5 TIPPS VON SOPHOS FÜR PRÄVENTIVE CYBERSECURITY

Jeder Cyberangriff kostet Zeit, Budget und Vertrauen – ist belastend für kleine Teams und bringt selbst die ausgereiftesten Security Operations an ihre Grenzen. Präventive Cybersecurity erkennt Bedrohungen frühzeitig, minimiert Störungen und ermöglicht Teams, sich auf das Wesentliche zu konzentrieren.

Hier finden Sie fünf Tipps, wie Sie präventive Cybersecurity mit Sophos-Lösungen umsetzen können – egal, wie groß Ihr Unternehmen und Ihr internes Team sind.

1. Ransomware frühzeitig stoppen

Ransomware wird immer raffinierter – vom schnellen Datendiebstahl zur verdeckten Remote-Verschlüsselung.

- **Sophos Endpoint** blockiert Bedrohungen, bevor sie Ihre Systeme beeinträchtigen – mithilfe von Deep-Learning-KI, Anti-Exploit-Funktionen und verhaltensbasierter Erkennung.
  - Ergänzen Sie **Sophos Endpoint Detection and Response (EDR)**, um detaillierte Einblicke in verdächtige Aktivitäten auf Computern und Servern zu erhalten, oder upgraden Sie auf **Sophos XDR** zum Schutz vor mehrstufigen Multi-Vektor-Angriffen.

2. Netzwerkbedrohungen unschädlich machen

Angreifer nutzen häufig gestohlene Zugangsdaten aus, um sich lateral fortzubewegen – insbesondere in hybriden Umgebungen.

- Die **Sophos Firewall** mit integriertem **ZTNA** und **NDR** kann beim Zugriff auf alle Anwendungen und Systeme MFA erzwingen, um Angriffe durch den Diebstahl von Zugangsdaten zu verhindern. Außerdem kann sie aktive Angreifer im Netzwerk erkennen und kompromittierte Systeme automatisch isolieren, um laterale Bewegungen zu verhindern.
- **Sophos Network Detection and Response (NDR)** bietet zusätzlich Deep Traffic Inspection, um verborgene Bewegungen tief im Netzwerk zu erkennen.

3. Phishing und BEC blockieren, bevor Sie in den Posteingang gelangen

Phishing und Business Email Compromise (BEC) sind bei über 90 % aller Cyberangriffe die Ursache – und der Eintrittspunkt bei **37 %** aller Ransomware-Angriffe.

- **Sophos Email** stoppt Bedrohungen proaktiv, bevor sie die Benutzer erreichen – dank KI-gestützter Erkennung. Die Lösung optimiert nahtlos Microsoft 365 und Google Workspace und integriert sich gleichzeitig in das gesamte Sophos-Ökosystem.

der erfolgreichen Cyberangriffe werden durch Phishing und BEC ausgelöst

der Vorfälle werden durch den Diebstahl legitimer Zugangsdaten verursacht

4. Identitätsmissbrauch sofort stoppen

Der Diebstahl legitimer Zugangsdaten ist mittlerweile der häufigste Eintrittspunkt für Angreifer – in **56 %** der Fälle.

- **Sophos Identity Threat Detection and Response (ITDR)** erkennt den Missbrauch von Zugangsdaten in Echtzeit, zeigt Schwächen bei der Identitätssicherheit und ermöglicht eine schnelle Reaktion auf Identitätsbedrohungen.

5. Sicherheitslücken finden und beheben, bevor Angreifer sie ausnutzen

65 % der Ransomware-Opfer geben an, dass eine bekannte oder unbekannte Sicherheitslücke zur Kompromittierung geführt hat.

- Die **Sophos Advisory Services** helfen Ihnen, diese Lücken aufzudecken und zu schließen, mit:
  - Internen und externen Penetrationstests
  - Penetrationstests für drahtlose Netzwerke
  - Web Application Security Assessments
- **Sophos Managed Risk** powered by **Tenable** deckt kritische Schwachstellen in Hardware und Software auf, bevor Angreifer sie ausnutzen können.

der Ransomware-Opfer geben an, dass eine bekannte oder unbekannte Sicherheitslücke zur Kompromittierung geführt hat.

Stoppen Sie Angriffe, bevor sie sich ausbreiten. Fangen Sie Bedrohungen ab, die andere übersehen. Schließen Sie Sicherheitslücken, bevor Angreifer sie ausnutzen – mit intelligenterer Technologie und Experten, die ständig wachsam sind.

Erfahren Sie mehr über präventive Cybersecurity unter **sophos.de/prevention**.

SOPHOS