STUDIENSKRIPT



## Netzwerksicherheit

DLMCSEESN01\_E



Übergeordnete Lernziele

##### Einführung 9



Die Informationstechnologie (IT) ist in vielen realen Umfeldern und unterschiedlichen Wirtschaftszweigen von entscheidender Bedeutung. Hierzu gehören unter anderem Bereiche wie die Gesundheit, Mobilität, Unterhaltung, Fertigung, Logistik und Finanzen. So ist eine sichere IT-Infrastruktur für Innovationen unerlässlich. Die IT-Sicherheit verhindert Wirtschaftsspionage, wirtschaftliche Schäden durch Hackerangriffe und körperliche Schäden durch manipulierte oder unzuverlässige eingebettete Systeme.

Bei der Entwicklung und Implementierung von IT-Systemen spielen fundierte Kenntnisse über den Schutz und die Zuverlässigkeit von Netzwerkinfrastrukturen eine entscheidende Rolle. Der Kurs Netzwerksicherheit vermittelt den nötigen Hintergrund zum Verständnis sicherer Netzwerktechnik. Er führt zudem in die Grundlagen der Computernetzwerke ein und setzt dabei die folgenden Schwerpunkte: Die Internetprotokollfamilie (TCP/IP), die Sicherung der Netzwerkinfrastruktur, das Verständnis von Netzwerksicherheitsproblemen und ‑bedrohungen, die Überprüfung auf Schwachstellen in der Netzwerksicherheit sowie die Vorstellung verschiedener Sicherheitsmechanismen zur Entschärfung von Angriffen und Identifikation von Schwachstellen. Die Kenntnis dieser Mechanismen ist für den Entwurf und die Implementierung von Netzwerksicherheitsstrategien unerlässlich.

Nach Abschluss dieses Kurses verstehen Sie, wie verschiedene Systeme in einer vernetzten Umgebung abgesichert werden, wie Systemsicherheit bewertet und Sicherheitsanforderungen und Abwehrmaßnahmen ermittelt werden. Der Kurs vermittelt ein Verständnis dafür, wie Geräte der Infrastruktur und die Kommunikation zwischen Computersystemen gesichert werden können. Darüber hinaus werden Sie mit einer Reihe von Strategien vertraut gemacht, darunter kryptografische Techniken, Cloud-Sicherheit sowie Mechanismen zur Erkennung von Angriffen und wie man diese verhindern kann.



# Lektion 1

## Netzwerksicherheit im Überblick

#### LERNZIELE

Nach Abschluss dieser Lektion werden Sie in der Lage sein, …

… die Grundlagen von Computernetzwerken zu verstehen, insbesondere die Internet-Protokollfamilie (TCP/IP).

… die Konzepte der passiven und aktiven Erfassung des Netzwerkverkehrs zu identifizieren.

… übliche Schwachstellen in der Netzwerksicherheit zu erkennen.

… Informationen zu den technischen Aspekten der Sicherung von Netzwerkprotokollen anzuwenden.

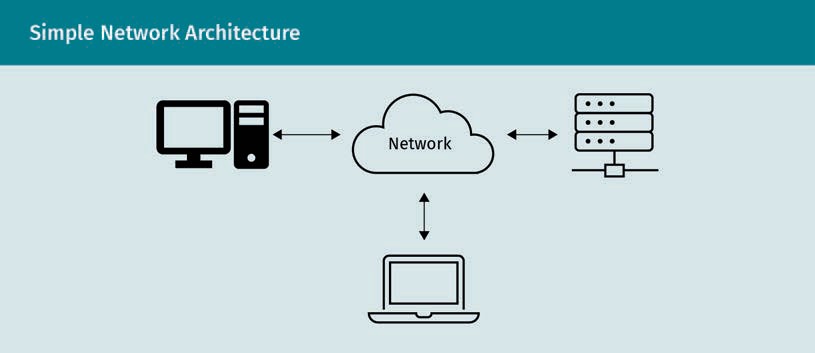
DL-E-DLMCSEESN01\_E-U01

1. Netzwerksicherheit im Überblick

### Einführung

Ein Netzwerk ist eine Gruppe von Geräten (Computern), die miteinander verbunden sind und Informationen austauschen. Jedes angeschlossene Gerät wird als Knoten im Netzwerk bezeichnet, was die Bezeichnung auf eine breite Palette unterschiedlicher Geräte verallgemeinert. Die folgende Abbildung zeigt ein Beispiel für ein einfaches Netzwerk mit drei Knoten, die an ein gemeinsames Netzwerk angeschlossen sind. Jeder Knoten kann mit unterschiedlicher Software oder Hardware ausgestattet sein. Daher muss jeder Knoten eine Reihe von Regeln befolgen, um mit den anderen Knoten im Netzwerk zu kommunizieren.

Die Kanten (Linien) zwischen den Knoten modellieren die Verbindungen zwischen den kommunizierenden Geräten. Das Netzwerk umfasst zwei verschiedene Arten von Topologien, eine physische und eine logische. Die physische Topologie beschreibt, wie die verschiedenen Komponenten im Netzwerk platziert sind (z. B. die Position der Geräte und die Verlegung der Kabel). Die logische Topologie hingegen gibt an, wie die Daten im Netzwerk fließen.



### Grundlegende Protokollschichtung

Bevor die Definition eines Netzwerkprotokolls erläutert wird, soll die Kommunikation zwischen zwei Parteien anhand eines Beispiels gezeigt werden. Stellen Sie sich zwei Professoren vor, von denen einer Englisch und der andere Chinesisch und Französisch spricht, wie in der nachstehenden Abbildung dargestellt (Tanenbaum & Wetherall, 2010). Da sie keine gemeinsame Sprache sprechen, nehmen sie einen Übersetzer hinzu, der wiederum eine Sekretärin bittet, die übersetzte Nachricht zu versenden. Der Professor gibt also eine Nachricht (auf Englisch) an seinen Übersetzer weiter, in der es heißt: „The deadline is on 1/5/2021“. Die Übersetzer haben sich darauf geeinigt, eine neutrale Sprache zu verwenden, die beide kennen, nämlich Deutsch. Die Meldung wird also in *„Einsendeschluss ist am 1.5.2021“* umgewandelt. Anschließend gibt der Übersetzer die Nachricht an die Sekretärin zur Übermittlung per E-Mail weiter. Nachdem die Nachricht bei der anderen Sekretärin angekommen ist, gibt diese sie an den Übersetzer vor Ort weiter. Dieser übersetzt sie ins Französische und leitet sie an den zweiten Professor weiter.

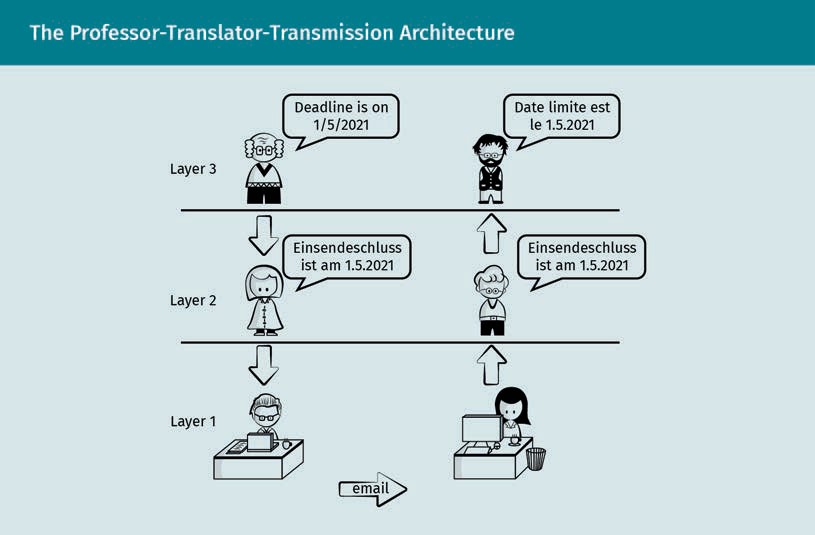
Anhand dieses Beispiels lassen sich die folgenden Begriffe einfach definieren. Wenn das Modell als Stapel übereinander liegender Schichten oder Ebenen organisiert wird, lässt sich die Komplexität des Professor-Beispiels verringern. Jede Schicht baut auf der darunter liegenden auf. Die Professoren befinden sich beispielsweise auf Ebene (Schicht) drei, und beide kontaktieren ihre Übersetzer auf der darunter liegenden Ebene (Ebene bzw. Schicht zwei). Die Übersetzer kommunizieren dann mit den Sekretärinnen in der ersten Ebene (Schicht). Die Parteien jeweils einer Schicht werden Peers *(deutsch Gleichgestellte, Ebenbürtige)* genannt. Die Peers können in Form von Geräten (Hardware), Menschen oder Software-Prozessen auftreten.

