Executive Summary

Kaspersky-Studie: Unternehmen in Deutschland verhindern Cyberangriffe durch Threat Intelligence / Data Feeds

Methodologie: Die Umfrage wurde von Censuswide im Auftrag von Kaspersky im November 2024 durchgeführt. Es wurden 500 IT-Entscheidungsträger in Deutschland zum Thema Threat Intelligence und Data Feeds befragt.

kaspersky

Top-Erkenntnisse für Deutschland

1. **66 %** der Unternehmen haben dank Threat Intelligence (TI) / Data Feeds bereits einen Cyberangriff verhindert.
2. **Drei Viertel (71 %)** der IT-Entscheider sind der Meinung, TI / Data Feeds sollten Teil jeder grundlegenden Sicherheitslösung sein.
3. **Ein Fünftel (21 %)** der Unternehmen plant TI / Data Feeds in 2025 einzuführen.
4. **Fast die Hälfte (42 %)** der Befragten verlassen sich für TI / Data Feeds auf private (bezahlte) Dienstleister. **51 % nutzen** eine Kombination aus verschiedenen Diensten und Anbietern.
5. Die meist eingesetzten TI / Data Feeds sind **IP Reputation (55 %)**, **URL Feeds (54 %)** und **APT & Crimeware Feeds (45 %).**

„Unternehmen setzen auf eine Multi-Vendor-Strategie bei Threat Intelligence, um ein umfassenderes Bild von Bedrohungen zu erhalten. So können sie ihre Infrastruktur kostengünstiger mit Threat Data Feeds verschiedener Provider anreichern und damit ihre Cybersicherheit flexibler und robuster gegen neue und sich entwickelnde Angriffe gestalten."

– Jan Oberbanscheid,
Prokurist bei Jo-Soft IT-Security GmbH

TI und Integration von TI in Data Feeds

1. **Mehrheit setzt auf TI / Data Feeds zum Schutz vor Angriffen:** 75 % der Unternehmen integrieren Threat Intelligence beziehungsweise Data Feeds in ihre IT-Security-Strategie. Zwei Drittel (66 %) konnten mithilfe von TI / Data Feeds sogar bereits Angriffe verhindern.

„Mit TI-Data-Feeds können Unternehmen Schwachstellen beziehungsweise Bedrohungen proaktiv und frühzeitig erkennen, und so das Risiko von Datenverlusten oder Betriebsunterbrechungen verringern. TI-Data-Feeds sollten daher bei allen Unternehmen zum Einsatz kommen."

– Frank Jonas
Head of Enterprise Sales DACH bei Kaspersky

2. **Mehrheit erkennt den Nutzen von TI / Data Feeds, allerdings erscheint sie vielen zu teuer:** 79 % der Unternehmen sind davon überzeugt, dass Threat Intelligence beziehungsweise Data Feeds effektiv beim Schutz vor Angriffen unterstützen. Dennoch betrachten 47 % der Entscheider die Kosten für TI / Data Feeds als zu hoch.

3. **Hürden für den Einsatz von TI / Data Feeds:** 11 % der Unternehmen, die derzeit TI / Data Feeds nutzen, wollen diese wieder abschaffen, da sie ihrer Meinung nach nicht effektiv ist. Unternehmen, die noch keine TI / Data Feeds nutzen, begründen dies am häufigsten mit zu hohen Kosten oder fehlendem Budget (40 %), dem hierfür benötigten Fachwissen (28 %) oder schlicht fehlender Zeit für die Implementierung (25 %).
4. **TI / Data Feeds werden vielfältig in die IT-Infrastruktur integriert:**
   - Mit 77 % stehen Cloud-Server an erster Stelle, danach Firewalls mit 57 %.
   - 53 % der Unternehmen nutzen Proxy-Server für TI / Data Feeds, während 52 % E-Mail-Server einbinden.
   - Endpoints werden von 34 % berücksichtigt, Intrusion Prevention Systeme (IPS) von 29 % und Security Information and Event Management (SIEM) von 15 %.
5. **Unterschiedliche TI / Data Feeds im Einsatz:** Unternehmen setzen bei TI / Data Feeds vor allem auf IP-Reputation (55 %) und URL-Feeds (54 %). APT- und Crimeware-Feeds werden von 45 % eingesetzt, während 33 % Hashes verwenden. Suricata-Regeln kommen bei 28 % zum Einsatz und YARA-Regeln bei 24 %.

„Threat Intelligence und Data Feeds können auch von kleinen und mittleren Unternehmen einfach in eine Firewall integriert werden. So werden viele Cyberbedrohungen schon direkt an der Peripherie automatisch abgefangen und unwirksam gemacht. Es kommt damit weniger auf die Endpunkte zu und das allgemeine Schutzlevel eines Unternehmens ist sofort um ein Vielfaches höher."

