Netzwerke Sicherheit

Siegmund Dehn

11. Ausgabe, April 2019

NWSI_2019

ISBN 978-3-86249-848-2

Plus

HERDT

Bevor Sie beginnen …

HERDT BuchPlus – unser Konzept:

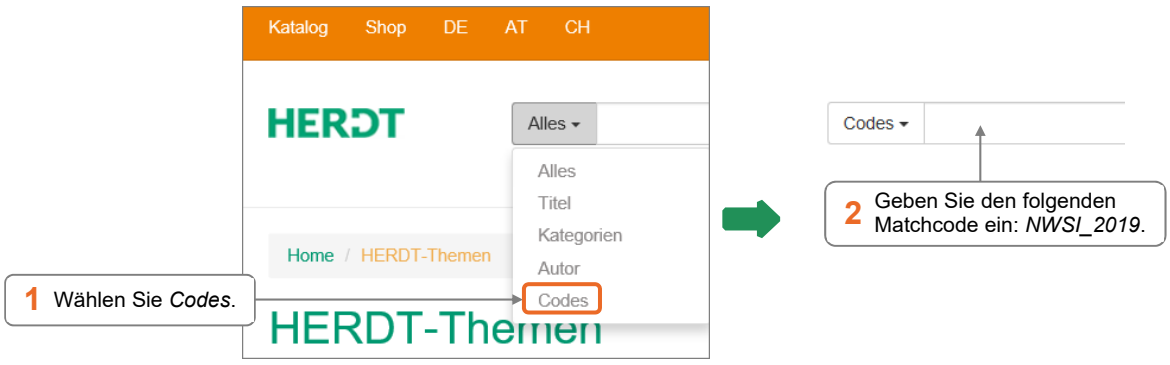
Problemlos einsteigen – Effizient lernen – Zielgerichtet nachschlagen

(weitere Infos unter *www.herdt.com/BuchPlus*)

Nutzen Sie unsere maßgeschneiderten, im Internet frei verfügbaren Medien:

So können Sie schnell auf die BuchPlus-Medien zugreifen:

- Rufen Sie im Browser die Internetadresse *www.herdt.com* auf.



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, Administratoren und Benutzer, 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 7/8/8.1/10 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.

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) 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) 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.
- **Datenschutz** (engl. privacy) ist die Fähigkeit einer natürlichen Person, sein Persönlichkeitsrecht bezogen auf die eigenen Daten wahrzunehmen, um einen etwaigen Missbrauch durch Dritte zu unterbinden.

1.2 Sicherheitsziel Vertraulichkeit

Unter dem Sicherheitsziel der **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.

1.3 Sicherheitsziel 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 an die Möglichkeit, die Integrität der Daten zu gewährleisten oder bestätigen zu können, auch eine Information über den Urheber oder Verfasser der Daten gekoppelt, so entsteht eine **Authentizität** (engl. authenticity) der entsprechenden Daten – sozusagen eine **digitale Unterschrift**.

Authentifizierung 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.

1.4 Sicherheitsziel Verfügbarkeit

Ein weiteres Hauptziel für die Sicherheit von Daten ist die Verfügbarkeit (engl. availability). Ein sicheres 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
- Redundante physikalische Server-Systeme (doppelte Netzteile, Controller, Netzwerkinterfaces, 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)
- 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

1.5 Rechtliche Aspekte

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 (*http://dejure.org/gesetze/StGB/202a.html*)
- § 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 (*http://dejure.org/gesetze/StGB/303a.html*)
- § 303a Datenveränderung
- § 303b Computersabotage
- Telekommunikationsgesetz (TKG, *http://dejure.org/gesetze/TKG/88.html*)
- 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)
- EU-Datenschutzgrundverordnung (EU-DSGVO)
- Besondere Vertragsbedingungen für die Beschaffung von DV-Leistungen (BVB)

IT-Sicherheitsgesetz

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 ihnen ein Bußgeld. Gleichzeitig werden Hard- und Software-Hersteller zur Mitwirkung bei der Beseitigung von Sicherheitslücken verpflichtet.

Durch das IT-Sicherheitsgesetz werden 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.