Die Peers verwenden **Protokolle**, um miteinander zu kommunizieren. So haben sich die beiden Übersetzer beispielsweise auf die Nutzung des Deutschen geeinigt. Mit anderen Worten: Sie haben sich für eine Kommunikationssprache entschieden. Außerdem haben sich die beiden Sekretärinnen für die Übermittlung per E-Mail entschieden. Manchmal kann ein Protokoll auf einer bestimmten Schicht geändert werden, ohne dass dies die angrenzenden oder benachbarten Schichten beeinträchtigt. So bemerken weder die darüber noch die darunter liegenden Schichten etwas davon. Im besagten Beispiel könnten die Sekretärinnen ihre Kommunikation von E-Mail auf Fax umstellen, ohne die anderen Ebenen (Schichten) zu informieren. Schließlich findet zwischen zwei benachbarten Schichten ein Austausch statt. Mit anderen Worten: Es gibt eine Schnittstelle zwischen jeweils zwei Ebenen (Schichten). Die Schnittstelle definiert die Dienste und Vorgänge (Operationen), welche die untere Schicht an die obere liefert. In Wirklichkeit werden keinerlei Daten direkt von Professor eins auf Professor zwei übermittelt. Stattdessen leitet jede Schicht Daten nach unten weiter, bis die unterste Schicht (d. h. die Sekretärin) erreicht ist. Hier findet die eigentliche Kommunikation statt, wie in der nachfolgenden Abbildung dargestellt.

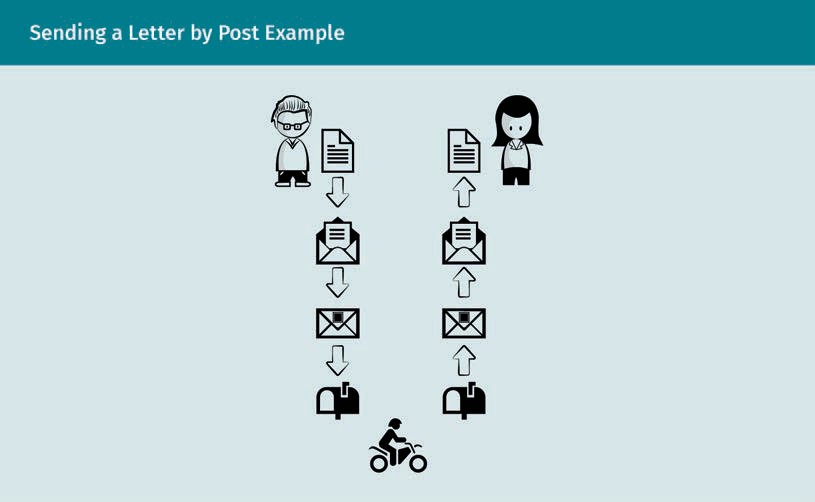
Der Inhalt der einzelnen Schichten und die Anzahl der Schichten können von einem Netzwerk zum anderen variieren. Die Aufgabe jeder Schicht ist es, den höheren Schichten spezifische Dienste anzubieten. Zugleich bleiben die Einzelheiten der Implementierung der angebotenen Dienste vor der höheren Schicht verborgen (Abstraktion). Abstraktion bedeutet also, dass eine Software (oder Hardware) den erforderlichen Dienst bereitstellt, ohne deren Details wie Algorithmen oder interne Architektur offenzulegen (Tanenbaum & Wetherall, 2010).

**Protokoll**

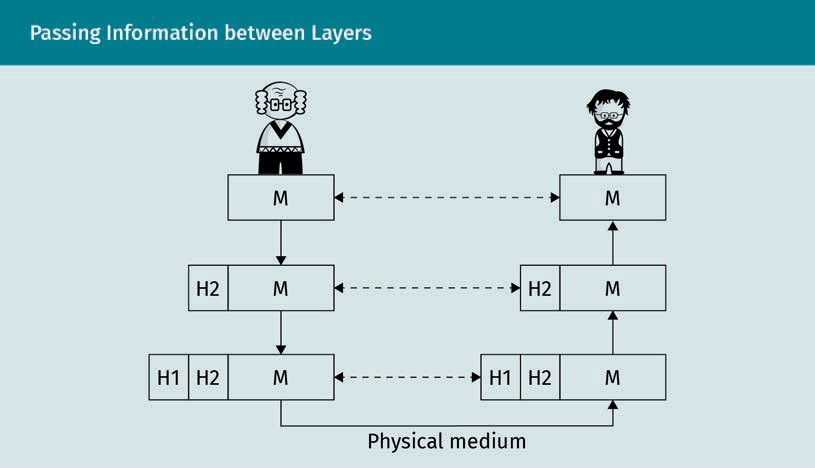
Eine Vereinbarung zwischen den Parteien darüber, wie die Kommunikation ablaufen soll.



Nach der Festlegung grundlegender Begriffe (Terminologie) soll noch ein weiteres Beispiel betrachtet werden: der Versand eines Briefes per Post, wie in der folgenden Abbildung dargestellt. Der Absender muss den Brief schreiben, ihn in einen Umschlag stecken und schließlich den Namen und die Adresse des Empfängers darauf notieren, bevor er den Umschlag in die Post gibt. Der Name und die Adresse werden als „Header“ (englisch für Kopfzeile oder Vorspann) bezeichnet. Am anderen Ende erhält der Empfänger später die Post, öffnet den Umschlag und liest den Brief. So können in jedem Schritt (bzw. auf jeder Schicht) bestimmte Informationen (jeweils „Header“ genannt) hinzugefügt werden, bevor die Nachricht an die nächste Schicht weitergegeben wird. Diese Header sind nur für die Peer-Schicht auf der Empfängerseite bestimmt. Einerseits interessiert sich der Postbote nicht für die Daten im Umschlag, sondern nur für die Adresse. Andererseits interessiert sich der Empfänger nur für den Brief und seinen Inhalt, nicht aber für den Umschlag. Die Akteure jeder Schicht fügen dem Brief also jeweils einen Header hinzu, wie zum Beispiel Versiegeln des Briefs, Aufschrift der Adresse usw. Die jeweils entsprechende Schicht auf der Empfängerseite entfernt diesen Header (Kopfzeile) des Briefes und kommt so zur eigentlichen Information dieser Schicht.



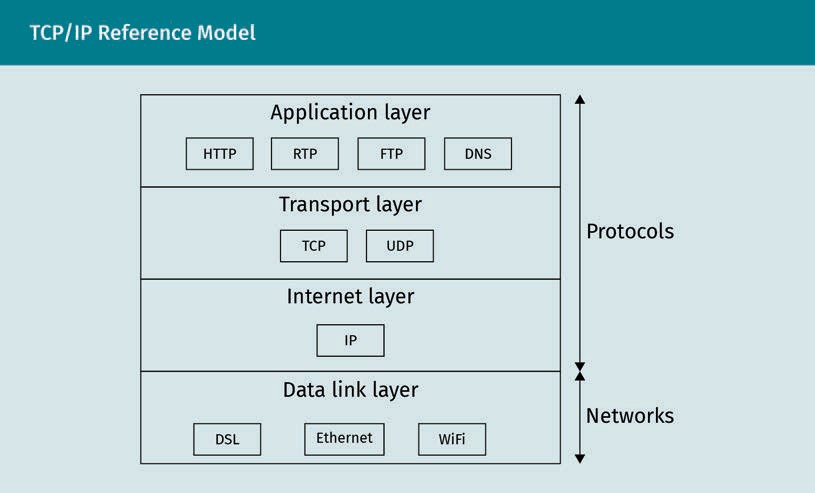
Nun soll ein eher technisches Beispiel mit einem dreischichtigen Netzwerk betrachtet werden. Angenommen, jede Schicht kommuniziert virtuell mit der entsprechenden Schicht, wie durch die gestrichelten Linien in der folgenden Abbildung gezeigt (d. h. Professor eins mit Professor zwei). In Wirklichkeit leitet jedoch jede Schicht Steuerungs- und Inhaltsdaten direkt an die darunter liegende weiter, bis die unterste Schicht (Schicht eins) erreicht ist. Schicht eins beschreibt das physische Medium, über das die eigentliche Kommunikation erfolgt, wie in der Abbildung mit durchgezogenen Linien dargestellt. Eine Nachricht M wird von einem Prozess in der dritten Schicht erstellt und zur Übertragung an die zweite Schicht gesendet. Ein Prozess in Schicht zwei fügt der Nachricht die Steuerungsinformationen (z. B. die Adresse des Zielrechners) hinzu und leitet das Ergebnis an Schicht eins zur physischen Übertragung weiter. Diese Steuerungsinformationen im „Header“ werden der Nachricht vorangestellt, damit die Schicht eins die Nachricht an den Zielcomputer übermitteln kann, wie in der folgenden Abbildung dargestellt. Auf dem Zielrechner wandert die Nachricht von Schicht zu Schicht nach oben, wobei die Header (Kopfzeilen) unterwegs entfernt werden. Es stellen sich jedoch folgende Fragen: Wie viele Schichten werden in einem Netzwerk benötigt, und welche Art von Informationen sollen zwischen den Schichten weitergegeben werden?



