Greenbone
Sustainable Resilience

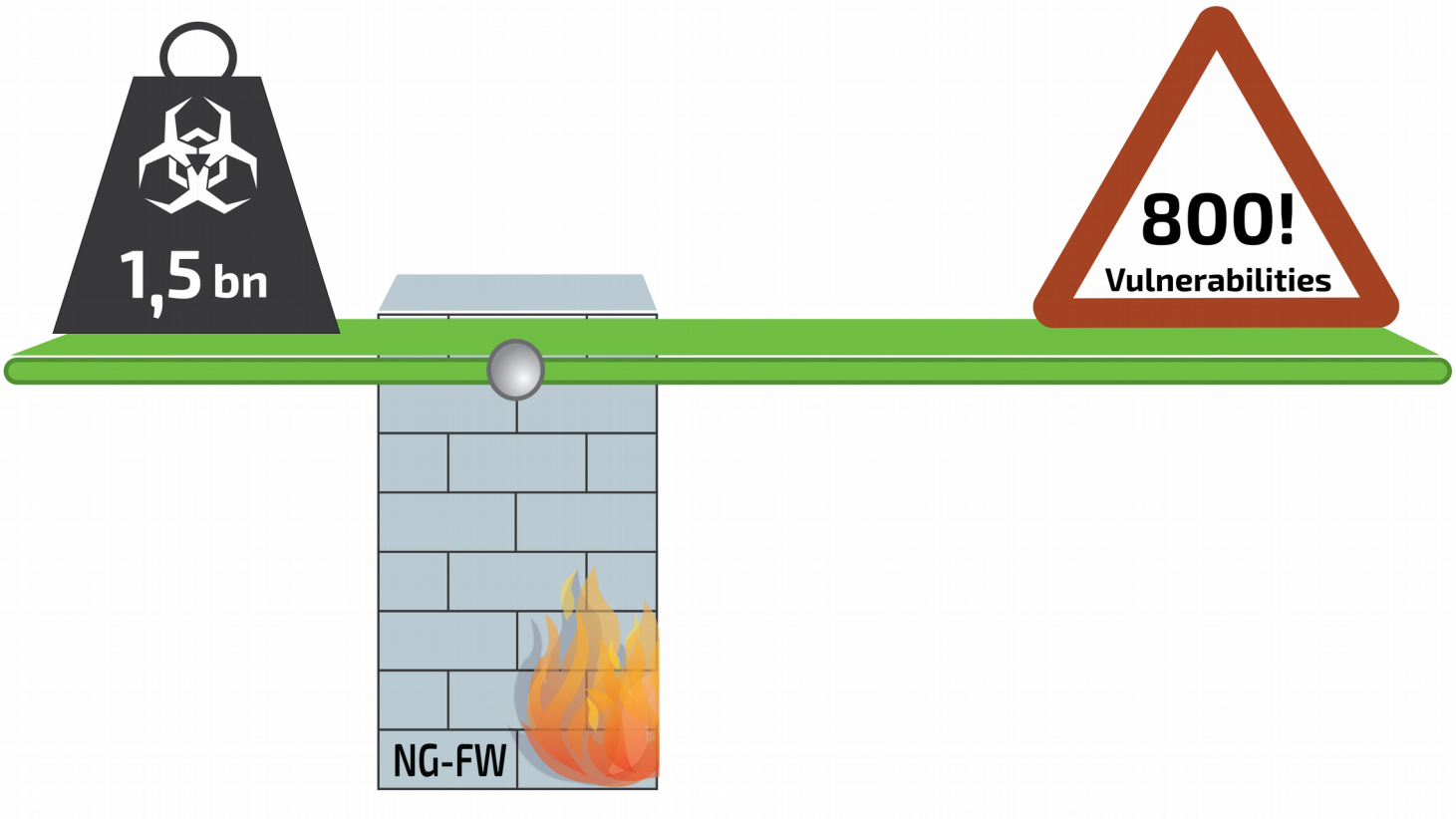
Schwachstellen-Management mit dem Greenbone Security Manager

