NIS2 - NEUE CYBERSECURITY-PFLICHTEN FÜR UNTERNEHMEN UND ÖFFENTLICHE EINRICHTUNGEN

Stephan Schmidt | TCI Rechtsanwälte

21.03.2024

WiTCOM
Digital. Vernetzt.

TCILAW.DE

Umsetzung der NIS-2 in Deutschland

- Richtlinie und keine Verordnung – „Europäische Überformung mit nationalstaatlichem Beurteilungsspielraum“
- Mitgliedstaaten müssen bis 17.10.2024 in nationales Recht umsetzen (Vorgängerregelung NIS-1 wird zum 18.10.2024 aufgehoben)

- Umsetzung erfolgt durch das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG*)
- Änderungsgesetz, das bestehende Gesetze ändert, insbesondere die KRITIS-Teile des BSI-Gesetzes
- Erfüllungsaufwand für die deutsche Wirtschaft: Jährlich 2,3 Milliarden Euro und für die erstmalige Einrichtung von Prozessen und Meldewegen 2 Milliarden Euro

- Neben NIS-2 wird das KRITIS-Dachgesetz kritische Betreiber regulieren (hierzu liegt seit Dezember 23 ein zweiter Referentenentwurf vor) – Begrifflichkeiten, Schwellenwerte, Zuordnungskriterien und Registrierungsanforderungen sollen harmonisiert werden

* alle Angaben zu §§ basieren auf dem BSIG-E des Referentenentwurf (Stand 22.12.2023)

Was bisher geschah…

NIS-2 Richtlinie

Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union

73 Seiten

1. Referentenentwurf

Entwurf eines Gesetzes zur Umsetzung der NIS-2-RL und zur Regelung wesentlicher Grundzüge d. Informationssicherheits-managements in der Bundesverwaltung

243 Seiten

2. Referentenentwurf

Entwurf eines Gesetzes zur Umsetzung der NIS-2-RL und zur Regelung wesentlicher Grundzüge d. Informationssicherheits-managements in der Bundesverwaltung

146 Seiten

Diskussionspapier und Werkstattgespräch

Wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-RL in Deutschland

58 Seiten

3. Referentenentwurf (Stand 22.12.2023)

Entwurf eines Gesetzes zur Umsetzung der NIS-2-RL und zur Regelung wesentlicher Grundzüge d. Informationssicherheits-managements in der Bundesverwaltung

163 Seiten

NIS2UmsuCG

Entwurf steckt derzeit mit Versendewiderspruch in der Ressortabstimmung fest

Verbändebeteiligung soll noch erfolgen

Grundlagen

- Cybersicherheit nicht nur für Kritische Infrastrukturen, sondern flächendeckend als allgemeine Compliance-Anforderung für die Wirtschaft (vgl. bereits nationales IT-SiG 2.0)
- NIS-2 ist mehr als nur ein Regelwerk – sie ist ein Handlungsaufruf, IT-Sicherheit zu etablieren, eine widerstandsfähige Organisation zu schaffen und aufrecht zu erhalten
- NIS-2 ist grundsätzlich anwendbar auf öffentliche + private Einrichtungen, die ihre Dienste in der Union erbringen oder ihre Tätigkeiten dort ausüben
- gilt für Sektoren mit hoher Kritikalität (Anlage 1) und sonstige kritische Sektoren (Anlage 2)

- auch Bundeseinrichtungen werden mit einigen Pflichten reguliert (§ 29)
- Einrichtungen der sozialen Sicherung und der Geschäftsbereich des Verteidigungsministeriums sowie öffentliche Verwaltung der Länder und Kommunen fallen nicht in den Anwendungsbereich

- Mitgliedstaaten erstellen bis zum 17.04.2025 eine Liste wesentlicher und wichtiger Einrichtungen