– Sören Kohls
Head of Channel DACH bei Kaspersky

Weitere Ergebnisse

1. **Mehrheit der Unternehmen in Deutschland von Sicherheitsvorfällen betroffen:** In den vergangenen 12 Monaten verzeichneten 69 % einen Sicherheitsvorfall. Angesichts der eingesetzten Sicherheitsmaßnahmen überrascht dies in einigen Fällen kaum: So setzen 30 % der befragten Unternehmen auf private Verbraucher-Lösungen und 14 % auf kostenlose Anwendungen.
2. **Schutz des Perimeters ist eine Mammutaufgabe:** Für 49 % der Befragten stellen Budget und Kosten eine zentrale Hürde beim Schutz dar. 39 % empfinden die Komplexität der Sicherheitsmaßnahmen als problematisch. Bei 36 % mangelt es an internen Ressourcen und 33 % nutzen zu viele unterschiedliche Tools, was die Effizienz und Übersichtlichkeit beeinträchtigt.
3. **Unternehmen setzen auf mehrschichtigen Schutzansatz:** Weiterhin führen 54 % Security Audits durch, 52 % identifizieren und schließen Schwachstellen und implementieren Firewalls. 48 % nutzen spezialisierte Sicherheitslösungen wie EDR, MDR oder XDR, während 44 % auf zusätzliche technische Lösungen wie Anti-Spam-Software zurückgreifen.
4. **Wunschliste der IT-Sicherheitsentscheider, wenn Geld und Zeit keine Rollen spielen würden:** 81 % würden Threat Intelligence beziehungsweise Data Feeds implementieren, 79 % ihre administrativen Tools in einer Plattform konsolidieren. Ein Security Operations Center (SOC) würden 75 % einrichten, 76 % auf Managed Services setzen. 70 % wünschen sich regelmäßige Strategie-Meetings, und 53 % würden auf ein Zero-Trust-Modell umstellen.

Kaspersky-Empfehlungen zum Schutz vor Cyberangriffen

- Das SOC-Team sollte Zugang zu **aktueller TI und Data Feeds** haben. Über das **Kaspersky Threat Intelligence Portal** können SOC-Teams auf die TI / Data Feeds des Unternehmens zugreifen und erhalten Zugang zu Cyberangriffsdaten und Erkenntnissen, die Kaspersky in über 25 Jahren gesammelt hat.
- Managed-Security-Services wie **Kaspersky Managed Detection and Response** und **Kaspersky Incident Response** helfen dabei, auf zusätzliche externe Expertise zurückzugreifen, um sich vor Cyberangriffen zu schützen, ohne weiteres Personal einstellen zu müssen.
- Maßgeschneiderte, anpassungsfähige und robuste Cloud-native Cybersicherheitslösungen wie **Kaspersky Next** entlasten IT-Sicherheitsteams und ermöglichen die Reduzierung der mittleren Zeit bis zur Bedrohungserkennung (MTTD – Mean Time To Detect) sowie eine schnelle automatisierte Vorfallreaktion.
- Da viele zielgerichtete Angriffe durch Phishing oder andere Social-Engineering-Techniken beginnen, sollten Unternehmen ihren Mitarbeitern praktische Schulungen zum Sicherheitsbewusstsein, beispielsweise über die **Kaspersky Automated Security Awareness Platform**, anbieten.

Warum Threat Intelligence und Data Feeds von Kaspersky?

Kaspersky Threat Intelligence und Threat Data Feeds unterstützen Unternehmen schon an der Peripherie dabei, alle Arten von Cyberbedrohungen aufzudecken und unwirksam zu machen. Branchenführende, internationale Cybersicherheitsexperten bieten Handlungsempfehlungen und Erkenntnisse zu spezifischen Bedrohungen, sodass es keiner zusätzlichen Spezialisten bedarf. Der leistungsstarke Service der Threat Data Feeds ermöglicht eine Reduzierung der Komplexität und einen Fokus auf die wirklich relevanten aktuellen Bedrohungen; die Daten können direkt von diversen Systemen automatisch angewendet werden. Kunden können auf Informationen aus zahlreichen Datenbanken zugreifen, darunter APT-, Crimeware-, ICS- und Digital Footprint Intelligence-Berichte, Profile von Bedrohungsakteuren sowie Quellen aus dem Dark Web, Surface Web und validierte OSINT IoCs.

Kontakt für weitere Informationen und Terminvereinbarungen:
Frank Jonas, Head of Enterprise Sales DACH: 0170 78 46 808, frank.jonas@kaspersky.com
Sören Kohls, Head of Channel DACH: 0160 58 944 16, soeren.kohls@kaspersky.com

Cyber Threats News: https://securelist.com/
IT-Sicherheitsnachrichten: kaspersky.de/blog/b2b/
IT-Sicherheit für KMU: kaspersky.de/business
IT-Sicherheit für Großunternehmen: kaspersky.de/enterprise

kaspersky

kaspersky.de