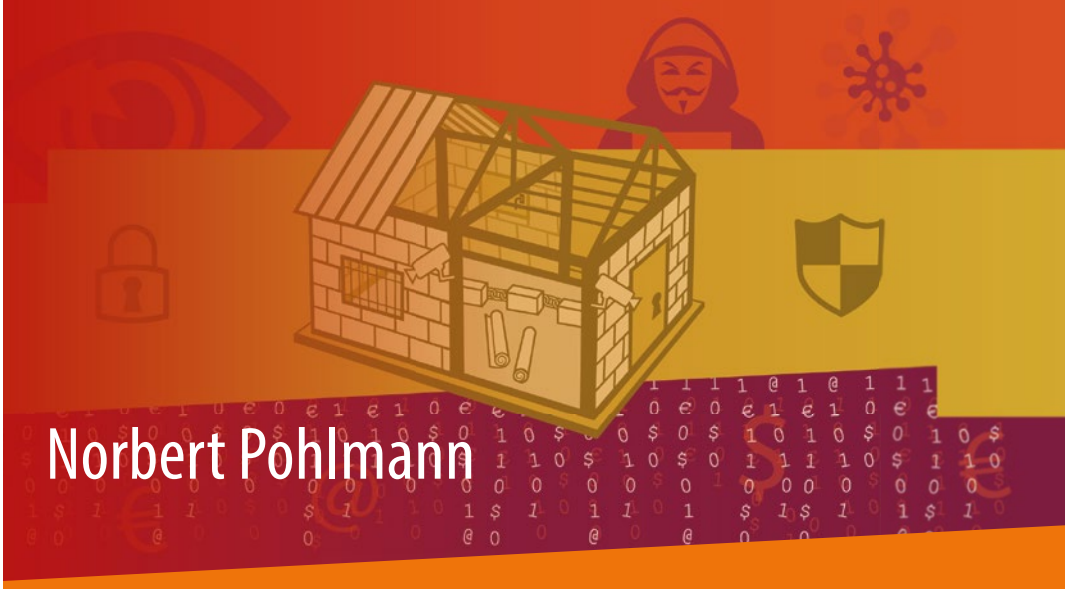


Norbert Pohlmann

Cyber-Sicherheit

Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung

2. Auflage

Springer Vieweg

Norbert Pohlmann

Cyber-Sicherheit

Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung

2. Auflage

Springer Vieweg

Vorwort

Wir leben inmitten der Zeit des digitalen Wandels, der eine radikale Umgestaltung unseres Alltags und unserer Arbeitswelt sowie aller Geschäftsmodelle und Verwaltungsprozesse bedeutet.

Wirtschaftskraft und Wohlstand sowie die Leistungsfähigkeit unserer modernen Gesellschaft werden durch den gelungenen digitalen Wandel bestimmt.

Nur mit angemessener Cyber-Sicherheit wird eine nachhaltige Digitalisierung gelingen!
Cyber-Sicherheit – Das Lehrbuch für Architekturen, Konzepte, Prinzipien, Mechanismen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung – soll helfen, ein sicheres und vertrauenswürdiges Fundament für unsere digitale Zukunft zu schaffen.

Veränderungen der zweiten Auflage:
In der zweiten Auflage dieses Buches wurden viele Änderungen umgesetzt. In allen Kapiteln wurden Texte und Bilder erweitert und optimiert, um die Lesbarkeit und das Verständnis zu verbessern. Außerdem sind Anregungen aus Rezensionen und Feedbacks in die 2 Auflage eingeflossen.

Das Kap. 1 „Sichtweisen auf die Cyber-Sicherheit im Cyber-Raum“ wurde neu strukturiert und Ergänzungen wie „Schäden“ und „Angriffsvektoren“ aufgenommen. Im Kap. 2 „Kryptografie“ wurde der Mode of Operation CCM-Mode (Counter with CBC-MAC) hinzugefügt, da dieser durch TLS 1.3 eine neue Bedeutung bekommen hat. Im Kap. 5 „Identifikation und Authentifikation“ wurde insbesondere der Teil „Biometrische Verfahren“ optimiert und mit „Gegenmaßnahmen von Präsentationsangriffen“ erweitert. Außerdem wurde ein Unterkapitel „Anonymität im Cyber-Raum“ ergänzt. Im Kap. 10 „IPSec-Verschlüsselung“ wurden Inhalte zu dem neuen Internet Key Exchange Protocol Version 2 (IKEV2) eingefügt. Das Kap. 11 „Transport Layer Security (TLS)/Secure Socket Layer (SSL)“ wurde mit der neuen Version TLS 1.3 ergänzt. Das Kap. 13 „E-Mail-Sicherheit“ wurde mit einer Abhandlung über Spam-E-Mails erweitert. Im Kap. 15 „Künstliche Intelligenz und Cyber-Sicherheit“ wurden Inhalte wie „Qualität der Eingabedaten“, „Manipulationen von Künstlicher Intelligenz“ sowie „Ethik und Künstliche Intelligenz“ hinzugefügt. Das Kap. 16 „Social Web Cyber-Sicherheit“ wurde mit einem Abschnitt „Cyber-Mobbing“ erweitert.

Ganz neu hinzugekommen sind die Kap. 18 „Self-Sovereign Identity (SSI)“, Kap. 19 „Vertrauen und Vertrauenswürdigkeit“, Kap. 20 „Weitere Aspekte der Cyber-Sicherheit“ mit „DNS over HTTPS (DoH)“, „Backup“, „Chancen und Risiken von Smart Home“, „Risiken und Sicherheit eines Homeoffice“ sowie „Upload-Filter“ und mit Kap. 21 wurde ein „Glossar“ mit Beschreibungen der verwendeten Begrifflichkeiten eingeführt.

Welchen Anspruch hat das Buch?
Das Lehrbuch Cyber-Sicherheit verfolgt das Anliegen, dem Leser eine fundierte und anwendungsorientierte Einführung in das Themenfeld Cyber-Sicherheit zu geben. Es werden Cyber-Sicherheitsarchitekturen vermittelt, die aufzeigen, wie zukünftige IT-Systeme besser aufgebaut werden können. Das Lehrbuch behandelt Cyber-Sicherheitskonzepte, die dabei unterstützen, einen angemessenen Level an Cyber-Sicherheit in der sich immer schneller verändernden Gesellschaft zur Verfügung zu stellen. Die Diskussion von Cyber-Sicherheitsprinzipien soll dazu dienen, sich in der komplexen Welt der Cyber-Sicherheit zurechtzufinden. Cyber-Sicherheitsmechanismen werden als Basisinstrumente ausführlich behandelt, weil sie die Grundlage eines Cyber-Sicherheitssystems sind. Aber auch die Cyber-Sicherheitseigenschaften werden aufgezeigt, um Wirksamkeit und weitere Aspekte von Cyber-Sicherheitslösungen beurteilen zu können.

Dabei wird der Schwerpunkt auf exemplarisches Lernen gelegt, da der Stoff zu mächtig ist, um vollständig behandelt zu werden. Es werden die wichtigen Aspekte der Cyber-Sicherheit als Grundlage mit exemplarischen Beispielen behandelt. Mithilfe von Übungsaufgaben kann das erworbene Verständnis überprüft werden.

Für wen ist das Buch gedacht?
Das Lehrbuch richtet sich in erster Linie an Studierende all der Fachbereiche, in denen die Digitalisierung eine besondere Rolle spielt, vor allem die Fachrichtungen Informatik, IT-Sicherheit, Internet- oder Cyber-Sicherheit und angrenzende Disziplinen.

Es ist aber auch geeignet für Auszubildende im Bereich Fachinformatik und für Mitarbeiter*innen aller Branchen und Unternehmen, die sich mit der Digitalisierung beschäftigen und das Thema Cyber-Sicherheit berücksichtigen wollen.

Um den Lesefluss nicht zu beeinträchtigen, wird in diesem Lehrbuch zwar hauptsächlich die männliche Form genannt, stets sind aber die weibliche Form und andere Formen gleichermaßen gemeint.

Als ich mit viel Freude begann, die 2. Auflage des Buches Cyber-Sicherheit zu schreiben, habe ich wie schon bei der ersten Auflage, feststellen müssen, dass ich den Umfang dieser selbstgewählten Aufgabe wieder weit unterschätzt habe, obwohl ich es mit meinen Erfahrungen hätte besser wissen müssen.

Meine Begeisterung ist dennoch geblieben, weil ich das Thema Cyber-Sicherheit spannend finde und die intensive Auseinandersetzung damit für mich persönlich eine Bereicherung darstellt.

Ich wünsche mir, dass meine Faszination für die Cyber-Sicherheit zu Ihnen überschwappt, weil wir sehr viele Cyber-Sicherheitsexperten brauchen, die helfen, den Weg der Digitalisierung mit sicheren und vertrauenswürdigen IT-Systemen und IT-Infrastrukturen auf ein stabiles Fundament für unsere digitale Zukunft zu setzen.

Besonders möchte ich den Menschen in meiner Umgebung für ihr Verständnis danken, dass meine Aufmerksamkeit und Energie während der Zeit des Schreibens nicht auf sie gerichtet war.

Mein besonderer Dank gilt den Cyber-Sicherheitsspezialisten des Instituts für Internet-Sicherheit, die immer wieder unverzichtbare Anregungen für Verbesserungen und Erweiterungen gegeben sowie bei der Konzeption und Umsetzung der Übungsaufgaben geholfen haben. Hierzu gehören Johnny Hoang, Dr. Tobias Urban und Alexander Stöhr. Aber ich möchte auch Ulla Coester danken, mit der ich in den letzten Jahren das Thema Vertrauen und Vertrauenswürdigkeit in vielen Artikel erarbeitet und beschrieben habe.

Besonders danke ich Farina Lehmann, die mir geholfen hat, alle Grafiken verständlich nach einem einheitlichen Schema zu gestalten und umzusetzen, um so das Verstehen für Sachverhalte deutlich zu verbessern. Ich danke auch Frau Nicola Pache, die Verantwortung für die Rechtschreibung übernommen hat.

Da ich dieses Buch nicht für mich, sondern für eine breite und interessierte Leserschaft geschrieben habe, bin ich sehr an Rückmeldungen interessiert und bitte alle Leser*innen, die Anmerkungen, Anregungen oder Verbesserungsvorschläge für die nächste Auflage haben oder Ideen, wie die Übungen auf den Webseiten optimiert und erweitert werden können, sich mit mir in Verbindung zu setzen.

Jedes Feedback ist wichtig und willkommen!
E-Mail: cyber-sicherheit@norbert-pohlmann.com

Ich wünsche allen Leser*innen dieses Lehrbuches, dass sie das finden, was sie suchen und Freude und Spaß beim Lesen haben.

Weitere Unterstützungen auf meiner Webseite
Auf dieser Webseite finden Sie weitere Informationen und Hilfestellungen, die das Buch Cyber-Sicherheit betreffen: https://norbert-pohlmann.com/cyber-sicherheit/

Die Ergebnisse der Übungsaufgaben aus dem Buch finden Sie unter:
https://norbert-pohlmann.com/cyber-sicherheit/uebungen/

Für alle stehen auch die Vorlesungen der einzelnen Kapitel als PDFs zum freien Download zur Verfügung.
https://norbert-pohlmann.com/cyber-sicherheit-vorlesungen/

Kollegen*innen, Lehrbeauftragte, Lehrer*innen und weitere Interessierte finden zu diesem Lehrbuch auch noch Folien mit den Bildern sowie darauf basierende Vorlesungen aus diesem Buch auf meiner Webseite:
https://norbert-pohlmann.com/cyber-sicherheit/vorlesungen/

Und vieles mehr …

Übersicht
Im Folgenden finden Sie einen Überblick über das Lehrbuch Cyber-Sicherheit

Sichtweisen auf die Cyber-Sicherheit
In dieser Art Einleitung werden unterschiedliche Sichtweisen auf die Cyber-Sicherheit diskutiert, um eine Grundlage für das Verständnis des Themas Cyber-Sicherheit, die Probleme, Herausforderungen, Rahmenbedingungen, Paradigmen, Wirksamkeitskonzepte, Bedürfnisse, Strategien, Motivationen, Angriffsvektoren, Schäden und Risiken aufzubauen.

Kryptografie
Im Kapitel Kryptografie werden Kenntnisse über den Aufbau, die Prinzipien, die Architektur und die Funktionsweise von grundlegenden kryptografischen Verfahren vermittelt. Kryptografische Verfahren spielen eine besondere Rolle bei vielen wichtigen Cyber-Sicherheitssystemen zur Gewährleistung der Cyber-Sicherheitsbedürfnisse, wie Vertraulichkeit, Authentifikation, Authentizität, Integrität und Verbindlichkeit.

Hardware-Sicherheitsmodule zum Schutz von Sicherheitsinformationen
Immer mehr Sicherheitsinformationen, wie zum Beispiel geheime Schlüssel und Transaktionsdaten, werden durch Bezahlsysteme sowie Verschlüsselungs- und Authentifikationslösungen im Internet genutzt. In diesem Kapitel werden unterschiedliche Hardware-Sicherheitsmodule beschrieben, die helfen, besonders sensible Sicherheitsinformationen angemessen zu schützen.

Digitale Signatur, elektronische Zertifikate sowie Public Key Infrastruktur (PKI) und PKI-enabled Application (PKA)
In diesem Kapitel werden die Themen digitale Signatur, elektronische Zertifikate sowie Public-Key Infrastrukturen und PKI-enabled Application behandelt. Diese Cyber-Sicherheitsprinzipien und Cyber-Sicherheitsmechanismen sind in einer modernen Informations- und Wissensgesellschaft von enormer Wichtigkeit und helfen dabei, zentrale Vertrauensdienste und ein modernes Schlüsselmanagement aufzubauen.

Identifikation und Authentifikation
Die Identifikation und Authentifikation spielen in der modernen IT und im Internet eine besondere Rolle. Aus diesem Grund werden in diesem Kapitel die Grundlagen dargestellt sowie unterschiedliche Identifikations- und Authentifikationsverfahren behandelt und die Vor- und Nachteile diskutiert.
Außerdem werden die Konzepte risikobasierte und adaptive Authentifizierung, FIDO, Identity Provider und weitere Ideen und Initiativen sowie Anonymität im Cyber-Raum behandelt.

Enterprise Identity und Access Management
Die Begriffe Enterprise Identity und Access Management beschreiben jeglichen Einsatz von digitalen Identitäten, deren Attributen, deren Berechtigungen für

IT-Systeme sowie IT-Dienste und schließen die Erzeugung, Nutzung, Pflege und Löschung dieser digitalen Identitäten mit ein. Ziel ist es, vertrauenswürdige, identitätsbezogene und regelkonforme Prozesse durchzusetzen, die unabhängig von Organisationen und Plattformen standardisiert nutzbar sind. Dazu wird ein Referenzmodell mit den entsprechenden Komponenten sowie den enthaltenen Funktionen in diesem Kapitel dargestellt und erläutert.

Trusted Computing
Trusted Computing ist eine Cyber-Sicherheits- und Vertrauenswürdigkeitstechnologie. Mithilfe von Trusted Computing stehen moderne und intelligente Cyber-Sicherheitsarchitekturen, -konzepte und -funktionen zur Verfügung, mit denen IT-Systeme mit einer höheren Robustheit und einem höheren Cyber-Sicherheitslevel umgesetzt werden können. Der besondere Schwerpunkt liegt dabei auf der Verifikation der Integrität eines IT-Systems.

Cyber-Sicherheit Frühwarn- und Lagebildsysteme
In diesem Kapitel geht es um die Bedeutung und Grundstruktur eines Cyber-Sicherheit Frühwarn- und Lagebildsystems. Die grundsätzliche Idee sowie unterschiedliche Sensoren werden beschrieben und diskutiert. Außerdem werden die notwendigen Prozesse und die Probleme, die durch die Entwicklung eines Cyber-Sicherheit Frühwarn- und Lagebildsystems entstehen, behandelt.

Firewall-Systeme
Ein Firewall-System ist ein Cyber-Sicherheitsmechanismus, der zwischen verbundenen Netzen durch Regulierung und Kontrolle Sicherheitsdomänen mit unterschiedlichem Schutzbedarf schafft. Es wird meist zum Schutz eigener Netze vor Risiken aus unsicheren Netzen wie dem Internet, aber auch zur Strukturierung eigener Netze in einer Organisation eingesetzt. Dabei müssen unterschiedliche Aspekte berücksichtigt werden, damit mithilfe eines Firewall-Systems das gewünschte Sicherheitsmaß auch erreicht werden kann. Durch eine Reduzierung von Kommunikationsmöglichkeiten über ein Firewall-System wird die Angriffsfläche und dadurch das Risikopotenzial minimiert. In diesem Kapitel werden Ideen, Definitionen, Grundlagen, Konzepte sowie Möglichkeiten und Grenzen von Firewall-Systemen behandelt.

IPSec-Verschlüsselung
Im Kapitel IPSec-Verschlüsselung werden die Cyber-Sicherheitsarchitektur, Cyber-Sicherheitsprinzipien, Cyber-Sicherheitsmechanismen und Cyber-Sicherheitsprotokolle des IETF Sicherheitsstandards für die Cyber-Sicherheit von IP-Paketen vermittelt.

Transport Layer Security (TLS)/Secure Socket Layer (SSL)
Das Kapitel TLS/SSL vermittelt die Cyber-Sicherheitsarchitektur, Cyber-Sicherheitsprinzipien, Cyber-Sicherheitsmechanismen und Cyber-Sicherheitsprotokolle des IETF Sicherheitsstandards für die Transport-Ebene.

Cyber-Sicherheitsmaßnahmen gegen DDoS-Angriffe
Die Gewährleistung der Verfügbarkeit von IT-Systemen und IT-Infrastrukturen ist ein wichtiges Cyber-Sicherheitsbedürfnis, um Informationen und Dienste immer nutzen zu können. In diesem Kapitel werden DDoS-Angriffe, Ziele von DDoS-Angriffsmethoden und hilfreiche Cyber-Sicherheitsmaßnahmen gegen DDoS-Angriffe beschrieben.

E-Mail-Sicherheit
Die E-Mail-Anwendung ist eine der wichtigsten Kommunikationsmöglichkeiten, insbesondere im Business-Bereich. Daher wird in diesem Kapitel das Thema E-Mail-Sicherheit behandelt und die verschiedenen Cyber-Sicherheitskonzepte und Möglichkeiten diskutiert. Außerdem wird das Thema Spam-E-Mail prinzipiell beschrieben und diskutiert.

Blockchain-Technologie
Dieses Kapitel erläutert und diskutiert die Grundzüge der Blockchain-Technologie, das Cyber-Sicherheitskonzept, die notwendigen Netzwerk-, Cyber-Sicherheits- und Vertrauenswürdigkeitsmechanismen sowie Beispielanwendungen der Blockchain-Technologie. Außerdem werden die Sicherheit und Vertrauenswürdigkeit der Blockchain-Technologie diskutiert.

Künstliche Intelligenz und Cyber-Sicherheit
In diesem Kapitel wird behandelt, wie die Algorithmen aus Maschinellem Lernen und Künstlicher Intelligenz genutzt werden können, um die Cyber-Sicherheit zu verbessern. Potenziale liegen in den Bereichen Verbesserung der Erkennungsrate von Angriffen, Unterstützung von Cyber-Sicherheitsexperten, die die Wirkung von Cyber-Sicherheitslösungen erhöhen. Es werden auch Beispiele aus der Cyber-Sicherheitsforschung dargestellt. Weitere Themen sind die Qualität der Eingangsdaten, die IT-Sicherheit von KI-Systemen sowie Ethik und Künstliche Intelligenz.

Social Web Cyber-Sicherheit
Soziale Netzwerke bringen Nutzer aus verschiedenen Gesellschaftsgruppen zusammen und ermöglichen ihnen, sich darzustellen, Informationen und Meinungen auszutauschen sowie sich einfacher und zielgerichteter real zu begegnen. Aber der Erfolg der sozialen Netzwerke hat auch bekannte Nachteile und Herausforderungen im Bereich der Cyber-Sicherheit, die in diesem Kapitel dargestellt und diskutiert werden. Behandelte Punkte sind: Fake-News, Social-Bots, Filterblasen, Echokammern, Psychometrie sowie Cyber-Mobbing mit den verschiedenen Aspekten.

Wirtschaftlichkeit von Cyber-Sicherheitsmaßnahmen
Cyber-Sicherheitsmaßnahmen sind kein Selbstzweck. Mithilfe von Cyber-Sicherheitsmaßnahmen kann das Risiko bei der Nutzung von IT-Systemen erheblich reduziert und damit ein Schaden verhindert werden. In diesem Kapitel werden die Kosten und der Nutzen der Cyber-Sicherheitsmaßnahmen behandelt. Das Modell „Return on Security Investment (RoSI)“ wird dargestellt und es wird anhand

eines Beispiels aufgezeigt, wie mit der Investition von Cyber-Sicherheitsmaßnahmen ein Return on Investment erzielt werden kann.

Self-Sovereign Identity (SSI)
In diesem Kapitel werden die Architektur, die Akteure, die Sicherheitsinfrastruktur und -mechanismen sowie die Prinzipien von Self-Sovereign Identity (SSI) erläutert. Self-Sovereign Identity (SSI) sorgt für eine sichere und vertrauenswürdige Digitalisierung. Nutzer können selbstbestimmt ihre digitale Identität und Nachweise wie Ausweis oder Bescheinigungen an Anwendungen weitergeben, die diese auf Echtheit automatisiert überprüfen können.

Vertrauen und Vertrauenswürdigkeit
Die Vertrauenswürdigkeit von IT-Lösungen und Hersteller-/Anbieterunternehmen ist die Basis für das Vertrauen und damit die Akzeptanz der Nutzer in die digitale Zukunft. Aus diesem Grund werden in diesem Kapitel die Begriffe Vertrauen und Vertrauenswürdigkeit sowie Mechanismen zur Vertrauensbildung und Vertrauenswürdigkeitstechnologie beschrieben und diskutiert.

Weitere Aspekte der Cyber-Sicherheit
In diesem Kapitel werden verschiedene Aspekte der Cyber-Sicherheit behandelt. Themen sind DNS over HTTPS (DoH), Backups, Chancen und Risiken von Smart Home, Risiken und Sicherheit eines Homeoffice und Upload-Filter.

Glossar
In diesem Kapitel werden wichtige Begriffe der Cyber-Sicherheit aufgelistet und erläutert, die im Buch verwendet werden.

Anhang
Im Anhang befindet sich eine Übersicht der im Lehrbuch Cyber-Sicherheit genutzten Symbole. Außerdem ist dort ein Sachwortverzeichnis zu finden.