Emanuel Moß

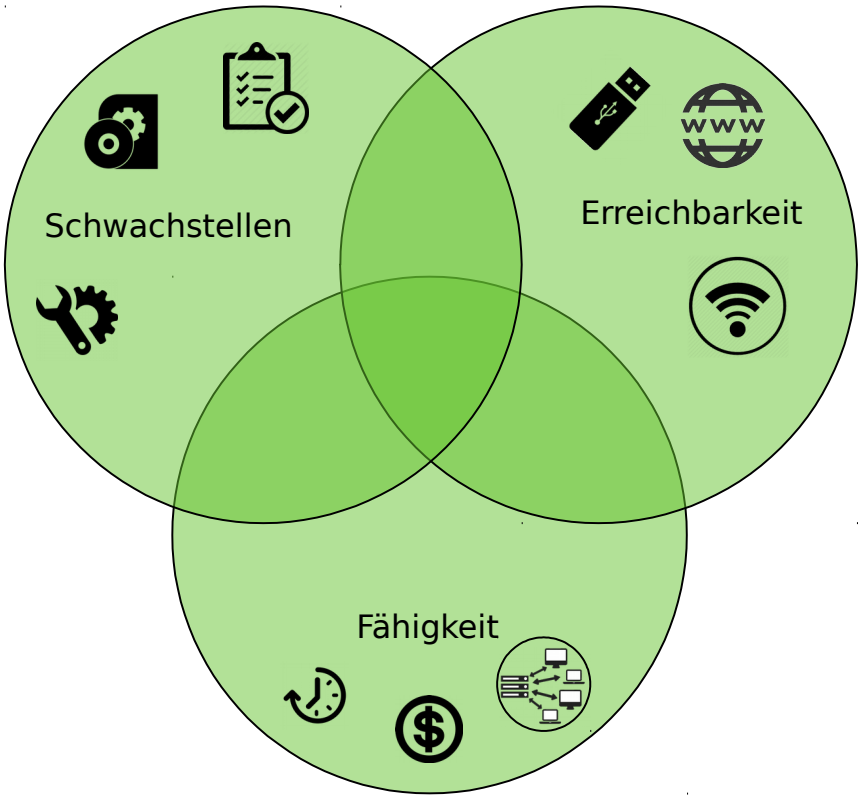
2019-02-28

Schwachstellen vs. Bedrohungen

Greenbone
Sustainable Resilience



Cyber Resilience

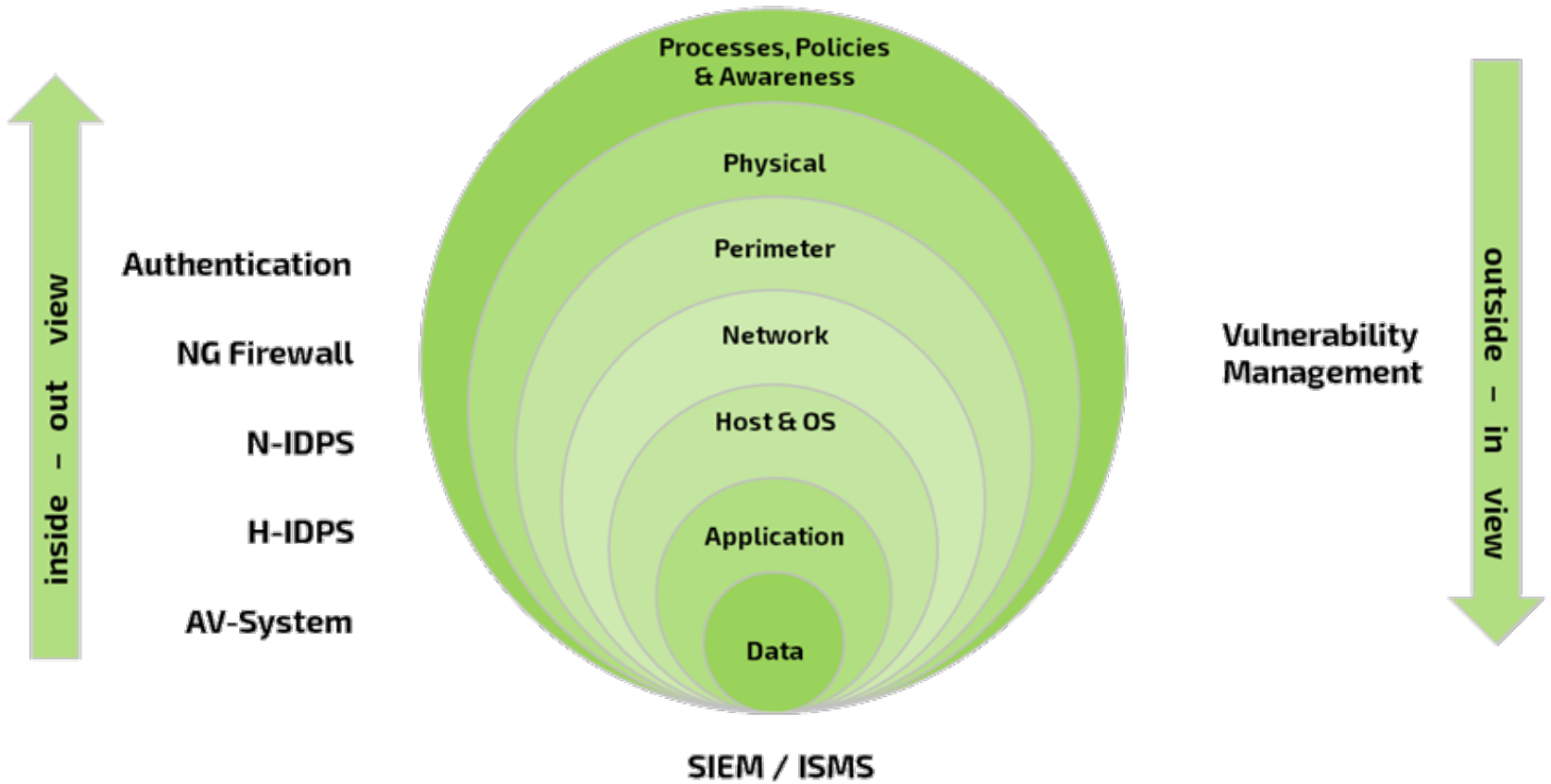


Mögliche Schwachstellen

- Software Fehler
- Basiskonfigurationen oder fehlerhafte Einstellungen
- Nicht-authorisierte oder unvermutete Installationen
- Abweichung oder Nicht-Einhalten von Richtlinien, Vorgaben oder Vorschriften