Unterschiede zur NIS-2 in der deutschen Umsetzung

- NIS2UmsuCG übernimmt die in der NIS verwendeten Begriffe und die Unterscheidung zwischen „wesentlichen“ und „wichtigen“ Einrichtungen nicht
- betroffene Einrichtungen werden in drei Kategorien unterteilt:
  - kritische Anlagen, besonders wichtige Einrichtungen und wichtige Einrichtungen
  - und in mittlere Unternehmen und Großunternehmen
- aus den bisherigen KRITIS-Betreibern (als Kritische Infrastruktur regulierte Anlagen), werden „Betreiber kritischer Anlagen“ (§28 Abs. 5) allein aufgrund der sachlichen Schwellenwerte
- KRITIS-Betreiber werden gleichzeitig zu „besonders wichtige Einrichtungen“ (§ 28 Abs. 1 Nr. 4).
- die bisherige KRITIS-Logik mit KRITIS-Sektoren, kritischen Dienstleistungen und KRITIS-Anlagen mit sachlichen Schwellenwerten soll weiterhin gelten, aber Streichung des Sonderwegs zu „Unternehmen im besonderen öffentlichen Interesse“

Sektoren (NIS2)

Sektoren mit hoher Kritikalität (Anhang I)	Sonstige kritische Sektoren (Anhang II)
Energie	Post- und Kurierdienste
Verkehr	Abfallbewirtschaftung
Bankwesen	Produktion, Herstellung und Handel mit chem. Stoffen
Finanzmarktinfrastrukturen	Produktion, Verarbeitung und Vertrieb von Lebensmitteln
Gesundheitswesen	Verarbeitendes Gewerbe/Herstellung von Waren, u.a. Datenverarbeitungsgeräte, Maschinenbau, Kraftwagen, Kraftwagenteile, Fahrzeugbau
Trinkwasser	Anbieter digitaler Dienste
Abwasser	Forschungseinrichtungen
Digitale Infrastruktur	
Verwaltung von IKT-Diensten	
Öffentliche Verwaltung, v.a. Zentralregierungen und regionale Ebene mit kritische gesellschaftlicher / wirtschaftlicher Bedeutung	
Weltraum	

Sektoren (NIS2UmsuCG)

Sektoren für kritische Anlagen (§ 28 Abs. 6)	Sektoren mit hoher Kritikalität (Anlage 1)	Sonstige kritische Sektoren (Anlage 2)
Energie	Energie	Transport und Verkehr
Transport und Verkehr	Transport und Verkehr	Siedlungsabfallentsorgung
	Bankwesen	Produktion, Herstellung und Handel mit chem. Stoffen
Finanz- und Versicherungswesen	Finanz- und Versicherungswesen	Produktion, Verarbeitung und Vertrieb von Lebensmitteln
Gesundheitswesen	Gesundheit	Verarbeitendes Gewerbe/Herstellung von Waren, u.a. Medizinprodukte, Datenverarbeitungsgeräte, Maschinenbau, Kraftwagen, Kraftwagenteile, Fahrzeugbau
Trinkwasser und Abwasser	Wasser und Abwasser	Anbieter digitaler Dienste
Informationstechnik und Telekommunikation	Informationstechnik und Telekommunikation	Forschung
Weltraum	Weltraum	
Ernährung		
Siedlungsabfallentsorgung		

www.NIS2-Check.de

Sektoren mit hoher Kritikalität

- Nr. 8 – Digitale Infrastruktur: Cloud-Computing-Dienste
  - Anbieter von Cloud-Computing-Diensten (ErwG 33): „[…] digitale Dienste […], die auf Abruf die Verwaltung und den umfassenden Fernzugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglichen[…]“
- Nr. 8 – Digitale Infrastruktur: Rechenzentrumsdienste
  - Anbieter von Rechenzentrumsdiensten (ErwG 35): „[…] Dienste […], mit denen Strukturen oder Gruppen von Strukturen für die zentrale Unterbringung, die Verbindung und den Betrieb von Informationstechnologie (IT) und Netzausrüstungen zur Erbringung von Datenspeicher- , Datenverarbeitungs- und Datentransportdiensten […]“
- Nr. 9 – Verwaltung von IKT-Diensten (B2B): Anbieter verwalteter Dienste
  - Anbieter verwalteter Dienste (Art. 6 Nr. 39): „eine Einrichtung, die Dienste im Zusammenhang mit der Installation, der Verwaltung, dem Betrieb oder der Wartung von IKT-Produkten, Netzen, Infrastruktur, Anwendungen oder jeglicher anderer Netz- und Informationssysteme durch Unterstützung oder aktive Verwaltung erbringt, die entweder in den Räumlichkeiten der Kunden oder aus der Ferne erbringt“
- Nr. 9 – Verwaltung von IKT-Diensten (B2B): Anbieter verwalteter Sicherheitsdienste
  - Anbieter verwalteter Sicherheitsdienste (Art. 6 Nr. 40): „einen Anbieter verwalteter Dienste, der Unterstützung für Tätigkeiten im Zusammenhang mit dem Risikomanagement im Bereich der Cybersicherheit durchführt oder erbringt“