4. Kritik am IT-Sicherheitsgesetz

Verfassungsrechtlich bedenklich hinsichtlich der Normenklarheit ist, dass eine auch nur einigermaßen konkrete Bestimmung des Begriffs der Kritischen Infrastruktur und eine Bestimmbarkeit der betroffenen Betreiber im Gesetz fehlt und auf den Verordnungsweg ausgelagert wird. Unklar sind auch die datenschutzrechtlichen Weitergabepflichten und -befugnisse. Die Datenschutzbeauftragten des Bundes und der Länder sind in die Meldewege nicht mit einbezogen.

Das BSI erhält zwar einen erweiterten Aufgabenbereich; mehr Selbstständigkeit gegenüber dem Bundesinnenministerium erhält es aber nicht. Es mangelt an präventiven Ansätzen, die proaktiv zur Verbesserung der IT-Sicherheit beitragen. Vorgesehen sind Meldepflichten und Bußgelder. Es fehlen aber Anreizsysteme wie z. B. die Zertifizierung von Verfahren, ebenso wie gesetzliche Kriterien, die zu einer Qualitätssteigerung von IT-Sicherheitskonzepten und Sicherheitsprüfungen wie z. B. Penetrationstests beitragen. Die Meldepflichten für Sicherheitsvorfälle bestehen erst, wenn es schon zu spät ist, nämlich „bei erheblichen Störungen“, statt bereits zu einem Zeitpunkt, in dem noch kein Schaden eingetreten ist. Die technischen Schutzstandards begnügen sich zu sehr mit einem angenommenen Stand der Technik (§ 8a Absatz 1 Satz 2 BSI-Gesetz), statt auf einem Weiterdenken in Form von Risikoanalysen.

EU-Datenschutzgrundverordnung (EU-DSGVO)

Nach mehrjähriger Debatte hat sich der EU-Trilog (Europäischer Rat, Europäisches Parlament, Europäische Kommission) im Dezember 2015 auf einen endgültigen Inhalt einer neuen EU-Datenschutzverordnung geeinigt. Sie soll die bisher geltende EU-Datenschutzrichtlinie (Richtlinie 95/94/EG) ersetzen und in den nächsten zwei Jahren vollständig in den EU-Mitgliedstaaten umgesetzt werden.

Ziel der Verordnung ist die Vereinheitlichung und die Vereinfachung der Datenschutzrichtlinien innerhalb der EU-Mitgliedstaaten. Mit dieser Verordnung werden die **Nutzerrechte** gegenüber den Verwertern von Nutzerdaten (z. B. Facebook oder Google) nachhaltig gestärkt. Der Nutzer hat das Recht, ausführlich zu erfahren, welche Daten und zu welchem Zweck über ihn gespeichert, verarbeitet und weitergegeben werden. **Personenbezogene Informationen** gehören nun dem Nutzer und nicht den mit der Datenverarbeitung befassten Internetanbietern. Auch wird das vollständige Löschen von personenbezogenen Daten im Internet erleichtert und die rechtswirksame Einwilligung für die Verarbeitung von persönlichen Daten auf ein Mindestalter von 16 Jahren angehoben.

Diese Regelung gilt nicht nur für europäische, sondern auch für nicht in Europa ansässige Unternehmen. Bei einer Verletzung des Datenschutzes sind laut Verordnung Bußgelder bis zu 4 % des Jahresumsatzes möglich.

Die EU-Datenschutzgrundverordnung ist in folgende Abschnitte unterteilt und in seiner übersetzten Fassung unter ***https://dsgvo-gesetz.de/*** verfügbar:

- Kapitel 1 Allgemeine Bestimmungen
- Kapitel 2 Grundsätze
- Kapitel 3 Rechte der betroffenen Person
- Kapitel 4 Für die Verarbeitung Verantwortlicher und Auftragsverarbeiter
- Kapitel 5 Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen
- Kapitel 6 Unabhängige Aufsichtsbehörden
- Kapitel 7 Zusammenarbeit und Kohärenz
- Kapitel 8 Rechtsbehelfe, Haftung und Sanktionen
- Kapitel 9 Vorschriften für besondere Datenverarbeitungssituationen
- Kapitel 10 Delegierte Rechtsakte und Durchführungsrechtsakte
- Kapitel 11 Schlussbestimmungen

Das europäische Parlament hat am 21.04.2016 die neue EU-Datenschutzgrundverordnung beschlossen, welche 2018 in nationales Recht umgesetzt wurde. Damit wird die als überholt geltende Richtlinie von 1995 ersetzt.

