Industrie: Finanzen und Bankwesen

Use Case: Bankhaus in Deutschland

Das Finanzinstitut hat 1200 Mitarbeiter, eine Bilanzsumme von 25 Milliarden Euro und 80 Niederlassungen in Deutschland und Zentraleuropa.

Als mittelgrosse Institution im deutschen Bankensektor steht sie vor spezifischen Herausforderungen in Bezug auf IT-Sicherheit und **Compliance**. Sie muss den Regularien der BaFin, den Vorgaben des BSI und der KRITIS-Verordnung sowie den Anforderungen der **DORA-Richtlinie** gerecht werden.

Die komplexe IT-Infrastruktur und die Vernetzung der Standorte erhöhen die Angriffsfläche für Cyber-Bedrohungen, wobei Finanzinstitute aufgrund der sensiblen Finanzdaten ohnehin besonders attraktive Ziele für Cyber-Kriminelle sind.

Frühjahr 2023 soll sich nicht wiederholen

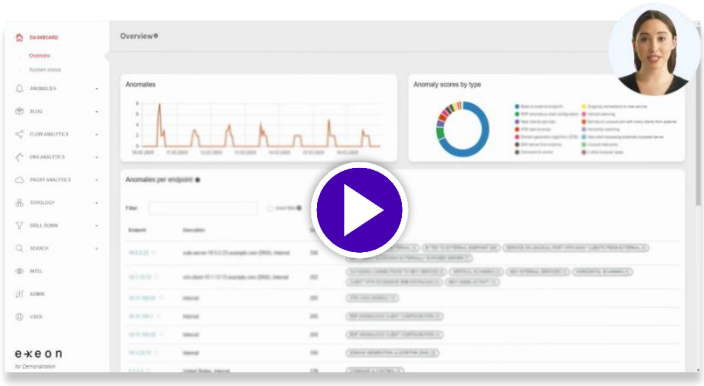
Die Digitalisierung eröffnet Banken und Versicherungen neue Möglichkeiten, macht sie aber auch anfälliger für Cyber-Bedrohungen, die die Datensicherheit und Verfügbarkeit der Dienstleistungen gefährden. Die EU hat mit DORA eine Verordnung eingeführt, die Finanzdienstleister dazu verpflichtet, ihre IT-Sicherheitsmassnahmen zu verstärken und eine operationelle Resilienz gegen Angriffe aufzubauen.

Eine grosse Herausforderung für die Finanzdienstleister besteht darin, den Schutz von Daten, einen reibungslosen Betrieb und die Einhaltung der regulatorischen Anforderungen in Einklang zu bringen. Insbesondere die Umsetzung der DORA-Anforderungen erfordert von den Banken eine Workflow-Abstimmung zwischen operativen IT-Prozessen und Cybersicherheitsmassnahmen.

Im Frühjahr 2023 wurde die Bank Ziel eines komplexen Cyberangriffs. Der Angriff begann mit einer Phishing-Kampagne, die darauf abzielte, Zugangsdaten von Mitarbeitern zu stehlen. Ein Angreifer konnte sich Zugang zum internen Netzwerk verschaffen und begann, sensible Daten zu exfiltrieren und Schadsoftware zu verbreiten. Infolgedessen wollte das Unternehmen die bestehenden Sicherheitseinrichtungen (Firewall, EDRs etc) verstärken und nahm darum verstärkt das Thema Netzwerk-Monitoring und Network Security in Augenschein. Es war für die Bank von Anfang an wichtig, dass eine europäische Lösung eingeführt würde und dass den Anforderungen der DSGVO durch die Möglichkeit, das Security-Produkt auch On-Premises und **Air-Gapped** zu hosten gegenüber **Cloud-Only** Produkten Rechnung getragen wird, um den Schutz personenbezogener Daten (Data Privacy) zu gewährleisten.

ATM-Maschinen weltweit überwachen

Demo-Video ansehen



exeon
Smart Cyber Security.