Sonstige kritische Sektoren

- Nr. 5 – Verarbeitendes Gewerbe: Datenverarbeitungsgeräte, elektronische und optische Erzeugnisse
  - NACE Rev. 2, Abschnitt C Abteilung 26 - Herstellung von Computern, peripheren Geräten, Telekommunikationsgeräten und ähnlichen elektronischen Erzeugnissen sowie von entsprechenden Produktkomponenten
  - Herstellung von Geräten der Unterhaltungselektronik, Mess-, Kontroll-, Navigations- und Steuerungsinstrumenten, […] sowie magnetischen und optischen Datenträgern
- Nr. 5 – Verarbeitendes Gewerbe: elektrische Ausrüstungen
  - NACE Rev. 2, Abschnitt C Abteilung 27 - Diese Abteilung umfasst die Herstellung von Produkten, die Elektrizität erzeugen, verteilen und verwenden. Diese Abteilung umfasst ferner die Herstellung elektrischer Beleuchtungs- und Signalgeräte sowie elektrischer Haushaltsgeräte.

Wer ist betroffen? (§ 28)

Size-Cap-Rule

- Besonders wichtige Einrichtungen nach Größe des Unternehmens in Sektoren der Anlage 1, wenn sie **250 oder mehr Mitarbeitende** beschäftigen **oder** einen Jahresumsatz von **über 50 Mio. EUR** und eine Bilanzsumme von **über 43 Millionen Euro** haben
- Wichtige Einrichtungen nach Größe des Unternehmens in Sektoren aus Anlage 1 und 2, wenn sie **50 oder mehr Mitarbeitende** beschäftigen **oder** einen Jahresumsatz **und** eine Jahresbilanzsumme von **über 10 Millionen Euro** haben (Vertrauensdienste auch ohne Erfüllung der Schwellenwerte)

(zu bestimmen nach der Empfehlung der EU-Kommission (2003/361/EG))

ABER – UNTERNEHMEN KÖNNEN AUCH INDIREKT BETROFFEN SEIN

- die unter NIS-2 verpflichteten Unternehmen müssen „Sicherheit der Lieferkette“ gewährleisten
- verpflichtete Unternehmen werden ihre Cybersicherheitsverpflichtungen regelmäßig an Dienstleister und Zulieferer weitergeben

Wer ist betroffen? (§ 28)

- Daten von Partner- oder verbundenen Unternehmen im Sinne der Empfehlung 2003/361/EG sind **nicht hinzuzurechnen, wenn das Unternehmen** unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände mit Blick auf die Beschaffenheit und den Betrieb der informationstechnischen Systeme, Komponenten und Prozesse, **unabhängig** von seinem Partner oder verbundenen Unternehmen ist
- Ausschlüsse
  - DNS, TLD, Cloud-Computing, Rechenzentren, Content Delivery Networks, Managed Services und Managed Security Services, Online-Marktplätze, Online-Suchmaschinen, soziale Netzwerke und Vertrauensdienste sind von §30 Abs. 2 ausgenommen (§30 Abs. 3)
  - Gematik und Einrichtungen gem. Art. 2 (4) der Verordnung (EU) 2022/2554 (DORA) (§28) sind von bestimmten Pflichten von Einrichtungen ausgenommen (§28 Abs. 1)
  - Betreiber öffentlicher TK-Netze und TK-Dienste, Energieversorgungsnetze und Energieanlagen sind von bestimmten Anforderungen ausgenommen (§28 Abs. 4)

