KRITIS – Nachweis angemessener IT-Sicherheit

Joachim Astel, 14.11.2023

noris network

KRITIS – Kritische Infrastruktur – Agenda

noris network

1. Einführung
2. Bedrohungen und Risiken
3. Sicherheitsmaßnahmen
4. Rechtliche und regulatorische Aspekte
5. Aktuelle Entwicklungen und Trends
6. Fallbeispiel: IT-Service-Provider
7. Ausblick, Q & A

Joachim Astel

Vita

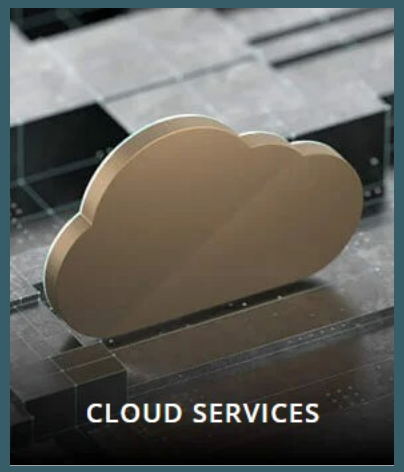
Joachim Astel ist Mitbegründer und Vorstand der **noris network** AG, in der er als Chief Regulatory Officer (CRO) die Bereiche Governance, Risk und Compliance, Zertifizierungen, Audits sowie die Interne Revision verantwortet. Darüber hinaus ist ihm das unternehmensweite Service-Prozess-Management und das „Security Operations Center“ zugeordnet.

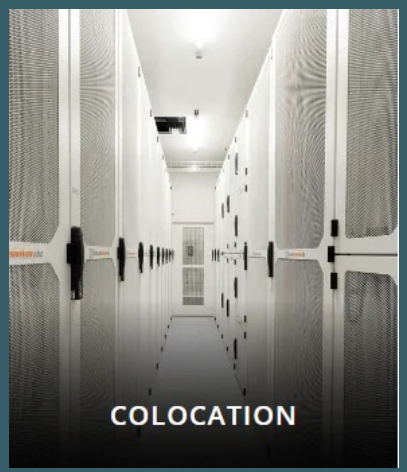
Gemeinsam mit seinen Kollegen Ingo Kraupa und Matthias Urlichs gründete Joachim Astel 1993 die noris network – als ersten Internet-Provider Nordbayerns. Früh erkannte der IT-Experte die wachsende Bedeutung des Themas IT-Security für Unternehmen und Gesellschaft.

Neben den Kerninteressen Security Management, Firewall- und IT-Security-Technologien gilt sein Hauptaugenmerk heute der Automatisierung und Optimierung von Geschäftsprozessen sowie dem Personalmanagement.

noris network

Cloud Services, Managed Services, IT-Outsourcing, Rechenzentren





TOP 100
top100.de
Top-Innovator 2023

Gründer in Unternehmens-führung seit **1993**

500 Mitarbeiter

145 Mio. € Umsatz

Über **16.500 m²** IT-Fläche

Insgesamt bis zu **34 MW** IT-Leistung

Einführung

KRITIS – Kritische Infrastrukturen

Definition von KRITIS:
Kritische Infrastrukturen (KRITIS) umfassen Sektoren und Einrichtungen, deren Ausfall oder Beeinträchtigung schwerwiegende Folgen für die öffentliche Sicherheit, das Gemeinwesen oder andere lebenswichtige Funktionen hätte.

Beispiele für KRITIS-Sektoren:
Dazu gehören Sektoren wie

- Energieversorgung
- Wasserwirtschaft
- Gesundheitswesen
- Transport
- Telekommunikation
- Finanzwesen

und weitere, die essenziell für das Funktionieren einer Gesellschaft sind.

Bedeutung von KRITIS:
Diese Infrastrukturen bilden das Rückgrat der modernen Gesellschaft und Wirtschaft. Ihr Schutz ist entscheidend, da Störungen oder Angriffe in diesen Bereichen weitreichende Auswirkungen auf das tägliche Leben haben können.

Herausforderungen und Risiken:
KRITIS ist ständig Risiken ausgesetzt, sei es durch Naturkatastrophen, menschengemachte Bedrohungen oder immer fortschrittlichere Angriffe aus dem Internet.

