Industrie: Finanzen und Bankwesen

Bekämpfung fortgeschrittener Cyber-Bedrohungen

Da die Finanzinstitute ihre Geschäfte weiter digitalisieren, müssen sie ihre IT-Sicherheit stärken, um die wachsende Zahl von Cyberangriffen zu bekämpfen, die erhebliche finanzielle und betriebliche Risiken darstellen, insbesondere angesichts ihrer systemischen Bedeutung für die Gesellschaft.

Die Unternehmen sehen sich mit Cyber-Bedrohungen durch nationalstaatliche und spezialisierten kriminellen Gruppen wie LockBit konfrontiert, QakBot, Grandoreiro und Emotet, die ausgefeilte Techniken für Ransomware-Angriffe und Advanced Persistent Threats (APT) einsetzen.

Laut IBM/Ponemon Institute betrugen die durchschnittlichen Kosten dieser Datenschutzverletzung im Jahr 2023 bei ca. 4,45 Millionen Dollar, in der Finanzindustrie sogar bei durchschnittlich 5,90 Millionen Dollar.

Im Jahr 2023 verloren Unternehmen in Deutschland insgesamt 205,9 Milliarden Euro durch Cyberkriminalität (Statista).

Kann es sich Ihr Unternehmen leisten, solche Verluste zu riskieren?

- Wachsende Angriffsflächen durch neue Technologien.
- Zunehmende Komplexität der Cybersicherheit in Multi-Cloud-Umgebungen.
- Schutz der sensibelsten Daten, die über Air-Gapped-Netzwerke gespeichert werden.
- Ressourcenintensive und obligatorische Anforderungen aufgrund von Compliance wie DORA.
- Bereit sein und bleiben, um digitale Vermögenswerte und Geldbörsen vor Verstößen zu schützen.
- Wachsende Sicherheitsherausforderungen bewältigen und von den Chancen der KI profitieren.

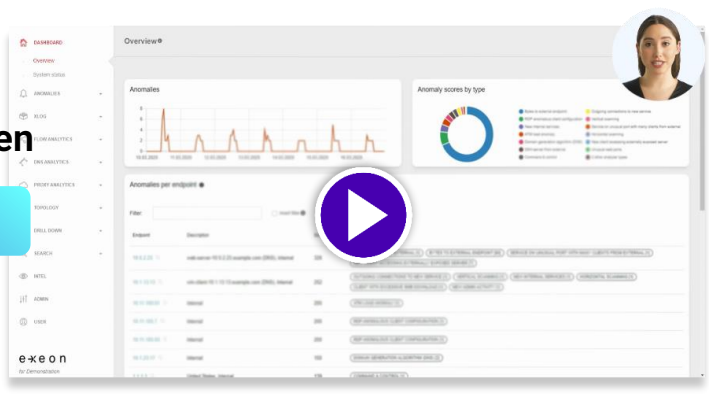
4-6 Mio. EUR Durchschn. Kosten für Datenverletzungen, 2023

Die 7 grössten Bedrohungen, auf die Sie achten sollten:

1. **Ransomware:** Verschlüsselt Daten und erpresst Lösegeld, stört den Geschäftsbetrieb und die Compliance mit erheblichen finanziellen und rufschädigenden Folgen.
2. **Social-Engineering-Angriffe:** Phishing verleitet Mitarbeitende dazu, vertrauliche Informationen preiszugeben, was zu kompromittierten Konten und Datendiebstahl führt.
3. **Exploits und Zero-Day-Angriffe:** Ausnutzung unbekannter Sicherheitslücken, um Sicherheitsmassnahmen in der Lieferkette zu umgehen, was zu schwerwiegenden Verstössen und finanziellen Verlusten führt.
4. **Banking-Trojaner:** Stehlen vertrauliche Informationen aus Online-Banking-Systemen, wobei Techniken wie Form-Grabbing und Code Injection genutzt werden.
5. **DDoS-Angriffe:** Durch Überlastung von Netzwerkressourcen werden Finanzdienstleistungen unterbrochen, was zu erheblichen Ausfallzeiten und finanziellen Verlusten führt.
6. **APTs:** Teilweise staatlich geförderte Unternehmen betreiben anhaltende Spionage und zielen auf Finanzunternehmen ab, um an sensible Daten zu gelangen.
7. **OT:** Angreifer manipulieren z. B. Geldautomaten, indem sie Malware einsetzen, um das Netzwerk zu infizieren und zu manipulieren.

ATM-Maschinen weltweit überwachen

Demo-Video ansehen



exeon
Smart Cyber Security.

Schnelle Erkennung, Schadensbegrenzung und Ursachenanalyse sind entscheidend für die Eindämmung unvermeidlicher Cyberangriffe. Die Trends betonen die Erkennung, Reaktion und Einhaltung von Vorschriften wie DORA. Zu den wichtigsten Schritten gehören kontinuierliche Überwachung, robuste Reaktionspläne und die obligatorische Berichterstattung zur Stärkung der IT-Sicherheit und der betrieblichen Widerstandsfähigkeit.

Rasche Aufdeckung

- **Stärkung Sie die Reaktion auf Vorfälle:** Regelmässige Aktualisierung der Reaktionspläne mit detaillierten Bedrohungsdaten und Risikobewertungen, um eine schnelle Eindämmung und Behebung zu gewährleisten.
- **Einführung von Sicherheitslösungen:** Implementierung von EDR, NDR und SIEM-Lösungen zur Überwachung und Sicherung der IT/OT-Infrastruktur.