Anlagen und Einrichtungen

- unter „**kritische Anlagen**“ fallen beispielsweise Anlagen in den Sektoren Energie, Transport und Verkehr, Finanz- und Versicherungswesen, Gesundheitswesen, Trinkwasser, Abwasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum sowie Siedlungsabfallentsorgung, die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind (§28 Abs. 6)
- unter „**besonders wichtige Einrichtungen**“ fallen insb. **Großunternehmen** der Sektoren der Sektoren Energie, Transport und Verkehr, Finanz- und Versicherungswesen, Gesundheitswesen, Trinkwasser, Abwasser, Informationstechnik und Telekommunikation, Verwaltung von IKT-Diensten (Business-to-Business) oder Weltraum und **mittlere Unternehmen**, die Anbieter von Telekommunikationsdiensten oder öffentlich zugänglichen Telekommunikationsnetzen sind (§28 Abs. 1)
- unter „**wichtige Einrichtungen**“ fallen insb. **mittlere Unternehmen** aus den Sektoren Energie, Transport und Verkehr, Finanz- und Versicherungswesen, Gesundheitswesen, Trinkwasser, Abwasser, Informationstechnik und Telekommunikation, Verwaltung von IKT-Diensten (Business-to-Business) oder Weltraum und **mittlere Unternehmen oder Großunternehmen** der Sektoren Logistik, Siedlungsabfallentsorgung, Produktion, Chemie, Ernährung, verarbeitendes Gewerbe, Anbieter digitaler Dienste oder Forschung (§28 Abs. 2)

Anforderungen an Betreiber und Einrichtungen

- weitergehende Anforderungen an Cybersicherheit-Prävention durch TOM gem. „Stand der Technik“
- Ergreifung und Dokumentation von geeigneten, verhältnismäßigen und wirksamen technischen und organisatorischen Maßnahmen, um Störungen und Sicherheitsvorfälle zu verhindern (§ 30 Abs. 1)
- Nach § 30 Abs. 2 müssen diese Maßnahmen mindesten umfassen:

- Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik, Bewältigung von Sicherheitsvorfällen
- Aufrechterhaltung des Betriebs, Backup-Management, Wiederherstellung, Krisen-Management
- Sicherheit der Lieferkette und zwischen Einrichtungen
- Sicherheit bei Erwerb, Entwicklung und Wartung
- Management von Schwachstellen
- Bewertung der Effektivität von Cybersicherheit und Risiko-Management
- Cyberhygiene und Schulungen zur Cybersicherheit
- Kryptografie und Verschlüsselung
- Personalsicherheit, Zugriffskontrolle und Anlagen-Management
- Multi-Faktor Authentisierung und kontinuierliche Authentisierung
- Sichere Kommunikation (Sprach, Video- und Text)
- Sichere Notfallkommunikation
- Einsatz von Systemen zur Angriffserkennung (nur Betreiber kritischer Anlagen - § 31 Abs. 2)

Technische und organisatorische Maßnahmen

- Ergreifung von geeigneten, verhältnismäßigen und wirksamen technischen und organisatorischen Maßnahmen, um Störungen und Sicherheitsvorfälle zu verhindern (§ 30 Abs. 1)
- ob und welche Maßnahmen von einem Unternehmen konkret ergriffen werden müssen, hängt aber auch von weiteren Faktoren ab:
  - mögliche Durchführungsrechtsakte nach Art. 21 Abs. 5 NIS2 (Implementing Acts), welche verbindlich wären und Regelungen des BSIG vorgehen würden (§30 Abs. 4)
  - vom BMI erlassene Rechtsakte nach § 30 Abs. 5
  - vom Sektor und der konkreten Tätigkeit des Unternehmens

VORHANDENE MASSNAHMEN PRÜFEN UND ERGÄNZEN

- es sollte frühzeitig und unter Berücksichtigung der jeweiligen Umstände des Einzelfalls geprüft werden, ob die ergriffenen technischen und organisatorischen Maßnahmen die Vorgaben von NIS-2 und dem BSIG-E erfüllen oder welche zusätzlichen Maßnahmen ergriffen werden müssen