Gelsenkirchen, Deutschland Norbert Pohlmann

Inhaltsverzeichnis

1 Sichtweisen auf die Cyber-Sicherheit im Cyber-Raum 1
1.1 Einleitung 1
1.2 Cyber-Sicherheitsherausforderungen im Cyber-Raum 5
1.2.1 Cyber-Sicherheitsherausforderung „Zu viele Schwachstellen in Software“ 6
1.2.2 Cyber-Sicherheitsherausforderung „Ungenügender Schutz vor zunehmender intelligenter Malware“ 7
1.2.3 Cyber-Sicherheitsherausforderung „Keine Lösungen für Identifikation und Authentifikation für den gesamten Cyber-Raum“ 9
1.2.4 Cyber-Sicherheitsherausforderung „Unsichere Webseiten im Internet“ 9
1.2.5 Cyber-Sicherheitsherausforderung „Gefahren durch die Nutzung mobiler Geräte“ 10
1.2.6 Cyber-Sicherheitsherausforderung „Mehr E-Mail – mehr Risiko“ 11
1.2.7 Cyber-Sicherheitsherausforderung „Unsichere IoT-Geräte und -Plattformen“ 12
1.2.8 Cyber-Sicherheitsherausforderung „Internetnutzer haben zu wenig Medien-Kompetenz im Cyber-Raum“ 14
1.2.9 Cyber-Sicherheitsherausforderung „Manipulierte IT und IT-Sicherheitstechnologien“ 15
1.2.10 Cyber-Sicherheitsherausforderung „Geschäftsmodell: Bezahlen mit persönlichen Daten“ 16
1.2.11 Cyber-Sicherheitsherausforderung „Fake News“ und weitere unerwünschte Inhalte 17
1.3 Problematische Rahmenbedingungen im Cyber-Raum 18
1.4 Gesellschaftliche Herausforderungen im Cyber-Raum 19
1.4.1 Privatsphäre und Datenschutz 19
1.4.2 Selbstbestimmung und Autonomie 21
1.4.3 Wirtschaftsspionage 22
1.4.4 Cyberwar 23
1.5 Wechseln vom Paradigmen im Cyber-Raum 24

1.5.1 Paradigmenwechsel „Verantwortung versus Gleichgültigkeit“ . . . 25
1.5.2 Paradigmenwechsel „Proaktive versus reaktive Cyber-Sicherheitslösungen“ . . . 25
1.5.3 Paradigmenwechsel „Objekt-Sicherheit versus Perimeter-Sicherheit“ . . . 26
1.5.4 Paradigmenwechsel „Cloud-Service versus Lokal-IT“ . . . 27
1.5.5 Paradigmenwechsel „Dezentrale versus zentrale Cyber-Sicherheit“ . . . 28
1.5.6 Paradigmenwechsel „datengetriebene- versus ereignisgesteuerte-Sicherheit“ . . . 28
1.5.7 Paradigmenwechsel „Zusammenarbeit versus Isolierung“ . . . 28
1.6 Konzept der Wirksamkeit von Cyber-Sicherheitssystemen . . . 29
1.6.1 Indirekte Angriffe auf die Werte . . . 30
1.6.2 Stärke eines Cyber-Sicherheitsmechanismus gegen einen direkten Angriff . . . 31
1.6.3 Überwindung des Cyber-Sicherheitsmechanismus durch einen direkten Angriff (unzureichende Wirkung) . . . 32
1.6.4 Erfolgreiche Abwehr eines Cyber-Sicherheitsmechanismus durch einen direkten Angriff (ausreichende Wirkung) . . . 32
1.7 Cyber-Sicherheitsbedürfnisse/Cyber-Sicherheitsziele . . . 33
1.8 Cyber-Sicherheitsstrategien . . . 34
1.8.1 Vermeiden von Angriffen . . . 35
1.8.2 Entgegenwirken von Angriffen . . . 38
1.8.3 Erkennen von Angriffen . . . 39
1.8.4 Reaktion auf Angriffe . . . 40
1.9 Angreifer und deren Motivationen . . . 42
1.9.1 Angreifer Motivationen . . . 43
1.9.2 Kategorien von Angreifern . . . 43
1.10 Angriffsvektoren und Angriffsbeispiele . . . 45
1.11 Das Pareto-Prinzip der Cyber-Sicherheit . . . 49
1.12 Cyber-Sicherheitsschäden . . . 50
1.13 Absichern des Cyber-Sicherheitsrisikos . . . 52
1.14 Zusammenfassung . . . 55
1.15 Übungsaufgaben . . . 56
Literatur . . . 59

2 Kryptografie . . . 61
2.1 Grundlagen der Kryptografie . . . 61
2.1.1 Grundlagen der Verschlüsselung . . . 62
2.1.2 Definition eines kryptografischen Verfahrens . . . 64
2.1.3 No Security by Obscurity . . . 64
2.1.4 Die wichtigsten Begriffe in Kurzdefinition . . . 65
2.1.5 Begriffe aus der Kryptoanalysis . . . 65
2.1.6 Strategien der Analyse eines Kryptosystems . . . 66

2.1.7 Bewertung der kryptografischen Stärke 67
2.1.8 Unterstützung bei der Einschätzung von Verfahren und Schlüssellängen 71
2.1.9 Zusammenfassung: Grundlagen der Kryptografie 71
2.2 Elementare Verschlüsselungsverfahren 72
2.2.1 Monoalphabetische Substitution 72
2.2.2 Homofone Substitution 73
2.2.3 Polyalphabetische Substitution 75
2.2.4 Transpositionsverfahren 76
2.2.5 Zusammenfassung: Elementare Verschlüsselungsverfahren . . . 77
2.3 Der Einmal-Schlüssel 77
2.4 Symmetrische Verschlüsselungsverfahren 78
2.4.1 Data Encryption Standard (DES) 79
2.4.2 Advanced Encryption Standard (AES) 80
2.4.3 Zusammenfassung von symmetrischen Verschlüsselungsverfahren 83
2.5 Verwaltung von Schlüsseln (Key Management) 84
2.6 Blockverschlüsselung/Mode of Operation 86
2.6.1 Betriebsart: Electronic Code Book Mode (ECB-Mode) 87
2.6.2 Betriebsart: Cipher Block Chaining Mode (CBC-Mode) . . . 87
2.6.3 Betriebsart: Cipher Feedback Mode (CFB-Mode) 89
2.6.4 Betriebsart: Output Feedback Mode (OFB-Mode) 90
2.6.5 Betriebsart: Counter Mode (CTR-Mode) 91
2.6.6 Betriebsart: Galois/Counter Mode (GCM-Mode) 92
2.6.7 Betriebsart: CCM-Mode (Counter with CBC-MAC) 93
2.6.8 Zusammenfassung: Modes of Operation 93
2.7 Steganografie 94
2.8 Asymmetrische Verschlüsselungsverfahren 95
2.8.1 Das RSA-Verfahren 98
2.8.2 Das Diffie-Hellman-Verfahren 100
2.8.3 Elliptische Kurven 102
2.8.4 Hybride Verschlüsselungsverfahren 102
2.9 Quantencomputer: Das Damoklesschwert der Verschlüsselung 103
2.10 One-Way-Hashfunktionen 104
2.10.1 Besondere Eigenschaften von Hashfunktionen 105
2.10.2 SHA-3 (SHA = Secure Hash Algorithm) 106
2.10.3 Message Authentication Code (MAC) 107
2.10.4 Keyed-Hashing for Message Authentication (HMAC) 107
2.11 Zusammenfassung 109
2.12 Übungsaufgaben 109
Literatur 117

3 Hardware-Sicherheitsmodule zum Schutz von Sicherheitsinformationen 119
3.1 Einleitung 119

3.2 Hardware-Sicherheitsmodul: Smartcards 120
3.3 Hardware-Sicherheitsmodul: Trusted Platform Module (TPM) 122
3.4 Hardware-Sicherheitsmodul: High-Level Security Module (HLSM) 124
3.5 Trusted Execution Environment (TEE) 127
3.6 Zusammenfassung: Kategorien von Hardware-Sicherheitsmodulen. 127
3.7 Evaluierung und Zertifizierung für eine höhere Vertrauenswürdigkeit von Hardware-Sicherheitsmodulen 128
3.8 Key-Management von Hardware-Sicherheitsmodulen 129
3.8.1 Das Management von TPMs 129
3.8.2 Vier-Augen-Prinzip 129
3.9 Zusammenfassung 130
3.10 Übungsaufgaben. 130
Literatur. 132

4 Digitale Signatur, elektronische Zertifikate sowie Public Key-Infrastruktur (PKI) und PKI-enabled Application (PKA) 133
4.1 Digitale Signatur 133
4.1.1 Eigenhändige Unterschrift als Äquivalent zur digitalen Signatur 133
4.1.2 Digitale Signatur mithilfe eines Public Key-Verfahrens 135
4.2 Elektronische Zertifikate/digitale Zertifikate 137
4.3 Public Key-Infrastrukturen 140
4.3.1 Idee und Definition von Public Key-Infrastrukturen 141
4.3.2 Offene und geschlossene PKI-Systeme 145
4.3.3 Umsetzungskonzepte von Public Key-Infrastrukturen 148
4.4 Vertrauensmodelle von Public Key-Infrastrukturen. 150
4.4.1 Vertrauensmodell: Übergeordnete CA (Wurzel-CA, Root CA) 150
4.4.2 Vertrauensmodell: n:n-Cross-Zertifizierung 151
4.4.3 Vertrauensmodell: 1:n Cross-Zertifizierung (Bridge CA) . . . 152
4.4.4 Fazit 153
4.5 Gesetzlicher Hintergrund 153
4.6 PKI-enabled Application (Beispiele) 157
4.6.1 E-Mail-Sicherheit. 157
4.6.2 Lotto – Online-Glückspiel 163
4.7 Zusammenfassung 165
4.8 Übungsaufgaben. 166
Literatur. 167

5 Identifikation und Authentifikation 169
5.1 Was ist eine Identifikation und Authentifikation? 169
5.1.1 Identifikation 169
5.1.2 Authentifikation 171
5.1.3 Klassen von Authentifizierungsverfahren 173

5.2 Identifikationsverfahren 174
5.2.1 Vorlage eines Personalausweises 175
5.2.2 Fernidentifizierung – Allgemeine Aspekte. 175
5.2.3 Videoidentifikation. 176
5.2.4 Das eID Verfahren des elektronischen Personalausweises . . . 179
5.2.5 Das PostIdent-Verfahren der Deutschen Post AG 181
5.2.6 Vergleich der verschiedenen Identifikationsverfahren. 182
5.2.7 Weitere Identifikationsverfahren 184
5.2.8 Abgeleitete Identitäten – vertrauenswürdige digitale Identität 186
5.3 Authentifikationsverfahren. 187
5.3.1 Passwort-Verfahren 187
5.3.2 Einmal-Passwort-Verfahren 198
5.3.3 Challenge-Response-Verfahren 200
5.3.4 Biometrische Verfahren 202
5.3.5 Weitere unterstützende Faktoren (Reputation, Technologie, Standort, Zeit) 214
5.4 Multifaktor-Authentifizierung 216
5.5 Konzept der risikobasierten und adaptiven Authentifizierung 217
5.6 Modernes Multifaktor-Authentifizierungssystem und Identifikationsverfahren 218
5.7 Fast Identity Online Alliance (FIDO) 223
5.7.1 Ziele der FIDO Alliance. 224
5.7.2 Die FIDO-Architektur 225
5.7.3 Authentifizierung des Nutzers 227
5.8 Identity Provider 227
5.8.1 OpenID. 228
5.8.2 OAuth 2.0. 231
5.8.3 OpenID Connect 235
5.9 Anonymität im Cyber-Raum 236
5.10 Zusammenfassung 237
5.11 Übungsaufgaben. 238
Literatur. 239

6 Enterprise Identity und Access Management. 241
6.1 Szenario eines Enterprise Identity and Access Management-Systems 243
6.2 Enterprise Identity and Access Management-Referenzmodell 244
6.3 Policies & Workflows. 244
6.3.1 Policy Management 245
6.3.2 Workflow Management 246
6.3.3 Beispiel für Policies & Workflows. 246
6.4 Repository Management 246
6.4.1 Auf einer Datenbank basierendes Directory 247
6.4.2 Metadirectory. 247

6.4.3 Virtual Directory 248
6.4.4 Identity Repository. 248
6.4.5 Policy Repository. 248
6.4.6 Beispiel für Repository Management 248
6.5 Life Cycle Management. 248
6.5.1 Identity-Administration 249
6.5.2 Provisionierung 249
6.5.3 Rollenmanagement 250
6.5.4 Privileged User Management. 250
6.5.5 Delegierte Administration 251
6.5.6 Synchronisierung 251
6.5.7 Self-Service 251
6.5.8 Credential Management. 252
6.5.9 Beispiel für Life Cycle Management. 252
6.6 Access Management 252
6.6.1 Authentisierungs- und Authentifizierungs-Management 253
6.6.2 Autorisierungs-Management 253
6.6.3 Single Sign-On/Single Log-out 254
6.6.4 Access Control. 255
6.6.5 Remote Access Control 255
6.6.6 Network Access Control 256
6.6.7 Policy Enforcement 256
6.6.8 Beispiel für Access Management. 257
6.7 Information Protection. 257
6.7.1 Secure Sharing 258
6.7.2 Information Rights Management. 258
6.7.3 Content Security. 258
6.7.4 Beispiel für Information Protection 259
6.8 Federation 259
6.8.1 Trust Management 259
6.8.2 Identity Federation. 260
6.8.3 Beispiel für Federation. 260
6.9 Compliance & Audit 260
6.9.1 Compliance Management 261
6.9.2 Monitoring 262
6.9.3 Reporting 262
6.9.4 Auditing 262
6.9.5 Beispiel für Compliance & Audit 262
6.10 Allgemeine Mehrwerte eines Enterprise Identity and Access Management-Systems 263
6.11 Zusammenfassung 266
6.12 Übungsaufgaben. 266
Literatur. 267

7 Trusted Computing 269
7.1 Einleitung 269
7.2 Trusted Computing auf den Punkt gebracht 272
7.2.1 Robustheit und Modularität 272
7.2.2 Integritätsüberprüfung 273
7.2.3 Trusted Process 274
7.2.4 Trusted Platform 275
7.3 Trusted Computing – Grundlagen 275
7.3.1 Kernelarchitekturen von Betriebssystemen 275
7.3.2 Core Root of Trust for Measurement (CRTM) 278
7.3.3 Identitäten von TPMs 279
7.3.4 TPM-Schlüssel und deren Eigenschaften 280
7.4 Trusted Computing-Funktionen 284
7.4.1 Authenticated Boot 285
7.4.2 Binding 286
7.4.3 Sealing (Erweiterung von Binding) 286
7.4.4 (Remote) Attestation (Beglaubigung, Überprüfung der Systemkonfiguration eines IT-Systems) 287
7.5 Trusted Platform (Security-Plattform, Sicherheitsplattform) 289
7.6 Beispielanwendungen 292
7.7 Trusted Network Connect (TNC) 296
7.7.1 Problemstellung 297
7.7.2 Anforderungen an heutige Netzwerke 298
7.7.3 Vertrauenswürdige Netzwerkverbindungen 298
7.7.4 Trusted Network Connect (TNC) im Detail 300
7.7.5 Anwendungsfelder 303
7.7.6 Kritische Diskussion 304
7.7.7 Zusammenfassung Trusted Network Connect (TNC) 306
7.8 Festlegung einer sicheren und vertrauenswürdigen Systemkonfiguration 306
7.9 Zusammenfassung 307
7.10 Übungsaufgaben 307
Literatur 308

8 Cyber-Sicherheit-Frühwarn- und Lagebildsysteme 309
8.1 Einleitung 309
8.2 Angriffe und ihre Durchführung 309
8.3 Idee eines Cyber-Sicherheit-Frühwarnsystems 317
8.3.1 Reaktionszeit für die Frühwarnung 317
8.3.2 Definition eines Cyber-Sicherheit-Frühwarnsystems 317
8.3.3 Obligatorische funktionelle Anforderungen 318
8.3.4 Asymmetrische Bedrohungen 318
8.4 Aufbau eines Cyber-Sicherheit-Frühwarnsystems 319
8.4.1 Rechtliche Rahmenbedingungen 319
8.4.2 Beteiligte Organisationen 319

8.5 Technische Realisierung eines Cyber-Sicherheit-Frühwarnsystems . . . 320
8.5.1 Architektur . . . 320
8.5.2 Sensoren . . . 321
8.5.3 Analyse- und Erkennungsmodul . . . 321
8.6 Prinzipielle Aspekte von Sensoren . . . 323
8.6.1 Grundprinzip von Sensoren . . . 324
8.6.2 Messmethoden . . . 325
8.6.3 Ort der Messung . . . 325
8.7 Diskussion unterschiedlicher Sensoren . . . 326
8.7.1 NetFlow-Sensor/IPFIX-Sensor . . . 327
8.7.2 Netzwerk-Sensor . . . 329
8.7.3 SNMP-Sensor . . . 332
8.7.4 Wireshark-Sensor . . . 334
8.7.5 Honeypot-Sensor . . . 336
8.7.6 Logdaten-Sensor . . . 337
8.7.7 Verfügbarkeitssensor . . . 339
8.8 Analysekonzepte . . . 341
8.8.1 Erkennen von bekannten sicherheitsrelevanten Aktionen . . . 341
8.8.2 Erkennen von Anomalien . . . 341
8.9 Cyber-Sicherheit-Frühwarnprozess . . . 343
8.10 Kommunikationslagebild . . . 344
8.11 Zusammenfassung . . . 351
8.12 Übungsaufgaben . . . 351
Literatur . . . 352

9 Firewall-Systeme . . . 353
9.1 Bedrohungen im Netz . . . 353
9.1.1 Angriffsmöglichkeiten in Kommunikationssystemen . . . 354
9.1.2 Passive Angriffe . . . 354
9.1.3 Aktive Angriffe . . . 355
9.2 Idee und Definition von Firewall-Systemen . . . 357
9.2.1 Elektronische Brandschutzmauer . . . 358
9.2.2 Elektronischer Pförtner . . . 358
9.3 Das Sicherheitskonzept . . . 358
9.4 Aufgaben von Firewall-Systemen . . . 359
9.5 Grundlage von Firewall-Systemen . . . 360
9.6 Definition eines Firewall-Elements . . . 367
9.7 Designkonzept aktiver Firewall-Elemente . . . 371
9.8 Umsetzungsmöglichkeiten eines Firewall-Systems mit unterschiedlichen Firewall-Elementen . . . 372
9.8.1 Packet Filter . . . 372
9.8.2 Zustandsorientierte Packet Filter (stateful inspection) . . . 375
9.8.3 Application Gateway/Proxy-Technik . . . 377
9.9 Next-Generation-Firewall . . . 381

9.10 Firewall-Konzepte 383
9.11 Konzeptionelle Möglichkeiten und Grenzen von Firewall-Systemen 386
9.11.1 Konzeptionelle Möglichkeiten eines Firewall-Systems 386
9.11.2 Konzeptionelle Grenzen eines Firewall-Systems 387
9.12 Das richtige Firewall-Konzept für jeden Anwendungsfall 390
9.13 Definition des Kommunikationsmodells mit integriertem Firewall-Element 392
9.14 Zusammenfassung 398
9.15 Übungsaufgaben 398
Literatur 401

10 IPSec-Verschlüsselung 403
10.1 Einleitung 403
10.2 IPSec Header 404
10.2.1 Authentication Header 405
10.2.2 Encapsulated Security Payload 406
10.3 Cyber-Sicherheitsdienste der IPSec-Header und Realisierungsformen 408
10.4 IPSec-Schlüsselmanagement 414
10.4.1 Manual Keying 414
10.4.2 Internet-Key-Exchange-Protocol (IKE) – Version 1 414
10.5 Phasen und Modi von IKEv1 416
10.5.1 Phase 1 (IKEv1): ISAKMP Security Association 416
10.5.2 Phase 2 (IKEv1): IPSec Security-Association 420
10.5.3 Phase 3: Integritätsgesicherte und verschlüsselte IP-Kommunikation 424
10.6 Phasen und Modi von IKEv2 425
10.7 Anwendungsformen von IPSec-Lösungen 427
10.8 Protokollmitschnitt (IKEv1) 429
10.9 Zusammenfassung 436
10.10 Übungsaufgaben 436
Literatur 438

11 Transport Layer Security (TLS)/Secure Socket Layer (SSL) 439
11.1 Einleitung 439
11.2 Einbindung in die Kommunikationsarchitektur 440
11.3 Protokolle der TLS/SSL-Schicht 442
11.4 TLS/SSL-Zertifikate 455
11.5 Authentifikationsmethoden 457
11.6 Anwendungsformen von TLS/SSL-Lösungen 460
11.7 Protokollmitschnitt 462
11.8 TLS 1.3 468
11.9 Zusammenfassung 471
11.10 Übungsaufgaben 472
Literatur 473

12 Cyber-Sicherheitsmaßnahmen gegen DDoS-Angriffe 475
12.1 Einleitung 475
12.2 Gezielte Überlastung von verfügbaren Ressourcen 477
12.3 Reflection und Amplification 478
12.4 Abwehrstrategien gegen Angriffe auf die Verfügbarkeit 479
12.4.1 Cyber-Sicherheitsrichtlinien zum Schutz vor Verfügbarkeitsangriffen 479
12.4.2 On-Site-Robustheitsmaßnahmen 480
12.4.3 Off-Site-Dienstleistungsmodelle 481
12.5 Präventiv gegen Beteiligung – Sichere Konfiguration von Diensten 486
12.6 Zusammenfassung 486
12.7 Übungsaufgaben 487
Literatur 487

13 E-Mail-Sicherheit 489
13.1 Einleitung 489
13.2 Generelle Cyber-Sicherheitsprobleme des E-Mail-Dienstes 490
13.3 E-Mail-Verschlüsselung 491
13.3.1 PGP und S/MIME sowie deren Unterschiede 492
13.3.2 Weitere Alternativen für E-Mail-Sicherheit 496
13.4 Spam-E-Mails 501
13.4.1 Definition und Hintergründe von Spam-Mails 501
13.4.2 Schäden, die durch Spam-Mails auftreten 502
13.4.3 Mechanismen zum Erkennen von Spam-Mails 503
13.4.4 Mechanismen zur Vermeidung von Spam-Mails 505
13.5 Zusammenfassung 507
13.6 Übungsaufgaben 507
Literatur 508

14 Blockchain-Technologie 509
14.1 Einleitung 509
14.2 Blockchain-Technologie auf den Punkt gebracht 509
14.3 Aufbau der Blockchain-Technologie 512
14.3.1 Element: Daten 512
14.3.2 Element: Block 513
14.3.3 Element: HashPrev 514
14.3.4 Element: Merkle Hash 515
14.3.5 Element: Transaktionen 516
14.3.6 Element: Node 519
14.3.7 Element: Blockchain-Teilnehmer 521
14.3.8 Element: Wallet 521
14.3.9 Element: Blockchain-Adresse 523
14.3.10 Prinzip: Keine „zentrale Instanz“ 524
14.3.11 Konsensfindungsverfahren 524
14.3.12 Struktur: Berechtigungsarchitektur 534

14.3.13 Ablauf der Verstetigung von Transaktionen. 536
14.4 Hard und Soft Forks von Blockchains 536
14.5 Anwendungsformen und Anwendungen der Blockchain 541
14.6 Blockchain-as-a-Service 547
14.7 Sicherheit und Vertrauenswürdigkeit der Blockchain-Technologie 548
14.7.1 Sicherheit der Blockchain-Infrastruktur 549
14.7.2 Sicherheit der Blockchain-Anwendung. 552
14.8 Gegenüberstellung PKI- und Blockchain-Technologien 555
14.9 Zusammenfassung 556
14.10 Übungsaufgaben. 557
Literatur. 558

15 Künstliche Intelligenz und Cyber-Sicherheit 561
15.1 Einleitung. 561
15.2 Einordnung der Künstlichen Intelligenz 562
15.3 Erfolgsfaktoren der Künstlichen Intelligenz 563
15.4 Das Prinzip des Maschinellen Lernens 565
15.5 Qualität der Eingabedaten 566
15.6 Kategorien und Algorithmen des Maschinellen Lernens. 569
15.6.1 Überwachtes Lernen 569
15.6.2 ML-Algorithmus: Support-Vector-Machine (SVM) 570
15.6.3 ML-Algorithmus: k-Nearest-Neighbor (kNN) 573
15.6.4 Unüberwachtes Lernen 576
15.6.5 ML-Algorithmus: k-Means-Algorithmus 577
15.6.6 ML-Algorithmus: Hierarchische Clustering-Verfahren. . . 579
15.6.7 Künstliche Neuronale Netze (KNN) 580
15.6.8 Deep Learning 585
15.7 Anwendungsszenarien von KI und Cyber-Sicherheit 586
15.8 Manipulationen von Künstlicher Intelligenz 589
15.9 Beispiele von KI und Cyber-Sicherheit 594
15.9.1 Alert-System auf der Basis eines kontinuierlichen Lagebilds über die aktuelle Gefahrenlage im Online-Banking 594
15.9.2 Identifikation/Authentifikation eines Nutzers mittels Smartphone-Sensoren 600
15.9.3 Erkennung von netzwerkbasierten Angriffen mittels Künstlicher Intelligenz. 602
15.10 Ethik und Künstliche Intelligenz 605
15.10.1 KI und Cyber-Sicherheit – eine Frage der Ethik? 606
15.10.2 Nachvollziehbarkeit von Entscheidungen als Prinzip 609
15.10.3 Ethik.KI.Tool 609
15.11 Zusammenfassung 611
15.12 Übungsaufgaben. 612
Literatur. 613

16 Social Web Cyber-Sicherheit 615
16.1 Einleitung 615
16.2 Soziale Netzwerke 616
16.3 Fake-News 618
16.3.1 Was sind Fake-News? 618
16.3.2 Social Bot (die digitale Propaganda-Maschine) 621
16.3.3 Wie können Fake-News erkannt werden? 622
16.4 Deep Fake 625
16.5 Filterblasen und Echokammern 626
16.6 Psychometrie bei sozialen Netzwerken 628
16.7 Cyber-Mobbing 629
16.8 Zusammenfassung 631
16.9 Übungsaufgaben. 632
Literatur. 632

17 Wirtschaftlichkeit von Cyber-Sicherheitsmaßnahmen 633
17.1 Einführung 633
17.2 Cyber-Sicherheit 635
17.2.1 Schutzbedarf von IT-Systemen 635
17.2.2 Wie sicher ist „sicher“? 635
17.2.3 Verwundbarkeit 636
17.3 Return on Security Investment RoSI – Nutzenaspekt 636
17.4 Beispielberechnung RoSI: Notebookverluste 638
17.5 Zusammenfassung 643
17.6 Übungsaufgaben. 643
Literatur. 644

18 Self-Sovereign Identity (SSI) 645
18.1 Self-Sovereign Identity (SSI) auf den Punkt gebracht. 645
18.2 Die Architektur von Self-Sovereign Identity (SSI) 648
18.3 Decentralized Identifier (DID). 650
18.3.1 Das Konzept dezentralen Identitäten (DID) 650
18.3.2 Ziele und Prinzipien von DIDs 652
18.4 Verifiable Credential (VC). 652
18.5 Hyperledger Aries 654
18.6 Akteure: Self-Sovereign Identity (SSI) 656
18.6.1 Aussteller (Issuer) von digitalen Nachweisen 656
18.6.2 Nutzer (Holder) von verifizierbaren digitalen Nachweisen. 657
18.6.3 Verifizierer, die digitale Nachweise für ihre Prozesse nutzen. 658
18.7 SSI-Blockchain-Infrastruktur als Verifiable Data Registry (VDR). 659
18.8 Zero-Knowledge Proofs (ZKP) 661
18.8.1 Selective Disclosure. 661
18.8.2 Predicate Proofs. 662

18.8.3 Signature Blinding . . . 663
18.8.4 Private Holder Binding . . . 663
18.9 Anwendungsbeispiele von Self-Sovereign Identity . . . 664
18.10 SSI-Ökosystem für digitale Identitäten in der Zukunft – Vorzüge und Vorbehalte . . . 667
18.10.1 Digitalisierung und Akzeptanz der Bürger . . . 667
18.10.2 Wirtschaftliche Relevanz eines SSI-Ökosystems für digitale Identitäten . . . 668
18.10.3 Technologische Souveränität . . . 669
18.11 Zusammenfassung . . . 669
18.12 Übungsaufgaben . . . 670
Literatur . . . 671

19 Vertrauen und Vertrauenswürdigkeit . . . 673
19.1 Zusammenhang zwischen Vertrauen, Vertrauenswürdigkeit und Cyber-Sicherheit . . . 673
19.2 Vertrauen . . . 674
19.3 Vertrauenswürdigkeitsmodell . . . 675
19.3.1 Vertrauenswürdigkeit der IT-Lösung . . . 678
19.3.2 Vertrauenswürdigkeit des Unternehmens . . . 681
19.3.3 Vertrauenswürdigkeit von Domänen . . . 685
19.3.4 Zusammenfassung: Vertrauenswürdigkeitsmodell . . . 687
19.4 Mechanismen zur Vertrauensbildung . . . 687
19.4.1 Eigene emotionale Referenz . . . 687
19.4.2 Neutrale Referenz . . . 688
19.4.3 Zusammenfassung: Mechanismen zur Vertrauensbildung . . . 690
19.5 Vertrauenswürdigkeitstechnologie . . . 691
19.6 Zusammenfassung . . . 693
19.7 Übungsaufgaben . . . 693
Literatur . . . 693

20 Weitere Aspekte der Cyber-Sicherheit . . . 695
20.1 DNS over HTTPS (DoH) . . . 695
20.2 Backup . . . 697
20.3 Chancen und Risiken von Smart Home . . . 700
20.4 Risiken und Sicherheit eines Homeoffice . . . 705
20.4.1 Risiken beim Homeoffice . . . 705
20.4.2 Sicherheitsmaßnahmen für das Homeoffice . . . 708
20.5 Upload-Filter . . . 712
20.6 Übungsaufgaben . . . 715
Literatur . . . 716

21 Glossar . . . 717

Symbole . . . 737

Stichwortverzeichnis . . . 741

Über den Autor

Norber Pohlmann ist Informatikprofessor für Verteilte Systeme und Informationssicherheit im Fachbereich Informatik und Kommunikation sowie geschäftsführender Direktor des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen.

