Netzwerke Sicherheit

(Stand 2024)

Dipl.-Ing. (FH) Oliver Gauer

1. Ausgabe, Juni 2024

NWSI_2024

ISBN 978-3-98569-179-1

Bevor Sie beginnen …

Empfohlene Vorkenntnisse

- Grundkenntnisse im Bereich der Informationstechnologie
- Netzwerke – Grundlagen

Lernziele

Dieses Buch vermittelt Ihnen die Grundlagen zu wesentlichen Aspekten der Sicherheit in Netzwerken. Es beschreibt sowohl allgemeine Sicherheitsanforderungen als auch spezielle, die bei der Nutzung von Komponenten und Protokollen in Netzwerken entstehen.

Sie lernen die IT-Sicherheit vernetzter Systeme aus der Sicht unterschiedlicher Gruppen, wie Management, Administration und Anwendern, zu betrachten. Nach dem Durcharbeiten des Buches wissen Sie, dass für die Herstellung eines angemessenen Sicherheitsniveaus eine Analyse der möglichen Gefahren, des Bedarfs für Sicherheit und eine Abschätzung des Risikos vorausgehen müssen.

Sie kennen den Planungsablauf von IT-Sicherheitsmaßnahmen und sind mit den wesentlichen technischen und organisatorischen Maßnahmen vertraut, mit denen bestimmte Sicherheitsbedrohungen bekämpft werden können. Sie können selbstständig anhand der Ihnen bekannten Kriterien die optimale Sicherheitsmaßnahme für eine Problemstellung auswählen.

Hinweise zu Soft- und Hardware

Die im Buch beispielhaft vorgestellte Hard- und Software wurde nicht unter der Prämisse ausgewählt, das jeweils beste Produkt in dieser Kategorie zu sein. Für Schulungszwecke sind die vorgestellten Produkte jedoch geeignet, da sie z. B. im Falle von Free- oder Shareware für Sie relativ leicht und kostengünstig zur Verfügung stehen oder – wenn es sich bei der dargestellten Software um kommerzielle Software handelt – sich gut für eine Demonstration der zu vermittelnden Lehrinhalte eignen, aus der Sie die wichtigsten Erkenntnisse für die Arbeit mit ähnlicher Software ableiten können.

Da es sich um ein Buch handelt, das verschiedene Aspekte der IT-Sicherheit in Computersystemen und Netzwerken beleuchten soll und nicht nur einen speziellen Teil, wurden auch die Inhalte auf der Grundlage verschiedener Betriebssysteme erstellt.

Da in der Praxis Microsoft-basierte Betriebssysteme die größte Verbreitung besitzen, kommen in diesem Buch verschiedene Varianten dieser Systeme, z. B. Windows Server 2008/2012/2019 oder Windows 8/8.1/10/11 zum Einsatz.

Inhaltliche Gliederung

Das Buch erklärt zuerst die Grundlagen der IT-Sicherheit und die Notwendigkeit entsprechender Maßnahmen. Anschließend werden die häufigsten Bedrohungsszenarien beschrieben. Im letzten Teil des Buches werden Ihnen dann die unterschiedlichen Abwehrstrategien für die beschriebenen Bedrohungsszenarien erläutert.

Typografische Konventionen

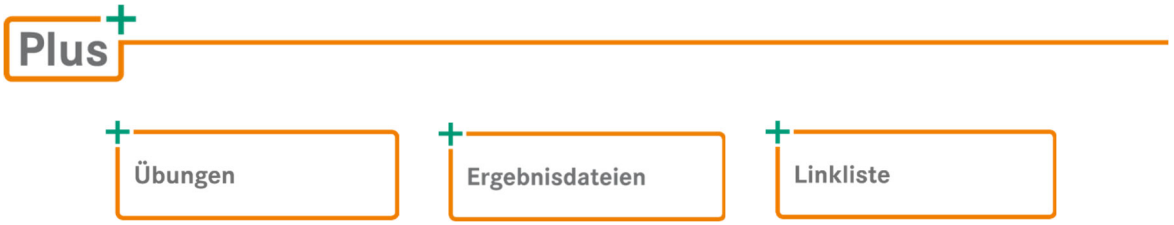
Damit Sie bestimmte Elemente auf einen Blick erkennen und zuordnen können, werden diese im Text durch eine besondere Formatierung hervorgehoben. So werden beispielsweise Bezeichnungen für Programmelemente wie Register oder Schaltflächen immer *kursiv* geschrieben und wichtige Begriffe **fett** hervorgehoben.