In der Regel einigen sich die für das Netzwerkdesign zuständigen Personen auf die Anzahl der Schichten, die in einem Netzwerk enthalten sein sollen, was von der Verwendung der einzelnen Schichten abhängt. Mit anderen Worten: Jede Schicht sollte bestimmte Funktionen erfüllen. Darüber hinaus wird versucht, die zwischen den Schichten weiterzugebende Datenmenge klein zu halten. Dadurch wird es einfacher, eine Schicht durch ein völlig anderes Protokoll oder eine andere Implementierung zu ersetzen. Mit Hilfe der von den Netzwerkdesignern angegebenen Informationen werden die Anzahl der erforderlichen Schichten und die entsprechenden Protokolle ermittelt. Dies wird als Netzwerkarchitektur bezeichnet (Tanenbaum & Wetherall, 2010).

### Das TCP/IP-Referenzmodell

TCP/IP ist heute faktisch das Standardprotokoll, wie es von modernen Netzwerken genutzt wird. Im TCP/IP-Protokoll werden zwei Hauptprotokolle kombiniert: das Internetprotokoll (IP) und ein Protokoll zur Übertragungssteuerung namens *Transmission Control Protocol* (TCP). TCP/IP unterteilt die Netzwerkkommunikation in vier Schichten, wie in der nachstehenden Abbildung dargestellt (Forshaw, 2017).



###### Data Link Layer (Datenverbindungsschicht)

**Media access   
control address** (MAC-Adresse)   
Eine MAC-Adresse  
ist eine eindeutige  
Seriennummer, die bei der Herstellung auf die Netzwerkkarte gebrannt wird.

Dies ist die unterste Schicht. Sie beschreibt den physikalischen Mechanismus, der zur Übertragung von Informationen zwischen den Knoten in einem lokalen Netzwerk genutzt wird. Zum Beispiel gehören sowohl das kabelgebundene als auch das drahtlose Ethernet und das Punkt-zu-Punkt-Protokoll (PPP) zu dieser Schicht (Forshaw, 2017). Adressen auf der Datenverbindungsschicht werden als MAC-Adressen (Media Access Control) bezeichnet. Eine **MAC-Adresse** ist eine fest eingespeicherte Kennzeichnung in einer Netzwerkkarte (z. B. einer Ethernet-Karte). Jede Netzwerkkarte hat also eine eindeutige MAC-Adresse.

###### Die Internetschicht *(Internet Layer)*

Diese Schicht stellt die Mechanismen zur Adressierung von Netzwerkknoten bereit und beinhaltet auch das Internetprotokoll (IP). Diese Schicht ermöglicht es Host-Rechnern auch, Pakete zu verschicken und sie erfolgreich am Ziel (möglicherweise in einem anderen Netzwerk) zuzustellen. Das Internetprotokoll (IP) ist entweder IP Version 4 (IPv4) oder, in modernen Netzwerken, IP Version 6 (IPv6). Die Pakete werden in einer bestimmten Reihenfolge versendet, können aber durcheinander ankommen, so dass eine Neuordnung der Pakete erforderlich ist. In diesem Fall muss die nächsthöhere Schicht die Pakete neu anordnen, wenn die Zustellung in der richtigen Reihenfolge gewünscht ist.

###### Die Transportschicht

Diese Schicht stellt durchgängige Verbindungen *(„End-to-End“)* zwischen Klienten (Clients) und Servern sicher und garantiert die richtige Reihenfolge der Pakete. Darüber hinaus bietet diese Schicht Dienstmultiplexing. Ein einzelner Knoten kann also mehrere Dienste unterstützen, indem er jedem Dienst eine andere Nummer zuweist. Diese Nummern werden als Portnummern bezeichnet (Forshaw, 2017). Diese Schicht umfasst zwei wichtige Transportprotokolle. Das erste ist das *Transmission Control Protocol* (TCP) zur Übertragungssteuerung. Dieses zuverlässige, verbindungsorientierte Protokoll ermöglicht es, von einem Rechner erstellte Pakete ohne Fehler an jeden anderen Rechner im Internet zuzustellen.

Das zweite Protokoll ist das *User Datagram Protocol* (UDP), ein minimales, nicht zuverlässiges und verbindungsloses Protokoll, das von Anwendungen genutzt wird, die keine Ablaufsteuerung oder Sequenzierung benötigen.

###### Die Anwendungsschicht *(Application Layer)*

Diese Schicht enthält Netzwerkprotokolle. Dazu gehören das *Simple Mail Transport Protocol* (SMTP) zur Übertragung von E-Mails, das *Hypertext Transport Protocol* (HTTP) zur Übertragung von Webseiteninhalten, das *Domain Name System Protocol* (DNS-Protokoll) zur Umwandlung eines Namens in eine Knoten-IP-Adresse im Netzwerk sowie das *Real-Time Protocol* (RTP) zur Übertragung von Echtzeit-Medien wie Aufnahmen oder Filmen (Cynet, 2021).

### Angriffe und Gegenmaßnahmen

Große Unternehmensnetzwerke sind auf zahlreiche verbundene Endpunkte angewiesen. Diese werden im Geschäftsbetrieb genutzt, um die Arbeitsabläufe zu vereinfachen. Allerdings stellt dies auch eine Herausforderung für die Sicherheit dar. Wenn sich böswillig Agierende Zugang zu einem Unternehmensnetzwerk verschaffen, können sie das Netzwerk gefährden und Schaden anrichten, häufig ohne das Wissen derjenigen, die es rechtmäßig nutzen. Diese Bedrohungen der Netzwerksicherheit bzw. Netzwerkangriffe machen Unternehmen sehr anfällig für Datenschutzverletzungen (Datenlecks). Unter Datenschutzverletzungen werden nachgewiesene Vorkommnisse verstanden, die zu unbefugtem Zugriff oder zur Offenlegung sensibler, vertraulicher oder anderer geschützter Daten führen können. Netzwerkangriffe umfassen demnach den unbefugten Zugriff, Datenmissbrauch, Passwortdiebstahl und andere bösartige Aktivitäten. Sie können in zwei Haupttypen eingeteilt werden:

1. Aktive Angreifer greifen auf ein Netzwerk zu und verändern die Daten. Sie können Daten ändern, löschen oder verschlüsseln.
2. Passive Angreifende greifen auf ein Netzwerk zu und überwachen oder stehlen sensible Informationen, ohne dabei Daten zu verändern.

Andere netzwerkgefährdende Angriffe sind Endpunkt- und Malware-Angriffe sowie Sicherheitslücken, wie in der folgenden Liste erläutert:

* Endpunkt-Angriffe: Dazu gehört die Gefährdung von Endnutzungsgeräten (z. B. Smartphones, Computer, Laptops), gemeinsamen Ordnern oder Servern. Die Endnutzungsgeräte sind in der Regel die Eintrittspunkte zum Netzwerk. Wenn sich Angreifende Zugang zu Endnutzungsgeräten verschaffen, können sie leicht das gesamte Netzwerk gefährden.
* Malware-Angriffe: Die Infizierung von IT-Ressourcen mit Malware (bösartiger Software) gefährdet das System, weil sie nicht autorisierte Handlungen auf dem Endgerät bzw. System des Angriffsopfers ermöglicht. Angreifende verwenden solche bösartige Software (d. h. Viren, Würmer, Trojaner, Spyware und Ransomware), um Systeme zu gefährden, auf Daten zuzugreifen und Schaden anzurichten.
* Schwachstellen: Schwachstellen sind Lücken oder Schwächen in Soft- oder Hardware aufgrund von Entwicklungs- oder Implementierungsfehlern. Durch Ausnutzen von Schwachstellen können Angreifende sich unbefugten Zugang zu Systemen verschaffen und sie gefährden.