Von 1988 bis 1999 war er geschäftsführender Gesellschafter der Firma KryptoKom, Gesellschaft für kryptografische Informationssicherheit und Kommunikationstechnologie mbH, in der forschungsnahe und innovative Cyber-Sicherheitsprojekte und -produkte realisiert wurden. Nach der Fusion der KryptoKom mit der Utimaco Safeware war er von 1999 bis 2003 Mitglied des Vorstandes der Utimaco Safeware AG, verantwortlich für Entwicklungsprojekte und Technologiearchitekturen der IT-Sicherheitsprodukte und -lösungen.

Seit April 1998 ist Prof. Norbert Pohlmann Vorstandsvorsitzender des Bundesverbands für IT-Sicherheit – TeleTrusT und seit Mai 2015 Mitglied des Vorstandes des Verbands der Internetwirtschaft – eco.

Außerdem ist Prof. Norbert Pohlmann Mitglied des wissenschaftlichen Beirates der Gesellschaft für Datenschutz und Datensicherung – GDD und Mitglied im Lenkungskreis der Initiative „IT-Sicherheit in der Wirtschaft“ des Bundesministeriums für Wirtschaft und Technologie – BMWK.

Seit 2020 ist Prof. Pohlmann Mitglied der Advisory Group der European Union Agency for Cypersecurity der ENISA, die Sicherheitsagentur der europäischen Gemeinschaft.

Norbert Pohlmann ist Träger des Preises der Stadt Aachen für Innovation und Technologie für wissenschaftliche und unternehmerische Leistungen 1997.

2011 wurde es als „Professor des Jahres 2011“ in der Kategorie „Ingenieurswissenschaften/Informatik“ ausgezeichnet.

Im Sommersemester 2013 war er als Gastprofessor an der Stanford University im Fachbereich Computer Science, Silicon Valley, USA und im Wintersemester 2008 am Stevens Institute of Technology in der Studienrichtung „Cybersecurity“, Hoboken, NJ, USA (New York Metropolitan Area) aktiv.

Mehr als 400 Fachartikel und 7 Bücher sowie viele Herausgeberschaften, über 400 Vorträge auf dem Gebiet der Cyber-Sicherheit dokumentieren seine Fachkompetenz und sein Engagement auf dem Gebiet Cyber-Sicherheit (siehe auch: www.norbert-pohlmann.com).

1 Sichtweisen auf die Cyber-Sicherheit im Cyber-Raum

Zusammenfassung

In diesem Kapitel werden unterschiedliche Sichtweisen auf die Cyber-Sicherheit im Cyber-Raum diskutiert, um eine Grundlage für das Verständnis des Themas Cyber-Sicherheit und dessen Probleme, Herausforderungen, Rahmenbedingungen, Paradigmen, Wirksamkeitskonzepte, Bedürfnisse, Strategien, Motivationen, Angriffsvektoren, Schäden und Risiken aufzubauen.

1.1 Einleitung

Informationstechnik (IT) und das Internet sind Motor und Basis für das Wohlergehen der modernen und globalen Informations- und Wissensgesellschaft. Fakt ist auch, dass seit Beginn der IT und mit der Digitalisierung die Cyber-Sicherheitsprobleme sich jedes Jahr stets vermehren. Eine wichtige Erkenntnis ist, dass die heutigen IT-Architekturen der genutzten IT-Systeme, wie Endgeräte, Server und Netzkomponenten, nicht sicher genug konzipiert und aufgebaut sind, um den Fähigkeiten von intelligenten Hackern standzuhalten. Die Komplexität der IT-Systeme und -Infrastrukturen wird immer größer, die Methoden der Angreifer werden ausgefeilter und die Angriffsziele kontinuierlich lukrativer. Entsprechend steigen die Risiken sehr stark an, was zu hohen Schäden führt, wie wir auch den aktuellen Umfragen entnehmen können: Durch Diebstahl, Spionage und Sabotage entsteht der deutschen Wirtschaft jährlich ein Gesamtschaden von mehr als 220 Milliarden Euro.

Täglich kann den Medien entnommen werden, wie sich kriminelle Hacker die unzureichende Qualität der Software für erfolgreiche Angriffe zunutze machen, Malware installieren, Passwörter sowie Identitäten stehlen und Endgeräte ausspionieren.

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2022

N. Pohlmann, *Cyber-Sicherheit*, https://doi.org/10.1007/978-3-658-36243-0_1

Eine angemessene, souveräne, sichere und vertrauenswürdige IT zu erreichen, ist für die digitale Zukunft entscheidend. Letztlich muss die voranschreitende Digitalisierung auch die Nachhaltigkeit als strategisches Ziel haben.

▶ **Wichtig** Die meisten der heutigen IT-Architekturen der genutzten IT-Systeme sind nicht sicher genug konzipiert und aufgebaut, um den Fähigkeiten von intelligenten Hackern standzuhalten.

Definition Cyber-Sicherheit

Cyber-Sicherheit oder auch Internet-Sicherheit befasst sich mit allen Aspekten der IT-Sicherheit, wobei das Aktionsfeld auf den gesamten Cyber-Raum ausgeweitet wird. Cyber-Raum umfasst in dieser Definition sämtliche mit dem globalen Internet verbundene IT und IT-Infrastrukturen sowie deren Kommunikation, Anwendungen, Prozesse mit Daten, Informationen und Intelligenzen, siehe Abb. 1.1. Aber auch die kriminellen Organisationen und weitere Angreifer gehören mit ihren immer intelligenteren Angriffsmethoden zum Cyber-Raum. Da der Cyber-Raum ein sehr komplexes System mit vielen Abhängigkeiten und Akteuren ist, der nicht vollständig kontrolliert werden kann, sind die Herausforderungen für einen robusten, sicheren und vertrauenswürdigen Betrieb sehr groß.

Mit der zunehmenden Digitalisierung wird im Cyber-Raum auch die strikte Trennung zwischen Arbeit und Freizeit aufgelöst. Angriffe im Cyber-Raum können Unternehmen, Institutionen, Behörden und Bürger treffen, also zu erheblichen Beeinträchtigungen der gesellschaftlichen und wirtschaftlichen Lebensgrundlagen führen. Aus diesem Grund spielt bei der Cyber-Sicherheit die übergreifende Sichtweise auf den Cyber-Raum eine wichtige Rolle. IT-Sicherheit ist Teil der Cyber-Sicherheit. ◀

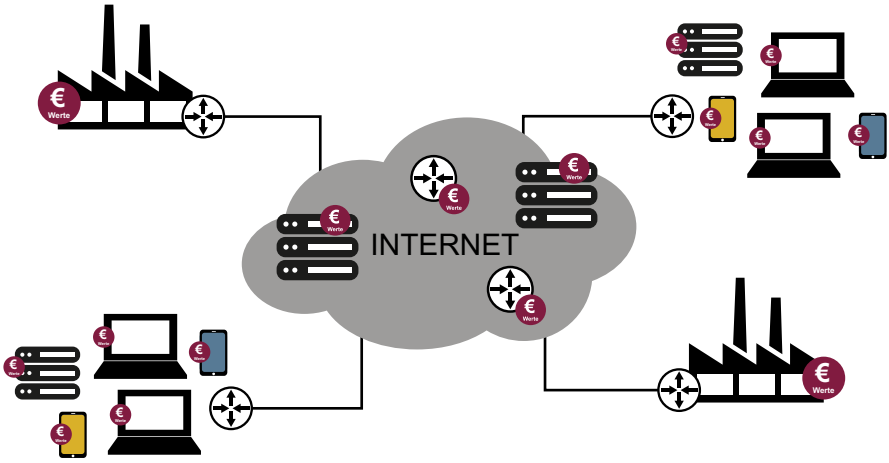


Abb. 1.1 Cyber-Sicherheit

Dabei sind:

IT-Infrastrukturen wie zum Beispiel alle Autonome Systeme – selbstständige Netze (ca. 70.000), DNS-Infrastruktur, Webdienste, IP-Telefonie, Konferenzsysteme und Soziale Medien.

Kommunikation wie zum Beispiel IP, TCP, UDP, ICMP, QUIC, HTTP, SMTP, DNS, OSPF, BGP, IPSec und TLS/SSL.

Intelligenzen Künstliche Intelligenz und Maschinelles Lernen und deren Anwendungen wie Assistenzsysteme, autonomes Fahren oder intelligente Angriffserkennungssysteme.

Angriffsmethoden wie zum Beispiel Malware-Infiltrationen über manipulierte Webseiten und schadhafte E-Mail-Anhänge mithilfe von Phishing- und Social Engineering-Angriffen sowie die daraus resultierenden Schadfunktionen der Malware: Ransomware, Keylogger, Click-Fraud, Spam, DDoS, Staatstrojaner, Adware, Trojanisches Pferd und Spyware.

Man-in-the-Middle-Angriffe, Angriffe mithilfe eines Software-Updates (Supply Chain-Angriff), Angriffe auf die Verfügbarkeit von IT-Systeme (DDoS-Angriff) sowie Advanced Persistent Threat (APT).

Definition IT-Sicherheit

Mithilfe der IT-Sicherheit sollen vorhandene Risiken, die durch Bedrohungen auf IT-Systeme wirken, auf ein angemessenes Maß reduziert werden. IT-Sicherheit befasst sich daher mit IT-Sicherheitsmaßnahmen, die Informationen auf IT-Systemen sowie IT-Systemen selbst vor dem Verlust von Vertraulichkeit, Authentifikation, Authentizität, Integrität, Verbindlichkeit, Verfügbarkeit und Anonymisierung/Pseudonymisierung schützen. IT-Sicherheit beinhaltet auch die Aspekte der Softwaresicherheit und Zuverlässigkeit von IT-Systemen. IT-Sicherheit schützt IT-Systeme, mit dem Ziel Schäden für Unternehmen, Behörden, Organisationen und Personen zu vermeiden oder zu mindestens zu verringern. Siehe Abb. 1.2. ◀

Definition Informationssicherheit

Informationssicherheit hat das Ziel, Informationen zu schützen. Die zu schützenden Informationen sind analog auf Papier (in Ordnern, Papierarchiven, …), digital auf IT-Systemen oder auch in den Köpfen der Menschen gespeichert, siehe Abb. 1.3. Die Informationssicherheitsbedürfnisse als Grundwerte der Informationssicherheit sind: Gewährleistung der Vertraulichkeit, Authentifikation,

Kryptografie

2

Zusammenfassung

Im Kapitel Kryptografie werden Kenntnisse über den Aufbau, die Prinzipien, die Architektur und die Funktionsweise von grundlegenden kryptografischen Verfahren vermittelt. Kryptografische Verfahren spielen eine besondere Rolle bei vielen wichtigen Cyber-Sicherheitssystemen zur Gewährleistung der Cyber-Sicherheitsbedürfnisse, wie zum Beispiel Vertraulichkeit, Authentifikation, Authentizität, Integrität und Verbindlichkeit.

Die Kryptografie prägt in immer stärkerem Maß das Alltagsleben [1]. Das gilt für die Verschlüsselung der gespeicherten Daten auf den IT-Systemen, aber auch für das Online-Banking oder den Remote-Zugriff auf Firmennetze, die ohne die Nutzung von Techniken wie TLS/SSL und IPSec praktisch nicht mehr vorstellbar sind: Selbst dort, wo Kryptografie zunächst nicht vermutet wird, sind heutzutage kryptografische Verfahren im Einsatz, zum Beispiel bei den elektronischen Wegfahrsperren in Autos, wenn das Smartphone eingeschaltet wird oder jemand sich beim Mobilfunknetz des Providers anmeldet oder bei Blockchain, Fernsehen, dem neuen Personalausweis, Fernbedienungen, Datenschutz usw.

2.1 Grundlagen der Kryptografie

Kryptografie ist eine moderne, mathematisch geprägte Wissenschaft, die für Informatiker eine wichtige Rolle spielt, um IT-Systeme, Anwendungen, Informationen und die Infrastruktur des Internets angemessen zu schützen. Die Kryptografie ist aus der Wissens- und Informationsgesellschaft nicht mehr wegzudenken, und jeder, der sich darin zurechtfinden will, sollte zumindest einige ihrer Grundprinzipien und Funktionsweisen kennen, um eine optimale und richtige Nutzung zu gewährleisten.

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2022

N. Pohlmann, *Cyber-Sicherheit*, https://doi.org/10.1007/978-3-658-36243-0_2

▶ **Wichtig** Kryptografie ist heute Bestandteil des Alltagslebens; ihre Prinzipien und Funktionsweisen zu kennen, hilft, sie optimal und richtig anzuwenden.

2.1.1 Grundlagen der Verschlüsselung

Das Ziel der Verschlüsselung besteht darin, Daten in einer solchen Weise einer mathematischen Transformation zu unterziehen, dass es einem Unbefugten unmöglich ist, die Originaldaten aus den transformierten, verschlüsselten Daten zu rekonstruieren. Damit die verschlüsselten Daten für ihren legitimen Nutzer dennoch verwendbar bleiben, muss es diesem aber möglich sein, durch Anwendung einer inversen Transformation aus ihnen wieder die Originaldaten zu generieren. Die Originaldaten werden als Klartext (clear text, plain text, message) bezeichnet, die transformierten Daten werden Schlüsseltext (Chiffretext, Chiffrat, Kryptogramm, cipher text) genannt. Die Transformation heißt Verschlüsselung (Encryption), ihre Inverse Entschlüsselung (Decryption).

▶ **Wichtig** Verschlüsselung dient zur Übertragung und Speicherung geheimer Informationen, die nur dem legitimen Empfänger/Besitzer zugänglich sein sollen.

Das generelle Ziel der Verschlüsselung kann folgendermaßen formuliert werden:
Die Entschlüsselung darf nur den legitimen Empfängern/Besitzern der übermittelten/gespeicherten Informationen möglich sein, nicht jedoch anderen Personen – im Extremfall nicht einmal den Absendern/Initiatoren selbst, die eine Information verschlüsselt haben.

Dieses Ziel lässt sich offensichtlich genau dann erreichen, wenn nur die legitimen Empfänger/Besitzer die zur Entschlüsselung benötigten Informationen kennen und es ohne diese Kenntnis nicht möglich ist, die ursprüngliche Information aus dem Schlüsseltext zu bestimmen. Es wäre also auf den ersten Blick ausreichend, wenn Sender und Empfänger eine nur ihnen bekannte Transformation untereinander absprechen und die Kenntnisse darüber geheim halten, siehe Abb. 2.1. Mit Transformation ist die Verschlüsslung und Entschlüsselung eines bestimmten Verschlüsselungsalgorithmus gemeint.

Dieser Ansatz ist jedoch aus drei Gründen nicht praktikabel:

1. Definition und Realisierung eines Verschlüsselungsalgorithmus erfordern einen erheblichen Aufwand. Dieses Argument wiegt umso schwerer, da es von Zeit zu Zeit notwendig ist, den Verschlüsselungsalgorithmus zu wechseln. In diesem Fall müsste ein neuer Verschlüsselungsalgorithmus entwickelt werden.

Abb. 2.1 Einfachste mögliche Vorgehensweise bei einer Verschlüsselung

▶ **Wichtig** Die Eigenentwicklung von Verschlüsselungsverfahren erfordert großen Aufwand sowie große Expertise und führt meist zu mangelhaften Resultaten.

2. Es besteht das Risiko, dass es einem Angreifer möglich ist, aus der Struktur der verschlüsselten Daten den Klartext oder die zur Verschlüsselung beziehungsweise Entschlüsselung verwendete Transformation abzuleiten, also die Verschlüsselung zu „brechen“. Da es sehr aufwendig ist, den Nachweis zu führen, dass ein neues Verschlüsselungsverfahren gegen derartige Angriffe durch „Kryptoanalysis“ sicher ist, und da ad hoc bestimmte Verschlüsselungsalgorithmen mit hoher Wahrscheinlichkeit unsicher sind, ist der Einsatz eigener Verfahren für jede einzelne Kommunikation praktisch unmöglich.

▶ **Wichtig** In der Praxis werden nur Verschlüsselungsalgorithmen eingesetzt, die etabliert und die nachweislich sicher sind. Ebenfalls muss der Algorithmus im Laufe der Zeit gewechselt werden, um die Aktualität des Verfahrens sicherzustellen.

3. Als letztes ist der untragbare Aufwand bei wechselnden Kommunikationspartnern zu nennen, da für jeweils zwei Partner ein separater Verschlüsselungsalgorithmus zur Verfügung stehen muss. Der mit dessen Entwicklung, Übermittlung, Aufbewahrung und Geheimhaltung verbundene Aufwand ist organisatorisch kaum zu bewältigen und wirtschaftlich nicht vertretbar.

▶ **Wichtig** Bei n verschiedenen Kommunikationspartnern werden $n*(n-1)/2$ verschiedene Verschlüsselungsalgorithmen benötigt. Das sind zum Beispiel bei 12 Kommunikationspartnern 66 Verschlüsselungsalgorithmen und bei 1000 Kommunikationspartnern 499.500 Verschlüsselungsalgorithmen. Diese Anforderung kann in der Praxis nicht erfüllt werden.

Als Lösung dieser Probleme bietet sich an, zur Verschlüsselung nur einige wenige Verschlüsselungsalgorithmen einzusetzen, deren Sicherheit aktuell erwiesen ist. Um dennoch die Forderung nach einer Vielzahl von Verschlüsselungsverfahren zu erfüllen, kann das Verschlüsselungsverfahren zusätzlich von einem Parameter abhängig gemacht werden, dem sogenannten **Schlüssel**, der den Ablauf der Transformation so stark beeinflusst, dass ohne seine Kenntnis keine Entschlüsselung möglich ist, siehe Abb. 2.2.

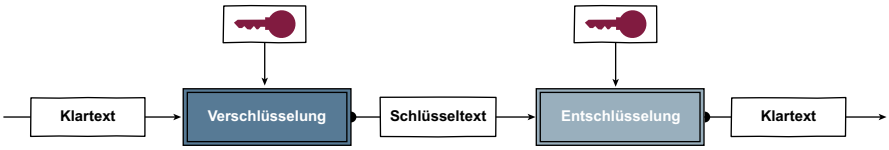


Abb. 2.2 Schlüsselabhängige Verschlüsselung

Hardware-Sicherheitsmodule zum Schutz von Sicherheitsinformationen

3

Zusammenfassung

Immer mehr sicherheitsrelevante Informationen, wie zum Beispiel geheime Schlüssel und Transaktionsdaten, werden durch Bezahlsysteme sowie Verschlüsselungs- und Authentifikationslösungen im Internet genutzt. In diesem Kapitel werden Hardware-Sicherheitsmodule (HSMs) beschrieben, die helfen, besonders sensible sicherheitsrelevante Informationen angemessen zu schützen.

3.1 Einleitung

Das Ziel eines Hardware-Sicherheitsmoduls ist ein hoher Schutz vor Auslesen und Manipulation von besonders sensiblen Sicherheitsinformationen innerhalb eines besonders geschützten Hardware-Bereichs [1].

Besonders sensible Sicherheitsinformationen, die in einem Hardware-Sicherheitsmodul geschützt werden sollen, sind zum Beispiel:

- geheime Schlüssel für Verschlüsselung, Authentifizierung, Signaturen usw.
- Programme, die nicht kopiert oder modifiziert werden sollen, im Sinne eines Softwareschutzes.
- Daten, die besondere Werte darstellen, wie zum Beispiel Transaktionsdaten, Coins usw.

Alle sicherheitsrelevanten Operationen, wie zum Beispiel „Verschlüsseln“, „Signieren“, „Zufallszahlen und Schlüssel generieren“ finden direkt im speziell geschützten Hardware-Sicherheitsmodul statt, siehe Abb. 3.1. Geheime Schlüssel können so benutzt werden, ohne sie zu kennen. Geheime Daten, digitale Werte und Software sind manipulationssicher im Hardware-Sicherheitsmodul gespeichert.

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2022

N. Pohlmann, *Cyber-Sicherheit*, https://doi.org/10.1007/978-3-658-36243-0_3

Abb. 3.1 Idee eines Hardware-Sicherheitsmoduls

In der Praxis haben sich unterschiedliche Umsetzungskonzepte von Hardware-Sicherheitsmodulen mit verschiedenen Sicherheitswirkungen und Einsatzumfeldern etabliert.

▶ **Wichtig** Hardware-Sicherheitsmodule (HSMs) schützen Sicherheitsinformationen besonders wirkungsvoll.

3.2 Hardware-Sicherheitsmodul: Smartcards

Eine Smartcard oder intelligente Chipkarte ist ein IT-System in der genormten Größe der EC-Karte (86 × 54 × 0,76 mm), das Personen IT-Sicherheitsdienstleistungen zur Verfügung stellt.

Eine Smartcard (siehe Abb. 3.2) enthält einen Sicherheitschip mit CPU, RAM- und ROM-Speicher, ein „schlankes“ und sicheres Betriebssystem im ROM, eine I/O-Schnittstelle, über die die gesamte Kommunikation stattfindet (Kontaktflächen oder kontaktloses Interface) und ein EEPROM (Electrically Erasable Programmable Read-Only Memory – nicht-flüchtiger Speicher, der elektrisch beschrieben und gelöscht wird), auf dem die geheimen Schlüssel, wie ein geheimer RSA-Schlüssel oder andere symmetrische Schlüssel sowie persönliche Daten (Passwörter etc.) sicher gespeichert sind. „Sonstiges“ ist beispielsweise ein Co-Prozessor, der symmetrische oder asymmetrische Verschlüsselung sehr schnell durchführt (Krypto-Prozessor) [2].

Der Sicherheitschip der Smartcard bietet zum Beispiel die folgenden Hardware-Sicherheitsmechanismen zum Schutz der Sicherheitsinformationen: Unter- und Überspannungsdetektion, Erkennung niedriger Frequenzen. Diese Sicherheitsmechanismen sorgen dafür, dass der Sicherheitschip immer in einem definierten Zustand arbeitet (Strom, Frequenz) und nicht bei einer Manipulation die Sicherheitsinformationen nach außen sendet.