Kursivschrift	kennzeichnet alle vom Programm vorgegebenen Bezeichnungen für Schaltflächen, Dialogfenster, Symbolleisten etc., Menüs bzw. Menüpunkte (z. B. *Datei - Speichern*), Internetadressen und vom Benutzer angelegte Namen (z. B. Rechner-, Benutzernamen).
`Courier`	wird für Systembefehle sowie für Datei- und Verzeichnisnamen verwendet. In Syntaxangaben werden Parameter kursiv ausgezeichnet (z. B. `cd` *`Verzeichnisname`*). Eckige Klammern `[]` kennzeichnen optionale Elemente. Alternative Eingaben sind durch einen senkrechten Strich `|` getrennt. Benutzereingaben auf der Konsole werden **`fett`** hervorgehoben.

HERDT BuchPlus – unser Konzept:

Problemlos einsteigen – Effizient lernen – Zielgerichtet nachschlagen

Nutzen Sie dabei unsere maßgeschneiderten, im Internet frei verfügbaren Medien:



Wie Sie schnell auf diese BuchPlus-Medien zugreifen können, erfahren Sie unter *www.herdt.com/BuchPlus.*

1

Was ist Sicherheit?

1.1 Grundforderungen an Sicherheit

Sicherheit und die in diesem Buch beschriebene IT-Sicherheit sind grundlegender Bestandteil der Unternehmenssicherheit. Sie umfasst alle Prozesse, Strategien und das Know-how eines Unternehmens, um es vor Eingriffen durch Dritte zu schützen.

Bei der IT-Sicherheit geht es grundsätzlich um:

- **Funktionssicherheit** (engl. safety)
  Sicherheit des Systems, welches als Hardware und/oder Software vorhanden ist. Dabei darf das System unter allen vorgegebenen Betriebsbedingungen keine Zustände annehmen, die unzulässig sind.
- **Datensicherheit** (engl. protection)
  Sie definiert die Eigenschaft eines funktionssicheren Systems, die zu keinem unautorisierten Zugriff auf die Ressourcen des Systems und insbesondere auf die Daten führen. Dazu nutzt man Protokolle, die Vertraulichkeit, Integrität und Verfügbarkeit umsetzen.

1.2 Datensicherheit = Datenschutz?

Während sich das Themengebiet Datensicherheit auf alle Arten von Daten bezieht, sind vom Datenschutz lediglich personenbezogene Daten betroffen.

Die Datenschutzgrundverordnung der Europäischen Union (EU-DSGVO) und das Bundesdatenschutzgesetz (BDSG) beziehen sich ausschließlich auf den Schutz personenbezogener Daten.

Jedes Unternehmen (oder jede Privatperson) trifft Vorkehrungen zur Datensicherheit und somit gegen den Verlust oder Beschädigung seiner Daten. Als Synergieeffekt werden gleichzeitig Forderungen des Datenschutzes zur Sicherheit in der Verarbeitung umgesetzt.

Die Datensicherheit hat primär den Schutz von allgemeinen Unternehmensdaten zur Aufgabe.

Dennoch sind beide Themenbereiche eng miteinander verknüpft. Die von den Unternehmen ergriffenen Maßnahmen zur Datensicherheit sind also auch zu einem Teil bereits für den Datenschutz hilfreich. Allerdings sind in Bezug auf die Verarbeitung personenbezogener Daten weitreichendere Maßnahmen erforderlich, werden jedoch nicht in diesem Buch behandelt. Weiterführende Informationen finden Sie z. B. im HERDT-Buch *Datenschutz – Grundlagen*).

Datensicherheit ist also nicht gleich Datenschutz!

1.3 Sicherheitsziele

Vertraulichkeit

Unter Vertraulichkeit (engl. confidentiality) wird verstanden, dass Informationen nur diejenigen erreichen, die diese Informationen auch besitzen dürfen. Bezogen auf Kommunikation in Netzwerken ist das Sicherheitsziel der Vertraulichkeit vergleichbar mit dem Briefgeheimnis. Wenn Sie eine E-Mail an einen bestimmten Empfänger absenden, erwarten Sie, dass nur der von Ihnen bestimmte Empfänger den Inhalt der E-Mail lesen kann.

