Erhöhen NIS-2 und DORA die Cybersicherheit?

Die Zahl und Komplexität von Cyberangriffen nehmen rasant zu. Vor diesem Hintergrund werden die NIS-2-Richtlinie und der Digital Operational Resilience Act (DORA) der EU als entscheidende Instrumente zur Stärkung der Cybersicherheit und digitalen Widerstandsfähigkeit betrachtet.

Von **Richard Werner und Elfrieda Neumann**

Die digitale Landschaft in Europa hat sich im Jahr 2023 rasant weiterentwickelt, wobei die Schweiz, Deutschland und Österreich weiterhin als wichtige Knotenpunkte in der globalen Informationsgesellschaft agieren. Mit dieser Entwicklung ist jedoch auch eine zunehmende Anzahl von Cyberangriffen verbunden, die sowohl öffentliche Einrichtungen als auch private Unternehmen betreffen. Diese Angriffe reichen von Ransomware und Phishing bis hin zu ausgeklügelten DDoS-Attacken (Distributed Denial of Service) und zielen darauf ab, sensible Daten zu stehlen, kritische Infrastrukturen zu stören und finanziellen Schaden anzurichten.

In der Schweiz wurden im Jahr 2023 über 8000 signifikante Cyberangriffe gemeldet, ein Anstieg von 15% im Vergleich zum Vorjahr. Die daraus resultierenden direkten finanziellen Schäden werden auf weit über 200 Millionen CHF geschätzt, wobei die indirekten Kosten durch Betriebsunterbrechungen und

AUTOREN

Dr. Richard Werner

EMBA, CEO – Future Intelligence Group AG, DACH

Elfrieda Neumann (Co-Autorin)

MBA, COO – Future Intelligence Group AG, DACH

Überblick

- NIS-2-Richtlinie: Erweiterung der Cybersicherheitsanforderungen über eine Vielzahl von Sektoren hinweg.
- Dora: Spezifischer Fokus auf die digitale Widerstandsfähigkeit im Finanzsektor.
- Gemeinsames Ziel: Stärkung der Cybersicherheit und Resilienz in der EU.
- Handlungsbedarf: Unternehmen müssen ihre Sicherheitsstrategien anpassen, um den neuen EU-Vorschriften zu entsprechen.

Reputationsschäden noch deutlich höher liegen.

Bedrohung stark gestiegen

Deutschland erlebte einen ähnlichen Trend mit über 15 000 gemeldeten Cyberangriffen, was einem Anstieg von 20% gegenüber 2022 entspricht. Der finanzielle Schaden für deutsche Unternehmen und Institutionen wird auf rund 1,5 Milliarden EUR beziffert und unterstreicht die Dringlichkeit einer robusten Cybersicherheitsstrategie.

Österreich verzeichnete ebenfalls einen Anstieg der Cyberangriffe um 18%, mit etwa 5000 Vorfällen und einem geschätzten Schaden von 300 Millionen EUR. Diese Zahlen verdeutlichen die kontinuierliche Bedrohung durch Cyberkriminalität in der DACH-Region und die Notwendigkeit verstärkter Sicherheitsmassnahmen.

Diese Entwicklungen unterstreichen die kritische Bedeutung von Cybersicherheit und digitaler Widerstandsfähigkeit. Vor diesem Hintergrund zielen die NIS-2-Richtlinie und der Digital Operational Resilience Act (DORA) darauf ab, ein höheres Mass an Sicherheit in der digitalen Umgebung der Europäischen Union zu gewährleisten, wobei der Schwerpunkt auf präventiven Massnahmen, verbesserten Meldepflichten und einer verstärkten Zusammenarbeit zwischen den Mitgliedsstaaten liegt.

Entwicklungen zur Regulierung und Resilienz

Die digitale Transformation und die zunehmende Vernetzung in der Europäischen Union (EU) haben die Bedeutung von Cybersicherheit und digitaler Widerstandsfähigkeit drastisch erhöht. Vor diesem Hintergrund zielen die NIS-2-Richtlinie (Network and Information Systems 2) und der Digital Operational Resilience Act (DORA) darauf ab, ein hohes Mass an Sicherheit für Netz- und Informationssysteme in der EU zu gewährleisten. Während NIS-2 eine breite Palette von Sektoren abdeckt, konzentriert sich DORA speziell auf den Finanzsektor. Beide Gesetzgebungen stellen wesentliche Pfeiler der EU-Strategie dar, um die Cybersicherheit zu stärken und die Resilienz gegenüber digitalen Bedrohungen zu erhöhen. Dieses Whitepaper bietet einen umfassenden Überblick

über die Ziele, den Anwendungsbereich und die wichtigsten Anforderungen beider Rechtsakte sowie praktische Ratschläge für deren Umsetzung.