Weitere Sicherheitsmechanismen im Sicherheitschip sind: Verwürfelte Busse, Sensoren für Licht, Temperatur usw., Passivierungs- beziehungsweise Metallisierungsschichten über Bus- und Speicherstrukturen oder über der gesamten CPU, Zufallszahlengenerator in der Hardware, spezielle CPU-Befehle für kryptografische Funktionen und Speicherschutzfunktionen.

Auch die Smartcard-Software bietet Software-Sicherheitsmechanismen an, wie Zugriffskontrolle auf Objekte und Zustandsautomaten, die in Abhängigkeit von Identifikations- und Authentisierungsmechanismen auf der Smartcard Befehle zulassen.

Die Sicherheit einer Smartcard beruht in der Regel auf zwei Faktoren: Wissen (PIN) und Besitz (Karte) – Zweifaktor-Authentifizierung (2FA). Der Nutzer muss die PIN kennen (Wissen) und die Smartcard mit dem Schlüssel haben (Besitz).

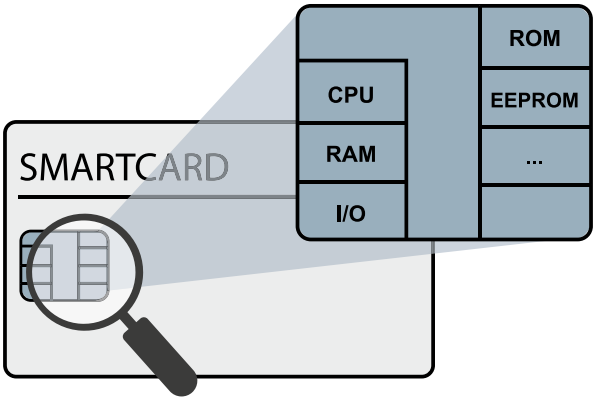


Abb. 3.2 Smartcard

Geheime Schlüssel verlassen den Sicherheitschip der Smartcard nie. Alle Operationen mit Sicherheitsinformationen finden direkt im Sicherheitschip der Smartcard statt. Geheime Schlüssel können indirekt über die Befehle der Smartcard benutzt werden, ohne sie zu kennen. Geheime Daten sind manipulationssicher im Sicherheitschip gespeichert.

Smartcardbasierte Sicherheitschips werden in Form von Smartcards, aber auch in der Form von USB-Token, NFC-Token usw. realisiert und genutzt. Die Nutzung der IT-Sicherheitsdienste kann dann aber performanter und ohne zusätzliches Lesegerät über USB und NFC vorgenommen werden.

Die Aktivierung mithilfe einer PIN hat einige praktische Herausforderungen. In der Regel werden nur vier bis sechs Zeichen für die Aktivierung gefordert, was die Anzahl der möglichen Kombination sehr einschränkt. Oft benutzen die Nutzer für alle Smartcards die PIN ihrer EC-Karte, was selbstverständlich ein Sicherheitsrisiko darstellt.

Wird das Fingerabdruckverfahren anstelle der üblicherweise verwendeten PIN zur Aktivierung einer Smartcard verwendet, ist „Match on Card“ ein notwendiges und passendes Sicherheitskonzept. Dabei erfolgt der Vergleich des aktuellen Fingerabdrucks mit dem gespeicherten Referenzwert direkt im Sicherheitschip der Smartcard. In der Regel werden mehrere Fingerabdrucktemplates im Sicherheitschip der Smartcard abgelegt, damit der Nutzer unterschiedliche Finger nutzen kann, zum Beispiel, wenn er eine Verletzung am Zeigefinger hat.

Die Vorteile des *Match-on-Card*-Verfahrens bezüglich Biometrie liegen vor allem in der hohen Sicherheit, da die Referenzwerte niemals den geschützten Bereich des Sicherheitschips der Smartcard verlassen und nicht ausgelesen werden können. Die sichere Speicherung des Referenzwerts nur im Sicherheitschip der Smartcard ist besonders datenschutzfreundlich, weil die personenorientierten Daten nicht zentral gespeichert werden müssen. Darüber hinaus ermöglicht ein direkt auf dem Sicherheitschip gespeicherter Referenzwert auch die Verwendung an verschiedenen Standorten (Roaming) oder auf offline betriebenen IT-Systemen.

4 Digitale Signatur, elektronische Zertifikate sowie Public Key-Infrastruktur (PKI) und PKI-enabled Application (PKA)

Zusammenfassung

In diesem Kapitel werden die Themen digitale Signatur, elektronische Zertifikate sowie Public Key-Infrastrukturen und PKI-enabled Application (PKA) behandelt. Diese Cyber-Sicherheitsprinzipien und Cyber-Sicherheitsmechanismen sind in einer modernen Informations- und Wissensgesellschaft von enormer Wichtigkeit und unterstützen dabei, zentrale Vertrauensdienste und ein modernes Schlüsselmanagement aufzubauen.

4.1 Digitale Signatur

In diesem Abschnitt werden die grundsätzliche Isdee und die notwendigen Funktionen einer digitalen Signatur behandelt.

4.1.1 Eigenhändige Unterschrift als Äquivalent zur digitalen Signatur

Um die grundsätzliche Idee der digitalen Signatur zu verstehen, sollen als erstes die Funktionen der eigenhändigen Unterschrift betrachtet werden.

Welche Bedeutung hat die eigenhändige Unterschrift, die Analogie zur digitalen Signatur? In Abb. 4.1 ist eine schriftliche Bestellung einer Waschmaschine zu finden.

Fragen, die bei einer eigenhändigen Unterschrift gestellt werden, sind:

- Welchen Wert hat eine eigenhändige Unterschrift?
- Wer hat etwas davon?
- Welche Bedeutung hat die eigenhändige Unterschrift?

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2022

N. Pohlmann, *Cyber-Sicherheit*, https://doi.org/10.1007/978-3-658-36243-0_4

Abb. 4.1 Schriftliche Bestellung einer Waschmaschine

- Welche Bedingungen müssen erfüllt sein, damit die eigenhändige Unterschrift einen Vorteil hat?

Funktionen einer eigenhändigen Unterschrift
Die eigenhändige Unterschrift hat unterschiedliche Funktionen:

1. **Abschlussfunktion – Vollendung einer Erklärung – hebt sich vom Entwurf ab**
   Wenn etwas unterschrieben wird, ist das Dokument in der Regel vollendet, das heißt, die Inhalte sind ausgehandelt, gegenseitig bestätigt usw. Mit der eigenhändigen Unterschrift wird der Abschluss dieser Aktivitäten dokumentiert.
2. **Identitätsfunktion – Unterschrift macht die Identität des Ausstellers kenntlich**

Identifikation und Authentifikation

5

Zusammenfassung

Die Identifikation und Authentifikation spielen in der modernen IT und im Internet eine besondere Rolle.

Bei den meisten IT-Anwendungen ist es wichtig zu wissen, wer gerade auf einem IT-System arbeitet oder einen IT-Dienst nutzen möchte. Es ist notwendig eine Zuordnung einer Person oder eines Nutzers zu einer ausgeübten Handlung zu haben. Aus diesem Grund muss verifiziert werden können, welche Person oder welches IT-System hinter einem aktuellen Zugriffswunsch steckt, bevor der Zugang gewährt wird.

▶ **Wichtig** Nur wenn identifiziert und authentifiziert werden kann, welche Person oder welches IT-System wirklich hinter einem Zugriffswunsch steckt, kann ein Zugriff zugelassen werden.

5.1 Was ist eine Identifikation und Authentifikation?

Wenn ein Nutzer Zugang zu einem IT-System haben möchte, muss er sich diesem gegenüber identifizieren und authentisieren, damit er den Zugang gewährt bekommen kann [1].

5.1.1 Identifikation

Die Identifikation ist die Überprüfung eines vorgelegten, kennzeichnenden Merkmals, zum Beispiel des Nutzernamens oder allgemein der Identität.

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2022

N. Pohlmann, *Cyber-Sicherheit*, https://doi.org/10.1007/978-3-658-36243-0_5

Eine Person wird weltweit eindeutig durch die Angabe der Attribute Vorname, Nachname, Geburtsort und Geburtstag identifiziert. In Deutschland wird die Eindeutigkeit der Identifikation durch die Regularien der Standesämter garantiert.

Im Cyber-Raum handelt es sich zum Beispiel bei der Identifikation um die Feststellung der digitalen Identität einer Person (Nutzer). Als digitale Identität – kennzeichnendes Merkmal – wird in der Regel der Nutzername (Name oder E-Mail-Adresse der Person) verwendet. Mit einer digitalen Identität lassen sich Nutzer in einem IT-System eindeutig zuordnen und identifizieren. Eine Person kann abhängig vom Kontext und den dadurch erforderlichen Attributen auch mehrere digitalen Identitäten besitzen. Siehe auch Kap. 18 „Self-Sovereign Identity (SSI)“.

Eine Identifikation muss immer innerhalb eines Systems (Organisation) abgesprochen sein, damit sie eindeutig ist. Ein System kann die Weltbevölkerung sein, die Bürger in Deutschland, die Kunden eines Webshops, die Mitglieder eines sozialen Netzwerks wie Facebook usw.

Damit eine solche Absprache mit verschiedenen Nutzern zustande kommt, müssen klar definierte Regeln bezüglich der Identifikation eingehalten werden. Als Beispiel hierfür kann die CCITT Recommendation X.509 beziehungsweise ISO 9594-8 betrachtet werden. Hierbei handelt es sich um ein standardisiertes Konzept eindeutiger, kennzeichnender Namen oder „Distinguishing Identifier“.

Beispiele von digitalen Identitäten:

E-Mail-Adresse
Bei vielen IT-Anwendungen und IT-Diensten wird als Nutzername eine E-Mail-Adresse verlangt und verwendet. Dies hat den Vorteil, dass von aktiven E-Mail-Adressen international keine Doppelungen auftreten können. Das heißt, dass die E-Mail-Adresse einer Person weltweit ein eindeutiges kennzeichnendes Merkmal ist. Die E-Mail-Adressen mit ihren entsprechenden Domänen werden als Baumstruktur verwaltet und sind daher eindeutig. rainer.maier@gmx.de gibt es nur ein Mal. Möchte ein zweiter Rainer Maier eine E-Mail-Adresse bei GMX haben, könnte er zum Beispiel rainer.maier2@gmx.de wählen.

Freie Wahl
Der Nutzer kann selbst einen Nutzernamen auswählen, zum Beispiel rmaier oder MickyMaus. Das IT-System muss dann prüfen, ob der gewählte Nutzername in diesem IT-System nicht schon vergeben ist. Wenn ja, muss der Nutzer einen anderen Namen finden, der noch nicht vergeben ist.

Das IT-System bestimmt
Es ist aber auch möglich, dass das IT-System den Nutzernamen bestimmt und dem Nutzer mitteilt.

Herausforderungen bezüglich digitaler Identitäten

Sehr viele Identitäten
Jeder Webdienst verwaltet die Identitäten unabhängig von anderen Webseiten. Aus diesem Grund haben die Nutzer in der Regel sehr viele unterschiedliche digitale Identitäten.

Der Level an Vertrauenswürdigkeit der digitalen Identitäten ist sehr unterschiedlich.
1.) Nicht verifizierte digitale Identitäten

Der Nutzer gibt seine kennzeichnenden Merkmale (Name und Adresse) und den Nutzernamen (E-Mail-Adresse) selber ein. Die Vertrauenswürdigkeit der digitalen Identität basiert nur auf der Selbstauskunft des Nutzers.

In diesem Fall ist völlig unklar, welche reale Person hinter einer digitalen Identität steckt.

2.) Verifizierte digitale Identitäten mithilfe des Beweises eines E-Mail-Kontos oder einer Telefonnummer

Der Nutzer beweist die Echtheit seiner digitalen Identität, indem er nachweisen kann, dass er im Besitz des Kontos der angegebenen E-Mail-Adresse ist. In der Regel muss er auf eine E-Mail, die im zugesendet wird, reagieren indem er auf einen Link klickt oder eine empfangene PIN auf einer Webseite eingibt.

Alternativ beweist er den Besitz einer definierten Telefonnummer, durch die Eingabe einer PIN, die an die Nummer gesendet wurde und auf einer Webseite eingegeben werden muss.

Indirekt kann über den E-Mail-Provider/Mobilfunkanbieter die reale Person identifiziert.

Über die Zahlungsfunktion können die Kunden durch die Provider immer identifiziert werden, weil ein Konto immer nur über die Vorlage eines Personalausweises eingerichtet werden kann.

3.) Verifizierte digitale Identitäten mithilfe von Identifikationsverfahren

Es findet eine starke Identitätsfeststellung einer realen Person mithilfe eines Identifikationsverfahrens wie das eID Verfahren des elektronischen Personalausweises oder eine Videoidentifikation statt, siehe Abschn. 5.2.

Hierbei wird von einer vertrauenswürdigen digitalen Identität gesprochen. Siehe auch 5.2.8. Abgeleitete Identitäten – vertrauenswürdige digitale Identität.

Es ist eindeutig, welche reale Person hinter einer vertrauenswürdigen digitalen Identität steckt.

5.1.2 Authentifikation

Authentifikation bezeichnet einen Prozess, in dem überprüft wird, ob „jemand“ oder „etwas“ echt ist. Daher bedeutet Authentifikation die Verifizierung (Überprüfung) der Echtheit beziehungsweise der Identität.

Die Überprüfung des Personalausweises einer Person ist eine solche Authentifikation in der realen Welt. Ein Prüfer kann, mithilfe eines Personalausweises, das Aussehen einer Person mit dem Lichtbild vergleichen.

Im Cyber-Raum wird bei der Authentifikation mit der Erbringung eines oder mehrere Nachweise bestätigt, ob es sich um die Person (Nutzer) mit der angegebenen und behaupteten digitalen Identität handelt. Damit wird die Echtheit der digitalen Identität eines Nutzers festgestellt.

Was muss und kann identifiziert und authentisiert werden?

1. **Nutzer,** wie Personen, Prozesse, Instanzen und weitere Entitäten.
2. **Medien,** wie Notebooks, Smartphones, Smartwatches, Serversysteme, Cyber-Sicherheitssysteme, Security Token usw.
3. **Nachrichten,** wie E-Mails, Dateien, Java-Applets, Datenpakete usw.

Grundsätzliche Architektur der Identifikation und Authentifikation

In Abb. 5.1 möchte der Nutzer Zugriff auf ein IT-System (Endgerät, Server, IT-Dienst, Cloud, …) erhalten.

Aus der Sicht des Nutzers und des IT-Systems werden IT-Sicherheitsfunktionen umgesetzt, die verschiedene Sicherheitsdienste erbringen.

Authentisierung: (Sichtweise Nutzer)

Der Nutzer authentisiert sich gegenüber einem IT-System (Endgerät, Server, IT-Dienst, Cloud, …), indem er einen Nachweis über seine digitale Identität, zum Beispiel den Nutzernamen, erbringt.

Authentifizierung: (Sichtweise IT-System)

Das IT-System (Endgerät, Server, IT-Dienst, Cloud, …) überprüft den Nachweis, um die Echtheit der digitalen Identität eines Nutzers im Rahmen der Authentifizierung festzustellen.

Autorisierung: (Sichtweise IT-System)

Wenn die Echtheit der digitalen Identität eines Nutzers erfolgreich verifiziert werden konnte, kann das IT-System (Endgerät, Server, IT-Dienst, Cloud, …) dem Nutzer definierte Rechte einräumen.

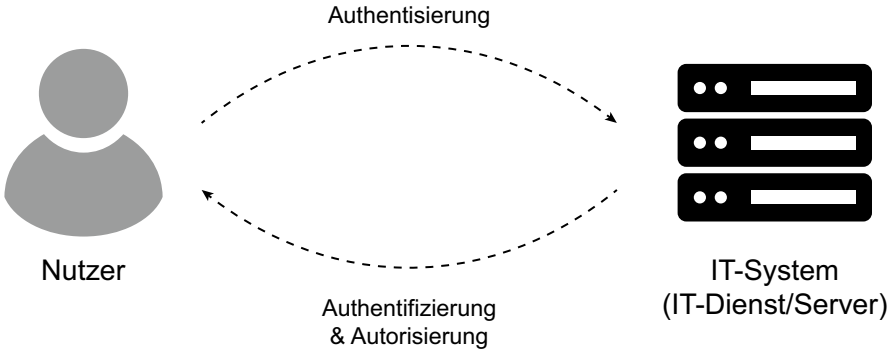


Abb. 5.1 Authentisierung, Authentifizierung und Autorisierung

Enterprise Identity und Access Management

6

Zusammenfassung

In diesem Kapitel werden Aufgaben, Prinzipien und Mechanismen eines „Enterprise Identity and Access Management-Systems“ dargestellt und erläutert.

Der Begriff Enterprise Identity and Access Management (EIAM) beschreibt jeglichen Einsatz von digitalen Identitäten, deren Attributen, deren Berechtigungen für IT-Systeme sowie IT-Dienste und schließt die Erzeugung, Nutzung, Pflege und Löschung dieser digitalen Identitäten mit ein. Ziel ist es, vertrauenswürdige, identitätsbezogene und regelkonforme Prozesse durchzusetzen, die unabhängig von Organisationen und Plattformen standardisiert nutzbar sind [1].

Enterprise Identity and Access Management (EIAM) bezieht sich im Kern auf die Kombination von Verfahren der Organisationsführung einerseits und IT-Technologie andererseits, die es Organisationen durch eine breite Palette von Prozessen und Funktionalitäten erlauben, die Einhaltung gesetzlicher Vorschriften sowie die Integrität, Vertrauenswürdigkeit und Verfügbarkeit von Informationen gewährleisten zu können.

Eine Entität (Person, Rechner etc.) setzt sich zusammen aus den sie beschreibenden Attributen, siehe Abb. 6.1.

Eine digitale Identität (siehe Abb. 6.2) ist die Teilmenge der Attribute einer Entität, die diese Identität in einem bestimmten Kontext im Unterschied zu anderen Entitäten bestimmbar machen. Eine Entität kann abhängig vom Kontext und den dadurch erforderlichen Attributen auch mehrere digitale Identitäten besitzen. Entitäten sind individuell identifizierbare Personen, IT-System usw.

Der Begriff Identity and Access Management (IAM) wird in den meisten Fällen synonym zu IdM (Identity Management) verwendet und soll verstärkt auf den Aspekt der Zugangskontrolle hinweisen. Das Access Management ist in dieser Definition als Teilmenge von IdM zu sehen. Das Wort Enterprise soll deutlich machen,

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2022

N. Pohlmann, *Cyber-Sicherheit*, https://doi.org/10.1007/978-3-658-36243-0_6

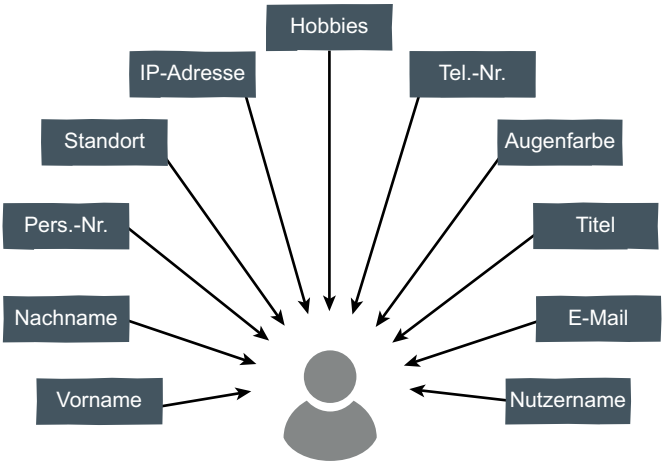
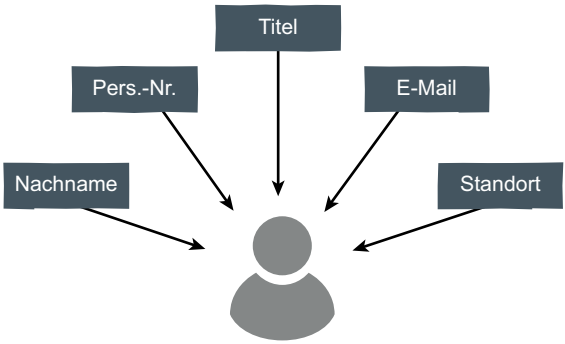


Abb. 6.1 Entität

Abb. 6.2 Digitale Identität



dass das Referenzmodell, das vorgestellt wird, insbesondere für größere Unternehmen und Organisationen gedacht ist.

Enterprise Identity and Access Management (EIAM) erbringt unterschiedliche Mehrwerte für ein Unternehmen. Die Mehrwerte gelten teilweise generell und für das ganze Unternehmen, teilweise auch nur für einzelne Teile. Das liegt daran, dass einzelne Teile eines Unternehmens durchaus widersprüchliche Anforderungen haben können. Es existieren Stellen, an denen eine möglichst hohe Automatisierung (weniger menschliches Personal) und ein reibungsloser Einsatz (Nutzerfreundlichkeit) von oberster Priorität sind. An anderen Stellen wiederum ist ein sehr hohes Maß an Cyber-Sicherheit die wichtigste Vorgabe, worunter unter Umständen die Kosten und die Nutzerfreundlichkeit leiden können.

▶ **Wichtig** Enterprise Identity and Access Management (EIAM) beschreibt jeglichen Einsatz von digitalen Identitäten, deren Attributen, deren Berechtigungen für IT-Systeme sowie IT-Dienste und schließt die Erzeugung, Nutzung, Pflege und Löschung dieser digitalen Identitäten mit ein.

Trusted Computing

7

Zusammenfassung

Trusted Computing (TC) ist eine Cyber-Sicherheits- und Vertrauenswürdigkeitstechnologie. Mithilfe von Trusted Computing stehen moderne und intelligente Cyber-Sicherheitsarchitekturen, -konzepte und -funktionen zur Verfügung, mit denen IT-Systeme mit einer höheren Robustheit und einem höheren Cyber-Sicherheitslevel umgesetzt werden können. Der besondere Schwerpunkt liegt dabei auf der Verifikation der Integrität eines IT-Systems.

▶ **Wichtig** Ein IT-System ist vertrauenswürdig, wenn es sich immer in der erwarteten Weise für den beabsichtigten Zweck verhält.

7.1 Einleitung

Der Begriff des Trusted Computing wurde primär durch die Trusted Computing Group (TCG) geprägt, die die grundlegenden Spezifikationen für ein vertrauenswürdiges IT-System erarbeitet hat. Die TCG ist ein Industriekonsortium, zusammengeschlossen aus ca. 200 Firmen. Darunter befinden sich Weltmarktführer wie Microsoft, Intel, AMD, HP, IBM, Cisco, HUAWEI, Lenovo und Infineon. Die Gruppe hat sich zur Aufgabe gemacht, offene Spezifikationen für vertrauenswürdige IT-Systeme zu entwickeln, um die Cyber-Sicherheit verteilter Anwendungen mit vertretbarem Aufwand zu erhöhen. Kern aller Bemühungen der TCG ist die Bildung einer „Trusted Platform“, einer sicheren und vertrauenswürdigen Basis für Anwendungen. Die Trusted Platform, in der Form einer Sicherheitsplattform, auf der Basis von intelligenten kryptografischen Verfahren, stellt eine sichere Umgebung zum Schutz von sicher-

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2022

N. Pohlmann, *Cyber-Sicherheit*, https://doi.org/10.1007/978-3-658-36243-0_7

heitskritischen Daten für sicherheitskritische Operationen bereit, die sehr viele heutige Cyber-Sicherheitsprobleme, wie Malware, reduzieren kann.

Veränderung von reaktiven zu proaktiven Cyber-Sicherheitssystemen

1. **Reaktive Cyber-Sicherheitssystemen**
   Bei den heutigen reaktiven Cyber-Sicherheitssystemen, wie Anti-Spam-, Anti-Malware-, Intrusion-Detection-Systemen, ist die grundsätzliche Idee, so gut und schnell wie möglich Cyber-Angriffe zu erkennen. Das bedeutet, wenn die Cyber-Sicherheitslösungen einen Angriff durch eine entsprechende Angriffssignatur oder eine Anomalie erkennen, dann wird versucht, das IT-System so schnell wie möglich zu schützen, um den Schaden zu reduzieren.
   Dies entspricht der **„Airbag-Methode“** – Wenn's passiert, soll es weniger wehtun! Siehe Abb. 7.1.
   Beispiele für reaktive Sicherheitssysteme sind: Intrusion Detection, Anti-Malwareprodukte und Anti-Spam/-Phishing-Lösungen.
2. **Proaktive Cyber-Sicherheitssysteme**
   Für die zunehmende Vielfalt und Komplexität der IT-Endgeräte (Wearables, Smartphones, Notebooks, PC, …), IoT-Geräte, Netzkomponenten und IT-Infrastrukturen werden deutlich verlässlichere, robustere und wirkungsvollere Cyber-Sicherheitskonzepte benötigt. Daher ist es sinnvoll, weniger reaktive und mehr moderne proaktive Cyber-Sicherheitssysteme zu verwenden, die eine Ausführung von intelligenter Malware, eines der größten Cyber-Sicherheitsprobleme zurzeit, verhindern können.
   Solche proaktiven Cyber-Sicherheitssysteme arbeiten mit einem kleinen Sicherheitskern (sichere Betriebssysteme) und Virtualisierung, können Software messbar machen und mit einer starken Isolation Anwendungen mit ihren Daten separieren und so nachhaltige und angemessene Cyber-Sicherheit bieten.
   Für proaktive Cyber-Sicherheitssysteme muss die Softwarearchitektur der IT-Endgeräte allerdings grundlegend anders aufgebaut sein als bisher. Außerdem müssen Sicherheits-Infrastrukturkomponenten gemeinsam umgesetzt werden, damit diese Cyber-Sicherheits- und Vertrauenstechnologien organisationsübergreifend genutzt werden können.
   Dies entspricht der **„ESP-Strategie“** – Verhindern, dass ein Auto überhaupt ins Schleudern kommt, siehe Abb. 7.2.