Das Sicherheitsziel der Vertraulichkeit beschränkt sich nicht nur auf E-Mails. Jede auf einem Computersystem gespeicherte Information dient einem bestimmten Zweck, und in den meisten Fällen ist es nicht erforderlich oder nicht erwünscht, dass diese Informationen öffentlich zugänglich sind.

In der realen Welt sind Schutzmaßnahmen für Vertraulichkeit z. B. ein Briefumschlag, in den man seine nicht öffentliche Nachricht steckt, oder eine abgesperrte Tür, die nur den Personen Zugang zu einem Raum gewährt, die den passenden Schlüssel besitzen.

Um Vertraulichkeit zu gewährleisten, können verschiedene Maßnahmen eingesetzt werden: beispielsweise eine Verschlüsselung von Dateien oder Nachrichten zwischen den Kommunikationspartnern oder eine Zugangskontrolle, die nur bestimmten Personen einen Einblick in das geschützte Datenmaterial erlaubt.

Integrität

Wenn mit Daten gearbeitet wird, muss ein sicheres IT-System gewährleisten können, dass die Daten korrekt sind (engl. integrity). Beispielsweise müssen Fehler bei der Übertragung von Daten verhindert oder wenigstens erkannt und ggf. korrigiert werden können. Es muss aber auch möglich sein, Daten und IT-Systeme gegen Manipulationen zu schützen.

Wird die Integrität der Daten gewährleistet oder bestätigt (z. B. durch eine zusätzliche Information über den Urheber oder Verfasser, gekoppelt an die Daten), sind die Daten authentisch – also „echt“.

Authentizität (engl. authenticity) stellt in gewisser Weise eine detailliertere Sicht von Integrität als Sicherheitsziel dar. In der aktuellen politischen Diskussion um digitale Signaturen wird eine weitere Stufe von Authentifizierung sichtbar:

Eine E-Mail, die eine Bestellung enthält, wird vor Gericht ohne weiteres keinen Bestand haben: Der Inhalt könnte beispielsweise manipuliert sein, oder es wurde sogar der Absender der E-Mail gefälscht, und der vermeintliche Auftraggeber weiß gar nichts von seiner Bestellung.

Selbst wenn hier Methoden zur Gewährleistung der Integrität des Inhalts (keine Manipulation mehr möglich) und zur Authentifikation (die Mail stammt wirklich vom genannten Absender) wahrgenommen wurden, reicht das im juristischen Sinne mitunter nicht aus, um eine gültige Willenserklärung zum Abschluss eines Kaufvertrages darzustellen. Es wäre immer noch relativ leicht möglich, einen Grund zu finden, warum diese E-Mail keine gültige Willenserklärung sein sollte.

Durch die eigene Unterschrift auf einem Stück Papier belegen Sie, dass Sie mit dem Inhalt des Textes einverstanden sind und seine Konsequenzen akzeptieren. Da Ihre Unterschrift durch das Papier direkt (und relativ schwer trennbar) mit dem unterschriebenen Text zusammengebracht wird, ist hier die Verbindlichkeit gewährleistet – aufgrund der Natur von Informationssystemen ist diese Untrennbarkeit von Inhalt und Unterschrift nicht ganz so einfach zu realisieren.

Als eine Forderung, die Authentifikation erweitert und der digitalen Signatur erst einen Sinn gibt, wird die Verbindlichkeit (engl. non-repudiation) einer digitalen Unterschrift definiert.

Ist in einem System die Verbindlichkeit für die Kommunikation sichergestellt, kann ein Teilnehmer nicht zu einem späteren Zeitpunkt behaupten, die Kommunikation habe nicht oder mit einem anderen Inhalt stattgefunden.

Verfügbarkeit

Ein weiteres Hauptziel für die Sicherheit von Daten ist die Verfügbarkeit (engl. availability). Ein funktionssicheres IT-System muss auch gewährleisten können, dass die Daten, die es verarbeitet, auch zugreifbar sind bzw. dass die Dienste, die angeboten werden, auch wirklich genutzt werden können.