Regulatorik zu KRITIS

NIS, IT-Sicherheitsgesetz, KRITIS

Wichtige Rolle von KRITIS für die Gesellschaft und Wirtschaft

NIS-Richtlinie (Europäische Union):
Die NIS-Richtlinie ist eine EU-weite Regelung, die darauf abzielt, die Sicherheit von **N**etz- und **I**nformations-**S**ystemen (NIS) in der EU zu verbessern und die **Resilienz** (Widerstandsfähigkeit) **Kritischer Infrastrukturen** gegen Cyberangriffe zu stärken.

Sie legt Mindestsicherheitsanforderungen für Betreiber von wesentlichen Diensten (OES) und Digital Service Providern (DSP) fest und erfordert die Meldung von schwerwiegenden Sicherheitsvorfällen an nationale Behörden.

BSI-Gesetz (BSIG) bzw. IT-Sicherheitsgesetz 2.0 (IT-SiG) in Deutschland:
Das IT-Sicherheitsgesetz in Deutschland legt Sicherheitsanforderungen insbesondere für Betreiber kritischer Infrastrukturen fest und verpflichtet sie, angemessene Maßnahmen zum Schutz vor Cyberbedrohungen zu ergreifen und Sicherheitsvorfälle zu melden.

BSI-Kritisverordnung (BSI-KritisV) für Kritische Infrastruktur (KRITIS):
KRITIS umfasst Sektoren, deren Störungen schwerwiegende Folgen haben könnten. Die Regulatorik wie die NIS-Richtlinie und das IT-Sicherheitsgesetz verlangen von Betreibern dieser Infrastrukturen, angemessene Sicherheitsmaßnahmen zu implementieren und Sicherheitsvorfälle zu melden.

Bedrohungen und Risiken

noris network

Kritische Infrastrukturen sind einer Vielzahl von Bedrohungen und Risiken ausgesetzt, die ihre Stabilität und Funktionsfähigkeit beeinträchtigen können. Diese Risiken können aus verschiedenen Quellen stammen:

1. **IT-Sicherheitsbedrohungen:**
   Angriffe – wie zum Beispiel durch Malware, Phishing-Angriffe, Ransomware, Denial-of-Service-Angriffe (DDoS) und andere Formen von Hacking-Aktivitäten – stellen eine massive Bedrohung für IT-Systeme und Netzwerke Kritischer Infrastrukturen dar. Solche Angriffe können zu Datenverlust, Systemausfällen, Betriebsunterbrechungen oder sogar zur Beeinträchtigung lebenswichtiger Dienste führen.

2. **Naturkatastrophen:**
   Erdbeben, Überschwemmungen, Stürme, Waldbrände oder extreme Wetterereignisse können schwerwiegende Auswirkungen auf Kritische Infrastrukturen haben. Sie können physische Infrastrukturen beschädigen, Stromausfälle verursachen, Transportwege blockieren oder Wasserversorgungssysteme beeinträchtigen, was zu erheblichen Störungen führt.

3. **Menschengemachte Gefahren:**
   Diverse Szenarien wie terroristische Anschläge, Sabotage, Industriespionage oder unbeabsichtigte menschliche Fehler können die Sicherheit und Stabilität von Kritischen Infrastrukturen gefährden.

4. **Unfallszenarien:**
   Unfälle – sei es in der industriellen Produktion, im Verkehrswesen oder in anderen kritischen Sektoren – können erhebliche Auswirkungen auf die Funktionsfähigkeit von Kritischen Infrastrukturen haben. Diese Unfälle können zu Betriebsstörungen, Umweltschäden und sogar zu Personenschäden führen.

Die Vielfalt der Bedrohungen erfordert eine ganzheitliche Herangehensweise an die Sicherheit von Kritischen Infrastrukturen, einschließlich präventiver Maßnahmen, um Risiken zu minimieren, sowie Pläne und Strategien zur Reaktion und Wiederherstellung im Falle eines Vorfalls – sowohl auf technischer als auch organisatorischer Ebene.