Die “veränderte” Perspektive

Greenbone
Sustainable Resilience



Penetration Testing vs. Schwachstellen-Management

Greenbone
Sustainable Resilience

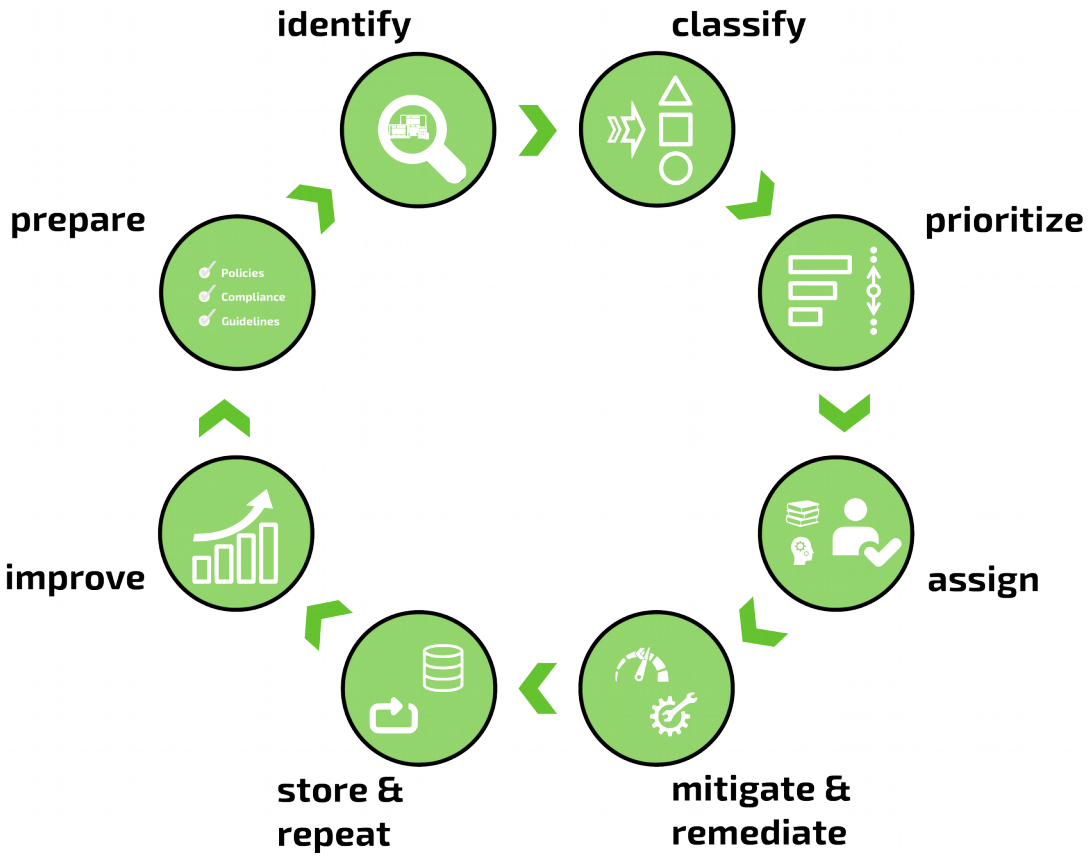
- **Penetration Testing** ist zielorientiert; sprich Übernahme der vollen Kontrolle über das Ziel, Verwischen von Spuren, Einbau von Hintertüren. Sobald das erreicht ist, sucht ein PenTester nicht weiter. Vulnerability Management schon.

