Weichenstellung in der Cybersicherheit

Was NIS-2, DORA und der Cyber Resilience Act für Unternehmen bedeuten

Cybersicherheit ist kein freiwilliges Upgrade mehr – sie wird zur Pflicht. Mit den neuen EU- Regularien NIS-2, DORA und dem Cyber Resilience Act (CRA) setzt Europa neue Maßstäbe für den Schutz digitaler Infrastrukturen. Unternehmen, die die Anforderungen unterschätzen, riskieren nicht nur hohe Strafen, sondern auch ihre Wettbewerbsfähigkeit.

Strengere EU-Regularien für mehr Cybersicherheit

2025 markiert einen Wendepunkt für IT-Sicherheit in Europa. Die EU führt mit drei zentralen Regulierungen schärfere Sicherheitsanforderungen für Unternehmen ein.

Autor:
Ari Albertini
CEO
FTAPI
www.ftapi.com

NIS-2

Mit NIS-2 (Network and Information Security Directive) werden die Regeln für IT-Sicherheit drastisch verschärft und auf eine breitere Unternehmenslandschaft ausgeweitet. Während sich die Vorgängerrichtlinie primär auf kritische Infrastrukturen konzentrierte, betrifft die neue Version nun auch zahlreiche mittelständische Unternehmen – darunter Hersteller, IT-Dienstleister, Pharmaunternehmen und Logistikbetriebe. Die betroffenen Organisationen müssen Angriffe innerhalb von 24 Stunden melden, geeignete Sicherheitsmaßnahmen etablieren und sich auf strengere Kontrollen einstellen. Verstöße können Bußgelder von bis zu 10 Millionen Euro oder 2 Prozent des weltweiten Jahresumsatzes nach sich ziehen.

Digital Operational Resilience Act

Für den Finanzsektor bringt der Digital Operational Resilience Act (DORA) umfassende neue Pflichten mit sich. Banken, Versicherungen und Fintechs müssen ihre gesamte IT-Lieferkette absichern und sich regelmäßigen Cyber-Resilienz-Tests unterziehen. Besonders betroffen sind auch externe IT-Dienstleister, die mit Finanzunternehmen zusammenarbeiten – sie müssen nun strenge Sicherheitsstandards nachweisen, um weiterhin als Geschäftspartner zugelassen zu werden.

Cyber Resilience Act

Der Cyber Resilience Act (CRA) zielt auf die Hersteller von Hard- und Software ab. Digitale Produkte müssen künftig Sicherheitsstandards von Beginn an („Security-by-Design“) erfüllen und über ihren gesamten Lebenszyklus hinweg mit Sicherheitsupdates versorgt werden. Wer Cybersecurity-Lücken zu spät schließt oder nicht konsequent nachbessert, riskiert hohe Strafen und Marktbarrieren.

Was das für Unternehmen bedeutet

Mit den neuen Regularien geht Europa über reine Schutzmaßnahmen hinaus – sie sind Teil einer langfristigen Strategie zur Stärkung der digitalen Souveränität. Unternehmen stehen nicht nur vor höheren Sicherheitsanforderungen, sondern auch vor einem veränderten Marktumfeld. Kunden und Geschäftspartner müssen verstärkt auf nachweisbare Sicherheitsstandards achten, und gleichzeitig nimmt die regulatorische Kontrolle zu.

„Die Zeiten, in denen Cybersicherheit eine rein technische Entscheidung war, sind vorbei. Jetzt geht es um wirtschaftliche Resilienz, digitale Souveränität und letztlich auch um persönliche Haftung“, sagt Ari Albertini, CEO von FTAPI. „Die neuen Regularien zwingen Unternehmen, Cybersicherheit strategisch zu denken – wer nicht handelt, wird abgehängt.“

Besonders für Geschäftsführer und IT-Verantwortliche haben die neuen Regeln weitreichende Konsequenzen. Neben Bußgeldern droht in einigen Fällen eine persönliche Haftung.

Cybersicherheit wird zur Management-Aufgabe: Wer IT-Risiken nicht strategisch bewertet und absichert, riskiert nicht nur finanzielle Folgen, sondern auch den Verlust von Vertrauen und Marktanteilen.

Fünf konkrete Maßnahmen, die Unternehmen jetzt ergreifen sollten

1. **Security-Standards überprüfen:** Unternehmen sollten ihre bestehenden Sicherheitsmaßnahmen mit den neuen gesetzlichen Anforderungen abgleichen und identifizieren, wo es Nachholbedarf gibt. Besonders wichtig sind Risikoanalysen, Audits und Notfallpläne.

2. **Meldeprozesse und Compliance-Strukturen etablieren:** Klare Abläufe für die Meldung von Sicherheitsvorfällen und die Erfüllung von Dokumentationspflichten sind essenziell, um regulatorische Anforderungen zu erfüllen.

3. **Cybersecurity als Unternehmensstrategie verankern:** IT-Sicherheit ist keine reine IT-Aufgabe mehr, sondern eine strategische Verantwortung, die aktiv von der Geschäftsführung gesteuert werden muss.

4. **Auf europäische Anbieter setzen:** Mit den neuen Regularien rückt digitale Souveränität stärker in den Fokus. Unternehmen, die frühzeitig auf europäische IT- und Security-Dienstleister setzen, profitieren von besserer Compliance und langfristiger Stabilität.

5. **Frühzeitig investieren und Wettbewerbsvorteile nutzen:** Unternehmen, die ihre Sicherheitsstandards bereits jetzt verbessern, sind nicht nur regulatorisch auf der sicheren Seite, sondern gewinnen auch Vertrauen bei Kunden und Geschäftspartnern.

Cybersecurity als Wettbewerbsvorteil

Mit den neuen EU-Regularien wird Cybersicherheit zur Chefsache. Unternehmen müssen sich jetzt intensiv mit ihren Sicherheitsstrategien auseinandersetzen, um gesetzeskonform zu bleiben und sich gegen zunehmende Cyberangriffe zu wappnen.

„Cybersicherheit ist kein notwendiges Übel, sondern ein Wettbewerbsvorteil. Wer frühzeitig in IT-Sicherheit investiert, gewinnt nicht nur regulatorische Sicherheit, sondern stärkt auch das Vertrauen von Kunden und Partnern“, so Ari Albertini. ◄