Forensik und Finanzen

Eine strategische Antwort auf die EU-Konformitätsanforderungen

Mit der Verabschiedung der NIS2-Richtlinie und der DORA-Verordnung über die digitale operationale Resilienz im Finanzsektor durch die EU steht die Finanzwirtschaft vor einem wichtigen Wandel. Beide Regelwerke unterstreichen die unbedingte Notwendigkeit einer verbesserten Netzwerkleistung und operationalen Resilienz. Sie erinnern die Unternehmen daran, was alles auf dem Spiel steht, wenn sie ihre Compliance vernachlässigen. Während die Leistung im Mittelpunkt steht, dreht sich hier doch alles darum, die strengen aufsichtsrechtlichen Vorgaben zu erfüllen, um die Finanzunternehmen vor den Auswirkungen einer Nichteinhaltung, einschließlich drastischer Sanktionen, zu schützen.

Wegweiser zur Einhaltung der aufsichtsrechtlichen Anforderungen

In der sich weiter entwickelnden Landschaft der finanzwirtschaftlichen Regulierungen formulieren die NIS2-Richtlinie und die DORA-Verordnung eine Reihe von Konformitätsanforderungen, die die traditionellen operativen und Sicherheitsrahmen in Frage stellen. Die Einhaltung dieser aufsichtsrechtlichen Vorgaben erfordert mehr als nur einen flüchtigen Blick auf die Netzwerkaktivitäten. Stattdessen ist eine tiefgehende Prüfung der komplexen Details aller Transaktionen und Kommunikationen im Netzwerk unverzichtbar. Diese Herausforderungen betreffen sowohl technische Aspekte, wie Latenz, Bandbreitenbeschränkungen und Infrastrukturkomplexität, als auch allgemeinere Kriterien, wie Zuverlässigkeit, Verfügbarkeit und allumfassende Maßnahmen zur Gewährleistung der Cybersicherheit, die eine Voraussetzung für den Schutz der Integrität des Netzwerks sind.

VIAVI Solutions befähigt die Finanzunternehmen, die wichtigsten Compliance-Herausforderungen mühelos zu bewältigen, indem das bisher ungenutzte Leistungspotenzial der Überwachung der Netzwerkkommunikation sowie der forensischen Analyse ausgeschöpft wird. Damit ist es möglich, die regulatorischen Hürden in strategische Vorteile umzuwandeln.

Die Nichteinhaltung der NIS2-Richtlinie kann erhebliche Sanktionen, darunter für wesentliche Einrichtungen Geldbußen von bis zu 10 Millionen Euro oder von bis zu 2 % des jährlichen weltweiten Umsatzes sowie die Haftung des Managements, zur Folge haben. Diese Auswirkungen unterstreichen die Bedeutung einer sorgfältigen Beaufsichtigung der IT-Abläufe.

Compliance-Herausforderungen und VIAVI Solutions

Drei wichtige Herausforderungen:

1. **Meldung von Vorfällen gemäß DORA:** Die fristgerechte und detaillierte Meldung von Sicherheitsvorfällen ist eine wesentliche Voraussetzung zur Einhaltung von DORA.
2. **IKT-Risikomanagement gemäß NIS2:** Die Identifikation und das Management von IKT-Risiken ist ein zentraler Bestandteil von NIS2.
3. **Management des Drittparteien-Risikos:** Sowohl NIS2 als auch DORA betonen die Bedeutung des Managements von Drittparteien-Risiken.

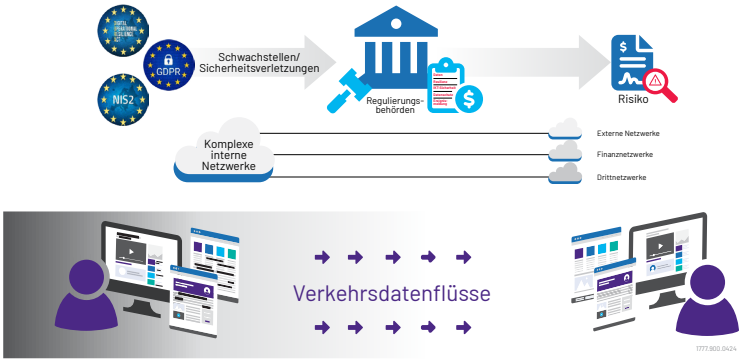
Unsere Lösungen:

Die Observer-Plattform von VIAVI setzt völlig neue Maßstäbe für die Konformität und die Bewältigung der Sicherheitsanforderungen von Netzwerken für Finanzunternehmen, da sie das Leistungspotenzial der präzisen Netzwerk-Forensik ausschöpft. Die Lösungen von VIAVI kombinieren Daten aus unzähligen Quellen, darunter IPFIX/NetFlow, Active Directory, Syslog, SNMP und Paketaufzeichnungen, um einen lückenlosen forensischen Fußabdruck zu erstellen. Diese durchdachte Herangehensweise versetzt die Finanzunternehmen in die Lage, Compliance-Vorfälle zu identifizieren, zu analysieren und deutlich vor Ablauf der von DORA festgelegten strengen 72-Stunden-Frist zu melden. Gleichzeitig ist es möglich, das proaktive Risikomanagement und die aufsichtsrechtlichen Compliance-Forderungen von NIS2 einzuhalten.