- **Vulnerability Assessment** ist eine einmalige Bestandsaufnahme einer IT-Infrastruktur, der zum Zeitpunkt bestehenden ‘security posture’ (Stichwort Halbwertszeit); **Vulnerability Management** ist dagegen der vollständige, kontinuierliche Prozess diese ‘security posture’ zu erfassen, zu erhalten bzw. zu verbessern und zu überprüfen.

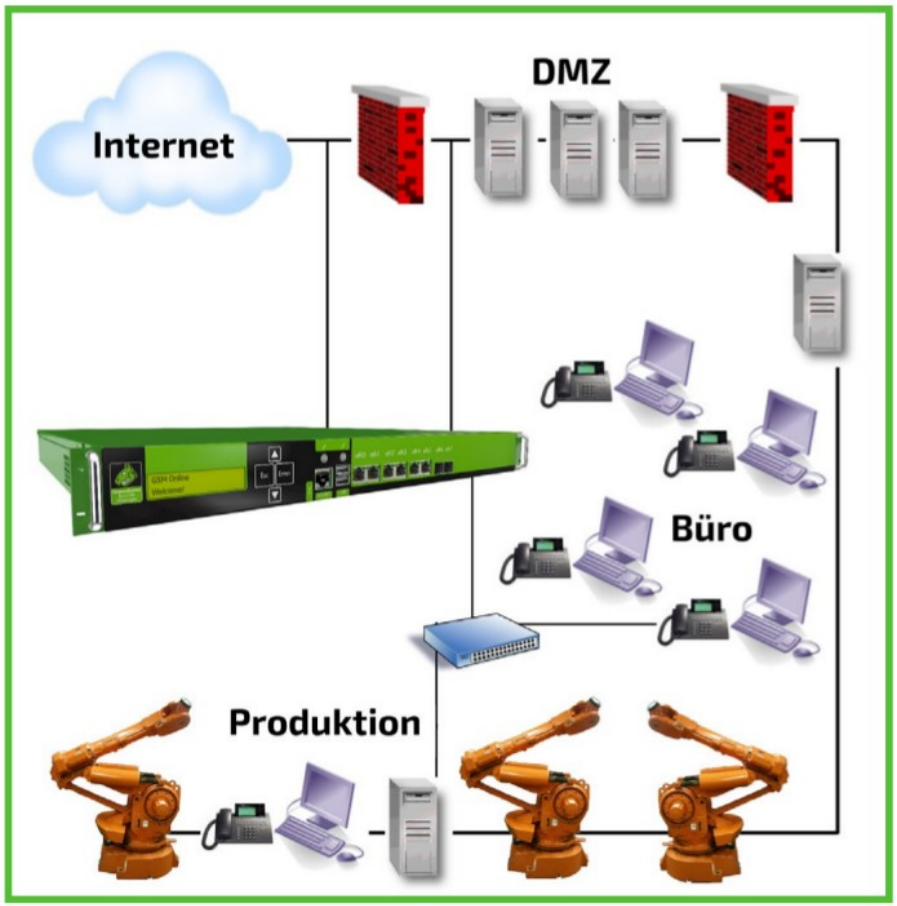
- **Patch Management** ist definitive ein wichtiger Baustein einer Informationssicherheits-Architektur!
  Allerdings, was ist zuerst da: die Schwachstelle oder der Patch? Wieviel Zeit vergeht zwischen der Verfügbarkeit und dem Einspielen eines Patches?

