NIS2 · KRITIS · BSI IT-GRUNDSCHUTZ

Endpoint Security:
Von AV zu EDR und XDR

Warum signaturbasierter Virenschutz gegen moderne Angriffe nicht ausreicht, welche Technologien den öffentlichen Sektor heute schützen und wie Vergabestellen EPP, EDR und XDR vergaberechtskonform ausschreiben.

< 50 %
AV-Erkennungsrate bei Zero-Days

11
Anbieter im MITRE ER7 (2025)

100 %
Top-EDR Detection Visibility (ER7)

EPP / EDR / XDR
3 Technologieklassen im Vergleich

Warum klassisches AV nicht mehr schützt

Signaturbasierte Erkennung scheitert an drei Angriffstypen, die heute Standard sind.

ZERO-DAYS UND POLYMORPHE MALWARE

Angreifer generieren automatisch Malware-Varianten ohne bekannte Signatur. Zwischen Erkennung durch den Hersteller und Signaturverteilung vergehen Stunden bis Tage. In dieser Zeit ist AV blind.

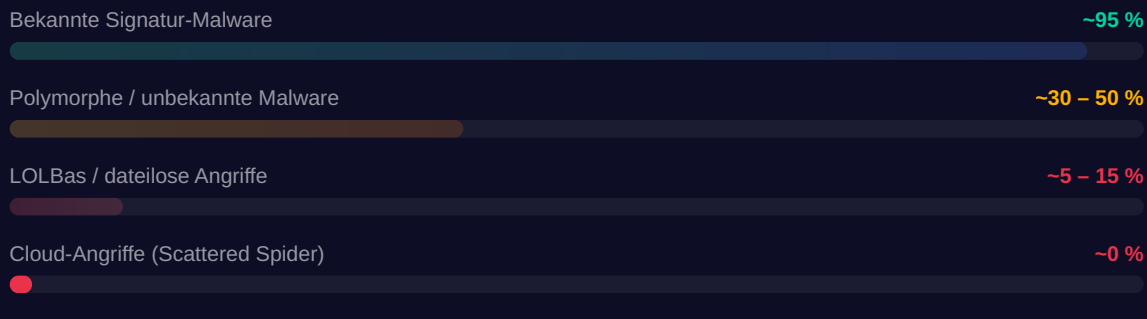
LIVING-OFF-THE-LAND (LOLBAS)

Angreifer wie Scattered Spider nutzen ausschliesslich legitime Windows-Tools: PowerShell, WMI, PsExec. Keine Malware, keine Datei, keine Signatur. AV sieht nur erlaubte Prozesse.

BSI IT-GRUNDSCHUTZ OPS.1.1.4

Das BSI fordert **"angemessenen Schutz vor Schadprogrammen"** inkl. verhaltensbasierter Erkennung und Reaktionsfähigkeit. Reiner Virenschutz erfüllt die Anforderung nicht mehr.

AV-ERKENNUNGSRATE NACH ANGRIFFSTECHNIK



Schätzwerte basierend auf ENISA Threat Landscape 2024 und MITRE ATT&CK Evaluations ER7

Praxiserfahrung: In Projekten, die wir begleiten, finden sich regelmässig AV-Installationen, die laufende Angriffe nicht erkannt hätten. Der Angreifer ist oft bereits seit Wochen im Netz.

Begriffe: EPP, EDR, XDR, MDR

Vier Klassen, die im Beschaffungsmarkt oft verwechselt werden. Im LV muss klar sein, was gefordert wird.

EPP

Endpoint Protection Platform

- Prävention im Vordergrund
- Signaturbasiert + NGAV
- Firewall, Web-Filter, Device Control
- Kein forensisches Toolset
- Kein Threat Hunting

Infektion verhindern

EDR

Endpoint Detection & Response

- Verhaltensanalyse + Telemetrie
- Forensik und Timeline-Analyse
- Threat Hunting
- Isolierung befallener Systeme
- MITRE ATT&CK-Mapping

Angriff erkennen und eindämmen

XDR

Extended Detection & Response

- Cross-Source-Korrelation
- Endpoint + Cloud + Netz + Identity
- Automatisierte SOAR-Integration
- OT/IoT-Sichtbarkeit (optional)
- Hersteller-nativ oder offen

Alle Vektoren sehen

MDR

Managed Detection & Response

- Kein Produkt: Betreibermodell
- 24/7 SOC als externer Dienst
- Threat Hunting durch Analysten
- Hersteller-nativ vs. neutral
- Incident Response inklusive

Betrieb ohne eigenes SOC

Praxiserfahrung: Begriffskonfusion ist das häufigste Problem bei EP-Ausschreibungen. Wer im LV nur "EDR" schreibt, ohne Scope, SLA und Betreibermodell zu definieren, bekommt unvergleichbare Angebote.

Technologiegenerationen im Überblick

Vier Entwicklungsstufen in 35 Jahren. Jede Generation schliesst blinde Flecken der Vorgänger.

1990er

Klassisches AV

Signaturdatenbank, dateibasiert. Erkennt bekannte Malware per Hash. Blind für Zero-Days, LOLBas und polymorphe Varianten.

2010er

NGAV / EPP

Machine-Learning-Erkennung, Verhaltenssignaturen, Exploit-Schutz. Kein forensisches Toolset, keine aktive Reaktionsfähigkeit.

ab 2013

EDR

Prozesstelemetrie, forensische Timeline, Threat Hunting, aktive Isolierung. Erkennt Lateral Movement und LOLBas. Heute Mindeststandard für KRITIS.

ab 2019

XDR

Korrelation über Endpoint, Cloud, Netzwerk und Identity. Erkennt cloud-basierte Angriffspfade. Hersteller-nativ oder offen (SIEM-Integration).