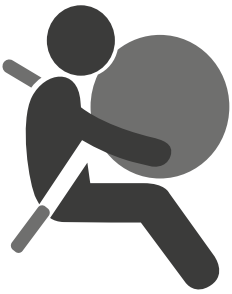


Abb. 7.1 „Airbag-Methode“ – „Wenn's passiert, soll es weniger wehtun“

Abb. 7.2 „ESP-Strategie“ – Verhindern, dass ein Auto überhaupt ins Schleudern kommt

Das Software-Qualitätsproblem als eine der wichtigsten Herausforderungen
Die Software stellt heute in allen Branchen einen immer größeren Wertschöpfungsanteil dar. Genutzt wird Software in Großrechnern, PCs, Notebooks, Smartphones, aber auch immer mehr in Autos, Industrieanlagen, Kühlschränken usw. Waren zum Beispiel bei Autos in der Vergangenheit nur mechanische Bauteile für die Funktion verantwortlich, steigt der Wertschöpfungsanteil der Software in Autos immer mehr. Heute werden oft die gleichen Motoren in Autos eingebaut und nur über die Software und deren Konfiguration kann entschieden werden, ob das Auto zum Beispiel 100, 130 oder 160 PS nutzen kann. Auch verfügen die Autos über immer mehr Sensoren, die von Software ausgelesen werden, um für mehr Sicherheit und Komfort zu sorgen. Das bedeutet aber auf der anderen Seite, dass die Software eine sehr hohe Qualität aufweisen muss, um verlässlich zu sein. Bei der Software in Autos wurde und wird sehr viel Aufwand in die Qualität und Verifikation von Software gesteckt, um diesem Anspruch zu genügen. Bei vielen Betriebssystemen und Anwendungen für PCs, Notebooks, Smartphones usw. ist es noch ein langer Weg, eine qualitativ hochwertige Software nutzen zu können [1].

IT-Sicherheitslücken sind in der Regel keine Absicht der Programmierer oder Hersteller, sondern ein Resultat von heutigen Entwicklungsprozessen. Software wird noch immer von Menschen entwickelt und so bleiben Fehler, trotz vieler Gegenmaßnahmen durch spezielle Programmiermethoden und Softwaregutachten, nicht aus [2]. Die Fehlerdichte einer Software wird anhand der Fehler pro 1000 Programmzeilen (lines of code, kurz: loc) gemessen. Der daraus resultierende Quotient sagt dann in etwa aus, wie anfällig ein Programm potenziell ist, wobei erst bei einer Fehlerdichte <0,5 ein Programm als wirklich stabil gilt. Eine so geringe Fehlerdichte ist vor allem dort Pflicht, wo Menschenleben von einer Anwendung abhängen, wie beispielsweise bei Steuerungssystemen von Flugzeugen. Akzeptanz finden Programme jedoch schon ab einem Fehlerquotienten von 5, obwohl in der Regel stets ein Quotient <2 angestrebt wird. Kommerzielle Software weist eine durchschnittliche Fehlerdichte von 0,76 auf, bei Open Source-Software sogar nur 0,61 [3].

▶ **Wichtig** Mit der Hilfe von Trusted Computing kann das Software-Qualitätsproblem in seiner Wirkung deutlich reduziert werden.

Cyber-Sicherheit-Frühwarn- und Lagebildsysteme

8

Zusammenfassung

In diesem Kapitel geht es um die Bedeutung und Grundstruktur eines Cyber-Sicherheit-Frühwarn- und Lagebildsystems. Die grundsätzliche Idee sowie unterschiedliche Sensoren werden beschrieben und diskutiert. Außerdem werden die notwendigen Prozesse und die Probleme, die durch die Entwicklung eines Cyber-Sicherheit-Frühwarn- und Lagebildsystems entstehen, behandelt.

8.1 Einleitung

Alle Organisationen sind zunehmend von der Verfügbarkeit der eigenen und öffentlichen IT-Infrastruktur im Cyber-Raum abhängig. Ausfälle und Störungen der weltweiten Kommunikation, der angebotenen Dienste und digitalen Geschäftsprozesse können zu unkalkulierbaren Schäden führen. Ein Cyber-Sicherheit-Frühwarn- und Lagebildsystem hilft, die Cyber-Sicherheitslage aktuell aufzuzeigen und möglichst früh Angriffspotenziale und reale Angriffe zu erkennen, um rechtzeitig Warnhinweise zu geben, damit Schäden auf die IT-Infrastruktur minimiert oder verhindert werden können.

▶ **Wichtig** Ein Cyber-Sicherheit-Frühwarn- und Lagebildsystem hilft, Sicherheit und Vertrauenswürdigkeit der IT-Infrastruktur nachhaltig zu erhöhen und widerstandsfähiger zu gestalten.

8.2 Angriffe und ihre Durchführung

In diesem Abschnitt werden Grundlagen von Angriffen aufgezeigt, um besser zu verstehen, wie Angriffe und Angriffspotenziale erkannt werden können.

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2022

N. Pohlmann, *Cyber-Sicherheit*, https://doi.org/10.1007/978-3-658-36243-0_8

Abb. 8.1 Werte

Ein Angriff ist ein Versuch, einen Wert zu stehlen, zu verändern, zu löschen oder sich unbefugten Zugriff auf ein IT-System und dessen Ressourcen zu verschaffen, siehe Abb. 8.1.

Dies tut der Angreifer in der Regel gezielt und absichtlich, siehe auch Abschn. 1.9 „Angreifer und deren Motivation".

Botnetz, Bots, Botmaster und Comand&Control

Ein Botnetz ist der Zusammenschluss von Bots in einem vom Botmaster kontrollierten Netzwerk. Ein Bot ist ein kompromittiertes IT-System (Endgerät, IoT-Geräte …), das mit Schadsoftware (Malware) infiziert ist und durch eine entfernte Stelle (Botmaster) ohne Einverständnis und Kenntnis des Besitzers des IT-Systems flexibel steuerbar ist. Das heißt, der Botmaster kann die Daten und alle weiteren Ressourcen des kompromittierten IT-Systems zu seinem Zwecke nutzen. Damit ist der Botmaster der Angreifer mit entsprechenden Angriffstechnologien, der die Kontrolle über das Botnetz hat. Er ist in der Lage flexibel unterschiedliche Schadfunktionen (Spam, DDoS, Keylogger, Ransomware, Spyware, Adware, Trojanisches Pferd …) in die intelligente Malware des kompromittierten IT-Systems herunterzuladen und diese aus der Ferne zu steuern. Die Comand&Control (C&C)-Kommunikation ist die Netzwerkkommunikation des Botmasters zur Steuerung und Kommandierung von Bots. Es gibt Botnetze mit 1000, 10.000, 100.000 oder sogar 1.000.000 Bots. Siehe Abb. 8.2 (der orange Käfer stellt die Malware dar).

Durchführung von Angriffen

Eine Möglichkeit, Angriffe zu unterscheiden, ist die Anzahl der Angreifer und Opfer als Kriterium zu verwenden. Im Folgenden werden einige Angriffsstrukturen diskutiert.

A) M:1-Angriff

Bei einem M:1-Angriff gibt es M Angreifer und ein Opfer.

Die M Angreifer sind zum Beispiel

- Bots, das sind kompromittierte IT-Systeme mit Malware und Teil eines Botnetzes, das von einem Botmaster gesteuert wird, siehe Abb. 8.3,

oder/und

- Aktivisten, die sich für einen gemeinsamen Angriff abgesprochen haben, siehe Abb. 8.4.

Das Opfer ist zum Beispiel ein Webserver oder ein anderer IT-Dienst im Internet

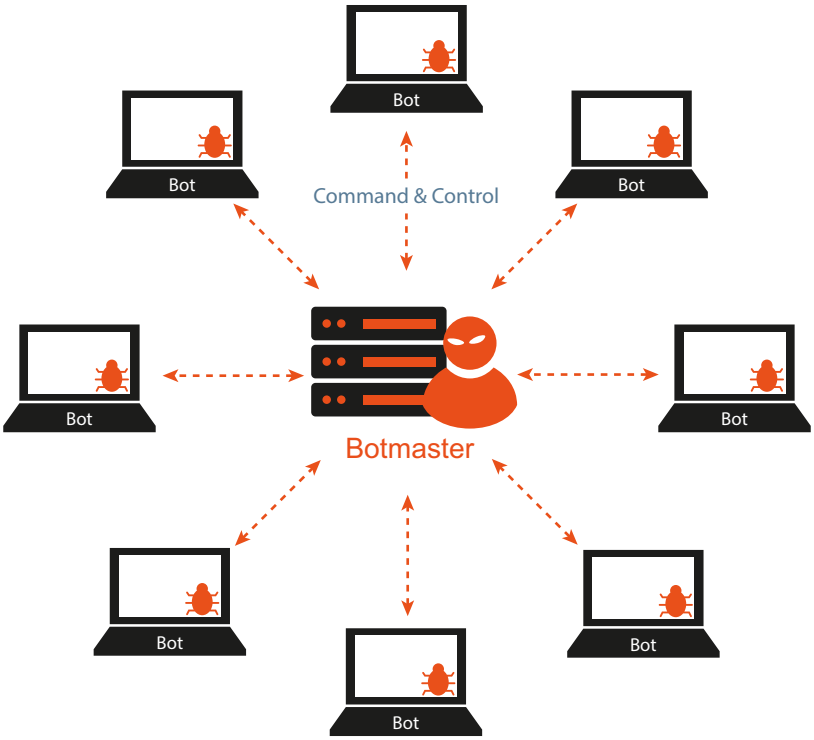


Abb. 8.2 Botnetz, Bots, Botmaster und Comand&Control

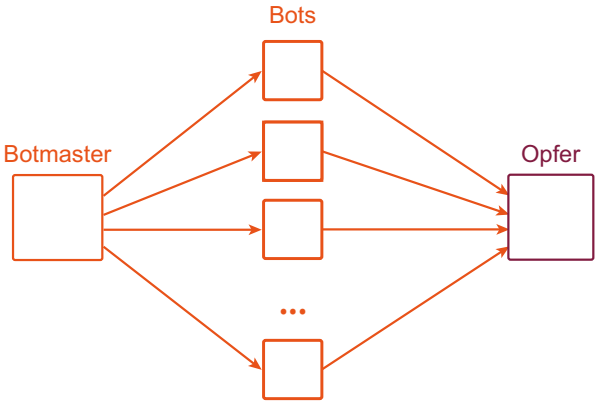


Abb. 8.3 M:1-Angriff mithilfe eins Botnetes

Firewall-Systeme

9

Zusammenfassung

Ein Firewall-System ist ein Cyber-Sicherheitsmechanismus, der zwischen verbundenen Netzen Sicherheitsdomänen mit unterschiedlichem Schutzbedarf schafft.

Es wird meist zum Schutz eigener Netze vor Risiken aus unsicheren Netzen wie dem Internet, aber auch zur Strukturierung eigener Netze in einer Organisation eingesetzt. Durch eine Reduzierung von Kommunikationsmöglichkeiten über ein Firewall-System wird die Angriffsfläche und dadurch das Risikopotenzial minimiert.

Dabei müssen unterschiedliche Aspekte berücksichtigt werden, damit mithilfe eines Firewall-Systems das gewünschte Sicherheitsmaß auch erreicht werden kann [1].

▶ **Wichtig** Mithilfe eines Firewall-Systems kann der Übergang zwischen einem unsicheren und einem zu schützenden Netz sicherer gestaltet werden.

9.1 Bedrohungen im Netz

Im folgenden Abschnitt werden die potenziellen Bedrohungen, die in Netzen wie dem Internet wirken, beschrieben. Außerdem werden gezielte Angriffe dargestellt, die auf der TCP/IP-Technologie beruhen, und prinzipielle Möglichkeiten, diesen Angriffen mithilfe von Firewall-Systemen entgegenzuwirken.

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2022

N. Pohlmann, *Cyber-Sicherheit*, https://doi.org/10.1007/978-3-658-36243-0_9

9.1.1 Angriffsmöglichkeiten in Kommunikationssystemen

Eine starke Bedrohung zielt auf das Kommunikationssystem, das heißt, auf die Nachrichten, die über Kommunikationssysteme wie Internet ausgetauscht werden.

Auf eine Nachricht (ein oder mehrere IP-Pakete) reagiert ein Empfänger mit einem bestimmten Verhalten, siehe Abb. 9.1.

Ein Angreifer, der die Kommunikationsverbindung abhört, kann das Verhalten des Empfängers und des Senders interpretieren. Der Angreifer kann die Reaktionen des Empfängers zielgerichtet beeinflussen, wenn er die Möglichkeit hat, die Nachricht zu wiederholen, zu verändern, zu löschen oder zu ergänzen.

Aus dieser Überlegung heraus werden grundsätzlich zwei Bedrohungsarten unterschieden: passive Angriffe und aktive Angriffe.

9.1.2 Passive Angriffe

Bei passiven Angriffen werden die übertragenen Nachrichten und der Betrieb des Kommunikationssystems nicht geändert. Passive Angriffe sind Bedrohungen, die vom Angreifer bewusst und gezielt durchgeführt werden, um sich unerlaubt Informationen zu beschaffen.

Passive Angriffe können zum Beispiel durch das Abhören der Leitung oder durch das Abfangen der Signale über die Luft durchgeführt werden. Ein passiver Angreifer bleibt oft gänzlich oder zumindest für lange Zeit unentdeckt und kann so latent über einen längeren Zeitraum großen Schaden anrichten, siehe Abb. 9.2.

Es werden die folgenden passiven Angriffsarten unterschieden:

Abhören von Daten
Ein Abhörender gelangt unmittelbar in den Besitz der Nachricht und kann sie zu seinem Zweck verwerten. Zum Beispiel kann ein Angreifer bei einer unverschlüsselten IP-Verbindung zwischen einem Webserver und einem Client während der Log-in-Prozedur den Nutzernamen und das Passwort eines Nutzers abhören und später mit diesen Zugangsinformationen unerlaubt Zutritt zum Webserver erlangen.

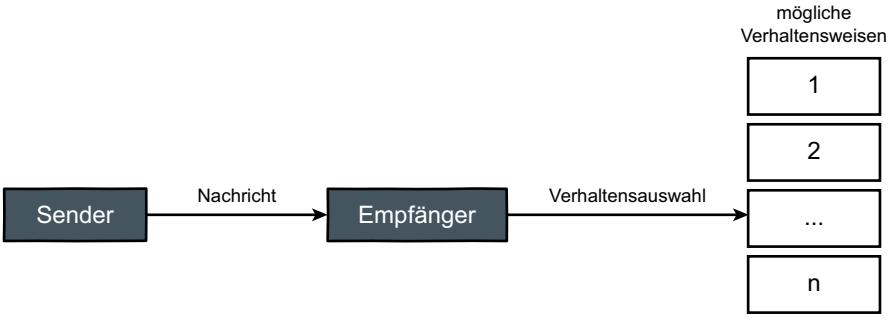


Abb. 9.1 Reaktionsmöglichkeiten des Empfängers einer Nachricht

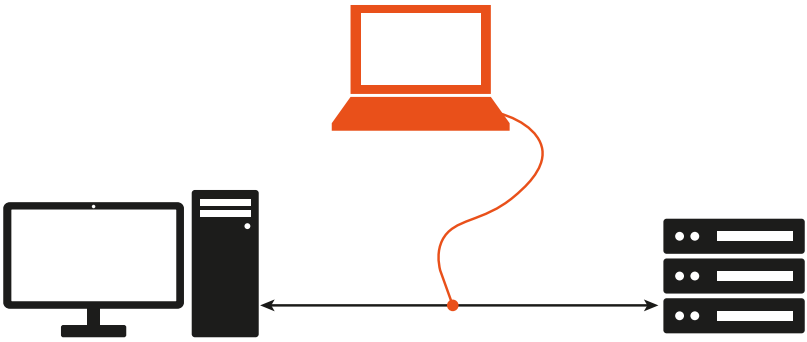


Abb. 9.2 Passive Angriffe auf Nachrichten oder auf das Kommunikationssystem

Weitere Beispiele sind das Abhören von vertraulichen Informationen, wie Entwicklungsunterlagen von neuen Produkten, oder das Abhören von Daten, die unter die EU-Datenschutzgrundverordnung fallen. Diese Angriffe sind prinzipiell problemlos durchführbar.

Abhören der Nutzer-Identitäten
Der Lauscher erfährt, welche Nutzer oder IT-Systeme untereinander eine Datenverbindung aufbauen und Daten austauschen. Allein aus der Kenntnis, wer mit wem zu welchem Zeitpunkt Nachrichten ausgetauscht hat, sind oft Rückschlüsse auf den Inhalt der Nachricht oder das Verhalten der Nutzer möglich. Wenn jemand zum Beispiel auf die WWW-Seiten eines Waschmaschinenherstellers zugreift, kann vermutet werden, dass er eine Waschmaschine kaufen wird.

Verkehrsflussanalyse
Auch wenn die Daten verschlüsselt sind, ist es einem Abhörenden möglich, durch eine „Verkehrsflussanalyse“ gewisse Informationen zu erhalten, wie zum Beispiel Größenordnungen, Zeitpunkte, Häufigkeit und Richtung des Datentransfers. Diese Informationen können für bestimmte spezielle Anwendungen interessant sein, zum Beispiel für Börsen-Transaktionen oder militärische Operationen.

9.1.3 Aktive Angriffe

Neben der Gefahr, abgehört zu werden, besteht die Möglichkeit von aktiven Angriffen, die den Nachrichtenstrom und/oder den Betrieb der Kommunikation verfälschen. Aktive Angriffe werden zum Beispiel durch Auftrennen der Übertragungsleitungen und/oder mithilfe der Emulation von Übertragungsprotokollen durchgeführt, siehe Abb. 9.3.

Bei aktiven Angriffen wird grob unterschieden zwischen Bedrohungen durch Dritte und Bedrohungen durch den Kommunikationspartner.

Bedrohungen durch Dritte sind zum Beispiel:

IPSec-Verschlüsselung

10

Zusammenfassung

Im Kapitel IPSec-Verschlüsselung werden die Cyber-Sicherheitsarchitektur, Cyber-Sicherheitsprinzipien, Cyber-Sicherheitsmechanismen und Cyber-Sicherheitsprotokolle des IETF Sicherheitsstandards für die Cyber-Sicherheit von IP-Paketen vermittelt.

10.1 Einleitung

Das Internet ist eine weltweite und offene Kommunikationsinfrastruktur, über die Unternehmen, Organisationen und deren Niederlassungen miteinander kommunizieren. Besonders für diesen Anwendungsfall wird heute der IPSec-Standard verwendet. IPSec steht für Internet Protocol Security und wurde von der Internet Engineering Task Force (IETF) entwickelt. Die grundsätzliche Idee von IPSec ist, eine offene, kostengünstige und weltweit verfügbare Kommunikationsinfrastruktur wie das Internet zu nutzen und allen Bedrohungen und Risiken möglichst sinnvoll entgegenzuwirken [1].

IPSec arbeitet direkt auf der Vermittlungsschicht und ist eine Weiterentwicklung des IP-Protokolls (IP). IPSec war als Feature in IPv6 gedacht und ergänzt aber auch das bestehende IPv4 Protokoll um wichtige Cyber-Sicherheitsfunktionen, siehe Abb. 10.1.

Ziel ist es, eine Cyber-Sicherheit auf Netzwerkebene bereitzustellen und somit Kommunikation auf der Basis des Internet-Protokolls (IP) zu schützen. Die IP-Pakete werden zwischen definierten Kommunikationsendpunkten geschützt.

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2022

N. Pohlmann, *Cyber-Sicherheit*, https://doi.org/10.1007/978-3-658-36243-0_10

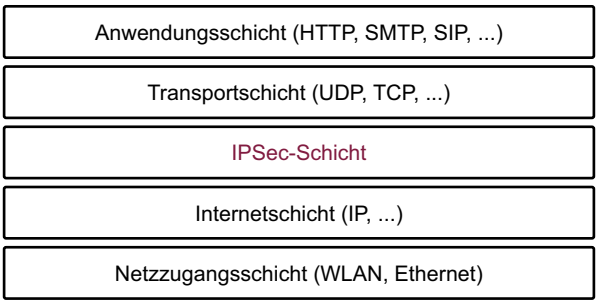


Abb. 10.1 IPSec im TCP/IP-Referenzmodell

Die folgenden Cyber-Sicherheitsfunktionen werden von IPSec angeboten:

- **Verschlüsselung** schützt die Vertraulichkeit der übertragenen Daten (jedes Paket kann verschlüsselt werden).
- **HMAC-Funktion** sorgt für die Authentizität und Unversehrtheit der übertragenen Daten (jedes Paket kann gegen Manipulation geschützt und auf die Echtheit überprüft werden).
- **Anti-Replay Mechanismus** schützt vor unberechtigter Wiedereinspielung von übertragenen Daten (jedes Paket kann vor Wiedereinspielung geschützt werden).
- **Authentifikation** gewährleistet die Eindeutigkeit und Echtheit der Kommunikationspartner (die Kommunikationspartner können authentifiziert werden).
- **Tunneling** verschleiert den Datentransfer für definierte Aspekte (die IP-Kommunikation kann gegen einen gewissen Grad der Verkehrsflussanalyse geschützt werden).

▶ **Wichtig** IPSec schützt IP-Daten auf der Netzwerkebene während der Übertragung.

10.2 IPSec Header

IPSec realisiert die zusätzliche Cyber-Sicherheit durch das Einfügen von Erweiterungs-Headern in die IP-Pakete. In den IPSec-Headern sind nur minimal notwendige Informationen untergebracht, die auf spezielle Datenbanken verweisen und mit Security Associations das Security-Management zwischen den Kommunikationsendpunkten umsetzen.

Diese zusätzlichen Header sind:

1. **Authentication Header (AH, RFC 2402)**
   Cyber-Sicherheitsdienste, die mit den Authentication Headern erbracht werden, sind:
   - Datenunversehrtheit
   - Authentifikation
   - Anti-Replay Service (optional, ist aber standardmäßig aktiv)

2. **Encapsulated Security Payload (ESP, RFC 2406)**
   Cyber-Sicherheitsdienste, die mit den Encapsulated Security Payload Headern erbracht werden, sind:
   - Datenunversehrtheit und Authentifikation (optional, ist aber standardmäßig aktiv)
   - Anti-Replay Service (optional, ist aber standardmäßig aktiv)
   - Verschlüsselung (optional, ist aber standardmäßig aktiv)

Diese zusätzlichen IPSec-Header können in verschiedenen Modi verwendet werden:

‚Transportmode'	Sicherheitsdienste für die Nutzdaten
‚Tunnelmode'	Sicherheitsdienste für die IP-Header und Nutzdaten

10.2.1 Authentication Header

Der Authentication Header (AH) sorgt für eine starke Integrität und Authentizität der IP-Pakete. Dabei wird mit der Hilfe einer HMAC-Funktion über das gesamte IP-Paket und das Authentication-Feld selbst ein HMAC berechnet. Die Felder, die während des Transports modifiziert werden, wie Time to Live (TTL), TOS, Flags und Header Checksum werden bei der HMAC-Berechnung ausgelassen, damit eine Ende-zu-Ende-Überprüfung möglich ist.

Abb. 10.2 zeigt den „Authentication Header" im Tunnel-Mode.

Beschreibung des IPSec-Headers „AH"
In Abb. 10.3 ist der IPSec-Header „AH" dargestellt.

- **Next Header** ist ein 8-Bit-Feld, das den Typ des nächsten Extension Headers hinter dem Authentication Header identifiziert (Mechanismus, wie in der IPv6-Spezifikation).
- **Payload Length** (8 Bit-Feld) beschreibt die Länge des AH in 32-bit Worten.
- **Reserved** ist reserviert für zukünftige Funktionen.