Verfügbarkeit umfasst in der Regel logische Schutzmaßnahmen (zum Beispiel gegen versehentliches Löschen) genauso wie geeignete Maßnahmen, die einen Betrieb bei Störungen von Hard- und Software aufrechterhalten können. Auch äußere Einflüsse, wie zum Beispiel Stromausfälle oder gezielte Manipulationen von Saboteuren mit dem Ziel, die Dienste dieses Systems für berechtigte Nutzer zu blockieren, sind Probleme, mit denen sich ein Verfügbarkeitskonzept befasst.

Speziell für Einsatzgebiete, in denen eine Verfügbarkeit der Dienste rund um die Uhr gewährleistet sein muss, gibt es angepasste Hochverfügbarkeitslösungen, die einerseits durch spezielle Hardware und anderseits durch angepasste Algorithmen in der Software versuchen, eine möglichst hohe Ausfallsicherheit zu erreichen.

Beispiele

- Feuer-, Wasser- und EMP-feste Auslegung der Serverräume
- Unterbrechungsfreie Stromversorgung (USV) zentraler Komponenten wie Server, Switches und Router

- Redundante physikalische Server-Systeme (doppelte Netzteile, Controller, Netzwerk-interfaces, RAID, etc.)
- Clustering von Servern (active/active oder active/passive)
- Virtualisierung der Daten und deren Backup
- „Watchdog“: Hard- oder Software, die das Funktionieren eines Systems überwacht
- Redundante physikalische Topologien (Ring- bzw. Maschentopologie)
- Redundante Layer-2-Verbindungen zur Erhöhung der Bandbreite (Link Aggregation Control Protocol IEEE 802.3ad oder Port Aggregation Protocol)
- Redundante Layer-2-Verbindungen (Spanning Tree Protocol, Rapid Spanning Tree Protocol, Multiple Spanning Tree Protocol, Shortest Path Bridging, TRILL)
- Redundantes statisches Routing über unterschiedliche Metrik
- Dynamische Routing-Protokolle bei vorhandenen physikalisch redundanten Wegen (z. B. Open Shortest Path First)
- Verfügbarkeitsprotokolle auf Layer 3 (z. B. Virtual Router Redundancy Protocol oder Gateway Load Balancing Protocol)
- Redundante Dienste (z. B. Primary Domain Controller und Backup Domain Controller)
- Verteilte Anwendungen

1.4 Ursachen von Sicherheitsproblemen

Die Hauptursache für Sicherheitsprobleme liegt – im Gegensatz zu den vorsätzlichen Sicherheitsverletzungen – in der Fehlbedienung durch Mitarbeiter aufgrund mangelnder Kompetenz. Viele Mitarbeiter erhalten, wenn überhaupt, nur eine kurze Einarbeitung in die IT-Umgebung am Arbeitsplatz. Findet diese statt, so ist sie meist auf das Ziel „Erfüllung der Aufgabe“ ausgerichtet, nicht aber auf die Sicherheit im Betrieb.

So ist es nicht überraschend, wenn viele Sicherheitsprobleme durch Fehlbedienung seitens der Benutzer entstehen. Teilweise wird dies auch durch Software mit verwirrenden Dialogen und umständlichen Bedienkonzepten gefördert. Zu den häufigsten Problemen gehören:

- versehentliches Löschen von Dateien,
- versehentliches Senden von sensiblen Daten an Unbefugte,
- falsche Änderungen an Datenbeständen.

Schaffung von Wissen über Vorschriften und Arbeitsvorgänge

Vielerorts wissen Mitarbeiter nicht um die speziellen Vorschriften, die für die IT-Sicherheit an ihrem Arbeitsplatz gelten. Noch so gründlich erarbeitete Sicherheitsrichtlinien (Policy) können von den Mitarbeitern nicht berücksichtigt werden, wenn diese niemals über deren Existenz unterrichtet worden sind. Solange der einzige Mitarbeiter, dem die Policy bekannt ist, der IT-Sicherheitsverantwortliche ist, der sie erstellt hat, kann die Policy auch nicht wirksam sein.

Daher ist eine Einführung in Vorschriften und Arbeitsvorgänge ein unerlässlicher Bestandteil der Einarbeitung.

Schulungsmaßnahmen dürfen sich nicht nur auf das IT-Personal und die IT-Sicherheitsmitarbeiter beschränken, sondern müssen die gesamte Belegschaft einschließen.