FÄHIGKEITSVERGLEICH

FÄHIGKEIT	AV	EPP	EDR	XDR
Signaturerkennung	✓	✓	✓	✓
Verhaltensanalyse	–	Teilw.	✓	✓
Forensik / Timeline	–	–	✓	✓
Threat Hunting	–	–	✓	✓
Cloud-Korrelation	–	–	–	✓
OT/IoT-Sichtbarkeit	–	–	Teilw.	Teilw.

MITRE ATT&CK als Bewertungsmassstab

Enterprise 2025 (ER7): Scattered Spider & Mustang Panda · 11 Anbieter · Dezember 2025

MITRE-TECHNIK	ID	AV	EDR
Credential Dumping (LSASS)	T1003	Gering	Hoch
Lateral Movement via SMB	T1021	Gering	Hoch
PowerShell LOLBas	T1059	Sehr gering	Hoch
Process Injection	T1055	Gering	Hoch
Exfiltration via Cloud	T1567	Keine	Mittel (XDR besser)

Quelle: MITRE ATT&CK Evaluations Enterprise 2025 (ER7), evals.mitre.org/enterprise/er7

ER7 SPITZENGRUPPE

CrowdStrike und Cynet: **100 % Detection Visibility** und 100 % Protection ohne False Positives. Erstmals testet MITRE auch Cloud-basierte Angriffsvektoren.

LV-FORMULIERUNG: MESSBAR DEFINIEREN

Statt "EDR liefern": **"Lösung muss in der jeweils aktuellen MITRE ATT&CK Evaluation mindestens 90 % Detection Visibility ohne False Positives erreicht haben."**

VERGABERECHTLICHER HINWEIS

Gartner-Leaders-Status und MITRE-Rangfolge dürfen nicht als Ausschlusskriterium verwendet werden. Nur Mindest-Performance-Werte sind vergaberechtlich zulässig.

Pflichtpositionen im Leistungsverzeichnis

01

Erkennungsleistung

- MTTD (Mean Time to Detect): max. X Minuten
- MITRE ATT&CK Coverage: mind. 90 %
- False-Positive-Rate: max. X Alerts/Tag
- Erkennungsmethode: verhaltensbasiert

02

Deployment-Architektur

- Agent/Agentless-Unterstützung
- Cloud/On-Premises/Hybrid
- OS-Coverage: Windows, Linux, macOS
- Datenhaltung und Souveränität

03

Scope

- Managed/Unmanaged Devices
- OT/IoT-Systeme (SCADA, Medizin)
- Mobile Endpoints
- Cloud-Workloads und VMs

04

Service Level

- 24/7-Betrieb und Alarmbearbeitung
- MTTR: max. X Minuten bis Eindämmung
- Eskalationspfade und Meldewege
- Incident-Response-Playbooks

05

Datensouveränität

- BSI C5 Testat oder gleichwertig
- Verarbeitung in Deutschland/EU
- Auftragsverarbeitungsvertrag (AVV)
- Exit-Klausel und Datenportabilität

Praxiserfahrung: Wer nur "EDR-Lösung" ausschreibt, bekommt Angebote, die sich in Scope, SLA und Datensouveränität um Faktor 3 bis 5 unterscheiden und nicht vergleichbar sind.

Typische Fehler bei EP-Ausschreibungen

Fünf Schwachstellen, die wir in der Angebotsprüfung immer wieder antreffen.

01 Produktname statt Leistungsanforderung

Das LV nennt konkrete Produkte ("CrowdStrike Falcon"), was nach GWB §97 Abs. 4 wettbewerbsbeschränkend ist. Stattdessen: messbare Mindestanforderungen formulieren.

02 Scope nicht vollständig definiert

Unmanaged Devices, OT/IoT-Systeme und Cloud-Workloads fehlen. Günstigster Bieter liefert nur PC-Schutz, Medizingeräte bleiben blind.

03 Kein MTTD/MTTR-SLA vereinbart

Ohne messbare Erkennungs- und Reaktionszeiten im Vertrag fehlt die Grundlage für Vertragsstrafen. Nachverhandlung nach Zuschlag ist kaum möglich.

04 Datensouveränität nicht gefordert

Kein BSI C5-Testat, keine Deutschlandklausel im LV. Telemetriedaten fliessen in US-Cloud. Nach Vertragsschluss ohne Kündigung nicht mehr korrigierbar.

05 Betreibermodell nicht spezifiziert

"EDR" ohne MDR-Anforderung bedeutet: kein 24/7, kein Threat Hunting, kein Incident Response. Öffentliche AG unterschätzen den eigenen Betriebsaufwand erheblich.

NÄCHSTER SCHRITT

EP-Security-Ausschreibung professionell vorbereiten

Vergaberechtskonforme Leistungsverzeichnisse, reale Ausschreibungsunterlagen und projektbegleitende Beratung für öffentliche Auftraggeber und KRITIS-Betreiber.

MUSTER-LVS

/produkte/muster-leistungsverzeichnisse

EDR, XDR, MDR, SzA: direkt einsetzbar

VERGABE-ARCHIV

/produkte/vergabe-archiv

Reale EP-Security-Ausschreibungsunterlagen

BERATUNG ANFRAGEN

/leistungen/ausschreibungsmanagement-oeffentliche-it-vergabe

IT-Ausschreibungsmanagement

Ihr Ansprechpartner
info@it-leistungsverzeichnisse.de · 06124 6059217