Bei einem Netzwerkangriff konzentrieren sich die Angreifenden darauf, in ein Unternehmensnetzwerk einzudringen und sich Zugang zu internen Systemen zu verschaffen. Wenn sie in ein Netzwerk eindringen, nutzen sie verschiedene Arten von Angriffen. Sie können zum Beispiel Malware verbreiten, Endnutzungsgeräte gefährden oder eine Sicherheitslücke ausnutzen. In den folgenden Lernzyklen werden einige der häufigsten Netzwerkangriffe erläutert.

###### Unbefugter Zugriff

Ein unbefugter Zugriff meint Nutzende, die ohne Erlaubnis auf ein Netzwerk zugreifen. Angriffe durch einen unbefugten Zugriff können etwa durch schwache Passwörter, manipulierte Konten, Systemschwachstellen, mangelnden Schutz vor sozialer Manipulation (z. B. Phishing) sowie Insider-Bedrohungen erfolgen.

Phishing ist eine Form der sozialen Manipulation (engl.: *social engineering*), bei der Angreifende eine betrügerische aber vertrauenswürdig erscheinende Nachricht verschicken (z. B. eine E-Mail von der Krankenkasse). Diese soll das Opfer zur Preisgabe seiner Zugangsdaten oder aber zur Einschleusung bösartiger Software in das System des Opfers verleiten.

###### DoS-Angriffe (DoS = *Denial of Service*, also Verweigerung des Dienstes)

Ein DoS-Angriff ist ein Netzwerkangriff, bei dem der Angreifer einen Rechner oder eine Netzwerkressource für die vorgesehenen Nutzenden nicht verfügbar bzw. unzugänglich macht. DoS wird erreicht, indem der Zielcomputer oder die Ressource mit einer übermäßigen Anzahl von Anfragen gefüttert wird. Das System wird überlastet und wird langsamer, bis es schließlich nicht mehr zur Verfügung steht und deshalb legitime Anfragen nicht erfüllt werden können. DoS-Angriffe können auch durch die Ausnutzung von Schwachstellen erfolgen, die das Zielsystem oder den Zieldienst zum Absturz bringen können.

DoS-Angriffe führen nicht zum Diebstahl oder Verlust von Informationen, aber sie können das Opfer viel Zeit kosten, wenn es versucht, auf den gestörten Dienst oder die gestörte Ressource zuzugreifen. DoS-Angriffe zielen in der Regel auf stark frequentierte Webserver oder Server von großen Organisationen wie Banken oder Behörden. DoS-Angriffe können entschärft werden, indem übermäßig hoher Datenverkehr von einer einzelnen IP-Adresse oder einem IP-Bereich identifiziert und blockiert wird.

Im Gegensatz zu DoS nutzt ein verteilter DDoS-Angriff mehrere Quellen (z. B. Computer an verschiedenen Orten), um das Ziel mit einer Flut von Anfragen oder Nachrichten zu überschwemmen. Das macht die Identifikation der Angreifenden schwer, und der Angriff kann nicht durch das Blockieren einer einzelnen Quelle entschärft werden. Darüber hinaus können DDoS-Angriffe auch über eine ganze Reihe von Geräten ausgeführt werden, die manipuliert und in ein orchestriertes System umgewandelt wurden, das als Botnet bezeichnet wird (Cynet, 2021).

###### Man-in-the-Middle-Angriffe

Bei einem Man-in-the-Middle-Angriff (MITM) fangen Angreifende den Datenverkehr zwischen zwei Parteien ab, die glauben, miteinander zu kommunizieren. Dabei können sie Nachrichten verändern. Angenommen, zwei vertrauenswürdige Parteien möchten Daten austauschen. Zugleich versuchen Angreifende, das Gespräch abzuhören.

Dabei wollen sie nicht nur auf die übertragenen Daten zugreifen, sondern auch eine manipulierte Nachricht an die beiden Parteien übermitteln, die glauben, direkt mit der anderen zu kommunizieren. MITM-Angriffe finden statt, wenn die Kommunikationsprotokolle zwischen den beiden Parteien nicht gesichert sind oder Angreifende eine Möglichkeit finden, als vertrauenswürdige Partei aufzutreten. Die Angreifenden können dann die übertragenen Daten stehlen und die Kommunikationssitzungen der Parteien kapern (Cynet, 2021).

###### Angriffe durch SQL-Einschleusung *(SQL Injection Attacks)*

SQL bzw. *Structured Query Language* ist eine sehr verbreitete Sprache für Datenbankzugriffe. Bei SQL Injection wird eine Sicherheitslücke (auch bekannt als Web-Sicherheitslücke) genutzt. Sie entsteht durch Websites oder Anwendungen, die Anfragen und Eingaben von Nutzenden akzeptieren, ohne sie zu überprüfen. Dadurch können Angreifende Daten zwischen einer Anwendung und ihrer Datenbank abfangen. Dabei kann es sich um die Daten anderer Nutzer oder um andere Daten aller Art handeln, auf welche die Anwendung zugreifen kann. Die Angreifenden können diese Daten in solchen Fällen ändern oder löschen und so den Inhalt oder das Verhalten der Anwendung dauerhaft verändern. Außerdem können sie anstelle der erwarteten Daten bösartigen Code versenden. Ein Server oder ein anderer Teil der Infrastruktur des Unterbaus (engl. *back-end*) führt diesen Code aus und ermöglicht Angreifenden so die Manipulation des Servers (Cynet, 2021).

###### Insider-Bedrohungen

Insider-Bedrohungen bestehen hauptsächlich aus Personen, die einen legitimen Zugang zu Unternehmensnetzwerken und ‑systemen haben und deren Zugang für die Manipulation des Systems ausgenutzt wird. Insider-Bedrohungen können durch aktuelle oder ehemalige Angestellte, Lieferanten oder Partner bestehen, die unbeabsichtigt vertrauliche Daten weitergeben oder absichtlich Daten zum persönlichen Vorteil ausspähen.

### Grundlegende Sicherheitsmodelle

Heutzutage werden in jedem Unternehmen Kontrollschritte, Prozesse und Lösungen für die Netzwerksicherheit implementiert, um die Sicherheit der Ressourcen zu gewährleisten (Cynet, 2021). Sicherheitslösungen werden auf der Grundlage von drei Hauptprinzipien implementiert, der so genannten CIA-Triade (engl. *Conﬁdentiality, Integrity, Availability*).

Die CIA-Triade umfasst also die drei Hauptprinzipien Vertraulichkeit, Integrität und Verfügbarkeit, mit denen die Sicherheit durchgesetzt und ein sicheres Netzwerk gewährleistet werden soll. Diese Grundsätze sind wie folgt zu verstehen:

* + Vertraulichkeit: Vertrauliche oder sensible Daten sollten nicht für unbefugte Parteien oder Entitäten zugänglich sein oder an diese weitergegeben werden. Außerdem sollten sensible Daten vor Bedrohungen, Angriffen und Datenschutzverletzungen geschützt werden.
  + Integrität: Daten sollten über ihren gesamten Lebenszyklus hinweg genau, konsistent und vertrauenswürdig bleiben. Jede Datenänderung aufgrund von Verarbeitungsschritten, Speicherung, Hardwarefehlern, inkonsistenten Datensicherungen oder menschlichem Versagen wird als Verletzung der Datenintegrität betrachtet.
  + Verfügbarkeit: Die Daten sind nur denjenigen zugänglich, die dazu berechtigt sind. Dadurch wird sichergestellt, dass die Daten jederzeit vollständig verfügbar und für berechtigt nutzende Personen zugänglich sind. Das bedeutet, dass Computersysteme (die zum Speichern und Verarbeiten von Daten verwendet werden) jederzeit verfügbar sein müssen, um Unterbrechungen des Dienstes aufgrund von Hardwareausfällen, Stromausfällen, System-Aktualisierungen und Software-Patches zu vermeiden. DoS-Angriffe sind schwerwiegende Angriffe, die sich direkt auf die Systemverfügbarkeit auswirken, weil sie Systeme außer Betrieb setzen (d. h. diese sind dann nicht mehr verfügbar).