Besondere Vertragsbedingungen für die Beschaffung von DV-Leistungen (BVB)

Die Vertragsbedingungen für die Beschaffung von DV-Leistungen dienen der öffentlichen Hand für die Planung und Beschaffung einer funktions- und datensicheren Hard- und Software, entsprechend der Forderungen der rechtlichen Rahmenbedingungen. Zusätzlich gelten ergänzende Vertragsbedingungen für die Beschaffung von Informationstechnik (EVB-IT Version 2 vom 17.03.2016), welche die besonderen Vertragsbedingungen für die Beschaffung von DV-Anlagen und Geräten (BVB) teilweise ablösen bzw. ergänzen.

Die Anwendung der EVB-IT und der BVB ist für Bundesbehörden gemäß Verwaltungsvorschrift zu § 55 BHO festgeschrieben. Auch die Länder richten sich größtenteils nach diesen Vorschriften.

Die aktuellen EVB-IT- und noch gültigen BVB-Dokumente können Sie unter *http://www.cio.bund.de/Web/DE/IT-Beschaffung/EVB-IT-und-BVB/Aktuelle_EVB-IT/aktuelle_evb_it_node.html;jsessionid=9E691728ADCBF026C7C35365E927456F.2_cid334* einsehen.

Das Vertrauensdienstegesetz (*http://www.gesetze-im-internet.de/vdg/)* regelt die wirksame Durchführung der Vorschriften über Vertrauensdienste in der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt. Das Gesetz wird von der Bundesnetzagentur und dem Bundesamt für Sicherheit in der Informationstechnik beaufsichtigt.

Das „Nationale Cyber-Abwehrzentrum“ (NCAZ) hat die Bundesrepublik mit Wirkung vom 01.04.2011 zur Abwehr von Angriffen auf die IT-Infrastruktur der Länder, des Bundes und der Wirtschaft geschaffen. Das NCAZ soll Informationen sammeln, Defizite bei IT-Lösungen aufzeigen, Angriffsanalysen und Hackerprofile erstellen und auf dieser Grundlage Empfehlungen für den Cyber-Sicherheitsrat bereitstellen. Der „Nationale Cyber-Sicherheitsrat“ (NCS) wird aufgrund der Empfehlungen die erforderlichen Schutzmaßnahmen und die notwendige Netzpolitik koordinieren. Unter der Aufsicht des Bundesamtes für Sicherheit in der Informationstechnik (BSI, *http:// www.gesetze-im-internet.de/bundesrecht/bsig_2009/gesamt.pdf*) sind Mitarbeiter des Bundesamtes für Verfassungsschutz (BfV) und des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BKK) im NCS tätig.

2

Risikolage für Unternehmen

2.1 Warum ist das Internet nicht „sicher“?

Die Entstehung des Internets

Das Internet und die dazugehörigen Protokolle wurden in den 60er-Jahren, zur Zeit des Kalten Krieges zwischen den USA und der Sowjetunion, entwickelt.

Die Computersysteme der damaligen Zeit waren zentral gesteuert. Der Ausfall eines zentralen Knotenpunktes (z. B. durch einen Angriff) hätte das gesamte angeschlossene Netz außer Betrieb gesetzt. Paul Baran (Rand Corporation), wurde mit der Konzeption eines ausfallsicheren Netzwerkes beauftragt.

Barans revolutionäres Konzept sah ein Netzwerk vor, bei dem prinzipiell jeder Rechner mit jedem anderen kommunizieren konnte – ein vollständig **dezentrales Netz**. Die Datenpakete sollten sich „selbstständig“ einen Weg von der Quelle zum Ziel suchen und, wenn notwendig, einen anderen Weg einschlagen, falls ein bestimmter Netzknoten ausgefallen war.