Die Wahrscheinlichkeit, dass ein erfahrener Administrator einen unverlangt von Unbekannten zugesendeten Mail-Anhang (Attachment) öffnet, ist deutlich geringer, als dass ein Mitarbeiter einer Nicht-IT-Abteilung aus Neugier ein derartiges Attachment ausführt.

1.5 Sensibilisierung der Mitarbeiter (Awareness)

Da ungeschultes bzw. unwissendes Personal den Großteil der Mitarbeiter und somit die größte Angriffsfläche für Datenmissbrauch darstellt, müssen alle Mitarbeiter für Sicherheitsprobleme und ihre verschiedenen Erscheinungsformen sensibilisiert werden.

Mitarbeiter sollten gleich zu Beginn des Arbeitsverhältnisses über Vorschriften mündlich bzw. schriftlich informiert werden. Darüber hinaus sollten Mitarbeiter gezielt nach Vorschriften fragen, so dass diese im Intranet veröffentlicht werden oder die Personalabteilung bzw. die EDV-Abteilung darüber informiert.

Durch regelmäßige Informationen (Kurzveranstaltungen, Aushänge am „Schwarzen Brett“, Rundmails zum Thema Sicherheit) werden Mitarbeiter auf neueste Bedrohungen hingewiesen.

2

Rechtsgrundlagen

2.1 Gesetzliche Grundlagen der Informationssicherheit

Das deutsche und europäische Recht bietet eine Reihe von juristischen Möglichkeiten, um der Sicherheit im Telekommunikationsbereich Rechnung zu tragen. Das sind in Deutschland insbesondere:

- Strafgesetzbuch 15. Abschnitt – Verletzung des persönlichen Lebens- und Geheimbereichs
  - § 202a Ausspähen von Daten
  - § 202b Abfangen von Daten
  - § 202c Vorbereiten des Ausspähens und Abfangens von Daten
  - § 206 Verletzung des Post- oder Fernmeldegeheimnisses
- Strafgesetzbuch 27. Abschnitt – Sachbeschädigung
  - § 303a Datenveränderung
  - § 303b Computersabotage
  - Telekommunikationsgesetz
  - Teil 7 – Fernmeldegeheimnis, Datenschutz, Öffentliche Sicherheit (§§ 88–115)
- Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz)
- Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)
- Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0)
- EU-Datenschutzgrundverordnung (EU-DSGVO)
- Besondere Vertragsbedingungen für die Beschaffung von DV-Leistungen (BVB)

2.2 „Hackerparagraf“ §§ 202a–c StGB

Die Regelungen des 41. Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität haben sich im Strafgesetzbuch (StGB) in §§ 202a–c Eingang gefunden. In Ihnen wird der unbefugte Zugang zu Daten, die Überwindung von Zugangssicherungen, die Anwendung hierzu erforderlicher technischer Mittel und die Herstellung von Computerprogrammen, deren Zweck die Begehung einer solchen Tat ermöglichen, unter Strafe gestellt.

Dazu gehören auch öffentlich zugängliche Programme wie Wireshark, Nmap und andere Penetrationstools. Den Konsequenzen aus dem „Hackerparagraf“ kann man entgehen, wenn man die Befugnis für den Zugang erhält bzw. Daten, die nicht vor einem unberechtigten Zugriff geschützt und aus technischer Sicht öffentlich abrufbar sind, aufzeichnet.

Im Mai 2021 hatte eine Sicherheitsforscherin auf gravierende Sicherheitsmängel der App CDU connect aufmerksam gemacht und wurde prompt von dieser Partei aufgrund dieses Paragrafen verklagt. Die Staatsanwaltschaft hat die Anklage nach einige Zeit aufgrund des oben geschilderten Sachverhaltes zurückgezogen.

Das Bundesamt für Sicherheit in der Informationstechnik soll dagegen den Hackerparagraf lt. IT-SiG 2.0 ohne Konsequenzen anwenden dürfen, um Sicherheitsrisiken bei Betreibern proaktiv zu erkennen.

2.3 IT-Sicherheitsgesetz (IT-SiG)

Das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) wurde am 12. Juni 2015 vom Bundestag beschlossen, am 24. Juli 2015 im Bundesgesetzblatt verkündet (BGBl. I, Nr. 31, S. 1324) und trat am 25. Juli 2015 in Kraft.

