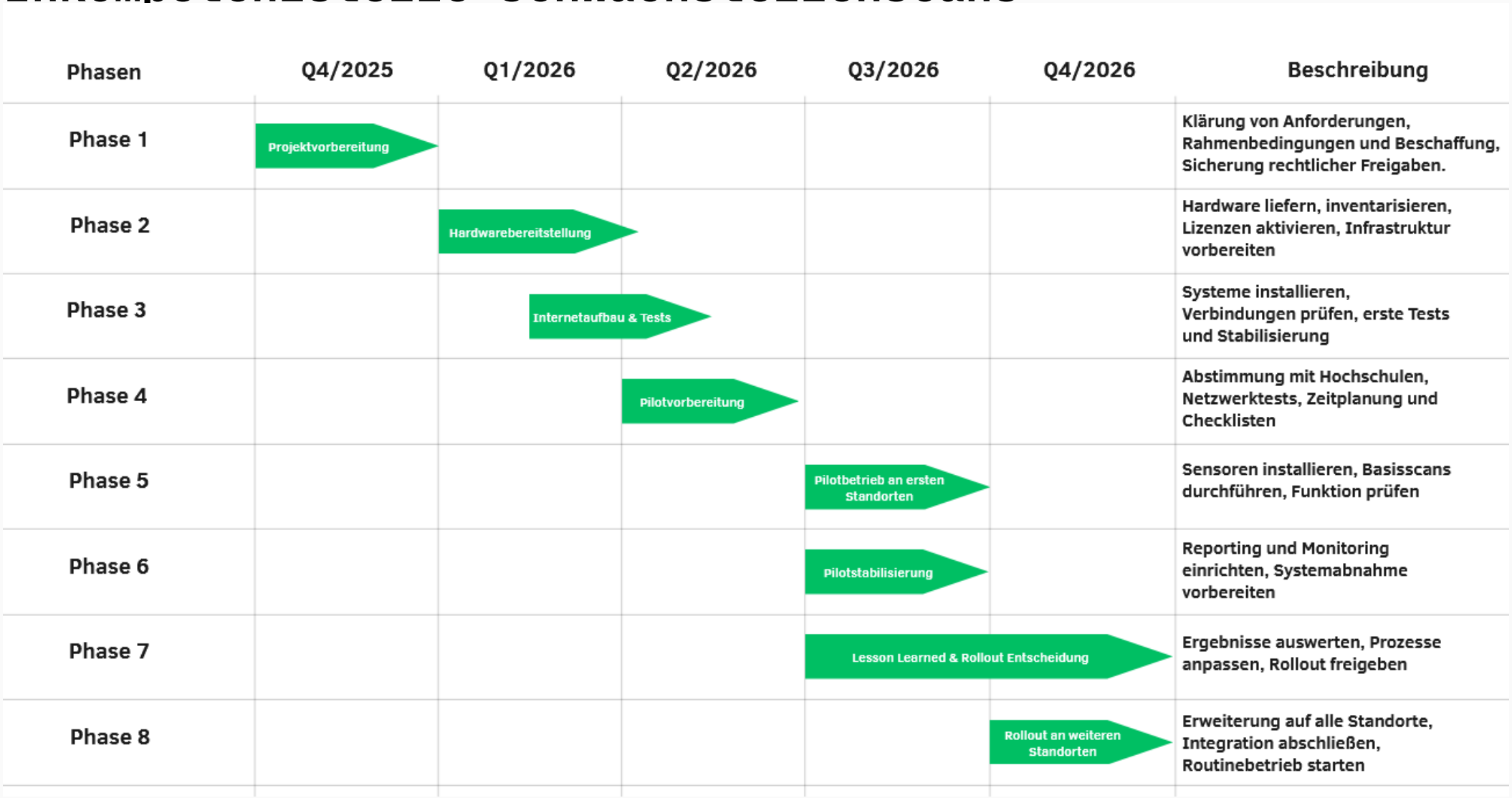
- Festlegen, welche VLANs / IP-Segmente gescannt werden dürfen
- Abgrenzung sensibler Systeme (z. B. Prüfungs- oder HR-Server)

STEP 5

Scan-Zeitplan festlegen

- Zeitfenster abstimmen (z. B. nachts, außerhalb der Lehrzeiten)
- Festlegung von Scan-Intervallen und Prioritäten

Ablauf- und Zeitplan des Projekts Kernkompetenzstelle Schwachstellenscans



Perspektive / Weiterentwicklung

Zentrales Schwachstellenportal (in Planung):
Übersicht aller Scans, Dashboards und Trendanalysen

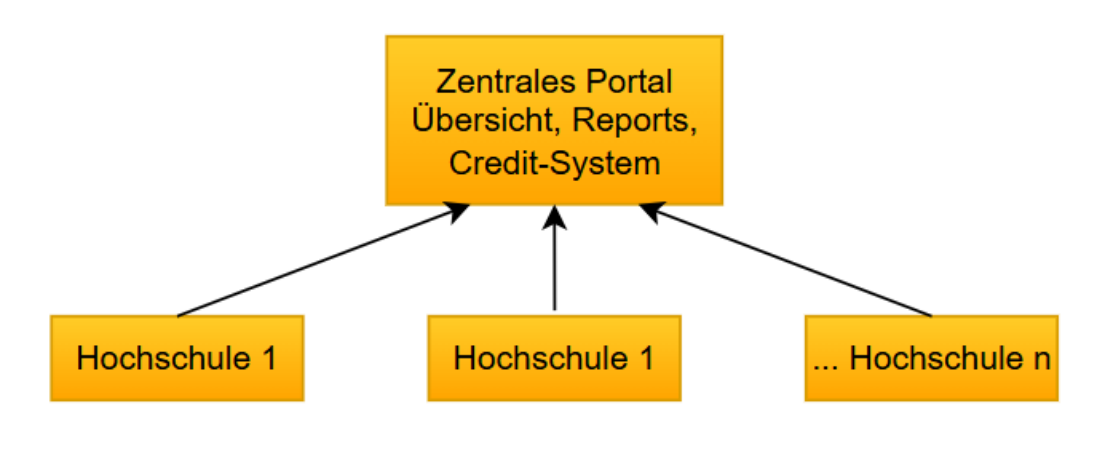
Credit-System:
Steuerung der Scan-Kapazitäten pro Hochschule

Automatisierte Berichterstellung:
Export in Ticketsysteme

Erweiterung des Monitorings:
Kombination mit Patch-Management

Hauptziel 2026:
Mehrzahl der Hochschulen mit aktivem Schwachstellenscan

Langfristige Perspektive:
Anbindung an SIEM und Aufbau einer nachhaltigen Sicherheitskultur über alle Hochschulen hinweg



Zentrum der
Brandenburgischen
Hochschulen für
Digitale Transformation

Danke für
Ihre Teilnahme.

Kontakt:
ahmed.mehmedovic@th-wildau.de

Technische
Hochschule
Wildau
Technical University
of Applied Sciences
WILDAU