Erhöhung der Informationssicherheit

Die EU-Richtlinie NIS 2 ersetzt die Vorgängerversion, die strengere Cybersicherheitsstandards für Unternehmen mit mindestens 50 Mitarbeitenden und 10 Millionen Euro Umsatz in bestimmten Sektoren vorschreibt. Die Verschärfung wurde als Reaktion auf die erhöhte Bedrohung von kritischen Infrastrukturen durch digitale Angriffe eingeführt, um solche potenziell katastrophalen Angriffe zu verhindern.

Die Einführung der Network and Information Systems Directive 2 (NIS-2) soll den Schutz der kritischen Infrastrukturen erhöhen. Seit dem Beginn des Ukrainekriegs 2022 haben Angriffe auf Stromversorger, Atomkraftwerke und weitere Betriebe zugenommen. In der Richtlinie steht als erster Punkt «Das Ziel der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates war der unionsweite Aufbau von Cybersicherheitskapazitäten, die Eindämmung von Bedrohungen für Netz- und Informationssysteme, die zur Erbringung wesentlicher Dienste in Schlüsselsektoren verwendet werden, und die Sicherstellung der Kontinuität solcher Dienste bei Vorfällen, um so zur Sicherheit der Union und zum reibungslosen Funktionieren ihrer Wirtschaft und Gesellschaft beizutragen.»

Dir Richtlinie definiert im Wesentlichen die folgenden Punkte:

- Nationale Cybersicherheitsstrategie
- Rolle der Behörden bei Cybersicherheitsvorfällen
- Cybersecurity Incident Response Team (CSIRT)
- Europäische Schwachstellendatenbank
- Verpflichtung der Leitung
- Risikomanagement
- Meldung von Vorfällen
- Sanktionen und Bussgelder

Die Richtlinie unterscheidet zwischen Sektoren mit hoher Kritikalität (Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, Digitale Infrastruktur, Verwaltung von IKT-Dienste (B2B), öffentliche Verwaltung sowie Weltraum) und sonstige kritische Sektoren (Post- und Kurierdienste, Abfallbewirtschaftung, Produktion, Herstellung und Handel mit chemischen Stoffen, Produktion, Verarbeitung und Vertrieb von Lebensmitteln, Verarbeitendes Gewerbe/Herstellung von Waren, Anbieter digitaler Dienste, Forschung). Es ist ersichtlich, dass es sehr viele Unternehmen betrifft. Allein in Deutschland sind schätzungsweise zwischen 29'000 bis 40'000 Unternehmen von der NIS 2 betroffen und müssen in der Folge ein Informationssicherheitsmanagementsystem (ISMS) implementieren.

Die Richtlinie unterscheidet weiter zwischen wesentlichen und wichtigen Einrichtungen (Artikel 3). Dies ist vor allem für die Haftung wichtig, die verschärft wurde. Für wesentliche Einrichtungen können Sanktionen von bis zu 10 Millionen Euro oder 2 Prozent des Jahresumsatzes verhängt werden, wobei der höhere Betrag massgeblich ist. Bei wichtigen Einrichtungen belaufen sich die Bussgelder auf bis zu 7 Millionen Euro oder 1,4 Prozent des Jahresumsatzes, wobei auch hier der höhere Betrag entscheidend ist. Im deutschen Entwurf haften die Leitungsorgane für die Einhaltung der Risikomanagementmassnahmen mit ihrem Privatvermögen bis zur Obergrenze von 2 Prozent des globalen Jahresumsatzes des Unternehmens.

Artikel	BSI-Gesetz	Anforderungen	ISO 27001:2022	
21.2 a)	§ 30 (4) 1	Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme	5.2	Politik
			6.1.2	Informationssicherheitsrisikobeurteilung
			6.1.3	Informationssicherheitsrisikobehandlung
			8.2	Informationssicherheitsrisikobeurteilung
			8.3	Informationssicherheitsrisikobehandlung
			A.5.1	Informationssicherheitsrichtlinien
21.2 b)	§ 30 (4) 2	Bewältigung von Sicherheitsvorfällen	A.5.24	Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen
			A.5.25	Beurteilung und Entscheidung über Informationssicherheitsereignisse
			A.5.26	Reaktion auf Informationssicherheitsvorfälle
			A.5.27	Erkenntnisse aus Informationssicherheitsvorfällen
			A.5.28	Sammeln von Beweismaterial
			A.6.8	Meldung von Informationssicherheitsereignissen
21.2 c)	§ 30 (4) 3	Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement	A.5.29	Informationssicherheit bei Störungen
			A.5.30	IKT-Bereitschaft für Business Continuity
			A.8.13	Sicherung von Information
			A.8.14	Redundanz von informationsverarbeitenden Einrichtungen
21.2 d)	§ 30 (4) 4	Sicherheit der Lieferkette einschliesslich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern	A.5.19	Informationssicherheit in Lieferantenbeziehungen
			A.5.20	Behandlung von Informationssicherheit in Lieferantenvereinbarungen
			A.5.21	Umgang mit der Informationssicherheit in der Lieferkette der Informations- und Kommunikationstechnologie (IKT)
			A.5.22	Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen
			A.5.23	Informationssicherheit für die Nutzung von Cloud-Diensten
21.2 e)	§ 30 (4) 5	Sicherheitsmassnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschliesslich Management und Offenlegung von Schwachstellen	A.5.37	Dokumentierte Bedienabläufe
			A.8.8	Handhabung von technischen Schwachstellen
			A.8.9	Konfigurationsmanagement
			A.8.20	Netzwerksicherheit
			A.8.21	Sicherheit von Netzwerkdiensten
21.2 f)	§ 30 (4) 6	Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmassnahmen im Bereich der Cybersicherheit	9.1	Überwachung, Messung, Analyse und Bewertung
			9.2	Internes Audit
			9.3	Managementbewertung
			A.5.35	Unabhängige Überprüfung der Informationssicherheit