KRITIS-Sektoren

Regulierte Kritische Infrastrukturen

… durch das Bundesamt für Sicherheit in der Informationstechnik (BSI):

1. **Energie:** Elektrizität, Gas, Mineralöl, Fernwärme (§ 2 BSI-KritisV)
2. **Wasser:** Öffentliche Wasserversorgung, öffentliche Abwasserbeseitigung (§ 3 BSI-KritisV)
3. **Ernährung:** Ernährungswirtschaft, Lebensmittelhandel (§ 4 BSI-KritisV)
4. **IT und Telekommunikation:** Telefon- und Internetanbieter, Datenübertragung, Housing, IT-Hosting,, PKIs (§ 5 BSI-KritisV)
5. **Gesundheit:** Medizinische Versorgung, Arzneimittel und Impfstoffe, Labore (§ 6 BSI-KritisV)
6. **Finanz- und Versicherungswesen:** Kreditinstitute, Börsen, Versicherungen, Finanzdienstleister (§ 7 BSI-KritisV)
7. **Transport und Verkehr:** Luftfahrt, See- und Binnenschifffahrt, Schienenverkehr, Straßenverkehr, Logistik (§ 8 BSI-KritisV)
8. **Siedlungsabfallentsorgung:** Sammlung, Beförderung, Verwertung, Beseitigung (ab 01.01.2024)
9. **Unternehmen im besonderen öffentlichen Interesse (UBI):** Firmen mit hoher inländischer Wertschöpfung (seit 2021)
10. **Anlagen für Liquid Natural Gas (LNG):** Einfuhr, Entladung, vorübergehende Speicherung, Einspeisung
11. **Seekabellandestationen:** Anbindungspunkt für Seekabel zur Sprach- und Datenübertragung

Kriterien sind typischerweise **„mehr als 500.000 versorgte Personen“**, je nach Sektor drückt sich das in anderen Schwellenwerten aus, z. B. im Bereich Gesundheitswesen „30.000 vollstationäre Fälle in einem Krankenhaus pro Jahr“ oder im Sektor Ernährung „Hergestellte Lebensmittel in Tonnen/Jahr“ (vgl. Anhang 1–7 BSI-KritisV).

… durch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK):

1. **Staat und Verwaltung:** Regierung und Verwaltung, Parlament, Justizeinrichtungen, Notfall-/Rettungswesen einschließlich Katastrophenschutz – nicht im BSI-Gesetz reguliert
2. **Medien und Kultur:** Rundfunk (Fernsehen und Radio), gedruckte und elektronische Presse, Kulturgut und symbolträchtige Bauwerke – nicht im BSI-Gesetz reguliert

Quelle: Wikipedia

Interdependenzen durch KRITIS

Sind auch KMUs durch KRITIS betroffen?

Kleine und mittlere Unternehmen (KMU) dürften aufgrund ihrer Größe und der damit verbundenen geringeren Kritikalität nur in seltenen Fällen direkt unter das IT-Sicherheitsgesetz (KRITIS) fallen, jedoch ist Folgendes zu beachten:

1. **Lieferanten und Dienstleister von KRITIS-Unternehmen:**

   Kleine und mittlere Unternehmen, die Lieferanten bzw. Dienstleister von Einrichtungen bzw. Unternehmen der **Kritischen Infrastruktur** sind, können integraler Bestandteil der Wertschöpfungskette sein. Ihre Einbindung in den Prozess kann die Sicherheit und Funktionsfähigkeit der Kritischen Infrastrukturen direkt beeinflussen.

   Selbst wenn ein mittleres oder kleines Unternehmen nicht direkt zur Kritischen Infrastruktur gehört, können Störungen oder Sicherheitsvorfälle in diesem Unternehmen aufgrund der Vernetzung und der Abhängigkeiten zu einem **Kaskadeneffekt** führen, der sich auf andere Betreiber von Kritischen Infrastrukturen ausbreitet.

   Diese Abhängigkeiten können dazu führen, dass sich Störungen oder Ausfälle von einer Kritischen Infrastruktur auf andere Bereiche ausweiten. Dies kann die Funktionalität lebenswichtiger Dienste beeinträchtigen und somit die Sicherheit und das Wohlergehen der Bevölkerung gefährden. Die Sicherheit der Lieferkette muss demnach gewährleistet bleiben.