Schwachstellen-Management als Zyklus

Greenbone
Sustainable Resilience



Verschiedene Blickwinkel

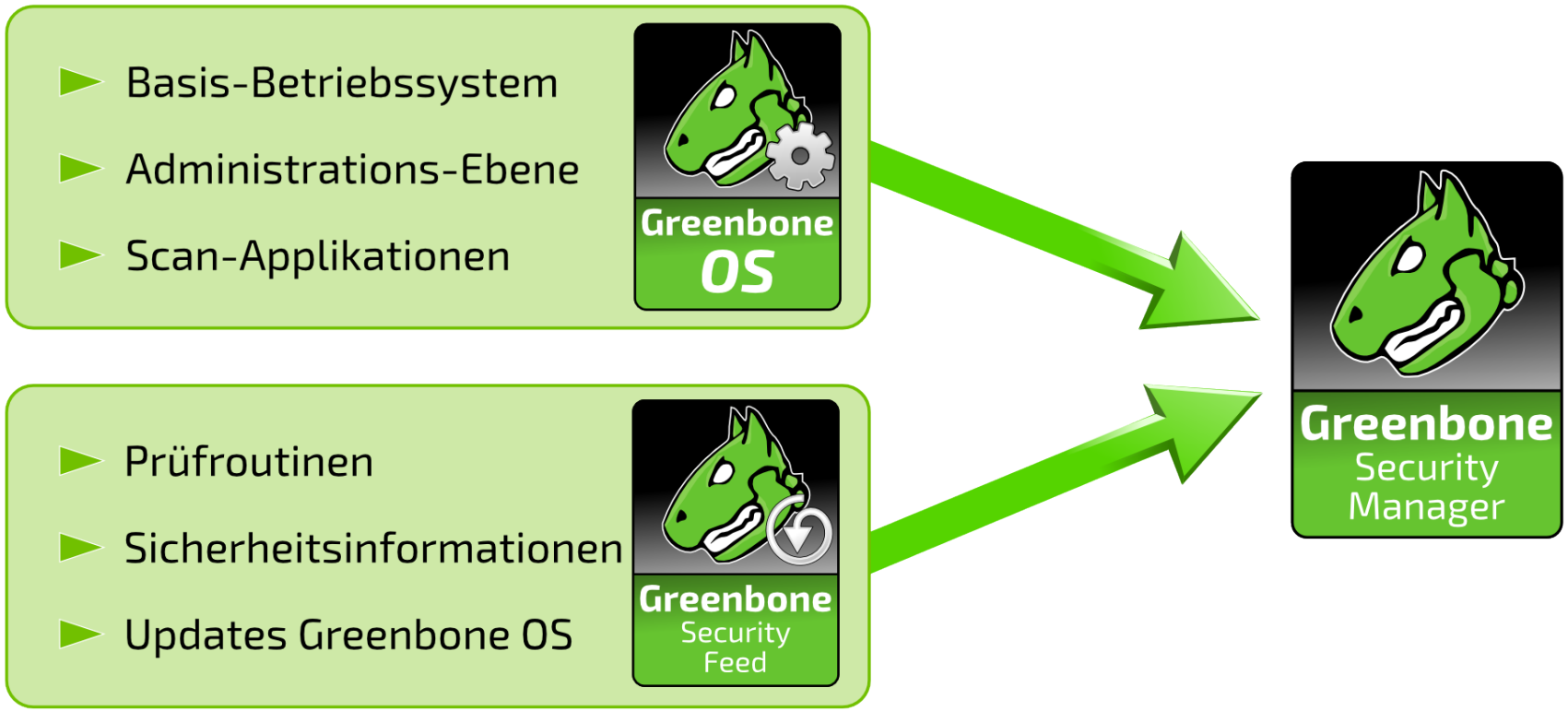


Extern:
- Blickwinkel des Angreifers von außen
- Erkennen schlecht konfigurierter Firewalls
- Aufdeckung von hoch sicherheitsrelevanten Fehlern