Registrierungspflicht

für besonders wichtige und wichtige Einrichtungen

- unter BISG-E/NIS-2 müssen sich alle betroffenen Unternehmen **selbst identifizieren** und beim Bundesamt für Sicherheit in der Informationstechnik spätestens innerhalb von drei Monaten **registrieren** (§ 33)
- Registrierung erfolgt unter Angabe verschiedener Unternehmensinformationen, u.a. unter Angabe des Sektors und Kontaktdaten
- BSI kann die Einzelheiten zur Ausgestaltung des Registrierungsverfahrens im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe festlegen. Die Festlegung erfolgt durch eine öffentliche Mitteilung auf der Webseite des BSI

- Verstoß gegen Registrierungspflicht ist bußgeldbewährte Ordnungswidrigkeit (§60 Abs. 2 Nr. 4)

Meldepflichten

BEI ERHEBLICHEN SICHERHEITSVORFÄLLEN SIND MINDESTENS DREI MELDUNGEN ABZUGEBEN (§ 32)

- frühe Erstmeldung (Frühwarnung) unverzüglich bzw. spätestens innerhalb von 24 Stunden nach Kenntniserlangung mit der Angabe, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte
- bestätigende Erstmeldung (aktualisierte Meldung) über den Sicherheitsvorfall unverzüglich bzw. spätestens innerhalb von 72 Stunden nach Kenntniserlangung mit Bestätigung oder Aktualisierung der Erstmeldung, mit einer ersten Vorfallsbewertung, einschließlich seines Schweregrads und seiner Auswirkungen
- auf Ersuchen des BSI Zwischenmeldung mit Statusaktualisierung
- Abschlussmeldung (Abschlussbericht) spätestens einen Monat nach Übermittlung der bestätigende Erstmeldung mit ausführliche Vorfallsbeschreibung mit Angaben zu Schweregrad und Auswirkungen, der Art der Bedrohung bzw. Vorfallsursache, zu Abhilfemaßnahmen und etwaigen grenzüberschreitenden Auswirkungen

Billigungs-,Überwachungs- und Schulungspflicht für Geschäftsleiter

- Geschäftsleiter besonders wichtiger Einrichtungen und wichtiger Einrichtungen trifft eine **Überwachungspflicht** (§38)
- Differenzierung wie in NIS-2 (Art. 20 und Art. 32 Abs. 6 NIS2) fehlt
- **Unklar, welche Möglichkeiten zur Delegation der Umsetzung bestehen** – insbesondere für Unternehmensgruppen schwierig
- §38 Abs. 2 sieht deutsche Sonderregelung hinsichtlich eines **Verbots des Verzichts auf Ersatzansprüche** vor
- Geschäftsleiter besonders wichtiger Einrichtungen und wichtiger Einrichtungen müssen regelmäßig an **Schulungen** teilnehmen (§38 Abs. 3)
- bisher unklar, welchen Inhalt die zu belegenden Schulungen haben müssen

- gestrichen wurde: „Mitarbeiter sollen regelmäßig an Schulungen teilnehmen“ – unvollständige Umsetzung von Art. 20 Abs. 2 NIS2)

Fristen

- Registrierung innerhalb von drei Monaten nach Identifizierung (§33 Abs. 1 und §33 Abs.2) und für bestimmte Einrichtungsarten (§63 Abs. 1 S. 1) bis zum 17. Januar 2025 (§34 Abs. 1)
- Änderungen müssen jährlich an das BSI gemeldet werden, „alle anderen Angaben“ unverzüglich spätestens jedoch (innerhalb) zwei Wochen ab dem Zeitpunkt, zu dem die Einrichtung Kenntnis von der Änderung erhalten hat (§ 33 Abs. 5)
- Teilnahme am Informationsaustausch innerhalb eines Jahres nach Inkrafttreten für Besonders wichtige Einrichtungen und Betreiber kritischer Anlagen (§30 Abs. 7)

Nur für Betreiber kritischer Anlagen:

- Erstmaliger Nachweis über Maßnahmenumsetzung spätestens zu einem vom BSI und BBK bei der Registrierung festgelegten Zeitpunkt, frühestens drei Jahre nachdem sie erstmals oder erneut als ein Betreiber einer kritischen Anlage gelten (§39 Abs. 1)
- bestehende KRITIS-Betreiber frühestens drei Jahre nach Erbringung des letzten Nachweises nach § 8a Absatz 3 BSI-Gesetz (§39 Abs. 3)
- Fortlaufende Nachweise über Maßnahmenumsetzung nach erstmaligem oder letztem Nachweis dann alle drei Jahre (§39 Abs. 1)

Sanktionsmöglichkeiten

- Unterscheidung der Einrichtungen ist überwiegend nur hinsichtlich der Sanktionen und des Aufsichtssystems relevant
  - maximalen Bußgeldhöhe
    - bei allgemeinen Tatbeständen 2 Mio. Euro (§60 Abs. 5)
    - bei wichtigen Einrichtungen 7 Mio. Euro oder bis zu 1,4 % des weltweiten Jahresumsatzes des Unternehmens, dem der Betroffene angehört, (§60 Abs. 6)
    - bei besonders wichtigen Einrichtungen 10 Mio. Euro oder bis zu 2 % des weltweiten Jahresumsatzes des Unternehmens, dem der Betroffene angehört, (§60 Abs. 7)
  - proaktives vs. reaktives Aufsichtssystems
  - Behörden dürfen verbindliche Anweisungen zur Beseitigung von Mängeln und Verstößen erlassen sowie Anweisungen erteilen, das entsprechende Verhalten einzustellen und nicht zu wiederholen oder nach bestimmten Vorgaben sicherzustellen, dass die Pflichten erfüllt werden, oder die Empfehlungen aus einer Sicherheitsüberprüfung umzusetzen
  - gegenüber besonders wichtigen Einrichtungen kann Anweisung erteilt werden, fristgebundene Maßnahmen zur Verhütung und Behebung eines Sicherheitsvorfalles vorzunehmen und Bericht zu erstatten (§64 Abs. 6)

Sanktionsmöglichkeiten

- BSI kann für besonders wichtige Einrichtungen einen Überwachungsbeauftragten benennen (§64 Abs.9)
- wenn eine besonders wichtige Einrichtung den Anweisungen einer Behörde nicht folgt, kann die Behörde nach §64 Abs. 10 als weitere Eskalationsstufe:
  - Genehmigungen für einen Teil oder alle von der Einrichtung erbrachten entsprechenden Dienste oder Tätigkeiten vorübergehend aussetzen und
  - den natürlichen Personen, die als Geschäftsführung oder gesetzliche Vertreter für Leitungsaufgaben in der besonders wichtigen Einrichtung zuständig sind, die Wahrnehmung der Leitungsaufgaben vorübergehend untersagen

  Beide Durchsetzungsmaßnahmen sind jedoch zeitlich bis zu dem Zeitpunkt begrenzt, in dem das Ziel, also die Umsetzung der Anweisung, erreicht wird

Mögliche Umsetzungspunkte

1. Betroffenheit ermitteln
2. Richtlinien für Risiken und Informationssicherheit erstellen und regelmäßig aktualisieren
3. Abhängigkeiten in der Lieferkette identifizieren – vertragliche Regelungen anpassen
4. Prävention, Erkennung und Bewältigung von IT-Sicherheits-Vorfällen sicherstellen
5. Prozesse für Backup-Management, Disaster Recovery und Krisenmanagement (inklusive Notfallkommunikation) definieren, dokumentieren und üben
6. IT-Sicherheitsmaßnahmen regelmäßig prüfen und bewerten
7. Verpflichtende Schulungen zum Thema IT-Sicherheit einführen
8. Richtlinien für Kryptografie und den Einsatz von Verschlüsselungstechnologien
9. (…)

Technology | Communication | Information

STEPHAN SCHMIDT

Rechtsanwalt

Fachanwalt für IT-Recht, CIPP/E

TCI Rechtsanwälte Mainz

+49 6131 30290460

sschmidt@tcilaw.de

Mitglied im | Member of
TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.
IT Security Association Germany