Auf Grundlage der beispiellosen Sichtbarkeit der Datenflüsse des Netzwerks und der Wechselbeziehungen mit Drittparteien gewährleistet VIAVI die umfassende Einhaltung der Sicherheitsstandards, sodass Schwachstellen und versteckte Risiken in den Netzwerken effektiv gemindert werden können.

- **Forensischer Fußabdruck:** Die äußerst präzisen forensischen Untersuchungen, die durch die Paketaufzeichnung von Observer GigaStor gestärkt werden, ermöglichen die retrospektive Analyse der Netzwerktransaktionen zur Gewährleistung einer beispiellosen Sichtbarkeit.

- **Enriched-Flow-Datensätze:** Nur die Observer-Plattform von VIAVI ist in der Lage, strukturierte und unstrukturierte Daten zu kombinieren und damit für jede Netzwerkkonversation einen „Super-Datensatz“ zu erstellen, der die Beschränkungen konventioneller Flussdatensätze überwindet.
- **Integrierte Datenquellen:** Durch das Auflösen von Datensilos fasst Observer Apex die forensischen Informationen der Datenpakete und Datenflüsse zu verwertbaren Einblicken zusammen, was die Arbeit der SecOps- und NetOps-Teams deutlich erleichtert.



VIAVI konfiguriert und verarbeitet die Verkehrsdatenflüsse, um den zur Gewährleistung der Konformität benötigten umfassenden Überblick zur Verfügung zu stellen.

Konformitätslücken schließen mit VIAVI

Durch die Erfassung der Verkehrsdatenflüsse im Netzwerk vermittelt VIAVI unschätzbare Einblicke dazu, wie die einzelnen Netzelemente Datenpakete empfangen, klassifizieren und verarbeiten. VIAVI unterscheidet sich von seinen Mitbewerbern durch seine einzigartige Fähigkeit, die Verkehrsdatenflüsse umgehend und lückenlos anbieterunabhängig, skalierbar und präzise zu erfassen. Dieses Leistungsmerkmal erlaubt den Unternehmen, die Datenflüsse im Netzwerk besser zu verstehen, um potentielle Konformitätslücken schnell zu identifizieren und zu priorisieren.

Hier ein Anwendungsfall zur Illustration:

Bei der Abwehr von Ransomware-Angriffen kommt es darauf an, die Sicherung (Backup) und die Wiederherstellung der Daten möglichst effektiv durchzuführen. Hier zeichnet sich VIAVI dadurch aus, dass die Unternehmen in die Lage versetzt werden, die Dienste und Server, die von einer Anwendung genutzt werden, zu erkennen. Durch die Erfassung der Datenfluss-Verbindungen können die Unternehmen die Wirksamkeit des Wiederherstellungsprozesses einschätzen und sicherstellen, dass kritische Funktionen auf einem zufriedenstellenden Niveau reaktiviert werden.

Compliance-Bereitschaft als nächster Schritt im Compliance-Puzzle

Die Vorbereitung auf die Einhaltung der von DORA und NIS2 gestellten Anforderungen umfasst eine Reihe von „No-Regret“-Maßnahmen, wie eine Lückenanalyse des IKT-Risikomanagements, um die Bedrohungserkennung und die Meldung von Sicherheitsvorfällen zu verbessern sowie kritische Ressourcen für Resilienz-Tests zu identifizieren. Von Finanzunternehmen könnte darüber hinaus verlangt werden, für DORA innerhalb von zwei Jahren ihr Management von Sicherheitsvorfällen zu verbessern und ein Drittparteien-Risikomanagement umzusetzen sowie die für die Einhaltung von NIS2 erforderlichen strategischen Anpassungen vorzunehmen.

In Zeiten von NIS2 und DORA darf die Konformität nicht vernachlässigt werden. VIAVI ist hervorragend positioniert, um den Finanzunternehmen zu helfen, diese aufsichtsrechtlichen Herausforderungen zuverlässig zu bewältigen. Durch Nutzung des Netzwerks als unmittelbarer Quelle der Wahrheit befähigt VIAVI Sie, die geforderte Compliance effektiv zu gewährleisten. Unsere Kompetenz auf dem Gebiet der Netzwerk-Forensik und Analyse setzt neue Maßstäbe für Ihren Konformitätsprozess, da kritische Bereiche, wie die Meldung von Sicherheitsvorfällen, das IKT-Risikomanagement und die Bewertung von Drittparteien-Risiken, berücksichtigt werden. Mit VIAVI als Partner können auch Sie Ihre Compliance-Position stärken und sicherstellen, dass Ihre Betriebsabläufe resilient und Sie den regulatorischen Vorgaben immer einen Schritt voraus bleiben.

Die DORA-Verordnung der EU über die digitale operationale Resilienz stellt wesentliche neue aufsichtsrechtliche Anforderungen an die Finanzdienstleister.

Quelle: What can we expect from the Digital Operational Resilience Act | Deloitte Niederlande

VIAVI Solutions

Kontakt **+49 7121 86 2222**

Sie finden das nächstgelegene VIAVI-Vertriebsbüro auf viavisolutions.de/kontakt

forensics-finance-fly-ec-de
30194608 900 0524