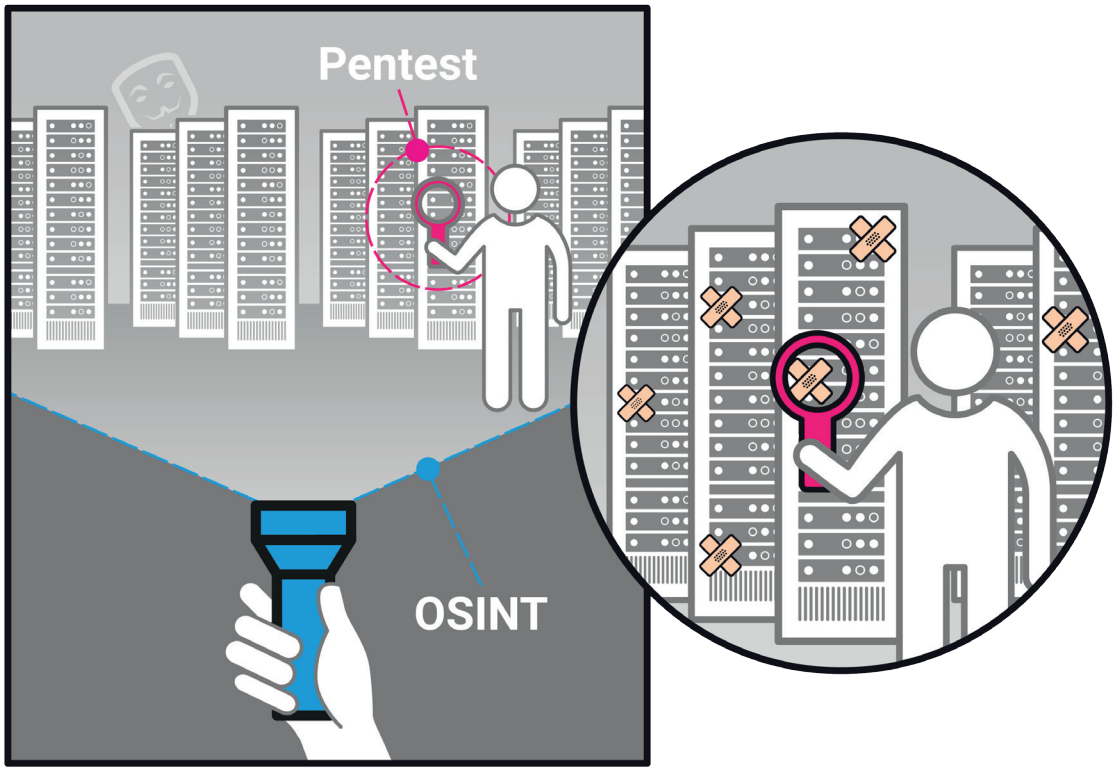
**WHITEPAPER**

Best Practice

# Asset-Discovery mit Luup

## und Abgrenzung zu Nessus / Metasploit

*[ "Der Verzicht auf unnötige Angriffsoberfläche ist die älteste Maßnahme in der IT Security" -- Felix von Leitner / fefe ]*



*Vor dem Hintergrund der sich rasant ausweitenden Ransomware / Data-Leak-Problematik sowie der gezielten Ausnutzung von Sicherheitslücken in Servern, Services und Appliances[1] sind Asset-Discovery, Asset-Management und Alarmierungsfunktionen bei kritischen Sicherheitslücken für Infrastrukturanbieter mittlerweile unverzichtbar, um eine anhaltende Sicherheit von Online-Systemen zu garantieren!*

**Durch die Erhöhung der Anzahl extern erreichbarer IT-Systeme wird folgerichtig die externe Angriffsoberfläche von Unternehmen vergrößert, womit deutlich mehr Einstiegspunkte für Hacker entstehen.**
Diese Feststellung ist ebenfalls daran ablesbar, dass sich der Fokus für Ransomware-Attacken oder Zero-Day-Exploits bis hin zu frischen Sicherheitslücken im ersten Halbjahr 2020 auf extern erreichbare Systemen verschoben hat, wie eine aktuelle Analyse zeigt[1].

**Gekaperte Systeme und sämtliche Zugänge zu Firmennetzen sind auf kriminellen SaaS-Plattformen heiß gehandelte Ware.**
Aktuell auftretende Angreifer sowie Erpesser sind inzwischen viel höher qualifiziert und gehen deutlich skrupelloser vor, was sich am zur Zeit "normalen" Modus-Operandi von Ransomware-Gangs darstellen lässt: entwendete Daten werden vor dem Verschlüsseln kopiert, um die Opfer mit deren Veröffentlichung  zu erpressen.

Ein weiterer, nicht unerwähnenswerter, Vorteil für die Angreifer ist sicherlich darin zu sehen, daß jede Ressource an administrativem Personal bzw. entsprechenden Dienstleistern endlich ist.