Es regelt, dass Betreiber sogenannter „Kritischer Infrastruktur“ (vgl. 1. b) ein Mindestniveau an IT-Sicherheit einhalten und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) IT-Sicherheitsvorfälle melden müssen. Werden keine Maßnahmen organisatorischer und technischer Art zur Vermeidung von Störungen getroffen, droht ein Bußgeld. Gleichzeitig werden Hard- und Software-Hersteller zur Mitwirkung bei der Beseitigung von Sicherheitslücken verpflichtet.

Durch das IT-Sicherheitsgesetz wurden mehrere bestehende Gesetze, darunter insbesondere das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz), das Atomgesetz, das Energiewirtschaftsgesetz, das Telemediengesetz, das Telekommunikationsgesetz, geändert.

1. Bundesamt für Sicherheit in der Informationstechnik (Änderung im BSI-Gesetz)

a) Aufgaben des BSI

Der Zentralstelle für das Chiffrierwesen wurde 1986 neben dem Chiffrieren von Verschlusssachen des Bundes der zusätzliche Aufgabenbereich der Computersicherheit zugewiesen. 1989 wurde daraus die „Zentralstelle für die Sicherheit in der Informationstechnik“. Das BSI (Bundesamt für Sicherheit in der Informationstechnik) wurde 1990 mit dem BSI-Errichtungsgesetz geschaffen.

Bislang war der Schutz der EDV-Anlagen der Bundesbehörden (Bundesministerien, Bundesämter) die Kernaufgabe des BSI. Die nicht zur Exekutive gehörenden Bundesorgane (Bundesrat und Bundestag, die neun Bundesgerichte) zählen aufgrund der Gewaltentrennung nicht zum Bund im Sinne des BSI-Gesetzes, (§ 2 Absatz 3 Satz 2 BSI-Gesetz).

Schon seit dem BSI-Gesetz vom 14.08.2009 durfte das BSI die Öffentlichkeit oder die betroffenen Kreise in Behörden vor Sicherheitslücken in informationstechnischen Produkten und Diensten oder vor Schadprogrammen warnen (§ 7 Absatz 1 BSI-Gesetz) und im Verbund mit der Privatwirtschaft „Kommunikationsstrukturen zur Krisenfrüherkennung, Krisenreaktion und Krisenbewältigung sowie Koordinierung der Zusammenarbeit zum Schutz der kritischen Informationsinfrastrukturen“ aufbauen (§ 3 Absatz 1 Satz 2 Nr. 15 alte Fassung BSI-Gesetz). Mit dem BSI-Gesetz wurde der Begriff „Kritische Informationsinfrastrukturen“ in „Informationstechnik Kritischer Infrastrukturen“ geändert.

Mit dem IT-Sicherheitsgesetz erhielten der Schutz der Öffentlichkeit und der Kritischen Infrastrukturen innerhalb der Aufgaben des BSI eine ähnlich starke Stellung wie der Schutz der EDV-Anlagen des Bundes. Das BSI darf nun z. B. auf dem Markt angebotene informationstechnische Produkte und Systeme untersuchen (Absatz 1 des durch das IT-Sicherheitsgesetz neu eingefügten § 7a BSI-Gesetz). Nachdem es den Anbietern Gelegenheit zur Stellungnahme gegeben hat, darf das BSI seine Prüfergebnisse weitergeben und veröffentlichen, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, (§ 7a Absatz 2 BSI-Gesetz).

b) Begriff der Kritischen Infrastrukturen

Das BSI-Gesetz enthält in § 2 Absatz 10 eine Definition für Kritische Infrastrukturen. Bei Kritischen Infrastrukturen handelt es sich um „Einrichtungen, Anlagen oder Teile davon, die …

1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und
2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.“

