Kontakt

Weststraße 4
57392 Schmallenberg

P : 02972 96396-01

M : 0173 8253824

E : b.richter@cybercomplete.de

w : www.cybercomplete.de

DORA

Digital Operational Resilience Act

Unser
Unternehmen

Das Team der Cyber Complete GmbH versteht die Informationssicherheit als ganzheitlichen Ansatz und eine der wichtigsten Säulen in heutigen Unternehmen. In der Industrie- und Wirtschaftswelt des 21. Jahrhunderts ist inzwischen eine Vernetzung und Globalisierung gegeben, die eine Cybersicherheit für Unternehmen, Konzerne und Privatpersonen unabdingbar macht und eine Grundvoraussetzung für ein erfolgreiches Wirken ist. Täglich erfolgen aus allen Winkeln des Globus unzählige Hackerangriffe und Versuche, in die Systeme von Firmen einzudringen – die Tendenz ist weiter steigend. Auch politische Institutionen und ganze Regierungen sind von diesen Entwicklungen betroffen, besonders wenn es dabei um sensible und besonders schützenswerte Inhalte und Daten geht.

Inhaltsverzeichnis

Was ist DORA?
EU Regulation Finanzsektor

Hinter DORA (Digital Operational Resilience Act) steckt eine finanzsektorweite Regulierung für die Cybersicherheit. Diese wird ab dem 17.01.2025 geltend gemacht mit der Absicht, die Vorschriften im Finanzsektor zu vereinheitlichen und die Resilienz gegen Cyberangriffe maßgeblich zu stärken.

Ziele von DORA

Schutz vor IT-Störungen, Cyberangriffen und anderen Bedrohungen, die die Geschäftsprozesse der Finanzmarktteilnehmer und deren Drittanbieter gefährden können.

Was wird in DORA angesprochen?

**Risikomanagement der Informationstechnologie
Ebenfalls auch Drittanbieter-Risikomanagement
Überwachung kritischer und wichtiger Drittanbieter, Resilienz- und Penetrationstests, Meldung von Vorfällen in der Informationstechnologie, teilen von Informationen bei Vorfällen und Angriffen.**

- ✓ Schutz vor IT-Störungen
- ✓ Schutz vor Cyber-Angriffen
- ✓ Überwachung kritscher & wichtiger Drittanbieter
- ✓ Meldung von Vorfällen & Angriffen

Risikomanagement

Risikomanagement ist die Basis für jedes Management-System. Somit der erste Schritt der Anforderungen. Bezieht sich auf die Identifikation, Bewertung und Steuerung von IT- & Cybersicherheitsrisiken, die die Geschäftsprozesse und die Sicherheit der IT-Systeme gefährden können.

Durch frühzeitige Identifikation und Bewertung von Risiken und proaktives Ergreifen von Maßnahmen werden Systemausfälle und finanzielle Schäden vermieden.

FINANZEN

Unternehmensfinanztransaktionen und Geschäftsbuchhaltung

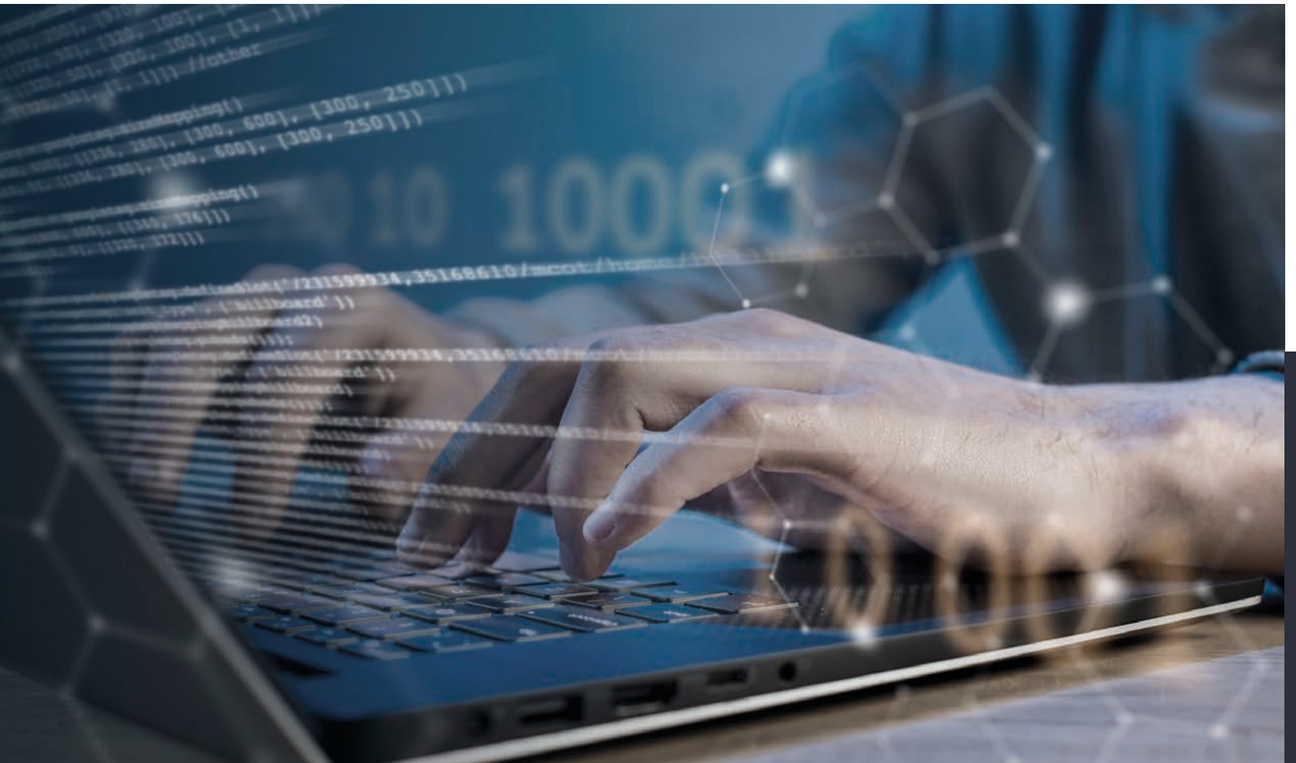
Was für Tools bieten sich an?