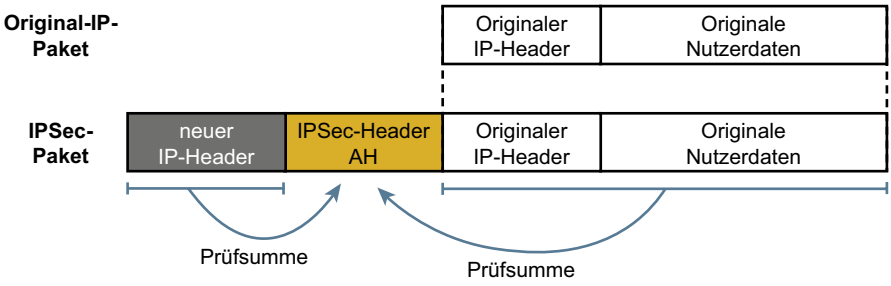


Abb. 10.2 Authentication Header im Tunnel-Mode

Transport Layer Security (TLS)/Secure Socket Layer (SSL) 11

Zusammenfassung

Im Kapitel „Transport Layer Security (TLS)/Secure Socket Layer (SSL) – TLS/SSL“ werden die Cyber-Sicherheitsarchitektur, Cyber-Sicherheitsprinzipien, Cyber-Sicherheitsmechanismen und Cyber-Sicherheitsprotokolle des IETF Sicherheitsstandards für die Transportebene vermittelt.

11.1 Einleitung

Da das Internet offen ist und die Angriffsmöglichkeiten sowie Angriffswahrscheinlichkeiten sehr groß sind, ist die Nutzung einer verschlüsselten und integritätsgesicherten Kommunikation zwischen Client und Server von besonderer Bedeutung.

Sehr viele Cyber-Sicherheitsaspekte im Web, wie Eingabe von Passwörtern und Kreditkarten-Informationen haben mit der Einrichtung einer vertrauenswürdigen Verbindung zwischen Client und Server zu tun [1].

Der vorherrschende Ansatz für die Transportverschlüsselung im Web ist die Verwendung von TLS (Transport Layer Security)/SSL (Secure Socket Layer) (siehe Abb. 11.1). TLS/SSL ist ein anwendungsunabhängiges Cyber-Sicherheitsprotokoll, das logisch auf einem Transportprotokoll aufsetzt. In diesem Abschnitt werden als erstes exemplarisch die Versionen TLS 1.2 und frühere Versionen behandelt. Im Abschn. 11.8 wird dann TLS 1.3 behandelt.

Die folgenden Cyber-Sicherheitsfunktionen werden von TLS/SSL angeboten:

- **Authentifikation** von Server und Client unter Verwendung von asymmetrischen Verschlüsselungsverfahren und elektronischen Zertifikaten.
- **Vertrauliche Client-to-Server Datenübertragung** mithilfe symmetrischer Verschlüsselungsverfahren unter der Nutzung eines gemeinsamen Sitzungsschlüssels.

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2022

N. Pohlmann, *Cyber-Sicherheit*, https://doi.org/10.1007/978-3-658-36243-0_11

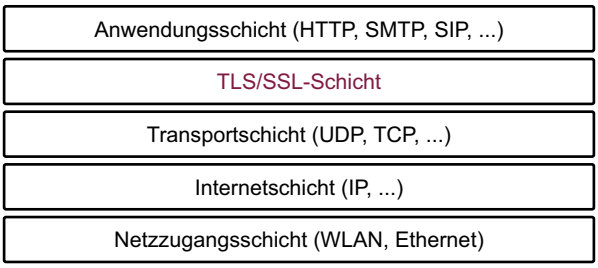


Abb. 11.1 TLS/SSL im TCP/IP-Referenzmodell

- **Sicherstellung der Integrität** der transportierten Daten unter Verwendung des HMAC-Verfahrens.
- TLS/SSL bietet auch die Komprimierung der Daten an.

▶ **Wichtig** TLS/SSL schützt TCP/UDP-Daten auf der Transportebene während der Übertragung.

Hinweis:
Die Idee kam von Netscape, die die erste Version von SSL 1994 veröffentlichte. 1999 wurde SSL von der IETF als Standard festgelegt und umbenannt zu Transport Layer Security (TLS). Da aber heute noch im Sprachgebrauch SSL fest verankert ist, wird im Weiteren immer von TLS/SSL gesprochen.

11.2 Einbindung in die Kommunikationsarchitektur

TLS/SSL kann eine Vielzahl höherer Anwendungsprotokolle unterstützen, wie HTTP, SMTP, SIP, IMAP, FTP, Telnet. Die genauen Eigenschaften des TLS/SSL-Kanals werden bei der Einrichtung der verschlüsselten und integritätsgesicherten Kommunikation zwischen Client und Server ausgehandelt und festgelegt. Sie können aber Anwendungsdaten-Fragmentierung und Komprimierung beinhalten, die in Kombination mit Authentifikation von Client und Server sowie Integrität, Authentizität und Vertraulichkeit der Transportdaten angewendet werden. Die TLS/SSL-Schicht ist in zwei Teil-Schichten angeordnet. Den Kern des TLS/SSL-Protokolls bildet eine TLS-Datensatz-Protokollschicht, die einen sicheren Kanal zwischen Client und einem Server implementiert.

Schichteneinordnung
Die TLS/SSL-Schicht befindet sich zwischen der Transport- und Anwendungsschicht. Sie übernimmt zusätzlich die Aufgaben der Sitzungs- und Präsentationsschicht (Schichten 5 und 6) des ISO/OSI-Modells. Ein wesentlicher Vorteil der Sitzungsschicht gegenüber der Transportschicht besteht darin, dass Zustandsinformationen über einen längeren Zeitraum und über verschiedene Einzelverbindungen hinweg gespeichert und für die Verwaltung genutzt werden können.

Für das zustandslose HTTP-Protokoll, das für jeden Zugriff auf eine Webseite eine neue TCP-Verbindung aufbauen kann, bedeutet das, dass mehrere solcher Verbindungen zu einer TLS/SSL-Sitzung gebündelt und damit effizienter als die jeweiligen Einzelverbindungen verwaltet werden können.

Die TLS/SSL-Protokolle sind erweiterbar und flexibel, um Zukunftssicherheit vor allem bei den Verschlüsselungsalgorithmen zu gewährleisten.

TLS/SSL arbeitet transparent, sodass es leicht eingesetzt werden kann, um Anwendungsprotokollen/-diensten, ohne eigene Cyber-Sicherheitsmechanismen, vertrauenswürdige Verbindungen zur Verfügung zu stellen.

Funktionsweise der TLS/SSL-Schicht

Die Umsetzung der TLS/SSL-Schicht funktioniert so, dass für die Anwendungsprotokolle eine weitere Port-Nummer als Transportadresse definiert wurde, die genutzt wird, wenn die Kommunikation zu diesen Anwendungen TLS/SSL-gesichert umgesetzt werden soll. Eine Kommunikationsanwendung hat dann zusätzlich eine Port-Nummer für die Nutzung der TLS/SSL-Sicherheitsdienste. Im Folgenden sind beispielhaft Kommunikationsanwendung, Port-Nummer und die passende Port-Nummer für die entsprechende TLS/SSL-gesicherte Kommunikation aufgezeigt, siehe Tab. 11.1.

Anhand der Portnummer lässt sich erkennen, um welches ursprüngliche Kommunikationsanwendungsprotokoll es sich bei den übertragenen Daten handelt. Beispielsweise ist Port 443 HTTPS, also wird auf der Kommunikationsanwendung das HTTP-Protokoll zwischen dem entsprechenden Client und Server genutzt.

In Abb. 11.2 ist am Beispiel der Kommunikationsanwendung HTTP die Integration der TLS/SSL-Schicht mit den Protokollen und den verschiedenen Port-Nummern dargestellt.

Der Client kann durch die Wahl des Ports entscheiden, ob die Kommunikation TLS/SSL-gesichert sein soll oder im Klartext:

- Port 80: http-Kommunikation im Klartext
- Port 443: http-Kommunikation TLS/SSL-gesichert

Tab. 11.1 Port-Nummer Kommunikationsanwendungen und entsprechende TLS/SSL-Zugänge

Kommunikationsanwendung	Port-Nummer	TLS/SSL Port-Nummer
Hypertext Transfer Protocol – HTTP	80	443
Simple Mail Transfer Protocol – SMTP	25	465
Internet Message Access Protocol – IMAP	143	993
Session Initiation Protocol – SIP	5060	5061
File Transfer Protocol – FTP	20, 21	989, 990
Teletype Network – TELNET	23	992
…	…	..

12 Cyber-Sicherheitsmaßnahmen gegen DDoS-Angriffe

Zusammenfassung

Die Gewährleistung der Verfügbarkeit von IT-Systemen ist ein wichtiges Cyber-Sicherheitsbedürfnis, um Informationen und Dienste immer nutzen zu können.

In diesem Kapitel werden DDoS-Angriffe, Ziele von DDoS-Angriffsmethoden und hilfreiche Cyber-Sicherheitsmaßnahmen gegen DDoS-Angriffe beschrieben.

12.1 Einleitung

Die Abkürzung DDoS steht für Distributed Denial of Service. Das sind in der Regel Angriffe von Internet-Aktivisten und/oder kompromittierten IT-Systemen mit Malware, die von Angreifern dazu genutzt werden, ausgesuchte Ziel-IT-Systeme koordiniert mit einer großen Last spezieller Anfragen durch Erschöpfung der verfügbaren Ressourcen (CPU, RAM, Bandbreite, …) lahmzulegen. Es gibt Botnetze mit sehr vielen Bots (kompromittierten IT-Systemen mit Malware): 1000, 10.000, 100.000 oder sogar 1.000.000. Wenn ein Angreifer 100.000 Bots gleichzeitig nutzen kann, jeder Bot nur 100 KBit/s upstream nutzen würde (also nur ein Bruchteil der verfügbaren Bandbreite), dann könnte der Angreifer mit 10 GBit einen DDoS Angriff durchführen. Bei 500.000 Bots und 200 KBit/s Bandbreite hätte der Angreifer 100 GBit/s zur Verfügung [1]. Botnetze sind schon länger als Bedrohung auch auf die Verfügbarkeit von Diensten im Internet bekannt. IoT-Botnetze stellen eine neue Stufe der Gefahr für die Infrastruktur des Internets dar [2]. Im Unterschied zu konventionellen Botnetzen bestehen IoT-Botnetze hauptsächlich aus kompromittierten IoT-Geräten. Die IoT-Geräte haben die Eigenschaft, dauerhaft und mit guter Bandbreite und nicht unter der direkten Kontrolle des Nutzers online

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2022

N. Pohlmann, *Cyber-Sicherheit*, https://doi.org/10.1007/978-3-658-36243-0_12

verfügbar zu sein. Dadurch stehen die IoT-Geräte, einmal unter der Kontrolle eines Angreifers, immer für einen Angriff mit einer hohen verfügbaren Bandbreite bereit.

Welches Gefahrenpotenzial die Masse an ungesicherten IoT-Geräten mit sich bringt, zeigten die massiven DDoS-Angriffe des Mirai Botnetzes. Das Botnetz Mirai bestand aus mehr als einer Million kompromittierter IoT-Geräte. Die Intensität der DDoS-Angriffe erreichte eine bis dahin nicht dagewesene Dimension, mit einem durch die Anfragen erzeugten Traffic von 665 Gigabit bis zu 1,5 Terabit pro Sekunde. Die Menge der kompromittierten IoT-Geräte bestand hauptsächlich aus ungesicherten, mit dem Internet verbundenen Sicherheitskameras, digitalen Videorekordern und Haushaltsgeräten. Die Analyse des Quellcodes zeigte deutlich, mit welch simpler, auf menschlicher Schwäche basierender Strategie die Malware agierte. Sie durchsuchte das Internet nach IoT-Geräten, testete, ob diese noch auf das Default-Passwort des Herstellers konfiguriert waren, und brachte sie dann unter ihre Kontrolle. Gegenüber den üblichen Methoden wie „Social Engineering“ oder „E-Mail-Poisoning“ ermöglichte diese Herangehensweise eine enorme Senkung des Aufwands. Stattdessen können die meist schlecht gesicherten IoT-Geräte über die Ports 22 (SSH) oder 23 (Telnet) direkt angegriffen und übernommen werden, um sie zum Beispiel für DDoS-Angriffe zu nutzen. Die ständige Verfügbarkeit der IoT-Geräte macht sie zu sehr attraktiven Bots. Basierend auf dem offenen Quellcode von Mirai entstanden viele Ableger des Botnetzes.

Solche Überlastungen sind schwierig zu kontrollieren und eine kontinuierlich wachsende Herausforderung. Heutzutage sollte sich jeder Verantwortliche einer IT-Infrastruktur mit den möglichen Cyber-Sicherheitsmaßnahmen auseinandersetzen, um im Angriffsfall vorbereitet zu sein und die verursachten Schäden im Rahmen halten zu können.

Durch die Nichterreichbarkeit der Internet-Dienste entstehen direkte Umsatzeinbußen, Service-Level-Agreement-Verletzung, Kundenabwanderung oder mögliche Reputationsschäden sowie oft hohe Schadsummen auf Seiten der Angegriffenen. Nicht nur „Big Player“ werden heutzutage regelmäßig Ziel solcher DDoS-Angriffe auf die Verfügbarkeit ihrer Internet-Dienste. Die finanziellen Schäden ziehen sich neben der IT- und Sicherheitsabteilung oft auch durch die Marketing-Abteilung, den Kundenservice und das Risiko-Management. Das macht DDoS-Angriffe natürlich insgeheim auch für Mitbewerber interessant. In erster Linie sind sie allerdings ein seit Jahren eingesetztes Mittel von Cyberkriminellen und Aktivisten. DDoS-Angriffe werden illegal und kriminell eingesetzt, um Firmen und Organisationen zu erpressen, gezielt hohen Geschäftsschaden zu verursachen oder um auf politische Ziele aufmerksam zu machen. Zu beliebten Zielen gehören ebenfalls Onlinespiele-Server, Onlinebanking-Portale, politische und ideologische Webseiten, Nachrichtenportale, VoIP-Dienstleister und viele mehr. Technisch wenig bewanderte Kriminelle können solche Angriffe für ihre Zwecke bei „Stresstest“-Dienstleistern und in einschlägigen Portalen einkaufen. Über die vergangenen Jahre haben sich DDoS-Angriffsmethoden zudem weiterentwickelt. Angriffe haben heutzutage ein deutlich höheres Datenvolumen oder zielen sogar auf bestimmte Schwachstellen in Anwendungen. Um eine adäquate Abwehrstrategie aufstellen zu können, sind verschiedene Cyber-Sicherheitsmaßnahmen zu beachten.

Solche oder ähnliche Angriffe finden in Deutschland jährlich mehrere 1000 Mal statt. Viele zahlen das Geld, um die Verfügbarkeit sicherzustellen, andere tragen den Schaden der Nicht-Verfügbarkeit. Allen gemeinsam: Sie erleiden einen Schaden!

Relativ einfach und preiswert durchzuführende DDoS-Angriffe zielen vermehrt auf die Verfügbarkeit von Internet-Diensten. Das Risiko, Ziel eines Angriffs zu werden, wird häufig unterschätzt. Jedermann kann – je nach Intensität und Dauer – so einen Angriff ab etwa 50 € von cyberkriminellen Dienstleistern im Internet buchen. Die auf der anderen Seite entstehenden Schäden wiederum gehen schnell in die Millionen. Firewalls und Intrusion Prevention Systeme liefern entgegen weitläufiger Meinung keinen ausreichenden Schutz gegen professionelle DDoS-Angriffe.

12.2 Gezielte Überlastung von verfügbaren Ressourcen

Durch eine Kombination unterschiedlicher DDoS-Angriffsmethoden kann ein Angreifer unterschiedliche Teile eines Internet-Dienstes speziell überlasten sowie flexibel auf unzureichende Abwehrmaßnahmen und deren Schwachstellen reagieren, siehe Abb. 12.1.

Folgende Teile der Dienst-Architektur können Ziel von DDoS-Angriffsmethoden werden:

Die Kommunikationsanbindung – durch Überlastung der **verfügbaren Bandbreite.** Der Angreifer produziert so viele unsinnige Datenpakete, dass die Bandbreite nicht mehr ausreicht, um die gewünschten Datenpakete zum Server zu transportieren. Bei hoher Last wird die Quality of Service schlecht und bei extremer Last muss der Router die meisten Datenpakete verwerfen, weil die Warteschlangen voll sind. Dadurch sind die eigentliche Anwendung oder der Dienst nicht mehr nutzbar.

Der **Netzwerk-Stack:** Hier kann ein Crash oder ein Überlastungszustand durch Angreifer aufgrund von Fehlern in der Implementierung oder Eigenarten verschiedener Protokollfamilien, insbesondere auch bei eingesetzten Verschlüsselungsverfahren, hervorgerufen werden. Ebenfalls kann eine Auslastung des **RAM** durch sehr viele unvollständige Verbindungsanfragen eines Angreifers gezielt hervorgerufen werden, was die Verfügbarkeit eines Dienstes schnell stark einschränkt.

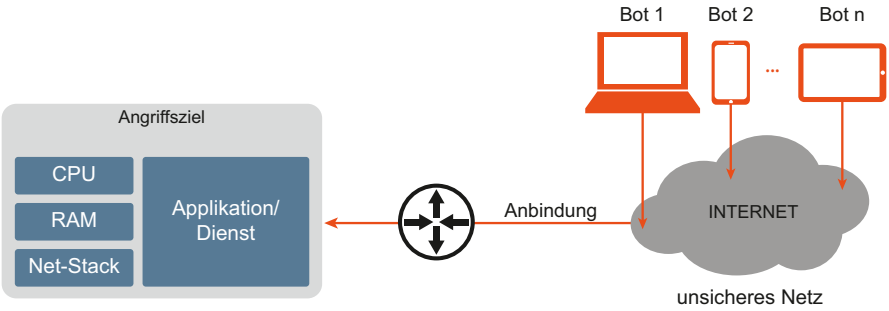


Abb. 12.1 DDoS – gezielte Überlastung von verfügbaren Ressourcen

E-Mail-Sicherheit

13

Zusammenfassung

Die E-Mail-Anwendung ist eine der wichtigsten Kommunikationsmöglichkeiten, insbesondere im Business-Bereich. Aus dem Grund wird in diesem Kapitel das Thema E-Mail-Sicherheit behandelt und die verschiedenen Cyber-Sicherheitskonzepte und Möglichkeiten werden diskutiert. Außerdem wird das Thema Spam-Mail prinzipiell beschrieben und diskutiert.

13.1 Einleitung

Der E-Mail-Dienst ist eine elastische Anwendung, in der diskrete, zeitunabhängige Medien, wie Text und Grafik, ausgetauscht werden. Der E-Mail-Dienst ist eine der am weitesten verbreiteten und meist genutzten Leistungen des Internets. Obwohl die E-Mail-Anwendung nicht als verlässlicher Dienst konzipiert wurde, wird sie als Mittel zur einfachen und professionellen nachrichtenbasierten Kommunikation im Internet eingesetzt [1].

Die Vorteile der E-Mail-Anwendung sind sehr klar zu erkennen: Einfache Handhabung macht sie für jeden zugänglich. Die E-Mails werden innerhalb weniger Sekunden weltweit übertragen und jeder kann jederzeit mithilfe von Mail-Boxen erreicht werden. Die Inhalte und Anhänge der E-Mails können sofort weiterverwendet werden, es tritt kein Medienbruch auf. Die E-Mail-Anwendung ist sehr kostengünstig, da in der Regel keine Gebühren für den Austausch von E-Mails bezahlt werden müssen. Der E-Mail-Dienst ist für die vernetzte Informations- und Wissensgesellschaft inzwischen eine nicht mehr wegzudenkende Anwendung.

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2022

N. Pohlmann, *Cyber-Sicherheit*, https://doi.org/10.1007/978-3-658-36243-0_13

13.2 Generelle Cyber-Sicherheitsprobleme des E-Mail-Dienstes

Der Basis-E-Mail-Dienst hat einige generelle Cyber-Sicherheitsprobleme, die bei der Nutzung grundsätzlich betrachtet werden müssen.

Weltweit kann jeder E-Mails versenden!
Für die erwünschten E-Mails ist das eine sehr gute Eigenschaft. Für die E-Mails, die nicht gewollt sind (E-Mails mit Werbung, politischen Inhalten, kriminellen Absichten, …), hat sich das Wort „Spam" etabliert. Es gibt aber auch E-Mails, die uns einen direkten Schaden zufügen sollen. Das sind E-Mails mit Malware (Viren, Würmen, Trojanern …) oder auch Phishing-E-Mails, mit denen Zugangsdaten „gefischt" werden sollen. Mit Phishing-E-Mails werden Nutzer motiviert, auf gefälschten Webseiten ihre persönlichen Daten einzugeben. Siehe auch Abschn. 1.10. Angriffsvektoren und Angriffsbeispiele.

Alle nicht erwünschten E-Mails stellen ein großes Problem für die E-Mail-Anwendung dar, insbesondere weil die eigene E-Mail-Infrastruktur das Senden nicht verhindert und der Sender nicht eindeutig verifiziert werden kann.

Laut einer Studie der ENISA ist der Spam-Anteil größer als 95 % in der E-Mail-Infrastruktur. Bei den Nutzern konnte zwar durch intelligente Spam-Filtermechanismen die Menge Spam-E-Mails in den E-Mail-Postfächern verringert werden, aber das Aufkommen ist immer noch hoch und produziert einen großen Schaden, weil 95 % der E-Mail-Infrastruktur für nicht gewollte E-Mails vorgehalten werden muss.

E-Mail-Anhänge werden dazu missbraucht, beim Empfänger Schadcode (Malware) auf das IT-System zu schleusen. Dies kann in Form einer Datei im E-Mail-Anhang geschehen, die der Nutzer erst selbst ausführen muss, damit der Schadcode ausgeführt wird. Oder der Dateianhang nutzt direkt eine Sicherheitslücke in dem verwendeten E-Mail-Programm, das die erhaltene E-Mail in einem bestimmten Format darstellt. Eine weitere Möglichkeit, Schadcode über E-Mails einzuschleusen, ist das Verlinken aus der E-Mail heraus auf eine kompromittierte Webseite. Solche E-Mails sind oftmals personalisiert und werden deshalb vom Nutzer als vertrauenswürdig eingestuft. Aber durch das Anklicken eines Links auf eine kompromittierte Webseite gelangt das Schadprogramm auf das eigene IT-System und wird infiziert. Aus diesem Grund müssen geeignete Anti-Malware-Systeme in die E-Mail-Infrastruktur eingebunden werden.

Eine E-Mail ist wie eine Postkarte!
Es wird vom E-Mail-Dienst keine Vertraulichkeit garantiert. Passwörter, Kreditkartennummern und weitere Bankdaten sowie vertrauliche Unternehmensinformationen, wie Kundendaten, Entwicklungsdaten, Kalkulationen, werden im Klartext übertragen und stellen so ein großes Risiko dar. Die Möglichkeiten, eine E-Mail im Internet oder in Bürogebäuden abzugreifen sind sehr hoch. In einigen Ländern werden alle E-Mails analysiert, um zum Beispiel an das Know-how von Firmen andere Länder zu kommen. Untersuchungen und Befragungen zeigen auf,

Blockchain-Technologie

14

Zusammenfassung

In diesem Kapitel werden die Grundzüge der Blockchain-Technologie, das Cyber-Sicherheitskonzept, die notwendigen Netzwerk-, Cyber-Sicherheits- und Vertrauenswürdigkeitsmechanismen sowie Beispielanwendungen der Blockchain-Technologie erläutert. Außerdem werden die Sicherheit und Vertrauenswürdigkeit der Blockchain-Technologie diskutiert.

14.1 Einleitung

Die Blockchain-Technologie ist eine spannende und faszinierende IT-Technologie, die das Potenzial hat, Politik, Verwaltung und Wirtschaftszweige zu revolutionieren. Sie ist eine Querschnittstechnologie mit hohem disruptivem Potenzial für viele Wirtschaftsbereiche und bietet kooperative Vertrauensdienste. Die blockchainbasierten Systeme könnten in vielen Bereichen zentrale Instanzen, wie Treuhänder, Banken oder Notare, ablösen. Das ist möglich, weil die verteilten Konsensfindungs- und Validierungsverfahren der Blockchain-Technologie ganz ohne Intermediäre die Vertrauenswürdigkeit der aufgezeichneten Transaktionsdaten garantieren. Sogenannte Smart Contracts machen eine vorprogrammierte, selbstausführende Vertragsabwicklung möglich. Mithilfe der Blockchain-Technologie wird eine Zusammenarbeit auf verschiedenen Ebenen effektiver, sicherer und vertrauenswürdiger umgesetzt.

14.2 Blockchain-Technologie auf den Punkt gebracht

In Abb. 14.1 und 14.2 werden eine herkömmliche zentrale Architektur und die dezentrale Blockchain-Architektur von Transaktionsspeichern aufgezeigt, um den Unterschied grob darzustellen.