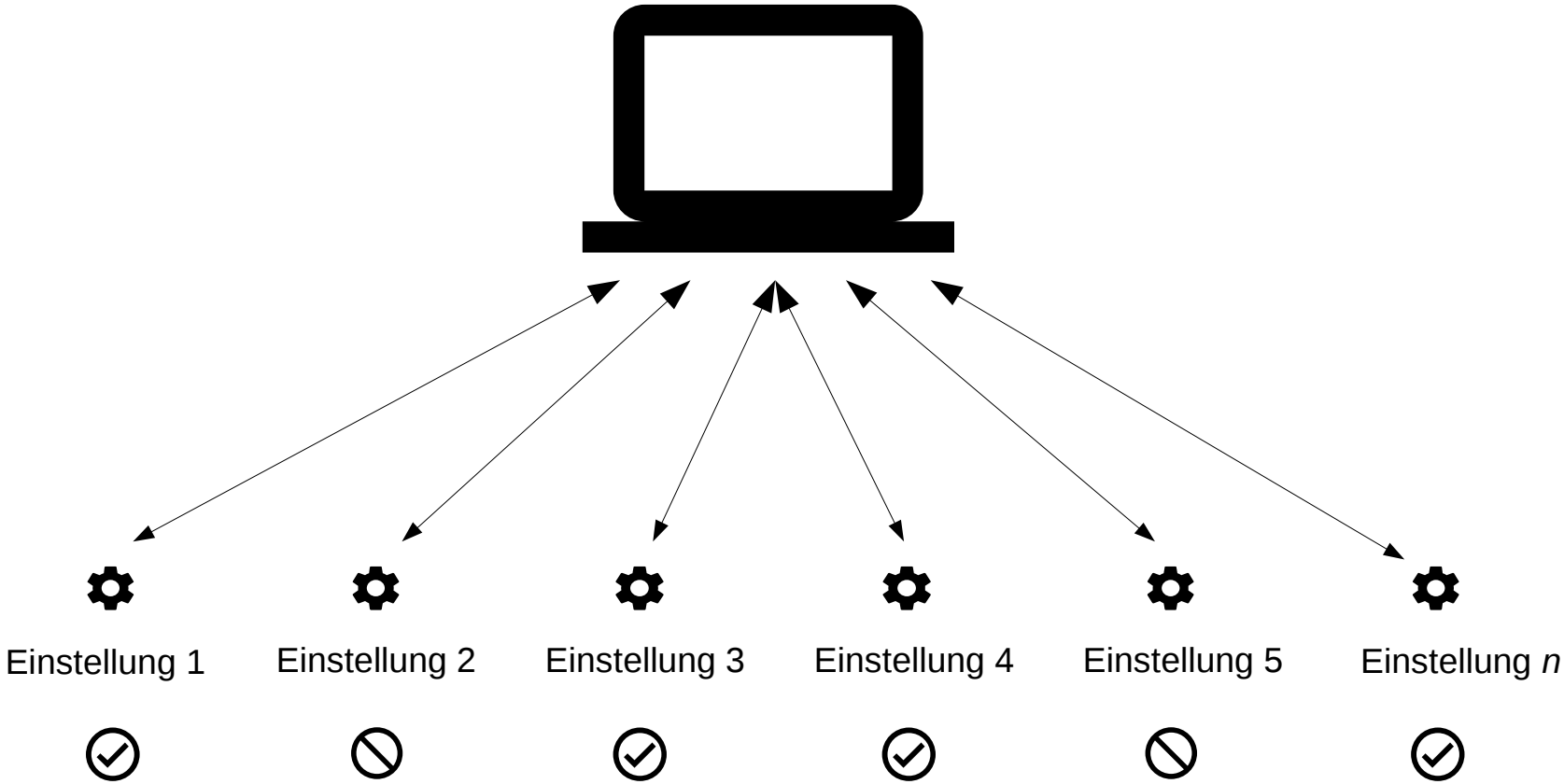
In der DMZ:
- Was wäre wenn ... die Firewall versagt
- Erkennen von Schwachstellen der Sicherheitszone

Im internen Netzwerk:
- Perspektive des internen Angreifers oder Computerwurms
- Schadensmöglichkeiten werden aufgedeckt und nach Risiko sortiert
- Vollständiger Detektionsumfang kann genutzt werden

Greenbone Komponenten



Prüfen einer Policy mit Greenbone



Mit einem authentifizierten Scan werden Einstellungen auf einem Host geprüft.

Greenbone
Sustainable Resilience

Vielen Dank für Ihre Aufmerksamkeit.

Fragen?