###### Bewährte Praktiken für den Netzwerkschutz

Es gibt mehrere Methoden zum Schutz von Netzwerken, die jeweils am sinnvollsten Punkt eingesetzt werden sollten.

Netzwerk-Unterteilung

Ein wesentlicher Bestandteil zur Vermeidung von Sicherheitsbedrohungen im Netzwerk ist die sicherheitsorientierte Aufteilung des Netzwerks in Sektoren. Diese Sektoren werden als Teilnetzwerke oder Netzwerksegmente bezeichnet. Die Unterteilung wird verwendet, um den Zugang zu jedem Teilnetz auf eine begrenzte Anzahl Nutzender zu beschränken. Das bedeutet, dass vertrauliche Informationen nur von berechtigten Nutzenden eingesehen werden können. Darüber hinaus begrenzt und isoliert die Unterteilung im Falle eines Netzwerkangriffs die potenziellen Auswirkungen des Angriffs auf ein Teilnetz und stoppt diesen, bevor er den Kern des Netzwerks erreicht.

Zugriffskontrolle

Die Zugriffskontrolle für Informationen erlaubt nur authentifizierten und autorisierten Nutzerinnen und Nutzern den Zugriff auf die Daten. Die Authentifizierung stellt sicher, dass ein Nutzer derjenige ist, der er zu sein vorgibt. Die Autorisierung hingegen legt fest, welche Zugriffsebene dem Nutzer gewährt wird.

Beim Online-Banking beispielsweise verwenden Nutzer:innen eine Kombination aus Login und Passwort, die nur ihnen bekannt ist. Die Bankanwendung nutzt also eine Anmelde- und Passwortkombinationen, um Nutzer zu authentifizieren. Einige Anwendungen stellen strengere Anforderungen an die Authentifizierung, wie z. B. die Zwei-Faktor-Authentifizierung oder die biometrische Identifizierung, wie einen Fingerabdruck oder einen Gesichts-Scan.

Nach der Authentifizierung können Nutzer:innen nur auf die Informationen zugreifen, für die sie autorisiert sind. Im genannten Beispiel bedeutet dies, dass ein Nutzer nur berechtigt ist, seine eigenen Kontodaten einzusehen, und nicht die Möglichkeit hat, auf die Konten anderer zuzugreifen. Im Gegensatz dazu können sich Bankangestellte über dieselbe Anwendung anmelden, jedoch nur den Finanzüberblick sehen.

Internet-Zugangsregulierung über Proxy-Server

Proxy-Server bieten einen Vermittlungsmechanismus, der Anfragen und Antworten zwischen dem Internet und den Computern der Nutzenden weiterleitet. Ein Proxy-Server verringert Datenverletzungen, weil er als zusätzliche Sicherheitsschicht zwischen den internen Netzwerkservern und dem Internet fungiert. Ein Proxy leistet also Folgendes: (a) Er sorgt für einen sicheren Zugang zwischen dem internen Netzwerk und dem Internet, (b) stellt einen Cache mit häufig angeforderten Websites zur Verfügung, (c) kontrolliert und überwacht das Verhalten der Nutzenden und (d) blockiert den Zugriff auf bestimmte Websites.

Firewalls

Firewalls bestehen aus Hard- und Software zur Netzwerksicherheit, die als Barriere zwischen dem laufenden Datenverkehr und dem internen Netzwerk fungieren. Firewalls prüfen den ein- und ausgehenden Netzwerkverkehr und entscheiden auf der Grundlage vordefinierter Richtlinien und Sicherheitsregeln, ob ein bestimmter Verkehr zugelassen oder blockiert wird. Für höhere Sicherheit werden Firewalls am Netzwerkrand und an jedem Knotenpunkt des Teilnetzes platziert.

Systeme zur Überwachung und Erkennung von Netzwerken

Netzwerküberwachungs- und ‑erkennungssysteme (Mangat, 2020) erkennen Bedrohungen und verstehen deren Kontext und Auswirkungen, indem sie eingehenden, ausgehenden und internen Netzwerkverkehr überwachen und scannen. Zu den Netzwerküberwachungs- und ‑erkennungssystemen gehören verschiedene Anwendungen, die sowohl den eingehenden als auch den ausgehenden Netzwerkverkehr überwachen und automatisch handeln, wenn anomale oder bösartige Netzwerkaktivitäten entdeckt werden. Beispiele für Netzüberwachungs- und ‑erkennungssysteme sind die folgenden:

* Intrusion-Prevention-Systeme (IPS), also Systeme zur Angriffsabwehr, scannen den Netzwerkverkehr und blockieren automatisch Versuche, in das Netzwerk einzudringen und sonstige verdächtige Aktivitäten.
* Intrusion-Detection-Systeme (IDS), also Systeme zur Eindringlingserkennung, überwachen Netzwerkpakete, um verdächtige Aktivitäten zu erkennen und zur Überprüfung zu markieren.
* Security Information and Event Management (SIEM) bietet eine Echtzeitanalyse von Sicherheitswarnungen, die von Netzwerkhardware und Anwendungen wie IPS oder IDS erzeugt werden. SIEM liefert wertvolle Protokolldaten, die Administratoren bei der Untersuchung von Sicherheitsvorfällen und bei der Suche nach verdächtigem Verhalten unterstützen.

Virtuelle private Netzwerke

Ein virtuelles privates Netzwerk (VPN) ist eine verschlüsselte Verbindung über das Internet, die den gesamten Netzwerkverkehr verschlüsselt und so die sichere Übertragung sensibler Daten gewährleistet. Außerdem verhindert es, dass Unbefugte den Datenverkehr abhören, erlaubt aber den berechtigten Nutzern die Arbeit aus der Ferne.

DDoS-Verhinderung

Eingehende Anfragen müssen analysiert werden, damit das Netzwerk für legitime Verbindungen erreichbar bleibt, andererseits aber verteilte Denial-of-Service-Angriffe (DDoS) entschärft werden. Durch diese Analyse können Administratoren illegalen Datenverkehr identifizieren und ausfiltern.

Anwendungssicherheit

Die Aufgabe der Anwendungssicherheit ist die Prüfung der Sicherheit auf Anwendungsschicht. Dazu wird die Verwendung sicherer Software im gesamten Netzwerk erzwungen. Anwendungssicherheit kann Hardware, Software und andere Verfahren umfassen, mit denen Sicherheitsschwachstellen identifiziert und minimiert werden. Die Anwendungssicherheit gewährleistet, dass die neuesten Software-Sicherheitspatches installiert und Anwendungen mit den neuesten Sicherheitsstandards und ‑protokollen entwickelt und ertüchtigt werden.

Antivirus- und Anti-Malware-Programme

Antivirus- und Anti-Malware-Programme sind Computerprogramme, die dazu dienen, bösartige Software (Malware) zu scannen, zu erkennen, einzudämmen und zu entfernen. Malware sind Programme, die über eine Hintertür in ein Netzwerk einzudringen versuchen. Eine Hintertür ermöglicht bösartiger Software oder einem Eindringling den Zugriff auf das Zielsystem, um dann vertrauliche und sensible Informationen zu stehlen. Zwischen Antiviren- und Anti-Malware-Programmen gibt es diverse Unterschiede. Bevor diese näher beschrieben werden, soll zunächst auf den Unterschied zwischen Viren und bösartiger Software (oder Malware) eingegangen werden.

Ein Virus besteht aus Programmcode, der sich selbst repliziert, um das Zielsystem zu schädigen. Es versucht, in die Daten einzudringen und sie zu verändern, gelegentlich auch bestimmte Daten zu löschen. Malware hingegen umfasst unterschiedliche bösartige Software wie Würmer, Spyware, Ransomware, wozu auch Viren gehören. Ein Wurm kann sich selbst replizieren und sich von einem Computer zu einem anderen im Netzwerk verbreiten. Mit Spyware versuchen Angreifende, persönliche Informationen zu stehlen. Trojaner können zwar Schaden anrichten, aber sie replizieren sich nicht und verbreiten sich daher nicht auf andere Computer. Ransomware wird verwendet, um durch Datenverschlüsselung den Zugang zu persönlichen Dateien zu blockieren. Nach Zahlung eines Lösegelds („Ransom“) kann der Zugang im Prinzip wiederhergestellt werden (Lutkevich, 2021).