Bei einem zentralen herkömmlichen Transaktionsspeicher werden die Zusammenarbeit oder das Eigentum von digitalen Werten durch eine zentrale Instanz

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2022

N. Pohlmann, *Cyber-Sicherheit*, https://doi.org/10.1007/978-3-658-36243-0_14

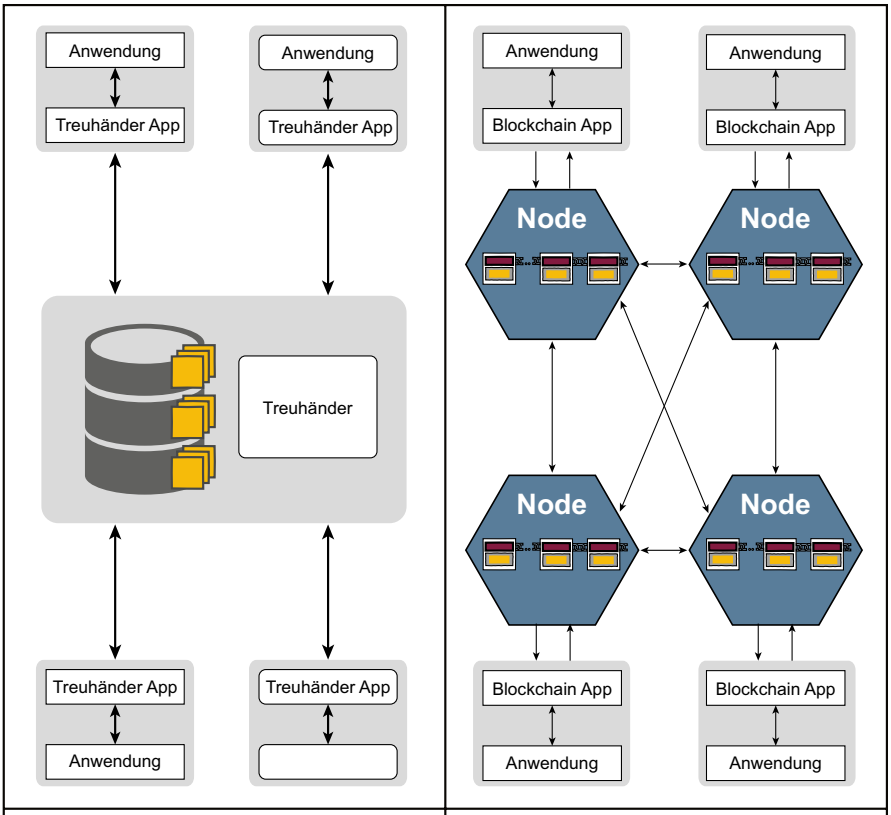


Abb. 14.1: Herkömmliche zentrale Architektur

Abb. 14.2: Dezentrale Blockchain-Architektur

oder einen Treuhänder verwaltet und verifiziert. Beispiel einer zentralen Instanz ist eine Public Key-Infrastruktur (PKI) und ein Treuhänder, zum Beispiel ein Notar, der die Abwicklung eines Vertrags kontrolliert und verwaltet, siehe Abb. 14.1.

In einem dezentralen Blockchain-Transaktionsspeicher werden die Zusammenarbeit oder das Eigentum von digitalen Werten durch verteilte und unabhängige Nodes eines Peer-to-Peer Netzwerks mithilfe von smarten Cyber-Sicherheits- und Vertrauenswürdigkeitsmechanismen verwaltet und verifiziert. Daher ist keine kostenaufwendige zentrale Instanz notwendig, siehe Abb. 14.2.

Unterschiedliche Sichtweisen auf die Blockchain-Technologie
Die verschiedenen Disziplinen können die Blockchain-Technologie aus sehr unterschiedlichen Blickwinkeln betrachten und bewerten.

Für einen **Informatiker** produziert die Blockchain-Technologie eine einfache Datenstruktur, die Blockchain, die Daten als Transaktionen in einzelnen Blöcken

verkettet und in einem verteilten Peer-to-Peer-Netz redundant verwaltet. Die Alternative wäre eine konventionelle Datenbank, die kontinuierlich von allen Teilnehmern repliziert wird.

Für die **Cyber-Sicherheitsexperten** hat die Blockchain-Technologie den Vorteil, dass die Daten als Transaktionen in den einzelnen Blöcken manipulationssicher gespeichert werden können, das heißt, die Teilnehmer der Blockchain sind in der Lage, die Echtheit, den Ursprung und die Unversehrtheit der gespeicherten Daten (Transaktionen) zu überprüfen. Die Alternative wäre hier zum Beispiel ein PKI-System als zentraler Vertrauensdienstanbieter.

Für den **Anwendungsdesigner** bedeutet die Nutzung der Blockchain-Technologie eine vertrauenswürdige Zusammenarbeit zwischen verschiedenen Organisationen, ohne die Einbindung einer zentralen Instanz, eines PKI-Systems, Notars usw. Die Alternative könnte hier ein kostenintensiver Treuhänder sein, der die Zusammenarbeit und Eigentumsübertragung zwischen den verschiedenen Organisationen verwaltet und verifiziert. Da die Blockchain-Technologie dies automatisiert macht, werden durch die vertrauenswürdige Zusammenarbeit die Prozesse auch sehr viel schneller und effektiver. Das macht einen Vertrauensdienst auf der Basis einer Blockchain-Technologie preisgünstiger und das Vertrauen verteilt sich auch die Node-Betreiber.

Die Blockchain-Technologie als Kollaborations-Tool

Grundsätzlich wird mit der Blockchain-Technologie eine Blockchain erzeugt, in der fälschungssichere, verteilte Datenstrukturen und in denen Transaktionen in der Zeitfolge protokolliert nachvollziehbar, unveränderlich und ohne zentrale Instanz abgebildet sind.

Die Cyber-Sicherheitseigenschaften einer Blockchain-Technologie werden prinzipiell mit den folgenden Cyber-Sicherheitsmechanismen umgesetzt:

- **„fälschungssicher/unveränderlich“** *mithilfe von One-Way-Hashfunktionen und digitalen Signaturen von Public Key-Verfahren*
- **„verteilte/redundante Datenstrukturen (Verfügbarkeit der Daten)“,** *viele Nodes des Peer-to-Peer-Netzwerks haben die Daten/Transaktionen in der Blockchain verteilt und redundant gespeichert*
- **„Transaktionen in der Zeitfolge protokolliert nachvollziehbar, unveränderlich“,** *wird zum Beispiel durch die Art der Verkettung mithilfe der Hashwerte „HashPrev“ und „Merkle Hash“ über die Daten in den Transaktionen sichergestellt*
- **„ohne zentrale Instanz abgebildet sind“,** *wird durch geeignete verteilte Vertrauenswürdigkeitsverfahren wie verteilte Konsensfindungsverfahren und verteilte Validierungsprozesse erzielt.*

Internet der Werte

Mit der Blockchain-Technologie werden neben der vertrauenswürdigen Zusammenarbeit auch Eigentumsverhältnisse (Digital Assets) direkter und effizienter als bislang gesichert und geregelt, da eine lückenlose und unveränderliche Datenauf-

Künstliche Intelligenz und Cyber-Sicherheit

15

Zusammenfassung

In diesem Kapitel wird behandelt, wie die Algorithmen aus Maschinellem Lernen und Künstlicher Intelligenz genutzt werden können, um die Cyber-Sicherheit zu verbessern. Weitere Themen sind die Qualität der Eingangsdaten, die Manipulation und IT-Sicherheit von KI-Systemen sowie Ethik und Künstliche Intelligenz.

15.1 Einleitung

Cyber-Sicherheitssysteme, die Künstliche Intelligenz (KI) berücksichtigen, werden in der Zukunft immer mehr helfen, deutlich besser die intelligenten Hacker und deren Angriffe zu entdecken, Schäden zu vermeiden und Risiken im gewünschten Digitalisierungsprozess zu minimieren. Mithilfe von Künstlicher Intelligenz kann die Erkennungsrate von Angriffen im Netzwerk und in ubiquitären IT-Endgeräten (Smartphone, Notebook, Server, IoT etc.) deutlich erhöht werden. Anders gesagt können die Erkennungsraten von IT-Systemen, die keine Form der Künstlichen Intelligenz verwenden, nicht dauerhaft auf dem gleichen Sicherheits- und Schutzniveau gehalten werden, wenn auch Angreifer heute schon Methoden der KI einsetzen, um IT-Systeme anzugreifen.

Somit hat Künstliche Intelligenz vermehrt Auswirkungen auf die Cyber-Sicherheitslage, die durch aktuelle Lagebilder aufzeigbar gemacht werden muss.

Eine große Herausforderung für die Verteidiger ist, für welche der vielen erkannten sicherheitsrelevanten Ereignisse zusätzliche, noch menschliche Analysten notwendig sind. Nicht alle Ereignisse können durch Spezialisten verarbeitet werden, da die Anzahl der Ereignisse die Verarbeitungsfähigkeit und Verarbeitungskapazitäten menschlicher Analysten an ihre Grenzen bringen. Diesen Umstand können Angreifer ausnutzen und die Verteidiger gezielt ablenken, um unbemerkt in das IT-System einzudringen. Künstliche Intelligenz kann dabei helfen, die Ereignisse in Echtzeit zu analysieren und situationsgerecht zu entscheiden, ob ein menschliches

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2022

N. Pohlmann, *Cyber-Sicherheit*, https://doi.org/10.1007/978-3-658-36243-0_15

Eingreifen überhaupt noch notwendig ist. In anderen Einsatzszenarien, bei denen eine Teilautonomie technisch nicht möglich ist und der Mensch zwingend eingebunden werden muss, kann der Einsatz von KI die Aufgaben und Tätigkeiten des Menschen wesentlich unterstützen und die Reaktionszeiten minimieren. Damit werden die vorhandenen Ressourcen gezielter eingesetzt und das Cyber-Sicherheitsniveau insgesamt erhöht. Situationsgerecht bedeutet dabei, dass klassische Verfahren auf Basis von Signaturen nur noch unterstützend eingesetzt werden und neuartige, verhaltensbasierte Verfahren, wie fortgeschrittene Anomalie-Erkennung oder Predictive Analysis, Einzug halten. Durch den Einsatz von KI können solche Verfahren möglich werden und einen deutlichen Fortschritt für die Cyber-Sicherheit bringen.

Weiterhin profitieren Identitäts- und Zugangsmanagementsysteme von der automatischen Auswertung der Bewegungsdaten von Nutzern, um nur berechtigten Nutzern den Zugriff zu IT-Systemen und Anwendungen zu geben. Die Sammlung, Verarbeitung und Speicherung von personenbezogenen Daten müssen jedoch im Einklang mit den datenschutzrechtlichen Bestimmungen (zum Beispiel DSGVO) stehen. Hierbei ist zu beachten, dass die Datenschutzkonformität eine Asymmetrie bei Angriffsszenarien zwischen Verteidiger und Angreifer darstellen kann.

Neuartige, passive Identifikations- und Authentifizierungsverfahren können einen Beitrag leisten und zu einer erhöhten Resilienz und Robustheit von IT-Systemen führen. Durch die fehlende aktive Nutzerinteraktion bei dieser Form der Identifizierung und Authentifizierung, beispielsweise durch die Auswertung von Sensordaten im Smartphone, können IT-Systeme sehr einfach sicherer gemacht werden. Aber auch im Bereich der risikobasierten und adaptiven Authentifizierung wird die KI helfen, angemessene Cyber-Sicherheit situationsbedingt umzusetzen und so die Schäden deutlich zu minimieren.

15.2 Einordnung der Künstlichen Intelligenz

Die Wissenschaft „Data Science“, ein Fachgebiet der Informatik, beschäftigt sich mit der Extraktion von Wissen aus den Informationen in Daten. Da es immer mehr Daten mit Informationen gibt, kann auch immer mehr Wissen aus den Informationen der Daten abgeleitet werden, insbesondere auch im Bereich der Cyber-Sicherheit, siehe Abb. 15.1.

Dabei setzt „Künstliche Intelligenz“ intelligentes Verhalten in Algorithmen um, mit der Zielsetzung, automatisiert „menschenähnliche Intelligenz“ so gut wie möglich nachzubilden.

Bei Künstlichen Intelligenzen kann zwischen schwacher und starker KI unterschieden werden. Eine starke KI soll eine Intelligenz schaffen, die dem Menschen gleichkommt oder sogar übertrifft. Singularität ist die Begrifflichkeit, bei dem das KI-System eine höhere künstliche Intelligenz besitzt als die menschliche Intelligenz. KI-Systeme können sich dann selbstständig verbessern und eigenständig sehr schnell Fortschritte erzielen, die für die Menschheit nicht mehr vorhersehbar sind.

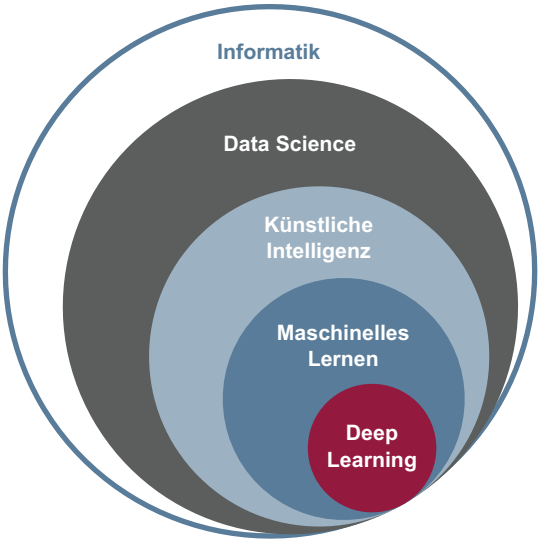


Abb. 15.1 Einordnung der Künstlichen Intelligenz

Wann und ob überhaupt eine Singularität erreicht werden kann, ist aus heutiger Sicht nicht absehbar und vielleicht auch gar nicht gewünscht. Eine schwache KI beschäftigt sich in der Regel mit konkreten Anwendungsproblemen des menschlichen Denkens. Maschinelles Lernen ist ein Teil der schwachen KI.

Maschinelles Lernen (Machine Learning/ML) ist ein Begriff im Bereich der Künstlichen Intelligenz für die „künstliche" Generierung von Wissen aus den Informationen in Daten mit der Hilfe von IT-Systemen. Mithilfe der Algorithmen des Maschinellen Lernens werden mit vorhandenen Datenbeständen Muster und Gesetzmäßigkeiten erkannt und verallgemeinert, um damit neue Problemlösungen umzusetzen. In Lernphasen lernen entsprechende ML-Algorithmen, aus vielen diversen Beispielen simple Muster und Strukturen, hin zu komplexen Merkmalen und Gesetzmäßigkeiten zu erkennen. Daraus entstehende Regeln können auf neue Daten und ähnliche Situationen angewendet werden, in denen die KI beispielsweise entscheiden muss, ob es sich um einen Angriff oder eine legitime Nutzeraktion handelt.

Maschinelles Lernen wird noch effektiver durch Deep Learning. Deep Learning ist eine Spezialisierung des Maschinellen Lernens und nutzt vorwiegend Künstliche Neuronale Netze (KNN).

15.3 Erfolgsfaktoren der Künstlichen Intelligenz

Die Erfolgsfaktoren der Künstlichen Intelligenz sind vielfältig. Die Entwicklung sowie die Zeit werden diesen Trend weiter fördern. Folgende Aspekte spielen eine Rolle:

Social Web Cyber-Sicherheit 16

Zusammenfassung

In diesem Kapitel werden einige Themen des Social Webs mit der besonderen Sichtweise auf die Cyber-Sicherheit dargestellt und diskutiert. Zu behandelnde Punkte sind: Fake-News, Social Bots, Filterblasen, Echokammern, Psychometrie sowie Cyber-Mobbing im Hinblick auf verschiedene Aspekte.

16.1 Einleitung

Soziale Netzwerke als Mitmach-Web, wie Facebook, Partnerbörsen, YouTube, Instagram, XING, LinkedIn, Twitter und Co. bringen Nutzer aus verschiedenen Gesellschaftsgruppen zusammen und ermöglichen ihnen, sich darzustellen, Informationen und Meinungen auszutauschen sowie sich einfacher und zielgerichteter real zu begegnen. Soziale Netzwerke schaffen auch neue Wege, Demokratie und Bürgerbeteiligungen zu gestalten [1].

Aber der Erfolg der sozialen Netzwerke hat auch bekannte Nachteile und Herausforderungen im Bereich der Cyber-Sicherheit. Social Bots, Fake-News, Psychometrie und Cyber-Mobbing können auch im Rahmen von Social Engineering-Angriffen verwendet werden.

Das typisch zugrunde liegende Geschäftsmodell bei sozialen Netzwerken, „Bezahlen mit persönlichen Daten“, ist für die informationelle Selbstbestimmung und den Datenschutz ein sehr großes Problem. Auch die Risiken des Verlusts der Privatheit und der Reputation der Nutzer werden immer größer mit der Bedeutung der sozialen Netze.

Die große Menge des „User generated contents“ der vielen Nutzer bei Mitmach-Web ist enorm, wird immer größer und macht zunehmend Probleme. „User-generated content“ ist der Inhalt, den die Nutzer selbst einstellen. Die Inhalte, die dabei Probleme machen, sind zum Beispiel rechtlich verboten, wie Kinderporno-

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2022

N. Pohlmann, *Cyber-Sicherheit*, https://doi.org/10.1007/978-3-658-36243-0_16

grafie, Hate Speech, aber auch Fake-News. Es geht aber auch um mit Rechten behaftete Objekte, wie Bilder, Musik, Filme usw.

Social Bots sind Meinungsroboter, die Stimmungsbilder und Reputationsverlust zum Beispiel von Politikern und Unternehmen zielgerichtet beeinflussen. Beispiele der Beeinflussung sind: Ukraine-Konflikt, BREXIT, US-Präsidentschaftswahlkampf, Islamfeindlichkeit, Fremdenhass schüren, Unternehmen diskriminieren und damit Kurse beeinflussen usw. In diesem Kapitel werden die Herausforderungen analysiert und potenzielle Auswege diskutiert.

Das Risiko persönlich beleidigt oder diskreditiert zu werden oder Information, die falsch sind, nicht erkennen zu können, wird immer größer. Aus diesem Grund spielt die Cyber-Sicherheit im Bereich des Social Webs eine immer wichtigere Rolle.

16.2 Soziale Netzwerke

Inhalte, die Nutzer in soziale Netzwerke einstellen, User-generated content genannt, sind in der Regel Texte, Bilder, Grafiken, Videos, Filme, Kommentare, Musik, Audiodateien, Quellcode usw., siehe Abb. 16.1.

Der Sinn und Zweck von sozialen Netzwerken ist in der Regel die Darstellung des Nutzers zur Generierung seines Images und der Austausch von Meinungen, Informationen und Erfahrungen. Die interaktive Zusammenarbeit vieler Nutzer und der Austausch von Informationen und Meinungen helfen, auf dem neuesten Stand zu bleiben, insbesondere in den Gruppen, für die sich die Nutzer am meisten inter-

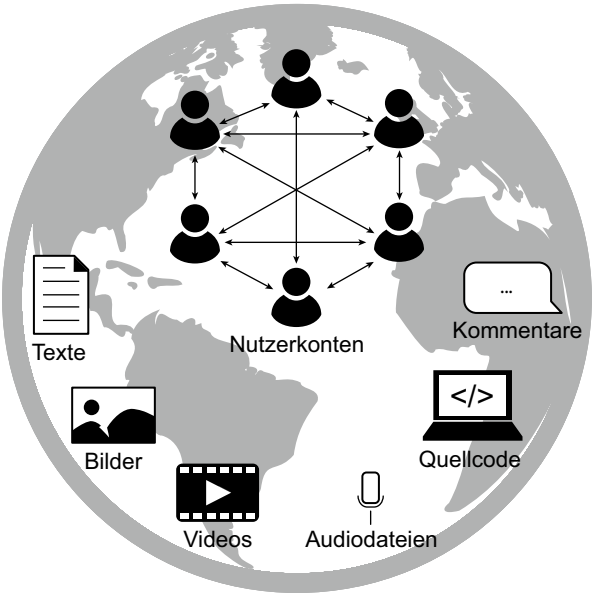


Abb. 16.1 Web 2.0-Anwendung – Soziales Netzwerk

Wirtschaftlichkeit von Cyber-Sicherheitsmaßnahmen

17

Zusammenfassung

Cyber-Sicherheitsmaßnahmen sind kein Selbstzweck. Mithilfe von Cyber-Sicherheitsmaßnahmen kann das Risiko bei der Nutzung von IT-Systemen erheblich reduziert und damit ein Schaden verhindert werden. In diesem Kapitel sollen die Kosten und der Nutzen der Cyber-Sicherheitsmaßnahmen diskutiert werden.

Da eine Cyber-Sicherheitsmaßnahme eine Investition für eine erfolgreiche Zukunft darstellt, sollten die Kosten-Nutzen-Aspekte schon bei der Planung von Cyber-Sicherheitsmaßnahmen besonders berücksichtigt werden [1].

17.1 Einführung

Die Aufgabe von IT-Systemen ist es, die Geschäftsprozesse in Unternehmen zu optimieren und dadurch Kosten zu reduzieren oder den Umsatz zu steigern, um letztlich mehr Profit zu erzielen. Die IT und die IT-Dienstleistungen dienen dem Zweck der Bestandssicherung und Gewinnmaximierung.

Dies kann zum Beispiel dadurch erreicht werden, dass Aufgaben vereinfacht oder beschleunigt werden, zum Beispiel durch die Nutzung der neuen Anwendungen wie sprachgesteuerte, intelligente persönliche Assistenten. Abläufe können mithilfe von IT-Systemen störungsfreier oder flexibler gestaltet werden. Die Digitalisierung stellt eine Vielzahl an innovativen Lösungen zur Verfügung.

Mitarbeiter können von Routineaufgaben entlastet und bei komplexen Aufgaben unterstützt werden.

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2022

N. Pohlmann, *Cyber-Sicherheit*, https://doi.org/10.1007/978-3-658-36243-0_17

Was für sämtliche Geschäftsbereiche eines Unternehmens gilt, gilt auch für den Einsatz von IT-Systemen: Sie müssen wirtschaftlich sein. Diese Wirtschaftlichkeit kann durch unterschiedliche Wirtschaftlichkeitsprinzipien erreicht werden:

Das **Minimierungsprinzip** hat den Schwerpunkt, bei einem gesetzten Ziel minimalen Aufwand zu betreiben. Wenn das Ziel ein bestimmter Gewinn ist, müssen bei gleichem Umsatz die Kosten gesenkt werden. Somit soll das Ziel Gewinn (Profit) durch den minimalen Mittelverbrauch (Kosten/Input) erreicht werden.

Das **Maximierungsprinzip** bedeutet, dass mit gegebenen Mitteln ein maximales Ziel erreicht werden soll. Der Gewinn ist dabei eine individuell wählbare Zielvorstellung und soll mit den gegebenen Mitteln maximiert werden. Die Mittel (Kosten/Input) sind also vorgegeben, der Umsatz (Output) ist jedoch ein Ziel, das bezüglich des Profits optimiert werden soll.

Das **generelle Extremumprinzip** ist so zu verstehen, dass Mitteleinsatz und Ergebnis so aufeinander abgestimmt sind, dass der durch sie definierte Prozess, gemessen an problemindividuellen Kriterien, optimal wird. Hierbei strebt keine Größe nach einem bestimmten Ergebnis oder Ziel, sondern Kosten und Umsatz stehen in einer variablen Wechselwirkung zueinander. Um den Prozess des Wirtschaftens zu optimieren, müssen Arbeitsschritte einer ständigen Qualitätskontrolle unterliegen.

Diese unterschiedlichen Wirtschaftlichkeitsprinzipien haben nichts mit Cyber-Sicherheit zu tun, sie stellen wirtschaftliche Ziele einer unternehmerischen Tätigkeit da. Dabei kann die Bewertung der Wirtschaftlichkeit nach den folgenden Aspekten durchgeführt werden:

Nach Kostenaspekten: Total Cost of Ownership
Total Cost of Ownership sind die Kosten für Anschaffung, Schulung, Installation, Betrieb, Wartung und Ersatz von IT-Systemen und Cyber-Sicherheitsmaßnahmen. Die Berechnung erfolgt durch die Kapitalwert-Methode, das heißt, was kostet ein Investment in der Summe aller Aspekte, die berücksichtigt werden müssen? Dieser Wert kann mit den Kosten verglichen werden, die zum Beispiel durch einen erfolgten oder geschätzten Schaden und dessen sofortige, mittelfristige und langfristige finanziellen Auswirkungen entstehen.

Nach Nutzenaspekten: ROI = Return on Investments
Hier wird der Nutzen den Kosten gegenübergestellt. Was nützt ein Investment bezüglich Kostenminimierung und/oder Umsatzsteigerung? Wann hat sich eine Investition amortisiert, das heißt, die Anschaffungskosten für eine Investition durch den mit der Investition erwirtschafteten Ertrag gedeckt? Je schneller eine Deckung erzielt wird, umso schneller kann ein Gewinn, zum Beispiel durch das Investment von Cyber-Sicherheitsmaßnahmen, generiert werden.