Schadensbegrenzung

- **Risikomanagement von Drittanbietern:** Identifizieren und entschärfen Sie Sicherheitslücken in den Diensten Dritter, um Angriffe auf Lieferketten zu verhindern.
- **Zero Trust:** Implementierung strenger Zugangs- und Verkehrskontrollen, die das inhärente Netzwerkvertrauen ausschliessen, um Daten zu schützen und Insider-Bedrohungen zu minimieren.

Analyse der Ursachen

- **Sicherheitsprüfungen und Penetrationstests:** Führen Sie regelmässig Sicherheitsaudits und Penetrationstests durch, um Sicherheitslücken im Netzwerk zu identifizieren und zu beseitigen.

Ihre 6 Schritte zur Cyber-Resilienz

1. **Definieren Sie klare Sicherheitsklassifizierungen.** Führen Sie klare Sicherheitsklassifizierungen für alle IT-Assets auf der Grundlage von Sensibilität, Zugriffsrechten und Geschäftsrelevanz. Dies ist wichtig, um das Risikopotenzial möglicher Anomalien zu verstehen und Prioritäten zu setzen.
2. **Stellen Sie fest, ob Sie den Datenfluss innerhalb Ihres Netzwerks kontinuierlich überwachen, um auch unbekannte Anomalien sofort zu erkennen.** Bedrohungsakteure hinterlassen immer Kommunikationsspuren in Ihrem Netzwerk. Sie benötigen nicht unbedingt Hardware, um Bedrohungen frühzeitig zu erkennen und Reaktionspläne für schnelle, effektive Massnahmen zu entwickeln. Wenn Sie Schwierigkeiten haben, Anomalien zu erkennen, sollten Sie KI-fähige Tools zur Erkennung von Bedrohungen in Betracht ziehen, um abnormale Netzwerkkommunikation zu identifizieren.
3. **Haben Sie blinde Flecken, bieten möglicherweise Bedrohungsakteuren ein Versteck?** Automatisieren Sie Ihre Bestandsermittlung und implementieren Sie Tools zur kontinuierlichen Inventarisierung aller IT-Ressourcen, einschliesslich derjenigen in Cloud- und Hybridumgebungen, um eine umfassende Transparenz und Verwaltung Ihrer Infrastruktur zu gewährleisten.
4. **Ihre Compliance-Anforderungen und Fähigkeiten, eine konsistente Berichterstattung zu gewährleisten.** Nur eine kontinuierliche und vollständige Überwachung gewährleistet die Einhaltung von Vorschriften wie DORA. Wenn Sie nicht konform sind, sollten Sie Lösungen zur Erkennung von und Reaktion auf Bedrohungen in Betracht ziehen, mit denen Sie Compliance-Abweichungen in Echtzeit korrigieren können, um Ereignisse zu dokumentieren, Gegenmassnahmen aufzuzeichnen und die Berichterstattung für alle IT-Ressourcen zu ermöglichen.

Finanzinstitute, die auf KI-gestützte Bedrohungserkennung vertrauen:

3 Banken IT PostFinance

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

exeon
Smart Cyber Security.

5. **Schätzen Sie die Arbeitsbelastung Ihres Sicherheitsteams realistisch ein, um zu verstehen, ob sie die wichtigsten Bedrohungen sofort erkennen können.** Zu viel Lärm; wenn das die Antwort ist, sollten Sie die Integration von KI in Betracht ziehen, um die Erkennung von und Reaktion auf Bedrohungen durch vorausschauende Analysen und automatisierte Intelligenz zu verbessern. Dies wird Ihrem Team helfen, sich zu konzentrieren.
6. **Wenn Sie SIEM verwenden, sollten Sie die Erkennung weiter verbessern.** Verbessern Sie die SIEM-Erkennungsfunktionen, indem Sie Fehlalarme und unzureichende Erkennung durch Echtzeitüberwachung und -analyse des Netzwerkverkehrs verringern.

Handeln Sie jetzt – fordern Sie Ihren Aktionsplan an.

Zum Download

Use Case

PostFinance, eines der führenden Finanzinstitute für Privatkunden in der Schweiz, hat diese wesentlichen Schritte bereits befolgt und die Cyber-Resilienz deutlich verbessert:

- Systemrelevantes Finanzinstitut in der Schweiz.
- Erfüllt alle speziellen Vorschriften bezüglich Datensicherheit und Vertraulichkeit.
- Hohe Integration von Network Detection and Response als mehrschichtiger Schutz von sensiblen und geschäftsrelevanten Systemen.
- ExeonTrace, mit seiner offenen und zukunftssicheren Architektur, ermöglicht dies ohne Hardware-Sensoren und mit voller Kontrolle über alle Datenflüsse.

„PostFinance hat sich wegen der offenen und zukunftsfähigen Architektur für ExeonTrace entschieden.
Dank der Möglichkeit auf Hardware Sensoren zu verzichten und der Kontrolle über die Datenflüsse musste PostFinance keine grossen Änderungen an der bestehenden Infrastruktur vornehmen.
Die Zusammenarbeit mit den kompetenten, technisch hochstehenden Exeon Mitarbeitenden hat überzeugt."

— **Head IT Security, PostFinance**

PostFinance

exeon
Smart Cyber Security.

Exeon Analytics AG
contact@exeon.com
exeon.com

Grubenstrasse 12
8045 Zürich
Switzerland