- **Assetmanagement für kritische Bereiche & Infrastrukturen**
- **Risikoanalyse und entsprechende Risikobehandlung**
- **Backup & Wiederherstellung von Informationen & Daten**
- **Business Continuity Strategien zur Vermeidung von Betriebsunterbrechungen**
- **Monitoring der sensiblen IT-Systeme und eine erweitere Anomalieerkennung**
- **Awareness-Kampagnen & Trainings für Mitarbeiter und Führungskräfte**

Warum ist ein Penetration-Testing sinnvoll?

In einem Penetration-Test werden Cyber-Angriffe auf die IT-Infrastruktur eines Unternehmens simuliert, um Schwachstellen und Sicherheitslücken aufzudecken.

Viele Sicherheitslücken werden erst durch gezielte Angriffe aufgedeckt. Ohne regelmäßige Überprüfungen bleiben Unternehmen anfällig für Hackerangriffe und Datenlecks.



Deepwebcheck

- **Unsere Threat Intelligence sucht im Darknet und anderen schwer zugänglichen Bereichen (u.a. Telegramm und IRC) des Internets nach gestohlenen Daten, Bedrohungen und potenziellen Angriffen. Sobald etwas auffälliges gefunden wird, gibt es eine entsprechende Alarmierung.**

Domainwatch

- **Häufig stellen Cyberkriminelle gezielt manipulierte und ähnlich klingende Webseiten ins Internet, um Daten von Usern abzufischen und dann zu ihren Gunsten zu nutzen. Sollte eine ähnliche Webseite im Internet online gestellt werden, bekommen die Kunden eine Alarmierung.**

Partner & Supplier

- **Erstellen Sie detaillierte Berichte über die Cyberrisiken Ihrer Partner und Zulieferer, um deren Sicherheitsstatus ebenfalls zu überprüfen. Dieser Bereich spielt auch eine immer größere Rolle bei den Themen, Lieferkettengesetz‘ und / oder NIS2.**

Unsere erstklassigen Dienstleistungen werden Ihnen dabei helfen, den Reifegrad in der Cybersicherheit nachweisend zu steigern.

Wir sind bereit, Ihnen bei den kommenden IT-Projekten mit unserem Fachwissen zu helfen.

Blick
in die Zukunft

Die Zukunft der Cybersicherheit wird von einer Reihe von Trends und Entwicklungen geprägt sein, die auf die ständig wachsenden und sich verändernden Bedrohungen im digitalen Raum reagieren. Hier sind einige Schlüsselaspekte der zukünftigen Cybersicherheit.

Künstliche Intelligenz und maschinelles Lernen

Diese Technologien werden immer mehr in Sicherheitslösungen integriert, um Anomalien zu erkennen, Bedrohungen vorherzusagen und automatisierte Reaktionen auf Vorfälle zu ermöglichen.

IoT-Sicherheit

Mit der zunehmenden Verbreitung von Internet of Things (IoT)-Geräten werden Sicherheitslösungen notwendig, die diese Geräte absichern und sie vor Missbrauch schützen.

Zero-Trust-Modell

Dieses Modell geht davon aus, dass niemandem, weder innerhalb noch außerhalb des Netzwerks, uneingeschränktes Vertrauen geschenkt werden sollte. Jede Aktivität und jeder Zugriff wird permanent überprüft und validiert.

Cloud-Sicherheit

Da immer mehr Unternehmen auf Cloud-Dienste umsteigen, wird die Sicherheit dieser Dienste eine kritische Rolle spielen. Cloud-orientierte Sicherheitslösungen und -praktiken werden weiterentwickelt, um Daten und Anwendungen zu schützen.

Sicherheit für kritische Infrastrukturen

Die Sicherheit von kritischen Infrastrukturen wie Energieversorgung, Verkehrssystemen und Gesundheitswesen wird eine wachsende Priorität darstellen, da Angriffe auf diese Systeme erhebliche Auswirkungen auf die Gesellschaft haben könnten.

Menschliche Faktoren

Der Faktor Mensch bleibt eine der größten Schwachstellen in der Cybersicherheit. Schulungen und Sensibilisierungsmaßnahmen werden wichtiger denn je sein, um Mitarbeiter vor sozialen Engineering-Angriffen zu schützen.

Die Zukunft der Cybersicherheit wird von einer Mischung aus fortschrittlichen Technologien, neuen Sicherheitsansätzen und erhöhtem Bewusstsein für die Bedeutung der Sicherheit im digitalen Zeitalter geprägt sein.