18 Self-Sovereign Identity (SSI)

Zusammenfassung

In diesem Kapitel werden die Architektur, die Akteure, die Sicherheitsinfrastruktur und -mechanismen sowie die Prinzipien von Self-Sovereign Identity (SSI) erläutert.

Self-Sovereign Identity (SSI) sorgt für eine sichere und vertrauenswürdige Digitalisierung. Nutzer können selbstbestimmt ihre digitale Identität und Nachweise wie Ausweis oder Bescheinigungen an Anwendungen weitergeben, die diese automatisiert auf Echtheit überprüfen können.

18.1 Self-Sovereign Identity (SSI) auf den Punkt gebracht

Derzeit dominieren im Cyber-Raum zentralisierte ID-Provider wie Google, Facebook und Apple die Verwaltung von Identitätsdaten bei sehr vielen IT-Diensten weltweit, siehe Abb. 18.1.

Eine digitale Identität ist eine Teilmenge von Attributen einer Person, mit der diese identifiziert werden kann. Dabei besitzt eine Person abhängig vom Kontext mehrere digitale Identitäten. Die Teilmenge von Attributen einer Person werden Identitätsdaten genannt. Bei ID-Providern wird zum Beispiele für die Identifikation und Authentifikation der Benutzername als Attribut der Identifizierung und das Passwort zur Verifizierung der digitalen Identität verwendet. Die weiteren Daten wie der vollständige Name, Adresse und Angaben zum Zahlungssystem sind weitere Identitätsdaten, die zur digitalen Identität gehören.

Diese Situation schafft eine große Abhängigkeit der Gesellschaft, Unternehmen und Nutzer in Bezug auf die Entwicklung der Digitalisierung. Außerdem nutzen die monopolistischen ID-Provider die sensiblen personenbezogenen Daten der Nutzer

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2022

N. Pohlmann, *Cyber-Sicherheit*, https://doi.org/10.1007/978-3-658-36243-0_18

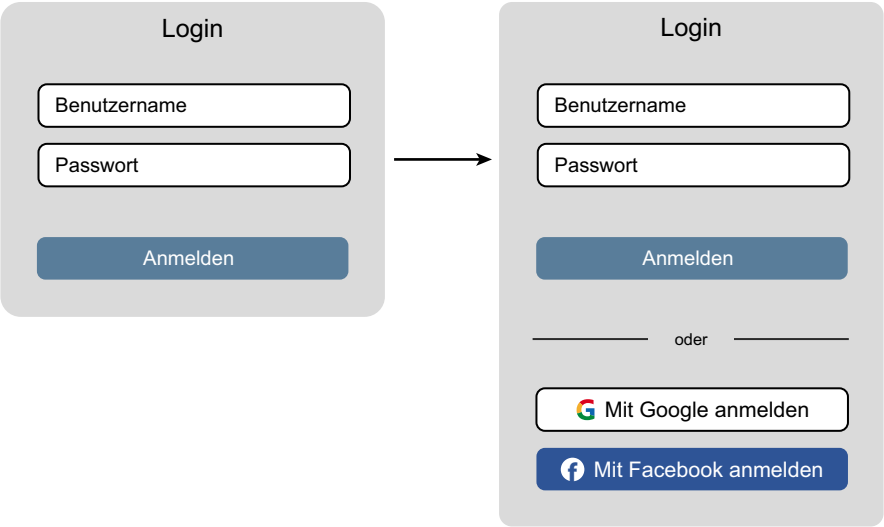


Abb. 18.1 Login ohne und mit monopolistischen ID-Provider

für eigene Werbezwecke oder andere ökonomische Interessen oder stellen diese weiteren Unternehmen zu Verfügung. Das schwächt die Privatsphäre der Nutzer und hat Folgen bezüglich der Akzeptanz unserer digitalen Zukunft [1].

Self-Sovereign Identity (SSI) wird helfen, da die Souveränität und der Schutz der Privatsphäre der Nutzer im Fokus des neuen Identitätsparadigmas „User-Centric-Identity“ stehen und deutlich besser und nutzerfreundlicher umgesetzt werden als bei der aktuellen „Enterprise-Centric-Identity“. Außerdem hat SSI das Potenzial, viele Prozesse und Abläufe einfacher, schneller, automatisiert, aber auch sicherer und vertrauenswürdiger umzusetzen, was in Hinblick auf die voranschreitende Digitalisierung nicht nur eine wirtschaftliche, sondern auch immer mehr eine gesellschaftliche und politische Relevanz hat. Insbesondere die Umsetzung einer sicheren, vertrauenswürdigen, interoperablen und souveränen digitalen Identität im Cyber-Raum ist bis heute eine der größten Herausforderungen der Digitalisierung.

Grundsätzlicher Aufbau und Ablauf des SSI-Ökosystem

Bei Self-Sovereign Identity (SSI) kontrollieren und besitzen Nutzer ihre digitalen Identitäten und weitere verifizierbare digitale Nachweise, ohne hierfür auf eine zentrale Stelle, wie etwa Google oder Facebook, angewiesen zu sein. Sie sind somit komplett unabhängig von Dritt-Instanzen und entscheiden vollkommen eigenständig, wer welche Identitätsdaten zur Verfügung gestellt bekommt, da alle Identitätsdaten ausschließlich bei ihnen in der SSI-Wallet sicher gespeichert werden.

Mit SSI ist ein einfacher, flexibler, sicherer und vertrauenswürdiger Austausch von manipulationssicheren digitalen Nachweisen zwischen Nutzer und Anwendungen möglich.

Im SSI-Ökosystem für digitale Identitäten spielen drei Akteure eine wesentliche Rolle, die gemeinsam mit der SSI-Blockchain-Infrastruktur interagieren (Prinzip:

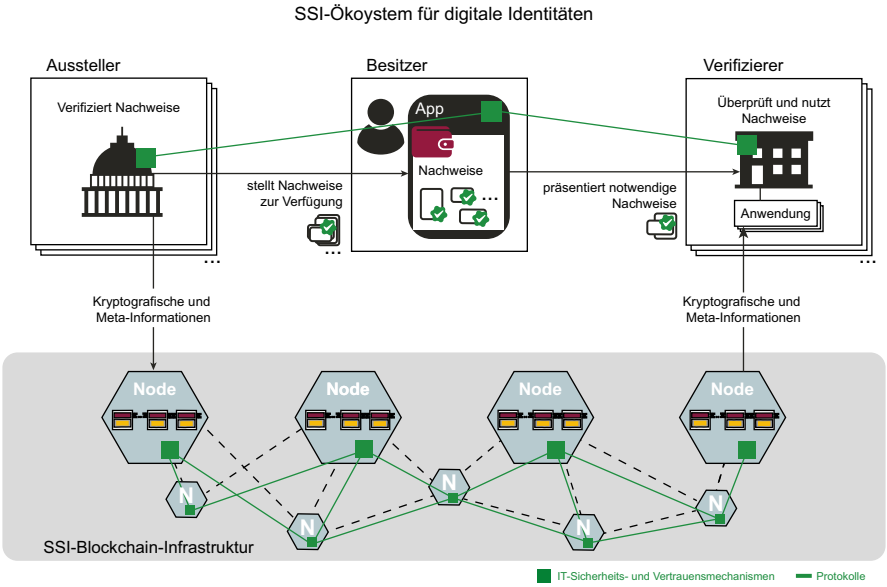


Abb. 18.2 SSI-Ökosystem für digitale Identitäten und Nachweise

Trust Triangle-Modell), siehe Abb. 18.2. Jeder dieser Akteure hat eine definierte Aufgabe, damit das SSI-Ökosystem erfolgreich umgesetzt werden kann.

Aussteller (Issuer) von digitalen Nachweisen
Im SSI-Ökosystem existieren Aussteller, die verifizierbare digitale Nachweise – eine Sammlung von sogenannten Verifiable Credentials – wie **Bescheinigungen** der Identität, **Bestätigungen, Befähigung**, **Befugnisse, Qualifikationen** oder Mitgliedsausweise ausstellen.

Aussteller sind Unternehmen oder Organisationen, die berechtigt oder in der Lage sind digitale Nachweise auszustellen, wie z. B. Einwohnermeldeämter, Straßenverkehrsämter, Schulen und Hochschulen, Berufsverbände, Behörden oder Qualifizierungs- und Prüforganisationen.

Verifizierer (Akzeptanzstelle, Anwendungen), die digitale Nachweise für ihre Prozesse nutzen
Die Akzeptanzstellen – Anwendungen – in diesem SSI-Ökosystem benötigen verifizierbare digitale Nachweise, um deren Inhalte, Teile davon oder auch nur Aussagen über bestimmte Attribute in einem Prozess oder einer Anwendung (Off- oder Online) zu nutzen und weiter zu verarbeiten.

Dies geschieht im Idealfall vollkommen automatisiert in einem digitalisierten Prozess und, durch die Verifizierung der digitalen Signatur, besonders sicher und eindeutig. Bei physischen Nachweisen muss durch den Faktor Mensch eine Fehlertoleranz bei der Verifikation einkalkuliert werden, da z. B. ungeschultes Personal

Vertrauen und Vertrauenswürdigkeit 19

Zusammenfassung

Die Vertrauenswürdigkeit von IT-Lösungen und Hersteller-/Anbieterunternehmen ist die Basis für das Vertrauen der Nutzer und damit ausschlaggebend für deren Akzeptanz der digitalen Zukunft.

Aus diesem Grund werden in diesem Kapitel die Begriffe Vertrauen und Vertrauenswürdigkeit sowie Mechanismen zur Vertrauensbildung und Vertrauenswürdigkeitstechnologie beschrieben und diskutiert.

19.1 Zusammenhang zwischen Vertrauen, Vertrauenswürdigkeit und Cyber-Sicherheit

Das Vertrauen von Nutzern wird zu einem großen Maß über die Vertrauenswürdigkeit von IT-Lösungen und Hersteller-/Anbieterunternehmen aufgebaut. Dabei sind die Umsetzung und Darstellung von Cyber-Sicherheit ein wichtiger Bestandteil der Vertrauenswürdigkeit. Siehe Abb. 19.1.

In Zukunft werden zunehmend mehr und vor allem auch neue Werte geschaffen, die (nur) digital vorhanden sind, und in der Konsequenz sowohl einen weitaus höheren als auch individuelleren Schutzbedarf aufzeigen. Dieses Schutzniveau zu erreichen ist aufwendiger als es je in der analogen Welt der Fall war – denn auf abgeschlossenen Unternehmensarealen ist es eher möglich Unternehmenswerte gut zu überwachen beziehungsweise sicher in Tresoren aufzubewahren und somit, auch für die Unternehmensleitung gut nachvollziehbar, zu schützen.

Im Gegensatz dazu unterliegt in der digitalen Welt der Schutz nicht mehr unmittelbar der Kontrolle der Anwendungsunternehmen. Nicht nur, dass sie die Absicherung ihrer digitalen Werte keinesfalls mehr physisch nachprüfen können – sie müssen gleichzeitig auch darauf vertrauen, dass die Hersteller bei Entwicklung, Auswahl und Umsetzung von Cyber-Sicherheitsmaßnahmen wie etwa Verschlüsselung, Multifaktor-Authentifikation oder Isolierung von Anwendungen alles tun, um die

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2022

N. Pohlmann, *Cyber-Sicherheit*, https://doi.org/10.1007/978-3-658-36243-0_19

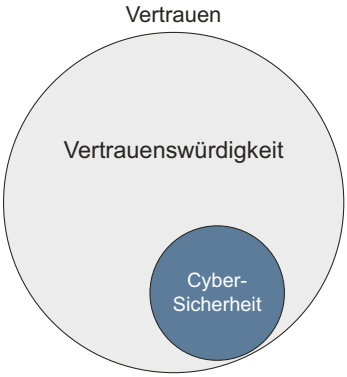


Abb. 19.1 Zusammenhang zwischen Vertrauen, Vertrauenswürdigkeit und Cyber-Sicherheit

richtige Vorgehensweise zu gewährleisten. Im Hinblick auf die Zukunftsfähigkeit von Anbieterunternehmen ist es wichtig zu sehen, dass dieser Aspekt – allein aufgrund der zunehmenden Vulnerabilität in der Digitalität durch immer versiertere Angriffe – mehrere Ebenen tangiert. Die Forderung nach einem gewissenhaften Umgang mit der Cyber-Sicherheit bezieht sich zum einen auf die Verantwortung der Hersteller dahingehend alle Maßnahmen zu ergreifen, um ihr eigenes Unternehmen vor Angriffen zu schützen. Zum anderen jedoch gleichzeitig, ihre IT-Lösungen gemäß Stand der Technik zu entwickeln, um so die bestmögliche Technologie zur Verfügung stellen zu können.

Hieran zeigt sich zum einen die Relevanz von Vertrauen beim Einsatz von IT-Lösungen seitens der Nutzer und unterstreicht gleichzeitig die Notwendigkeit, dass Unternehmen vertrauenswürdig agieren müssen, damit dieses Vertrauen auch gerechtfertigt ist.

In den folgenden Unterkapiteln werden ein Modell sowie Aspekte, Mechanismen und Technologien zur Schaffung von Vertrauenswürdigkeit und zum Aufbau von Vertrauen dargestellt sowie diskutiert.

19.2 Vertrauen

Durch die immer schnellere und komplexere Digitalisierung werden innovative IT-Lösungen aus Sicht des Nutzers zunehmend weniger berechenbar – sie sind nicht mehr in der Lage, die Technologie zu durchdringen. Dass dies mit Folgen verbunden ist zeigt sich auch an den Ergebnissen des Online-Vertrauens-Kompass des „Bundesverband Digitaler Wirtschaft“ in der 46 Prozent der Befragten angeben „Die schnelle Veränderung unserer Lebensbedingungen durch zunehmende Technisierung und Vernetzung macht mir Angst“ [3].

Um hier ihre Vertrauenswürdigkeit glaubhaft zu demonstrieren und damit das Vertrauen sowie die Akzeptanz in ihr Unternehmen sowie ihre Cyber-Sicherheitslösungen oder IT-Lösungen mit Cyber-Sicherheitsmechanismen zu manifestieren, sind zusätzlich weitere Aspekte zwingend notwendig.

Im Hinblick auf Unternehmen bedeutet dies, neben der Cyber-Sicherheit auch in die Aspekte Zutrauen, Zuverlässigkeit, Integrität und Sicherheit zu investieren und alles zu tun, um diese Aspekte so weit wie möglich für die Nutzer transparent zu machen. Also eine reale Überprüfbarkeit dahingehend zu bieten, dass es möglich ist sich auf ein Unternehmen und/oder auf eine IT-Lösung zu verlassen. In Bezug auf IT-Lösungen lässt sich in dem Kontext unter anderem ableiten, dass diese allgemein vertrauenswürdig sind, wenn sie sich immer in der erwarteten Weise für den beabsichtigten Zweck verhalten.

▶ Die Vertrauenswürdigkeit der Unternehmen spielt somit eine besondere Rolle, weil Nutzer zunehmend IT-Lösungen nur noch akzeptieren werden, wenn sie diesen beziehungsweise dem Hersteller/Anbieter vertrauen können.

19.3 Vertrauenswürdigkeitsmodell

Mit der Digitalisierung zeigt sich, dass eine starke Abhängigkeit zwischen Herstellern, Diensteanbietern und Nutzer entstanden ist. In dieser Wechselbeziehung kann letztendlich auch die Akzeptanz der IT-Technologie und einzelner IT-Lösungen sowohl positiv als auch negativ beeinflusst werden [5].

Dabei greifen folgende Mechanismen: Einerseits, dass die Nutzer deutlich mehr prinzipielle Möglichkeiten zur Kontrolle der Handlungsweise und Leistung von Herstellern haben. Denn über die sozialen Medien können die Nutzer unmittelbar kundtun, wenn ihnen etwas missfällt oder bestimmte Aktivitäten der Hersteller beurteilen. Das heißt, den Nutzern steht ein Mittel der direkten Einflussnahme zur Verfügung.

Andererseits haben die Nutzer – aufgrund der gestiegenen Komplexität – zunehmend weniger Möglichkeiten die IT-Lösungen zu durchdringen, was teilweise ihre Urteilsfähigkeit einschränkt und ihre Entscheidungsmacht verringert. Dadurch wird ihnen bei deren Einsatz eine höhere Vertrauensbereitschaft abverlangt. Dieser grundlegende, und für den Erfolg von IT-Lösungen und Unternehmen relevante Faktor muss aufgrund eines weiteren Parameters noch differenzierter betrachtet werden: Denn es gilt auch zu berücksichtigen, dass die Interessen der beteiligten Parteien teilweise diametral sind: Etwa dann, wenn der Hersteller möglichst viele Kundendaten mit seiner IT-Lösung generieren sowie für jegliche Zwecke verwenden möchte und dies weder im Sinne des Nutzers ist noch seinen Wünschen entspricht. Ob und in welchem Maße sich dieser Zielkonflikt auf die Vertrauensfähigkeit beziehungsweise -bereitschaft auswirkt, lässt sich nicht pauschal beantworten, da diese Eigenschaft individuell unterschiedlich ausgeprägt ist. Dabei spielen verschiedene weitere Faktoren eine Rolle. Zum Beispiel, ob der Nutzer mit der Nutzung des Dienstes aus seiner Sicht ein hohes Risiko eingeht – aber ebenso, welche Intention er dabei verfolgt und ob für ihn die eigentliche Zweckerfüllung an erster Stelle steht [1, 2, 4].

Weitere Aspekte der Cyber-Sicherheit 20

Zusammenfassung

In diesem Kapitel werden verschiedene Aspekte der Cyber-Sicherheit behandelt.

Themen sind DNS over HTTPS (DoH), Backup, Chancen und Risiken von Smart Home, Risiken und Sicherheit eines Homeoffice sowie Upload-Filter.

20.1 DNS over HTTPS (DoH)

Die Idee von DNS over HTTPS (DoH) ist, dass sich die Manipulation von DNS-Anfragen für missbräuchliche Zwecke verhindern lässt [1].

DNS-Anfragen an den DNS-Server, die von Browsern, E-Mail-Komponenten, SIP-Client usw. erfolgen, werden in der Regel unverschlüsselt in der Kommunikationsinfrastruktur durchgeführt.

Das damit einhergehende Sicherheitsrisiko bezüglich Privatheit und IT-Sicherheit könnte mit dem DoH-Protokoll insbesondere bei der Nutzung von öffentlichen Netzen verringert werden, weil die DNS-Anfrage aus der Anwendung zu einem DoH-Dienst eingeht, bei dem die Kommunikation verschlüsselt und integritätsgesichert über HTTPS realisiert ist und damit einige Angriffe nicht mehr umgesetzt werden können. Auch die Gefahr einer Manipulation von DNS-Anfragen mithilfe eines Man-in-the-Middle (MITM) Angriffs in nicht vertrauenswürdigen Netzwerkumgebungen könnte deutlich reduziert werden.

Traditionelles Domain Name System (DNS)

Das Domain Name System (DNS) wird hauptsächlich benutzt, um Domänen-Namen auf IP-Adressen abzubilden. Bei der Nutzung eines traditionellen Domain Name Systems (DNS) wird in einem ersten Schritt das Betriebssystem des suchenden IT-Systems (Notebook, Smartphone usw.) durch die Anwendung, z. B. den Browser initiiert, gefragt, welcher DNS-Resolver – der typischerweise im Heim-

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2022

N. Pohlmann, *Cyber-Sicherheit*, https://doi.org/10.1007/978-3-658-36243-0_20

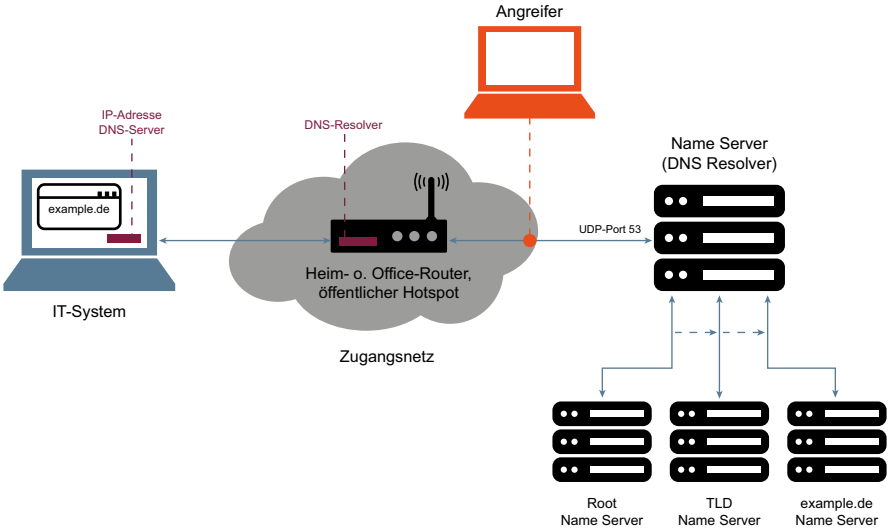


Abb. 20.1 Traditionelles Domain Name System (DNS)

oder Office-Router oder in einem öffentlichen Hotspot integriert ist – verwendet werden soll.

Dieser DNS-Resolver ist dafür verantwortlich, die IP-Adresse zu finden, die passend zum Domänen-Namen ist, den ein Nutzer in seinem IT-System (Notebook, Smartphone, …) im Browser eingegeben hat. Falls der DNS-Resolver im Router diese Information noch von einem früheren Besuch gespeichert hat, kann er diese sofort zurückgeben.

Ist dies nicht der Fall, leitet der DNS-Resolver im Router die Anfrage an den DNS-Resolver (Name Server) des ISPs oder des Unternehmens weiter. Wenn dieser die Anfrage erhält, wird überprüft, ob die passende IP-Adresse zum Domänen-Namen in seinen Cache gespeichert ist. Falls ja, sendet er das Ergebnis sofort zurück und falls nicht, startet er eine rekursive Auflösung. Der DNS-Resolver (Name-Server) hat dann die Aufgabe, solange nach einem passenden Name-Server für die entsprechende Domäne zu suchen, bis er die Anfrage beantworten kann.

Im Fall der traditionellen DNS-Anfrage kann ein Angreifer prinzipiell die DNS-Kommunikation im Klartext mitlesen und manipulieren, siehe Abb. 20.1.

DNS über HTTPS

Das DoH-Protokoll ändert im Prinzip nur den Kommunikationsweg zum DNS-Resolver (Name Server). Statt das unverschlüsselte DNS-Protokoll zum UDP-Port 53 zu verwenden, wird die DNS-Anfrage jetzt über TLS verschlüsselt und integritätsgesichert Kommunikation (HTTPS) zu einem Web-Server (DoH-Server) zum TCP-Port 443 gesendet. Die Anwendung, zum Beispiel der Browser, E-Mail- oder SIP-Client kann dann – unabhängig von der im Betriebssystem beschriebenen und

Glossar

21

Zusammenfassung

In diesem Kapitel werden wichtige Begriffe der Cyber-Sicherheit aufgelistet und erläutert, die im Buch verwendet werden.

Angriffsfläche
Die (Cyber-)Angriffsfläche beschreibt die Gesamtheit der vorhandenen Schwachstellen und Angriffsvektoren, die ein Angreifer für einen erfolgreichen Angriff ausnutzen kann. Die Angriffsfläche bezieht sich auf das Netzwerk, die IT-Systeme mit den verschiedenen Betriebssystemen, Anwendungen und Daten sowie die Anwender, die diese nutzen, in einer festgelegten Einheit, wie einer Organisation oder einem Unternehmen. Das gilt für die eigenen IT-Infrastrukturen, aber auch für alle Cloud-Dienste, die genutzt werden.

Die Angriffsfläche ist bestimmt durch die Anzahl der genutzten IT-Systeme und -Dienste und die vorhandenen Cyber-Sicherheitsmaßnahmen, aber auch durch die Innovationen der Angreifer, die immer neue Angriffsvektoren innovieren und nutzen.

Je größer sie ist, desto höher ist die Wahrscheinlichkeit eines erfolgreichen Angriffs.

Asymmetrie zwischen Angreifer und Verteidiger
Ein Angreifer braucht in der Regel nur einen Angriffsvektor abgestimmt auf eine bestehende Schwachstelle, um erfolgreich seine Ziele umsetzen zu können. Demgemäß muss sich jede Organisation entsprechend verteidigen und dafür sorgen, dass alle Schwachstellen geschlossen sind, damit kein Angriffsvektor umgesetzt werden kann. Da die meisten Schwachstellen bei allen Organisationen/Unternehmen gleich sind, sollten diese enger kooperieren, um sich gemeinsam effektiver gegen Angriffe schützen zu können.

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2022

N. Pohlmann, *Cyber-Sicherheit*, https://doi.org/10.1007/978-3-658-36243-0_21