Der Vorschlag wurde vom Pentagon ignoriert. Kurz darauf wurde die Projektgruppe Advanced Research Project Agency mit der Entwicklung eines dezentralen Netzes beauftragt. Ende der 60er-Jahre wurde das nach ihr benannte ARPANET in Betrieb genommen.

In den 70er-Jahren wurde das Übertragungsprotokoll **TCP** entwickelt. TCP war dafür konzipiert, Datenströme in Pakete aufzuteilen und diese über das Netzwerk zu versenden. Auf der Empfängerseite konnte TCP die Datenpakete wieder korrekt zu einem Datenstrom zusammensetzen. Auch E-Mail und andere Dienste wurden nach und nach entwickelt.

Bis Ende der 80er-Jahre war das ARPANET und spätere Internet in der Hand der amerikanischen Regierung und vernetzte Militär- und Forschungseinrichtungen.

Anfang der 90er-Jahre begann die amerikanische Regierung sich aus dem Internet zurückzuziehen und es für kommerzielle Firmen zu öffnen.

Der Internet-Boom

Der Boom des Internets begann mit der Entwicklung von **HTTP** (Hypertext Transfer Protocol) und dem ersten **Internet-Browser**, der es auch technisch nicht versierten Benutzern erlaubte, über eine grafische Bedienoberfläche vernetzte Inhalte abzurufen.

Seit mehreren Jahrzehnten ist das Internet ein öffentliches Netz, das von Privatpersonen, Firmen und Behörden weltweit genutzt werden kann. Für die Frage nach der Sicherheit des Internets sind folgende Fakten wichtig:

Die Internetprotokolle wurden im Hinblick darauf entwickelt, eine Datenübertragung auch nach einem Ausfall eines oder mehrerer Netzknoten zu gewährleisten. Die automatische Wegfindung im Netzwerk (auch **Routing** genannt) war hier das Hauptziel.

Für die Übertragung wurden hierfür **TCP** (Transmission Control Protocol) und **UDP** (**User Datagram Protocol**) standardisiert. TCP realisiert eine **verbindungsorientierte** Übertragung, d. h., es wird gewährleistet, dass nicht empfangene Daten-Segmente nochmals versendet werden. UDP arbeitet dagegen **verbindungslos** – d. h., es findet keine Quittierung der empfangenen Segmente statt – und wird vorwiegend für Realtime-Anwendungen genutzt.

Vernetzung: jeder mit jedem

Da die Entwickler nicht absehen konnten, dass dieses Netzwerk später nicht nur die Rechenanlagen des amerikanischen Militärs, sondern Computer weltweit vernetzen würde, wurde auch kein Mechanismus eingebaut, der die Korrektheit der Angaben in den Protokollen sicherstellt. Somit ist es möglich, Datenpakete mit gefälschten Daten oder gezielt manipulierte Pakete in das Netz zu senden.

Da die Internetprotokolle mit dem Ziel entwickelt wurden, dass alle an das Internet angeschlossener Computer miteinander kommunizieren können, haben auch Kriminelle über ihre Rechner Zugriff auf das Internet.

2.2 Schadensmöglichkeiten

Was passieren kann

Wenn ein oder mehrere Rechner eines Unternehmens an das Internet angeschlossen sind, gibt es zahlreiche Möglichkeiten, wie der Einsatz der IT vom Sollzustand abweichen kann. Aus dem Internet kann bösartige Software wie Viren in das Unternehmensnetzwerk gelangen und dort Datenverluste sowie Ausfallzeiten verursachen. Spam und E-Mail-Viren können E-Mail-Server überlasten und Netzwerk-Bandbreiten belegen.

Vertrauliche und geheime Informationen könnten unkontrolliert das Unternehmen verlassen, wenn Hacker in die Netzwerke eindringen, um Informationen auszuspähen und zu stehlen, oder wenn Mitarbeiter unvorsichtig Dokumente versenden. Erlangen unautorisierte Personen von intern als auch von extern Zugriff auf Dateien und Systeme, können Daten manipuliert und Netzwerke modifiziert werden.