Antiviren- und Anti-Malware-Programme wurden als Antwort auf diese Bedrohungen entwickelt und können wie folgt unterschieden werden:

* + Antivirus-Programm: Eine vorbeugende Maßnahme, um Systeme vor einer Infektion zu schützen.
  + Anti-Malware: Damit werden Netzwerke geschützt, indem bösartige Programme, die bereits heruntergeladen wurden und in das Netzwerk eingedrungen sind, aufgespürt und zerstört werden.

Drahtlose Sicherheit (engl. *wireless security*)

Drahtlose Sicherheit ist notwendig, um den Zugriff und die Nutzung des Netzwerks durch nicht autorisierte Nutzende zu verhindern. Dies wird durch die Beschränkung des Zugriffs über MAC-Adressen und die Verschlüsselung der über drahtlose Netzwerke übertragenen Daten erreicht. Durch drahtlose Sicherheit kann ein drahtloses Netzwerk auch vor Angreifenden geschützt werden, welche die Verfügbarkeit des Netzwerks beeinträchtigen wollen.

Mobile Sicherheit

Intelligente Geräte wie Smartphones, Laptops und Tablets werden durch Sicherheit für mobile Geräte vor Netzwerkbedrohungen geschützt. Um die mobile Sicherheit zu gewährleisten, werden Sicherheitsschwachstellen im Netzwerk überwacht und entschärft. Darüber hinaus gibt die mobile Sicherheit den Administratoren folgende Möglichkeiten:

* + Isolierung sensibler Daten auf mobilen Geräten,
  + Installation nur von erlaubten Anwendungen,
  + Ortung verlorener oder gestohlener Geräte,
* Durchsetzung der Datenverschlüsselung sowie
* Löschen sensibler Daten aus der Ferne.

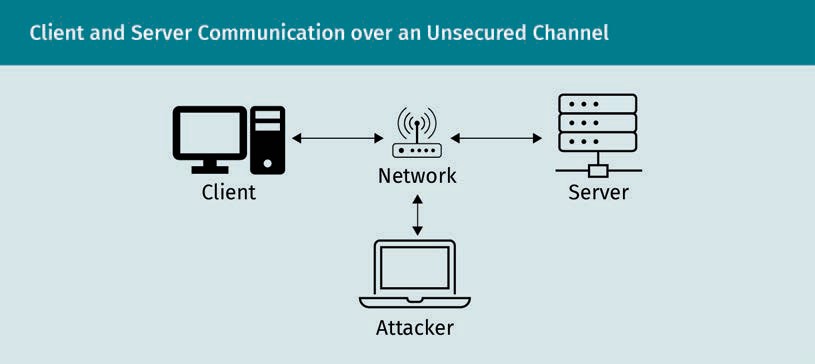
### Praktische Beispiele

Es sind zwei verschiedene Angriffsszenarien möglich: passiv und aktiv. Passive Angriffe greifen nicht direkt in den Verkehr ein. Stattdessen extrahieren sie Daten während des Übertragungsvorgangs („Abhören, Lauschen“). Dies ist von Werkzeugen wie Wireshark bekannt. Aktive Angriffe hingegen stören den Datenverkehr zwischen einer Client-Anwendung und dem Server. Dies bietet viele Möglichkeiten, kann aber auch zu Komplikationen führen. Diese aktive Erfassung kann man sich in Form von Proxies oder sogar Man-in-the-Middle-Angriffen vorstellen. Betrachten wir die aktiven und passiven Techniken etwas näher (Forshaw, 2017).

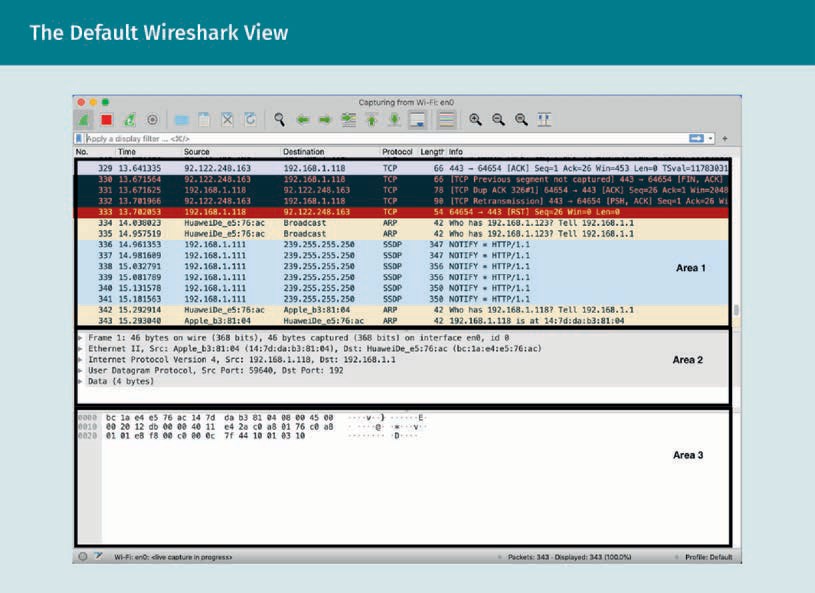
###### Passives Abhören des Netzwerkverkehrs

Das passive Abhören von Daten ist eine relativ einfache Technik. In der Regel ist weder spezielle Hardware noch eigener Code erforderlich. Die folgende Abbildung zeigt ein gängiges Szenario: ein Client und ein Server kommunizieren über ein Ethernet-Netzwerk.

Passiv Angreifende können das Netzwerk beobachten, indem sie den Datenverkehr abhören oder direkt auf dem Client- oder Server-Host „herumschnüffeln“.



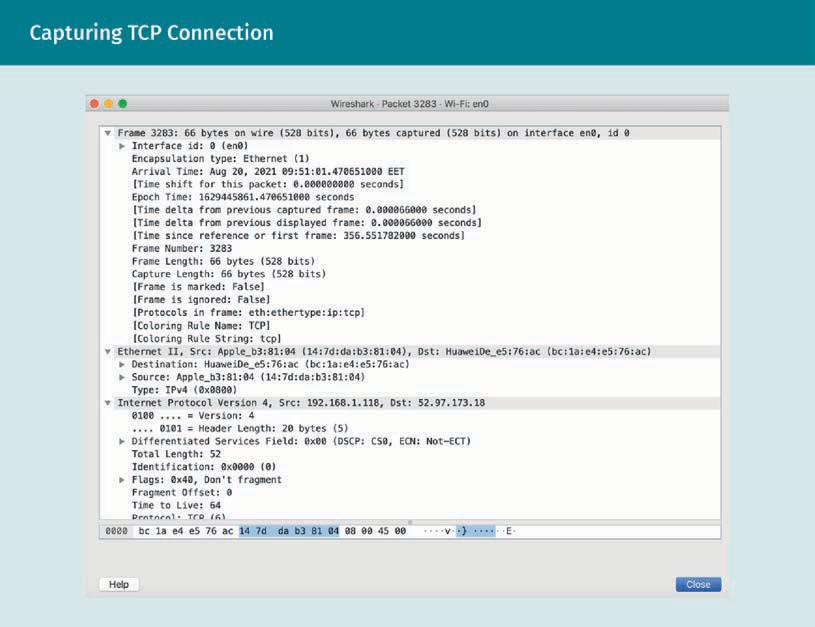
Wireshark ist die beliebteste Anwendung zum Schnüffeln von Datenpaketen auf dem Markt. Die folgende Abbildung zeigt eine Standardansicht von Wireshark beim Abhören von Daten von einer Ethernet-Schnittstelle.



In der obigen Abbildung sind drei Bereiche der Standardansicht zu sehen.

* + Bereich eins zeigt eine Zeitleiste der aus dem Netzwerk aufgezeichneten Rohdatenpakete. Die Zeitleiste enthält eine Liste der Quell- und Ziel-IP-Adressen sowie eine Übersicht der dekodierten Protokollinformationen.
  + Bereich zwei zeigt eine detaillierte Ansicht des Pakets, unterteilt in die unterschiedlichen Protokollschichten nach dem OSI-Netzwerkstapelmodell (Open Systems Interconnection).
  + Bereich drei zeigt das abgehörte Paket in seiner Rohform.