[1] *https://zero.bs/ransomware-vs-infrastruktur-de.html*

## WAS IST ALSO ZU TUN?

### Erkennen der eigenen, externen Angriffsfläche

Nur, wer jeden Tag überblicken kann, welchen Stand die eigene Angriffsfläche hat, kann pro-aktiv Maßnahmen einleiten!

### Agile Frühwarnungen zu relevanten Angriffsmöglichkeiten

Nur, wer jeden Tag gezielt Informationen zu bestehenden Angriffsmöglichkeiten erhält, kann im Vorfeld reagieren!

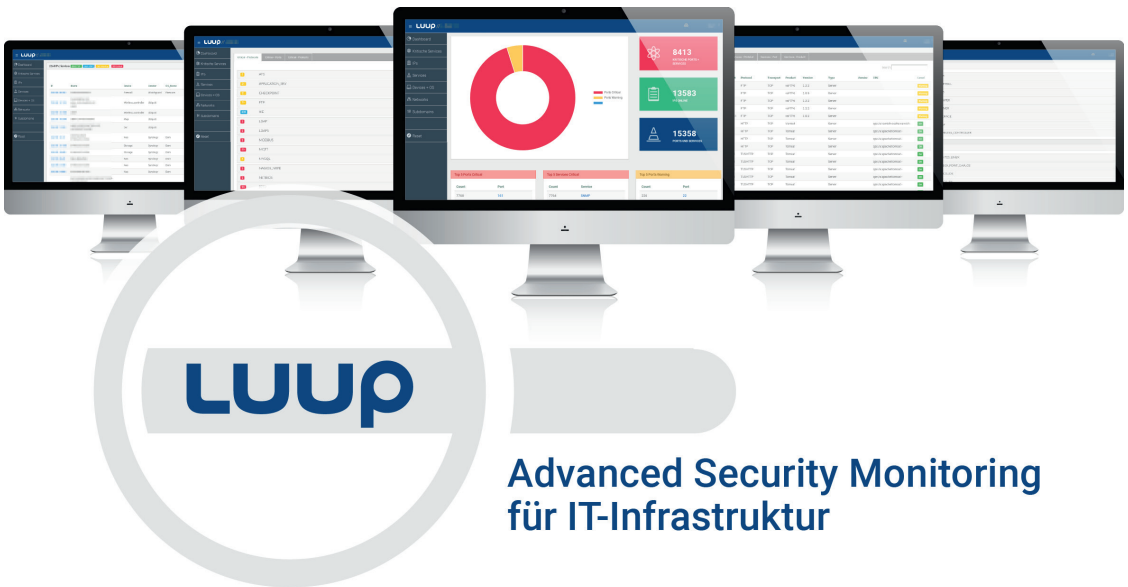
### Rechtzeitige Informationen zu nachhaltigen Abwehrmöglichkeiten

Nur, wer vor einem Angriff informiert wird, welche Abwehrmöglichkeiten möglich sind, kann sinnvoll und nachhaltig reagieren!

### In allen auf geführten Punkten hilft Luup Ihnen dabei, ...

- die Übersicht zu behalten,
- den IST-Zustand zu analysieren,
- Schwachpunkte zu erkennen und
- bei Sicherheitslücken Informationen zu erhalten.

**Dashboards, Bewertungen, Sichten, Suchmasken und Downloads aller Daten helfen, Action-Items sofort zu erkennen und abzuleiten.**




Advanced Security Monitoring
für IT-Infrastruktur

## LUUP VS. NESSUS

Luup beantwortet individuelle Fragen (Asset-Management), die von Tools mit anderem Fokus nur bedingt adressiert werden können, so z.B. EOL-Systeme, Analyse von Risiken oder eine gezielte Suche nach einzelnen Installationen.

**Der Vorteil von Luup:** es ist non-intrusive und kann damit jederzeit eingesetzt werden.

**Tabelle zum Überblick und Vergleich**

| | Luup | Nessus | Metasploit |
|---|---|---|---|
| **Fokus** | Erkennung von potentiellen Einbruchsmöglichkeiten | Vorbereitung eines Einbruchs | Durchführung eines Einbruchs |
| **Arbeitsweise** | Suche nach potentiellen Risiken | Suche nach konkreten Lücken | Ausnutzen potentieller Lücken |
| **Intrusive** | nein | ja | ja |
| **Sicht** | Eagle-Eye, von oben, ganzheitlich | fokussiert, auf Applikationen | fokussiert, auf Applikationen |
| **Monitoring** | ja | nein | nein |
| **Automationsgrad** | sehr hoch | mittel | niedrig |
| **Zeitpunkt** | aktuell und zukunftsorientiert | aktuell | aktuell |
| **Inventarisierung** | ja | bedingt | nein |
| **Alarmierung** | ja | nein | nein |