   Angesichts dieser nicht-linearen Interdependenzen ist es entscheidend, dass alle Akteure, einschließlich mittlerer und kleiner Unternehmen, angemessene Sicherheitsmaßnahmen ergreifen und mögliche Risiken erkennen, um die Resilienz des Gesamtsystems zu stärken. Entsprechende Meldewege einzuhalten, ist wichtig, damit im Ernstfall eine Störung der KRITIS-Anlage gemäß § 8b (4) BSI-Gesetz an das BSI gemeldet werden kann.

2. **IT-Sicherheitsgesetz 3.0**

   Das kommende IT-Sicherheitsgesetz wird mehr Unternehmen, ggf. auch Kleinere, in den Fokus nehmen.

Sicherheitsmaßnahmen

IT-Sicherheit und Resilienz

1. **Risikobewertung und -Management für Kritische Infrastrukturen:**
   Die Risikobewertung und -managementprozesse umfassen die systematische Identifizierung, Analyse und Bewertung potenzieller Risiken, die die Infrastrukturen beeinträchtigen könnten. Ziel ist es, die Bedrohungen zu verstehen, Schwachstellen zu identifizieren und angemessene Maßnahmen zur Risikominderung bzw. –vermeidung zu ergreifen.

2. **Schutzmaßnahmen gegen IT-Sicherheits-Angriffe:**
   Angemessene Schutzmaßnahmen gegen IT-Sicherheits-Angriffe umfassen technische, organisatorische und personelle Maßnahmen. Dazu gehören Netzwerk-Sicherheitslösungen, Zugangs- und Zugriffskontrollen, Systeme zur Angriffserkennung, regelmäßige Software-Updates, Awareness-Trainings für Mitarbeiter und adäquate Wiederanlaufverfahren im Schadensfall, wie etwa funktionsfähige Backups im Restorefall, entsprechende Notfallpläne.

3. **Resilienz und Notfallplanung (Business Continuity Management):**
   Resilienz bezieht sich auf die Widerstandsfähigkeit gegen Störungen, sich anzupassen und sich nach einem Vorfall schnell zu erholen. Die Notfallplanung konzentriert sich darauf, angemessene Strategien und Maßnahmen zu entwickeln, um auf kritische Vorfälle oder Ausfälle angemessen reagieren zu können und die Auswirkungen auf die Funktionsfähigkeit des Systems zu minimieren. Im Zusammenspiel zwischen KRITIS-Unternehmen und Lieferanten/Dienstleister können gemeinsam abgestimmte Notfallpläne, beiderseitige Zuständigkeiten und Kommunikationsketten (Meldewege, Ansprechpartner) und gemeinschaftliche Notfallübungen hilfreich sein.

4. **Zertifizierung zum Nachweis angemessener IT-Sicherheit:**
   Verschiedene Zertifizierungen und Standards wie **ISO 27001** oder branchenspezifische Zertifizierungen dienen als „**Nachweis angemessener Sicherheit“**. Darüber hinaus können für KRITIS-Unternehmen Zertifizierungen nach **BSI-Gesetz § 8a** verpflichtend sein. Durch die Zertifizierung können Konformität und Effektivität in der IT-Sicherheit demonstriert werden.

Branchenspezifische B3S-Kataloge

des Bundesamts für Sicherheit in der Informationstechnik

B3S im Sektor Energie:
- Sicherheitsstandard für Anlagen oder Systeme zur Steuerung/Bündelung elektrischer Leistung
- Sicherheitsstandard für die Verteilung von Fernwärme (Fernwärmenetze)

B3S im Sektor Wasser:
- Sicherheitsstandard Wasser/Abwasser

B3S im Sektor Ernährung:
- Sicherheitsstandard für die Ernährungsindustrie
- Sicherheitsstandard für den Lebensmittelhandel

B3S im Sektor IT und Telekommunikation:
- Sicherheitsstandard für Housing, Hosting und Content-Delivery-Networks

B3S im Sektor Gesundheit:
- Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus

B3S im Sektor Finanz- und Versicherungswesen:
- Sicherheitsstandard für gesetzliche Kranken- und Pflegeversicherer
- Sicherheitsstandard des Bundesverbandes der electronic-cash-Netzbetreiber
- Sicherheitsstandard Versicherungswesen für die Allianz Deutschland AG

B3S im Sektor Transport und Verkehr:
- Sicherheitsstandard für die Verkehrssteuerungs-und Leitsysteme im kommunalen Straßenverkehr
- Sicherheitsstandard für die Verkehrssteuerungs- und Leitsysteme der Bundesautobahn

Quelle: BSI

Aktuelle Entwicklungen und Trends

Systeme zur Angriffserkennung

KRITIS-Betreiber sind seit 01.05.2023 dazu verpflichtet, Systeme zur Angriffserkennung einzusetzen.

„Betreiber Kritischer Infrastrukturen haben die Verpflichtung, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen."

Dazu gehören insbesondere **Intrusion Detection Systeme (IDS)**, [ggf. auch **Security Information Event Management (SIEM)** Systeme], um Datenverkehr und Protokolle auf Angriffe zu prüfen.

„Derartige Systeme stellen eine effektive Maßnahme zur (frühzeitigen) Erkennung von IT-Sicherheits-Angriffen dar und unterstützen insbesondere die Schadensreduktion.

Das Bundesamt für Sicherheit in der Informationstechnik bietet hierzu eine Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung (oh-sza.pdf) an. Hierbei wird auf Bausteine aus dem IT-Grundschutz-Kompendium des BSI verwiesen: OPS.1.1.4 Schutz vor Schadprogrammen, OPS.1.1.5 Protokollierung, NET.1.2 Netzmanagement, NET.3.2 Firewall, DER.1 Detektion von sicherheitsrelevanten Ereignissen, DER.2.1: Behandlung von Sicherheitsvorfällen

Quelle: BSI

Fallstudie

Aus der Sicht eines IT-Service-Providers

noris network zählt selbst zur Kritischen Infrastruktur. Erfahrungswerte:

1. **Registrierungspflicht:**
   Fällt das Unternehmen unter eines der Kriterien der Kritis-Verordnung (Anhang 1–7 BSI-KritisV)?
   Wenn ja: Registrierung des Unternehmens beim Bundesamt für Sicherheit in der Informationstechnik ist notwendig –
   Verpflichtung gemäß BSI-Gesetz § 8 b (3).

2. **Zertifizierung:**
   Es ist nach BSI-Gesetz § 8 a eine externe Prüfung des KRITIS-Unternehmen durch eine Zertifizierungsstelle notwendig (derzeit alle 2 Jahre). In unserem Fall haben die bereits bestehenden Zertifizierungen (ISO 27001 u. ä.) exzellente Grundlagen für die Einhaltung der technischen und organisatorischen Sicherheitsmaßnahmen geliefert, jedoch sind ergänzend die **B3S**-Anforderungen für Kritische Infrastrukturen zu beachten.

3. **Meldepflichten (im Störfall):**
   Im Falle kritischer Störungen (insbesondere bei IT-Sicherheits-Vorfällen) muss eine Meldung an das BSI abgegeben werden.

Allgemein gilt: Bei Verstößen gegen das BSI-Gesetz sind **Bußgelder bis zu 20 Mio.** EUR möglich (seit IT-SiG 2.0, vorher waren es 50–100 Tsd. EUR)

Prüfbescheinigung

Hiermit wird bescheinigt, dass

noris network

noris network AG
Thomas-Mann-Straße 16-20
90471 Nürnberg
Deutschland

ein **Informationssicherheits-Managementsystem** eingeführt hat und anwendet.

Geltungsbereich:
Lösungen, Produkte und Services in den Bereichen IT-Outsourcing, Cloud Services, Managed Services, Network & Security sowie Rechenzentrumsinfrastrukturen und -betrieb

Durch ein Audit, dokumentiert in einem gesonderten Bericht, wurde festgestellt, dass der Scope des Informationssicherheits-Managementsystem und des ergänzenden Prüfkatalogs (aufgebaut nach der Orientierungshilfe zum B3S) nach

§ 8a Abs. 3 BSIG

die kritische Infrastruktur bzw. die kritische Dienstleistung vollständig erfasst.