Welche Einrichtungen, Anlagen oder Teile davon im Einzelnen „von hoher Bedeutung“ sind, wird in die Hände des Bundesinnenministeriums gelegt. Dieses hat in einer Rechtsverordnung die kritischen Infrastrukturen zu benennen. Eine Zustimmung des Bundesrats zu der Verordnung ist nicht erforderlich; allerdings hat das BMI vor Erlass der Rechtsverordnung Vertreter der Wissenschaft, der betroffenen Betreiber und der betroffenen Wirtschaftsverbände anzuhören, (§ 10 Absatz 1 BSI-Gesetz). Hinsichtlich ihrer jeweiligen Fachbereiche ist die Verordnung im Einvernehmen mit anderen Bundesministerien zu erlassen, darunter die Ressorts für Finanzen, Verteidigung, Wirtschaft und Energie, Gesundheit, Verkehr und Digitale Infrastruktur sowie Umwelt und Reaktorsicherheit, (§ 10 Absatz 1 BSI-Gesetz).

c) Schutz der Kritischen Infrastrukturen

Vier neu ins BSI-Gesetz eingefügte Paragrafen dienen dem Schutz der Kritischen Infrastrukturen, die §§ 8a bis 8d. Sie enthalten Rechte und Pflichten sowohl des BSI als auch von Betreibern Kritischer Infrastrukturen.

Unternehmen, die in der Rechtsverordnung des Bundesinnenministeriums als Betreiber Kritischer Infrastrukturen bezeichnet werden, erhalten zwei Jahre Zeit, um „organisatorische und technische Vorkehrungen zur Vermeidung von Störungen“ zu treffen, (§ 8a Absatz 1 Satz 1 BSI-Gesetz).

2. Änderung Telemediengesetz und Telekommunikationsgesetz

Diensteanbieter nach dem Telemediengesetz werden verpflichtet, im Rahmen der wirtschaftlichen Zumutbarkeit und technischen Machbarkeit, unerlaubte Zugriffe auf die für die Telemedien genutzten Einrichtungen sowie Verletzungen persönlicher Daten zu verhindern, (Art. 4 IT-Sicherheitsgesetz = neuer § 13 Absatz 7 Telemediengesetz).

Diensteanbieter nach dem Telekommunikationsgesetz erhalten die Erlaubnis, Bestands- und Verkehrsdaten der Teilnehmer und Nutzer zu erheben und zu verwenden, um Störungen oder Fehler der Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen, (Art. 5 Nr. 2 IT-Sicherheitsgesetz = Neufassung § 100 Absatz 1 Satz 1 Telekommunikationsgesetz).
Es wurde eine Mitteilungspflicht des Netzbetreibers oder Erbringers öffentlich zugänglicher Telekommunikationsdienste eingeführt, wenn Störungen zu beträchtlichen Sicherheitsverlusten führen oder führen können, (Art. 5 Nr. 3c IT-Sicherheitsgesetz = neuer § 109 Absatz 5 Telekommunikationsgesetz). Die Bundesnetzagentur darf die erhaltenen Informationen über Sicherheitsmängel an das BSI weitergeben, (Art. 5 Nr. 3e IT-Sicherheitsgesetz = neuer § 109 Absatz 8 Telekommunikationsgesetz).

3. Der europarechtliche Rahmen

Die Richtlinie 2008/114/EG des Rates verpflichtet die Mitgliedstaaten, zum einen kritische Infrastrukturen im Energie- und Verkehrssektor zu ermitteln und auszuweisen, zum anderen zu bewerten, inwieweit es notwendig ist, ihren Schutz zu verbessern. Die Richtlinie verpflichtet die EU-Staaten weiter, dafür zu sorgen, dass Betreiber kritischer Infrastrukturen von grenzüberschreitender Bedeutung (EKI) Risikoanalysen durchführen und Sicherheitspläne aufstellen. Für Betreiber von Anlagen sieht die Richtlinie jedoch keine Meldepflichten bei schwerwiegenden Sicherheitsverletzungen vor.

Die Richtlinie enthält folgende Definition: Kritische Infrastrukturen sind eine „Anlage, ein System oder ein Teil davon, die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind und deren Störung oder Zerstörung erhebliche Auswirkungen auf einen Mitgliedstaat hätte, da diese Funktionen nicht aufrechterhalten werden könnten“. Europäische kritische Infrastruktur (EKI) ist demnach eine Störung oder Zerstörung, die erhebliche Auswirkungen in mindestens zwei anderen EU-Staaten hätte.