NIS-2-Richtlinie

Die NIS-2-Richtlinie erweitert den Geltungsbereich der ursprünglichen NIS-Richtlinie signifikant und umfasst nun wesentliche und wichtige Einrichtungen in kritischen Sektoren wie Energie, Verkehr, Bankwesen, Gesundheitswesen und digitale Infrastrukturen. Zudem fallen Anbieter digitaler Dienste, wie Cloud-Computing-Dienste, unter diese Richtlinie. Ein zentraler Aspekt von NIS-2 ist die Einführung strengerer Sicherheitsanforderungen und Meldepflichten für Cybersicherheitsvorfälle. Unternehmen müssen fortan Risikomanagementmassnahmen implementieren und ernsthafte Vorfälle den nationalen Aufsichtsbehörden melden. Durch diese Massnahmen soll ein hohes Mass an Sicherheit und Vertrauen in der digitalen Umgebung der EU gewährleistet werden. Darüber hinaus erweitert die Richtlinie die Zahl der Organisationen, die in den Anwendungsbereich fallen. Für die Geschäftsleitung der betroffenen Organisationen werden strengere Haftungsregeln gelten.

Digital Operational Resilience Act (DORA)

DORA stellt einen spezialisierten Rechtsakt dar, der darauf abzielt, die digitale Widerstandsfähigkeit des Finanzsektors zu stärken. Dazu zählen Kreditinstitute, Versicherungsunternehmen, Investmentfirmen, Zahlungsdienstleister und weitere Finanzmarktinfrastrukturen. DORA schreibt vor, dass diese Unternehmen umfassende ICT-Risikomanagementverfahren implementieren, regelmässige Cybersicherheitstests durchführen und schwere ICT-Vorfälle melden müssen. Die Verordnung sieht zudem strenge Anforderungen für das Management von Risiken vor, die mit Drittanbietern, einschliesslich Cloud-Diensten, verbunden sind. DORA zielt darauf ab, ein einheitliches hohes Niveau der digitalen Widerstandsfähigkeit im gesamten EU-Finanzsektor zu schaffen und somit die finanzielle Stabilität und Integrität zu sichern.

«In Deutschland wirkte die KRITIS-Gesetzgebung bislang insbesondere auf grössere Institutionen. Mit NIS-2 wird Cybersicherheit und Resilienz nun auch für die breite Masse der Unternehmen in Europa zum Top-Thema.»

Vergleich und Wechselwirkungen

Obwohl NIS-2 und DORA unterschiedliche Sektoren ansprechen, verfolgen sie das gemeinsame Ziel, die Cybersicherheit und digitale Widerstandsfähigkeit in der EU zu verbessern. Beide Rechtsakte ergänzen sich, indem sie auf sektorspezifische Risiken eingehen und gleichzeitig übergreifende Sicherheitsstandards setzen. Eine wesentliche Wechselwirkung besteht in der Erkenntnis, dass der Finanzsektor auch kritische Infrastrukturen nutzt, die unter NIS-2 fallen, wodurch eine enge Abstimmung zwischen den Regelungen erforderlich wird. Unternehmen, die sowohl unter NIS-2 als auch DORA fallen, müssen eine kohärente Strategie zur Einhaltung beider Rechtsakte entwickeln, um Doppelarbeit zu vermeiden und Synergien zu nutzen.

Schlussfolgerungen und Ausblick

Die Einführung der NIS-2-Richtlinie und von DORA markiert einen wichtigen Schritt der EU, um die Cybersicherheit und die digitale Widerstandsfähigkeit innerhalb ihrer Grenzen zu stärken. Diese Regelungen reflektieren das wachsende Bewusstsein für die Bedeutung einer robusten digitalen Infrastruktur als Grundlage für die wirtschaftliche und soziale Stabilität in Europa. Unternehmen sind nun gefordert, ihre Sicherheits- und Resilienzstrategien anzupassen, um den neuen Anforderungen gerecht zu werden. Dies erfordert eine kontinuierliche Bewertung und Anpassung der Sicherheitsmassnahmen, um nicht nur compliant zu sein, sondern auch einen Beitrag zur allgemeinen Sicherheit der digitalen Gesellschaft in der EU zu leisten.

Vorgehensweise zur Implementierung:

1. Risikobewertung: Durchführung einer detaillierten Risikobewertung der IT-Systeme und Prozesse zur Identifizierung potenzieller Schwachstellen und Bedrohungen.
2. Incident-Response-Plan: Entwicklung und Implementierung eines umfassenden Incident-Response-Plans, inklusive klar definierter Rollen, Kommunikationsstrategien und Wiederherstellungsmassnahmen.
3. Schulungsprogramme: Etablierung regelmässiger Schulungs- und Bewusstseinsprogramme für alle Mitarbeiter, um das Verständnis und die Erkennung von Cybersicherheitsrisiken zu fördern.
4. Überprüfung der Drittanbieter-Sicherheit: Implementierung von Prozessen zur Überprüfung und Bewertung der Cybersicherheitsmassnahmen von Drittanbietern und Lieferanten.
5. Technologische Sicherheitsmassnahmen: Einsatz fortschrittlicher Sicherheitstechnologien und -verfahren, wie Multi-Faktor-Authentifizierung und Verschlüsselung, zur Stärkung der Sicherheitsinfrastruktur.
6. Regelmässige Audits: Durchführung regelmässiger interner und externer Sicherheitsaudits zur Überprüfung der Compliance mit NIS-2 und DORA sowie zur Identifizierung von Verbesserungsmöglichkeiten