Herausforderungen aus DORA und durch Hacker Bedrohungen

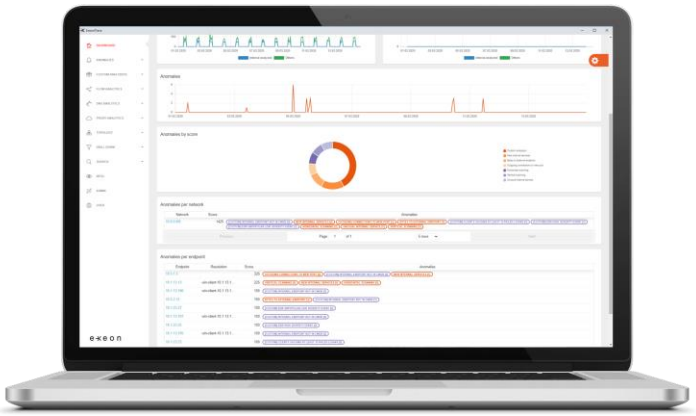
DORA verlangt von Finanzdienstleistern die Identifizierung und Minimierung von IT-Risiken, ein effektives Incident-Management zur schnellen Reaktion auf Cyberangriffe sowie die Umsetzung technischer und organisatorischer Cybersicherheitsmassnahmen. Darüber hinaus muss die Möglichkeit eines kontinuierlichen Reportings über Sicherheitsvorfälle und deren Folgen an die Aufsichtsbehörden zu jedem Zeitpunkt gegeben sein. Die Nichteinhaltung von DORA kann für Finanzdienstleister zu erheblichen finanziellen und Reputationsschäden führen.

Finanzinstitute verarbeiten hochsensible und regulierte Daten. Sie müssen daher sicherstellen, dass sie die Datenschutzanforderungen erfüllen, und sich ständig im Visier von Hackern aus aller Welt befinden; Angriffe, die den Geschäftsbetrieb stören, Daten beschädigen oder vertrauliche Informationen preisgeben, z. B. Cyberangriffe wie **Ransomware**, Insider-Bedrohungen, **Advanced Persistent Threats (APTs)** und DDoS-Angriffe, müssen daher mit allen Mitteln überwacht und verhindert werden.

Easy as Pie: Implementierung von NDR in die bestehende IT-Infrastruktur

1. POC: Konkrete Sicherheitsbedrohungen und Szenarien

ExeonTrace war im "Beauty Contest" der Bank die erfolgreichste Lösung bei der Erkennung von getesteten Anwendungsfällen (Red Teaming/Proof of Concept). Diese beinhalteten u.a: Lateral Movement; Domain Generation Algorithmen; Hidden DNS Channels und Command and Control Channels.



Für den Kunden war es besonders wichtig, dass mehrere Standorte durch eine 360° Sicht auf ihr Netzwerk unterstützt werden. Das **SOC-Team** der Bank begeisterte die intuitive Navigation in ExeonTrace durch aktuelle und historische Logdaten für vollständige Transparenz in einem einzigen Dashboard.

2. Einfache Implementierung

Die Bank nutzt eine heterogene IT-Infrastruktur mit verschiedenen Standorten und Cloud-Diensten, was die Komplexität des Netzwerks erhöht. Die Integration von ExeonTrace in die IT-Landschaft der Bank begann mit einer detaillierten Analyse der aktuellen Infrastruktur und einer Überprüfung der Netzwerkarchitektur, um die spezifischen Anforderungen der Bank zu erfüllen und in bestehende Sicherheitslösungen wie Firewalls zu integrieren. ExeonTrace soll bei dem Unternehmen alle Netzwerksegmente überwachen, also interne und externe Netzwerke und auch Schnittstellen zu Drittanbietern und Cloud-Anwendungen.
Nach der Implementierung sammelt und analysiert ExeonTrace Netzwerkmetadaten, die aus der gesamten IT-, Cloud- und OT-Infrastruktur exportiert werden. Dazu gehören Informationen wie IP-Adressen, Ports, Protokolle, Datenübertragungsraten und Verbindungszeiten.

ExeonTrace verwendet Graphdatenbanken, um den Speicherbedarf zu reduzieren, indem die Daten in Form von Knoten und Kanten gespeichert werden. Diese Struktur ermöglicht eine effiziente Speicherung und Abfrage hochgradig vernetzter Daten, da Beziehungen direkt und ohne zusätzliche Indizes abgebildet werden. Da ExeonTrace keine vollständigen Netzwerkpakete spiegelt, sondern nur Metadaten analysiert, bleibt die Menge der verarbeiteten Daten zusätzlic reduziert. Die gewonnenen Metadaten werden mit hochentwickelten trainierten und untrainierten KI-Algorithmen auf potenzielle Bedrohungen abgeglichen. Die Integration in den bestehenden Systemen funktionierte nahtlos und ist einfach skalierbar, da ExeonTrace ohne Hardware Appliances arbeiten, in bestehenden Sicherheits- und IT-Managementsysteme der Bank integriert werden kann und z.B. Firewall-Logs in die Kommunikationsüberwachung von Exeon integriert werden.