2.4 IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0)

Das IT-Sicherheitsgesetz 2.0 wurde am 23. April 2021 im Bundestag verabschiedet und ist am 28.05.21 in Kraft getreten (siehe auch BGBl 2021 Teil I Nr. 25). IT-SiG 2.0 verfolgt nun einen fast ganzheitlichen Ansatz. Es verbessert und erweitert die im IT-Sicherheitsgesetz als verfassungsrechtlich bedenklich eingestufte Normenklarheit der konkreten Bestimmung des Begriffs der Kritischen Infrastrukturen (KRITIS) und eine Bestimmbarkeit der betroffenen Betreiber. Die Schwellenwerte bezüglich zukünftiger Auflagen, technischer Sicherheit und der Einbeziehung externer Dienstleister wurden konkretisiert.

Zur Einstufung als KRITIS zählen die Sektoren:

- Staat und Verwaltung
- Gesundheit
- Transport und Verkehr
- Energie
- Informationstechnik und Telekommunikation (IT und TK)
- Wasser
- Ernährung
- Siedlungsabfallwirtschaft
- Medien und Kultur
- Finanzen und Versicherungen
- Unternehmen im besonderen öffentlichen Interesse (UNBÖFI) und deren Zulieferer

Sofern ein Betreiber den o. g. Sektoren angehört und definierte Schwellenwerte überschreitet, gilt er als KRITIS-Betreiber (Listen der Anlagen und Betreiber sind nicht öffentlich, Schätzungen gehen von ca. 2000 KRITIS-Betreibern in Deutschland aus, Stand 04/24). Die Werte sind als Anlagen im IT-SiG 2.0 definiert (siehe auch *https://www.openkritis.de/it-sicherheitsgesetz/kritis-anlagen_kritisv_itsig20.html*).

KRITIS-Betreiber müssen Vorsorgepflichten erfüllen, d. h. sie müssen Systeme der Angriffsvorbeugung und -erkennung verbindlich einsetzen und angemessene Vorkehrungen zur Vermeidung von Störungen in ihren Systemen, Komponenten und Prozessen nach dem neuesten Stand der Technik implementieren. Der Nachweis der Maßnahmen ist dem BSI im Turnus von zwei Jahren nachzuweisen. Er besteht weiterhin eine Regelung zur Untersagung des Einsatzes von kritischen Komponenten, für die eine Pflicht der Zertifizierung besteht.

Die datenschutzrechtlichen Weitergabepflichten und -befugnisse wurden erweitert und die Datenschutzbeauftragten des Bundes und der Länder in die Meldewege einbezogen. Des Weiteren wurden durch dieses Gesetz zusätzliche Änderungen in weiteren Gesetzestexten vorgenommen (u. a. BSI-Gesetz, BKA-Gesetz, Telemedien- und Telekommunikationsgesetz, Energiewirtschaftsgesetz, Außenwirtschaftsverordnung).

Das BSI bekommt in dem IT-Sicherheitsgesetz 2.0 erweiterte Kontroll- und Prüfbefugnisse gegenüber der Bundesverwaltung. Dazu gehören verlängerte Aufbewahrungsfristen von Protokollinformationen (Loggingdaten) auf bis zu 18 Monaten. Das BSI erhält auch vermehrt die Befugnis, Schwachstellen in Telekommunikation- und Telemediennetzen zu detektieren und proaktiv Analyseverfahren zu deren Erkennung (Honeypots) einzusetzen. Aus den gewonnenen Erkenntnissen kann das BSI gegenüber den Netzbetreibern und Unternehmen Maßnahmen zur Gefahrenabwehr rechtlich einfordern. Es soll damit zur zentralen Anlaufstelle für IT-Sicherheit in Deutschland avancieren.

Auch dem Verbraucherschutz wurde im Gesetz durch die Einführung eines IT-Sicherheitskennzeichens Rechnung getragen. Hierbei können Anbieter (leider nur) freiwillig dem BSI die Sicherheitseigenschaften ihrer Produkte in einer Herstellererklärung mitteilen. Das BSI erhält die Möglichkeit (nicht die Verpflichtung), diese Vorgaben regelmäßig zu prüfen.

Um der Umsetzung des IT-SiG 2.0 Rechnung zu tragen, wurden bei Rechtsverletzungen hohe Anpassungen der Bußgelder zur Anwendung gebracht, die auf Vorgaben zur Harmonisierung innerhalb der EU basieren. Die Höchstbeträge sind nach Schweregrad gestuft und können im Extremfall bis zu 20 Millionen Euro annehmen.