Diese Zertifikatsergänzung ist nur gültig in Verbindung mit dem DQS-Zertifikat mit der Registrier-Nr. 358515 ISMS17

Zertifikat-Registrier-Nr.	358515 KRITISV
Gültig ab	2021-04-21
Gültig bis	2024-04-20

DQS BIT GmbH

Andre Dubsky
Geschäftsführer

Zertifizierungsstelle: DQS BIT GmbH, Gartenäckerstraße 13, 86825 Bad Wörishofen 1 / 2

Ausblick

Internationale Standards und Entwicklungen

2016 NIS-1-Richtlinie (Europäische Union): Verbesserung der Cybersicherheit in der Europäischen Union mit Mindestanforderungen für Betreiber von Diensten von allgemeinem Interesse (wie Energie, Verkehr, Gesundheitswesen, Finanzwesen usw.) Richtlinie zur Netz- und Informationssicherheit

- erhöhte Kapazitäten im Bereich der Cybersicherheit auf nationaler Ebene,
- verstärkte Zusammenarbeit auf EU-Ebene,
- Verpflichtungen für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste in den Bereichen Risikomanagement und Meldung von Sicherheitsvorfällen.

IT-SiG 1.0 "Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme" vom 25.07.2015:
Rechtsrahmen für die Gewährleistung von Cybersicherheit in Deutschland mit Das Gesetz sieht im Kern IT-Mindeststandards und Meldepflichten für Betreiber Kritischer Infrastrukturen im BSI-Gesetz (TKG, Energiewirtschaftsgesetz und Atomgesetz);
Nennung einer Kontaktstelle an das BSI, Nachweise für die Einhaltung der Sicherheitsstandards.

IT-SiG 2.0 vom Mai diesen Jahres

Die Richtlinie umfasst neben „Sektoren mit hoher Kritikalität“ wie bspw. Energieversorger, Verkehrsunternehmen, Cloud-Anbieter, Banken und Gesundheitsdienstleister auch „sonstige kritische Sektoren“ wie Post- und Kurierdienste, Unternehmen der Abfallwirtschaft oder Lebensmittelproduktion. Insbesondere mit Blick auf die strengen Meldepflichten bei Vorfällen, erforderliche technische und organisatorische Maßnahmen und auch bezogen auf die hohen drohenden Bußgelder von bis zu zehn Millionen Euro oder zwei Prozent des weltweiten Umsatzes bei Verstößen gegen die Anforderungen, lassen sich Parallelen zur DSGVO erkennen.

KRITIS aktuell: ca. 4500 Betreiber erfasst, durch das zukünftige IT-SiG 3.0 etwa 30.000 (Beck-Verlag) bis 40.000 (Manager-Magazin)
NIS 2 muss bis 17.10.2024 abgeschlossen sein,) Die „NIS 2-Richtlinie“ mündet demnach in das IT-Sicherheitsgesetz 3.0 / Kritis Dach-Gesetz. Die genaue Definition ist derzeit in Finalisierung durch Gesetzgeber und Regulatoren.

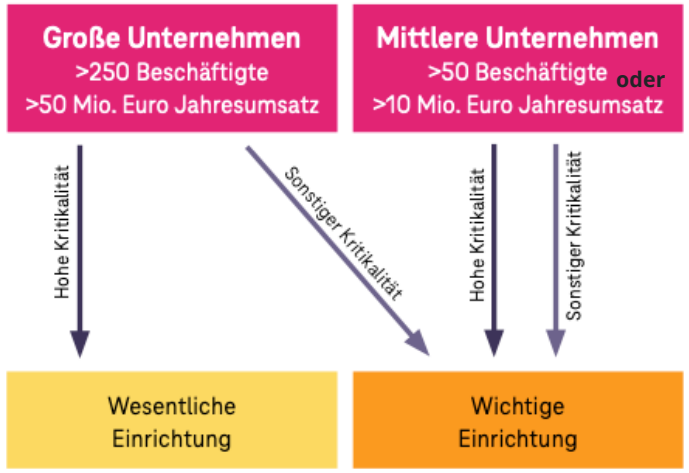
Ausblick

Aktuelle Neuerungen durch NIS2 (EU) und kommendes KRITIS-Dachgesetz / KRITIS 3.0

Die NIS2-Richtlinie der EU ist verabschiedet und muss in den Mitgliedsstaaten bis zum 17.10.2024 in nationales Recht umgesetzt werden. Die Sektoren wurden umstrukturiert, aus den bisher ca. 4.500 gemeldeten Unternehmen werden schätzungsweise 40.000:

Sektoren mit hoher Kritikalität:

- Energie
- Verkehr
- Bankwesen
- Finanzmarktinfrastrukturen
- Gesundheitswesen
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- Verwaltung von IKT-Diensten
- Öffentliche Verwaltung
- Weltraum



Quelle: Telekom

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
  - Herstellung von Medizinprodukten
  - Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen
  - Herstellung von elektrischen Ausrüstungen
  - Maschinenbau
  - Herstellung von Kraftwagen und Kraftwagenteilen
  - Sonstiger Fahrzeugbau
- Anbieter digitaler Dienste
- Forschung

Sonderfälle: (unabhängig von Unternehmensgröße)

- Vertrauensdiensteanbieter (PKI-Betreiber u. ä.)
- DNS-Diensteanbieter
- mittelgroße Anbieter öffentlicher elektronischer Kommunikationsnetze
- Öffentliche Verwaltung
- Unternehmen mit entscheidender Dienstleistung in einem EU-Mitgliedsstaat (UBI)
- Unternehmen, deren Ausfall einen erheblichen Einfluss auf das öffentliche Leben hätte
- Unternehmen, die als kritisch gemäß der EU-Resilienz-Richtlinie gelten
- Unternehmen, die vor dem 16. Januar 2023 bereits als kritisch eingestuft wurden

UBI

Unternehmen im besonderen öffentlichen Interesse (UBI) gemäß BSI-Gesetz

Unternehmen im besonderen öffentlichen Interesse sind:

1. Unternehmen, „die Güter nach § 60 Absatz 1 Nummer 1 und 3 der Außenwirtschaftsverordnung in der jeweils geltenden Fassung herstellen oder entwickeln.“

   Darunter fallen die Unternehmen, die im Bereich **Waffen, Munition und Rüstungsmaterial** oder im Bereich von Produkten mit **IT-Sicherheitsfunktionen zur Verarbeitung staatlicher Verschlusssachen** oder für die IT-Sicherheitsfunktion **wesentliche Komponenten** solcher Produkte tätig sind.

2. Unternehmen, „die nach ihrer inländischen Wertschöpfung zu den **größten Unternehmen in Deutschland** gehören und daher von erheblicher volkswirtschaftlicher Bedeutung für die Bundesrepublik Deutschland sind“. Die genauen wirtschaftlichen Kennzahlen zur Identifizierung der größten Unternehmen werden noch per Rechtsverordnung festgelegt. Nach Vorliegen dieser Verordnung und Feststehen des Betroffenenkreises dieser Kategorie von UBI kann das BMI in einer weiteren Verordnung bestimmen, welche Alleinstellungsmerkmale maßgeblich dafür sind, dass Zulieferer für diese Unternehmen von wesentlicher Bedeutung sind und daher ebenfalls unter die gesetzlichen Bestimmungen des BSI-Gesetzes fallen.

3. Betreiber „eines Betriebsbereichs der oberen Klasse im Sinne der **Störfall-Verordnung** in der jeweils geltenden Fassung" oder Betreiber, die, "nach § 1 Absatz 2 der Störfall-Verordnung diesen gleichgestellt sind.“ Das sind Unternehmen, die einen Bereich betreiben, in dem **gefährliche Stoffe in Mengen** vorhanden sind, die die in Spalte 5 der Stoffliste in Anhang I der Störfall-Verordnung genannten Mengenschwellen erreichen oder überschreiten.

Quelle: BSI

noris network

Mehr Leistung als Standard

noris network AG
Thomas-Mann-Straße 16 – 20
90471 Nürnberg

Telefon: +49 911 9352-0
www.noris.de

Joachim Astel
joachim.astel@noris.de

IT Sicherheit
Made in Germany