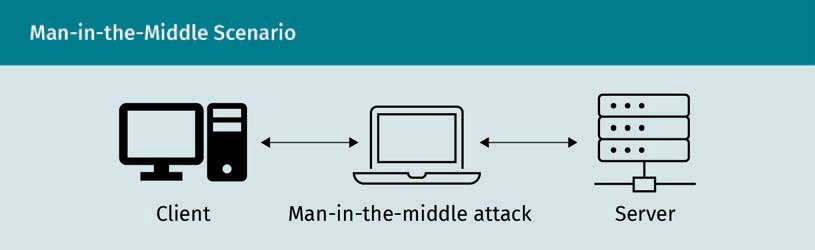
Glücklicherweise bietet Wireshark aufgeschlüsselte Informationen für bekannte Protokolle. So wird in der Regel der gesamte Datenstrom analysiert und alle Informationen werden an einem Ort bereitgestellt. In der folgenden Abbildung ist beispielsweise ein TCP-Verbindungspaket in der Zeitleistenansicht hervorgehoben.



###### Aktiver Eingriff in den Netzwerkverkehr

Der aktive Eingriff unterscheidet sich vom passiven Abhören dadurch, dass aktive Angreifende den Datenverkehr beeinflussen wollen. In der Regel geschieht dies durch einen Man-in-the-Middle-Angriff auf die Kommunikation im Netzwerk. Die folgende Abbildung zeigt, dass das den Datenverkehr erfassende Gerät in der Regel zwischen der Client- und der Serveranwendung sitzt und als Brücke fungiert. So können Angreifende den Datenverkehr modifizieren und Funktionen wie Verschlüsselung oder Komprimierung deaktivieren, was die Analyse und Ausnutzung eines Netzwerkprotokolls erleichtert.

Angreifende können zum Beispiel die Netzwerkadresse des Servers oder Clients beim Proxy ändern. Die Anwendung kann dadurch getäuscht werden, sodass sie den Datenverkehr an die falsche Stelle leitet. Ein Proxy-Server in der Informationstechnologie ist eine Serveranwendung, die als Vermittler zwischen Nutzern, die eine Ressource anfordern, und dem Server, der diese Ressource bereitstellt, fungiert.



Ein Nachteil dieser Methode ist, dass Angreifende den Datenverkehr der Anwendung durch ihr aktives Abhörsystem umleiten müssen, was die Komplexität erhöht (Forshaw, 2017).

Zusammenfassung

Diese Lektion lieferte einen Überblick über die Grundlagen der Netzwerksicherheit. Es wurden einige der Protokolle beschrieben, die in realen Netzwerken anzutreffen sind, und veranschaulicht, wie Daten zwischen Knoten durch eine Schichtstruktur übertragen werden. Als nächstes wurden die Netzwerktopologien dargestellt. Darüber hinaus wurden Bedrohungen der Netzwerksicherheit, Netzwerksicherheitsprozesse und Lösungen zur Entschärfung dieser Bedrohungen erläutert.

Zum Schutz der Netzwerkumgebung ist es wichtig, das grundlegende Sicherheitsmodell, die gängigen Angriffsarten und die entsprechenden Gegenmaßnahmen zu verstehen, die zur Abwehr dieser Angriffe eingesetzt werden. In dieser Lektion wurde zwischen aktiven und passiven Angriffen unterschieden und ihre gemeinsamen Merkmale wurden besprochen. Zudem wurden einige Angriffe, welche die zentralen Netzwerksicherheitseigenschaften Vertraulichkeit, Integrität und Verfügbarkeit *(CIA, Confidentiality, Integrity, Availability)* beeinträchtigen, detailliert beschrieben. Jeder Angriff kann auf eine oder mehrere Sicherheitseigenschaften abzielen.

Außerdem wurden Sicherheitslösungen und Pläne zur Entschärfung dieser Bedrohungen vorgestellt. Durch diese Lösungen können diverse Bedrohungen individuell entschärft werden. Durch die Kombination mehrerer Lösungen lassen sich aber auch variable Bedrohungen begrenzen. Schließlich wurden Netzwerkprotokolle auch aus der Perspektive der Erfassung und Analyse von Netzwerkverkehr betrachtet. Wie bei den unterschiedlichen Angriffsarten wurden auch bei den Eingriffen in den Netzwerkverkehr zwei Arten unterschieden, nämlich aktive und passive Eingriffe.



# Lektion 2

## Infrastrukturkomponenten

#### LERNZIELE

Nach Abschluss dieser Lektion werden Sie …

… die miteinander verbundenen Geräte der Netzwerkinfrastruktur identifizieren können.

… beschreiben können, wie Firewalls lokale Netzwerke schützen.

… verstehen, wie man Techniken zur Datenzugriffskontrolle einsetzt.

… Bedrohungen für Netzwerkinfrastrukturgeräte und Abwehrmaßnahmen dagegen identifizieren können.

DL-E-DLMCSEESN01\_E-U02

1. Infrastrukturkomponenten

### Einführung

Das Internet ist eine revolutionäre Erfindung, die den Nutzerinnen und Nutzern ein grenzenloses Maß an Wissen, Unterhaltung, Kommunikation und Datenaustausch bietet. Der Internetzugang ist für das tägliche Leben unverzichtbar geworden, gleichzeitig ermöglicht er Cyberkriminellen, in jede Organisation einzudringen, indem sie lokale Ressourcen erreichen und mit ihnen interagieren. Zur Sicherung von Netzwerken ist es unerlässlich, sich mit Netzwerk-Infrastrukturgeräten und den Schwachstellen in Computernetzwerken vertraut zu machen, genauso wie mit den unterschiedlichen Angriffsarten und Abwehrmaßnahmen, die in solchen Netzwerken durchgeführt werden.

Die Netzwerkinfrastruktur besteht aus miteinander verbundenen Geräten, die Daten übertragen, Computer und Kommunikation ermöglichen, Anwendungen nutzen und Multimedia-Dateien austauschen können. Für effektive Netzwerkdienste zwischen Nutzenden werden in der Netzwerkinfrastruktur Server, Geräte wie Router und Switches, Softwareprogramme (wie Software-Firewalls) und Anwendungsprogramme eingesetzt. Der Schutz und die Stärkung der Netzwerkinfrastruktur ist für die Sicherheit, also für die Eindämmung von Systemrisiken, Schwachstellen, Angriffen und Datendiebstahl, von entscheidender Bedeutung. Der Schutz von Prozessen umfasst u. a. das Blockieren unbefugten Zugriffs, die Gewährleistung von Datenvertraulichkeit und ‑integrität sowie die Sicherstellung der Systemverfügbarkeit.

### Netzwerkinfrastruktur-Geräte

Netzwerkgeräte sind für den Schutz von Organisationen unverzichtbar. Eine falsche Gerätekonfiguration kann jedoch eine Organisation ernsthaft in Gefahr bringen. Sie kann beispielsweise zu unbefugtem Zugriff auf das Netzwerk führen, was die Tür zu Datenschutzverletzungen, Datenverlusten, Systemausfällen, der Aussperrung berechtigter Nutzer und vielen anderen Problemen öffnet. Zu den Netzwerkgeräten gehören Switches, Router und Firewalls.

###### Switch

Über Switches (engl. für Schalter bzw. Netzwerkweiche) werden mehrere Endgeräte (z. B. Computer, Handys, Tablets und Drucker) in einem Computernetzwerk verbunden. Ein Switch arbeitet als zentraler Dreh- und Angelpunkt (engl. *Hub*), über den die Endgeräte im selben Computernetzwerk kommunizieren. Dies wird als lokales Netzwerk bezeichnet. Das bedeutet, dass ein Switch mehrere Verbindungen handhaben kann, indem er Datenframes (engl. *data frames*) von Quell- zu Zielgeräten empfängt und weiterleitet. Hierzu werden MAC-Adressen *(Media Access Control)* genutzt (John, 2017; Tanenbaum & Wetherall, 2010).

Der Switch lernt die MAC-Adressen der Quell- und Zielgeräte aus den Datenframes und speichert sie in einer Tabelle, um bei einer erneuten, ähnlichen Anfrage den Standort des Endgeräts bestimmen zu können. Wenn er eine Frame-Anforderung mit einer noch nicht in der Tabelle enthaltenen Ziel-MAC-Adresse empfängt, sendet der Switch die Anforderung an alle Anschluss-Schnittstellen (engl. *Ports*). Dies wird Broadcasting des Frames genannt. Wenn der Switch eine Antwort erhält, speichert er die neue MAC-Adresse in der Tabelle.

Ein Switch kann gleichzeitige Verbindungen zwischen vielen Endgeräten verarbeiten, ohne dass eine der Verbindungen die anderen stört. Im Gegensatz zu einem Switch, der nur Endgeräte im selben lokalen Netzwerk und nicht mit solchen in anderen Netzwerken verbinden kann, ermöglichen Router die Kommunikation zwischen verschiedenen Netzwerken (Tanenbaum & Wetherall, 2010).