Die geforderten Massnahmen im Vergleich zur ISO 27001.

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

In Artikel 20 verlangt die Richtlinie, «dass die Mitglieder der Leitungsorgane wesentlicher und wichtiger Einrichtungen an Schulungen teilnehmen müssen, und fordern wesentliche und wichtige Einrichtungen auf, allen Mitarbeitenden regelmässig entsprechende Schulungen anzubieten, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.»

Ein wesentlicher Artikel ist die 21: Risikomanagementmassnahmen im Bereich der Cybersicherheit. Unternehmen müssen geeignete und verhältnismässige technische, operative und organisatorische Massnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten.

In Artikel 23 werden die Berichtspflichten aufgeführt. Die Grenzen sind sehr eng gefasst. Für schwerwiegende Vorfälle gelten folgende Fristen:

23.4 a) § 31 (1) 1
unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntnisnahme des erheblichen Sicherheitsvorfalls, eine Frühwarnung, in der gegebenenfalls angegeben wird, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte;

23.4 b) § 31 (1) 2
unverzüglich, in jedem Fall aber innerhalb von 72 Stunden nach Kenntnisnahme des erheblichen Sicherheitsvorfalls, eine Meldung über den Sicherheitsvorfall aktualisiert werden und eine erste Bewertung des erheblichen Sicherheitsvorfalls, einschliesslich seines Schweregrads und seiner Auswirkungen sowie gegebenenfalls die Kompromittierungsindikatoren angegeben werden;

23.4 b) § 31 (1) 3
auf Ersuchen eines CSIRT oder gegebenenfalls der zuständigen Behörde einen Zwischenbericht über relevante Statusaktualisierungen;

23.4 d) § 31 (1) 4
spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls einen Abschlussbericht zustellen

Da es sich um eine Richtlinie handelt, müssen die Mitgliedstaaten diese in nationales Recht umwandeln. Die Deadline für die Umsetzung als Gesetz ist der 17. Oktober 2024. Nach Artikel 40 der Richtlinie prüft die EU-Kommission bis zum 17. Oktober 2027 die Einhaltung dieser Richtlinie und dann alle 36 Monate wieder. Bis dahin sollten auch alle Unternehmen die Anforderungen umgesetzt haben.

Die NIS 2 kann unter https://eur-lex.europa.eu/eli/dir/2022/2555 oder mittels QR-Code in verschiedenen Sprachen heruntergeladen werden.

Artikel	BSI-Gesetz	Anforderungen	ISO 27001:2022	
21.2 g)	§ 30 (4) 7	grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit	7.3 7.4 A.6.3	Bewusstsein Kommunikation Informationssicherheitsbewusstsein, -ausbildung und -schulung
21.2 h)	§ 30 (4) 8	Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung	A.8.24	Verwendung von Kryptographie
21.2 i)	§ 30 (4) 9	Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen	A.5.9 A.5.10 A.5.15 A.5.16 A.5.17 A.5.18 A.6.1 A.6.2 A.6.4 A.6.5 A.6.6	Inventar der Informationen und anderen damit verbundenen Werten Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten Zugangssteuerung Identitätsmanagement Informationen zur Authentifizierung Zugangsrechte Sicherheitsüberprüfung Beschäftigungs- und Vertragsbedingungen Massregelungsprozess Verantwortlichkeiten nach Beendigung oder Änderung der Beschäftigung Vertraulichkeits- oder Geheimhaltungsvereinbarungen
21.2 j)	§ 30 (4) 10	Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung	A.5.14 A.5.16 A.5.17	Informationsübertragung Identitätsmanagement Informationen zur Authentifizierung
21.3		Sicherheit der Entwicklungsprozesse	A.8.25 A.8.26 A.8.27 A.8.28 A.8.29 A.8.30 A.8.31 A.8.32 A.8.33	Lebenszyklus einer sicheren Entwicklung Anforderungen an die Anwendungssicherheit Sichere Systemarchitektur und technische Grundsätze Sichere Kodierung Sicherheitsprüfung in Entwicklung und Abnahme Ausgegliederte Entwicklung Trennung von Entwicklungs-, Prüf- und Produktionsumgebungen Änderungssteuerung Informationen zur Prüfung
21.4		angemessenen und verhältnismässigen Korrekturmassnahmen	10.2	Nichtkonformität und Korrekturmassnahmen