Den Herausforderungen aus DORA und CyberCrime begegnen: ExeonTrace at work!

ExeonTrace bietet vollständige Transparenz in der hochgradig virtualisierten IT-Infrastruktur der Bank. Mithilfe der KI und Verhaltensanalysen können bekannte und neue Angriffe besser erkannt und schneller darauf reagiert werden. ExeonTrace analysiert die Kommunikationsmuster und alarmiert bei Anomalien. Beispiele für Bedrohungen, die mit NDR identifiziert und gemanagt werden, sind **Advanced Persistent Threats (APTs)** (langfristige, Cyberangriffe, die darauf abzielen, unentdeckt zu bleiben), Insider-Bedrohungen, Ransomware, DDos Attacken, **Zero-Day Exploits** (das System erkennt frühe Anzeichen von Ransomware-Angriffen, z. B. ungewöhnliche Datenbewegungen oder Ransomware-Aktivitäten im Netzwerk). Die Fähigkeit auch unbekannte Angriffe zu identifizieren, ungehende Reaktionsmechanismen und ein verbessertes Reporting unterstützen besonders auch die DORA-Anforderungen. Im Vergleich zu Firewalls und EDRs bietet NDR einen netzwerkzentrierten Ansatz, der auch Bedrohungen erkennt, die nicht direkt auf den Endgeräten sichtbar sind, und schützt Bereiche, in denen keine Sensoren oder Agenten installiert werden können, etwa für die die Überwachung von branchenspezifischen Assets wie Geldautomaten und anderer OT.

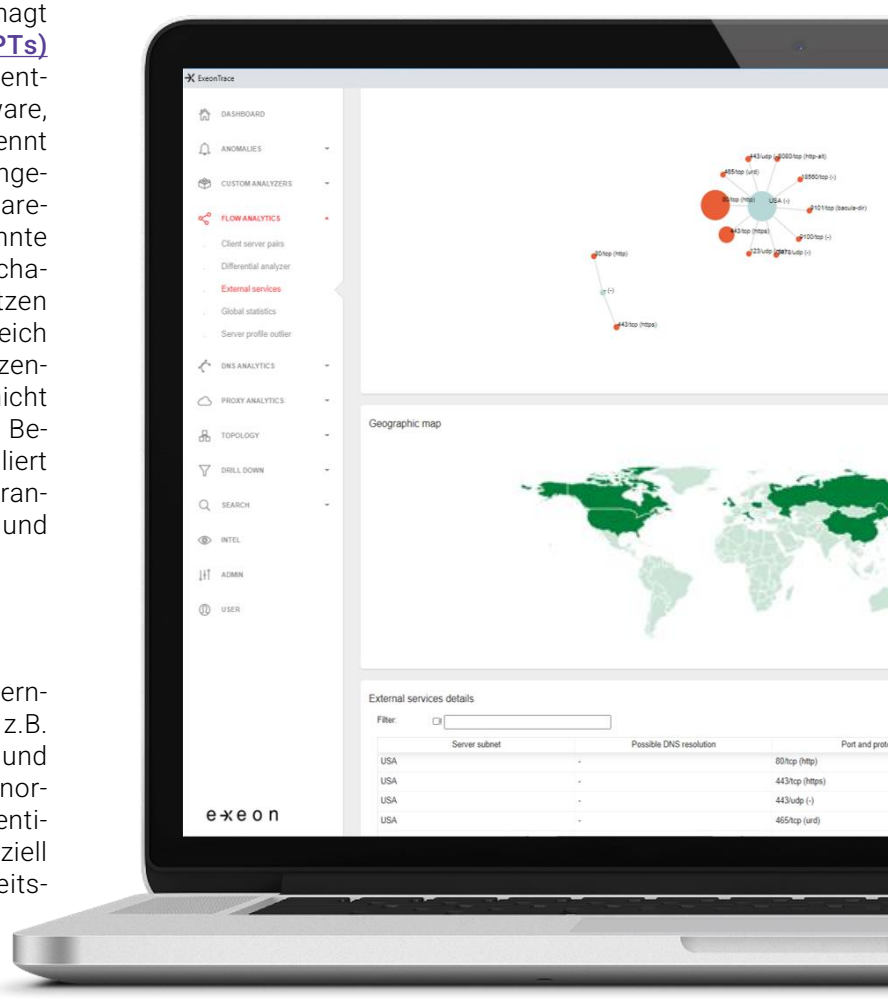
Der Impact von NDR konkret

ExeonTrace erkannte bereits nach einer kurzen Lernphase ungewöhnliche Netzwerkaktivitäten, wie z.B. erhöhte Datentransfers an unbekannte IP-Adressen und ungewöhnliche Anmeldeversuche ausserhalb der normalen Arbeitszeiten. Mit Hilfe von KI-Algorithmen identifiziert ExeonTrace diese Aktivitäten als potenziell bösartig und generiert Alarme, die an das Sicherheitsteam der Bank weitergeleitet werden.

Es ist hinfort möglich die betroffenen Systeme zu isolieren, infizierte Geräte vom Netzwerk und verdächtige IP-Adressen zu blockieren, um die Ausbreitung von Malware durch Lateral Movement zu verhindern, die Kommunikation von Command and Control Channel (C&C Channels) zu unterbrechen. Andere unregelmässige Aktivitäten, wurden vorab mit dem SOC-Team auf eine Whitelist gesetzt und werden keine Alarme mehr auslösen. Durch die schnelle Erkennung und Reaktion kann die Bank potenziellen Schaden minimieren, die intelligenten Algorithmen und das Whitelisting reduzieren die Zahl der False Alerts und damit den Workload des Security Teams der Bank.

Für das SOC-Team ist die „Überwachung des Netzwerkverkehrs auf ungewöhnliche Aktivitäten, um Cyberangriffe frühzeitig zu erkennen und zu melden“, wie es die DORA-Richtlinien vorschreiben, von einer zeitaufwändigen und fehleranfälligen, manuellen Überwachung nun stark automatisiert worden.

Das Sicherheitsteam nutzt die umfassenden Incident-Management-Möglichkeiten von ExeonTrace, um Vorfälle zu analysieren und zu dokumentieren, wobei alle Schritte protokolliert wurden, um eine lückenlose Nachverfolgung zu gewährleisten. Die detaillierte Protokollierung und Berichterstattung der Kommunikation im Netz ermöglicht es der Bank, die regulatorischen Anforderungen aus DORA an das Reporting zu erfüllen.



Smart Cyber Security.

Da ExeonTrace nicht mit Packet Mirroring arbeitet und keine Daten in einer PublicCloud verarbeitet, bleiben alle sensiblen Informationen innerhalb der sicheren Umgebung der Bank. Die verarbeiteten User-Daten werden durch Hashen die personenbezogenen Informationen anonymisiert, was den Schutz der Privatsphäre der Kunden erhöht und die Einhaltung der DSGVO-Richtlinien unterstützt.

Die Möglichkeit, ExeonTrace in einer vollständig isolierten Umgebung (Air-Gapped) zu betreiben, bietet zusätzlichen Schutz vor externen Bedrohungen und gewährleistet, dass keine Daten das sichere Netzwerk der Bank verlassen.

Das entscheidende Ergebnis

Die Erfolgsmessung der Implementierung von ExeonTrace erfolgte nach 6 Monaten anhand verschiedener KPIs, darunter die Anzahl der erkannten Bedrohungen, die Reaktionszeit, die Reduzierung von Fehlalarmen durch den Einsatz fortschrittlicher Algorithmen, der DORA-Readiness und der Erfüllung anderer Cybersicherheits- und Compliance-Regularien für die Finanzindustrie, sowie durch die Zufriedenheit und die reduzierten Workloads der IT- und Sicherheitsteams der Bank mit ExeonTrace.

Allianz für Cyber-Sicherheit

CYBERSECURITY MADE IN EUROPE

ATTESTA ISO 27001 CERTIFIED

Exeon Analytics AG
contact@exeon.com
exeon.com

Grubenstrasse 12
8045 Zürich
Switzerland

LinkedIn
YouTube