###### Router

Ein Router verbindet verschiedene Netzwerke miteinander, so dass Informationen von einem Endgerät (d. h. einem Knoten) zu einem anderen gelangen können. Ein Router ist auf eine Internetprotokoll-Adresse (IP) angewiesen, um die Daten zwischen den Knoten (von der Quelle zum Ziel) weiterzuleiten. Router können dazu verwendet werden,

* physisch getrennte Knotenpunkte miteinander zu verbinden (z. B. Router zu Hause, die Endgeräte mit dem Internet verbinden), und
* physisch verbundene Teilnetzwerke in logische Teilnetzwerke zu unterteilen, was den Datenverkehr von einem Teilnetz in ein anderes verhindert (John, 2017; Tanenbaum & Wetherall, 2010).

Ein Router prüft jede Quell- und Ziel-IP-Adresse eines Pakets und speichert sie in einer Tabelle, der so genannten Routing-Tabelle. Der Router sucht das Ziel des Pakets in der Routing-Tabelle und leitet das Paket an einen anderen Router oder Switch weiter, um so die Kommunikation zwischen Netzwerken zu ermöglichen. Dieser Vorgang wird fortgesetzt, bis die Ziel-IP-Adresse erreicht ist und die Ziel-IP (der Rechner) antwortet. Wenn es mehr als einen Pfad gibt, um den Zielcomputer zu erreichen, wählt der Router den kürzesten (d. h. den wirtschaftlichsten) Pfad. Wenn das Ziel des Pakets nicht in der Routing-Tabelle enthalten ist, wird das Paket an den Standard-Router gesendet, und wenn dort kein Eintrag für das Zielpaket vorhanden ist, wird es verworfen.

Router können nicht nur Pakete und Daten an einen Zielknoten senden, sondern auch Daten vom Quellknoten an alle anderen Knoten im Zielnetz weiterleiten („Rundfunk“, engl. *one-to-all broadcast*). Normalerweise werden Broadcasts eher zur Verwaltung der Datenkommunikation zwischen Endgeräten als zur Datenübertragung verwendet.

Normalerweise wird der Router von einem Internetanbieter (engl. *Internet Service Provider, ISP*) bereitgestellt. Der ISP weist jedem Router eine Router-IP-Adresse (eine öffentliche IP-Adresse) und mehrere private Adressen zu, welche die Endnutzenden konfigurieren können. Beim Surfen im Internet werden Endnutzende nach außen hin durch ihre öffentliche IP-Adresse identifiziert. Für alle verwendeten Endgeräte (z. B. Desktop, Laptop, iPad, TV-Medienbox oder Drucker) werden jedoch private IP-Adressen verwendet. Dabei hat jedes Endgerät eine andere private IP-Adresse. Andernfalls wäre der Router nicht in der Lage, die Anfragen der einzelnen Endgeräte zu erkennen (Tanenbaum & Wetherall, 2010).

###### Firewall

Firewalls sind die erste Verteidigungslinie gegen Netzwerkbedrohungen und Cyberangriffe. Für eine Firewall gibt es folgende Möglichkeiten: (a) Ein einzelnes Hardwaresystem, (b) eine Gruppe von zwei oder mehr Hardwaresystemen, welche die Firewall-Funktion im Zusammenspiel erfüllen, oder (c) eine Software-Lösung. Eine Firewall wird zwischen den lokalen (vertrauenswürdigen) Netzwerken und dem externen Netzwerk oder dem Internet platziert, um den ein- und ausgehenden Datenverkehr in einem Netzwerk einzuschränken.

Die Einschränkung basiert auf vordefinierten Sicherheitsrichtlinien und ‑regeln, wie in Bolar (2020) und Bellovin & Cheswick (1994) erläutert. Die Firewall blockiert alle Verbindungen, die diesen Sicherheitsregeln nicht entsprechen.

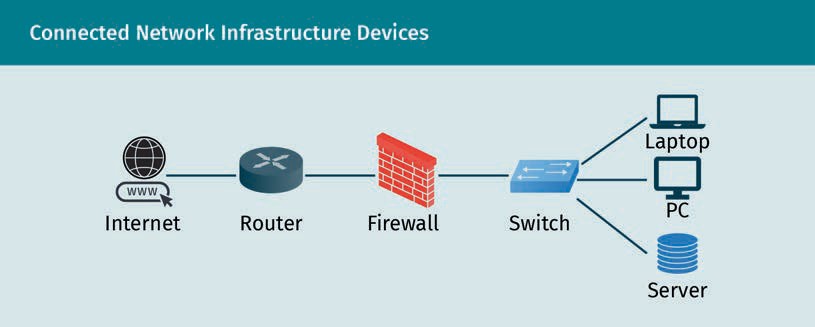
Firewalls können auch im lokalen Netzwerk eingesetzt werden, um die Verbindungen zwischen Abteilungen zu kontrollieren und den Zugriff auf vertrauliche Ressourcen zu steuern. Unternehmen verwenden beispielsweise Firewalls, um die Anbindung an sensible Abteilungen wie Buchhaltung oder Finanzabteilung einzuschränken. Nur befugte und vertrauenswürdige Personen haben Zugang zu diesen Abteilungsnetzwerken. Darüber hinaus kann ein Unternehmen den unbefugten Zugriff auf seine privaten Aktivposten (d. h. seine Systeme und Ressourcen) mit einer gut konfigurierten Firewall einschränken. Die Eigenschaften der Firewall-Konfiguration werden in Bolar (2020) und Bellovin & Cheswick (1994) erläutert. Als nächstes wird der Fokus auf die Eigenschaften einer Firewall gerichtet sowie auf Sicherheit, Zugriffsdatenlisten und das Konzept eines vertrauenswürdigen Systems.

###### Wie sind Router, Firewalls und Switches miteinander verbunden?

**Lokales Netzwerk** Ein lokales Netzwerk (LAN) ist ein Computernetzwerk, das mehrere Knoten innerhalb eines begrenzten   
Bereichs miteinander verbindet.

**Weitverkehrsnetzwerk**   
Ein Weitverkehrsnetzwerk (WAN) ist ein Computernetzwerk, das mehrere Knotenpunkte über ein großes geografisches Gebiet miteinander verbindet.

Normalerweise ist der Router in einem **lokalen Netzwerk (LAN = Local Area Network)** unverzichtbar, da er die Verbindung zwischen dem LAN und dem **Wide Area Network (WAN)** oder dem Internet herstellt. Zwischen dem LAN und dem Router befindet sich eine Netzwerk-Firewall, die alle ein- und ausgehenden Verbindungen filtert. Der Switch verbindet verschiedene Netzwerkgeräte im selben LAN, wie in der folgenden Abbildung dargestellt. Die typische Konfiguration wäre also: Internet, Router, Firewall und Switch (John, 2017).



### Firewalls

Firewalls können das lokale Netzwerk und die Systeme vor Bedrohungen der Netzwerksicherheit schützen, indem sie den Zugang zum Internet kontrollieren. Der folgende Lernzyklus liefert einen Überblick über das Design und die Funktionsweise von Firewalls (Stallings & Brown, 2012).

###### Ziele beim Firewall-Design

Zuallererst besteht die Hauptaufgabe von Firewalls darin, jeden Zugriff auf das lokale Netzwerk zu blockieren. Dies geschieht unter Umgehung des gesamten Datenverkehrs vom lokalen Netzwerk zum Internet und umgekehrt. Danach können verschiedene Konfigurationen vorgenommen werden, um den Zugang zum Netzwerk zu ermöglichen, wie später noch erläutert wird (Bellovin & Cheswick, 1994; Stallings & Brown, 2012).

Zweitens richten Firewalls eine Sicherheitsrichtlinie ein, die nur den berechtigten Datenverkehr zulässt. Es können mehrere Arten von Sicherheitsrichtlinien und ‑regeln definiert und von verschiedenen Arten von Firewalls verwendet werden, wie nachfolgend ausführlicher dargestellt wird.

Drittens soll eine Firewall verdächtige Versuche zur Gefährdung der Netzwerksicherheit abwehren. Mit anderen Worten: Firewalls sollten immun gegen das Eindringen sein. Dies wird durch die Implementierung von Firewalls unter Verwendung eines vertrauenswürdigen Systems mit einem sicheren Betriebssystem erreicht. Firewalls nutzen die folgenden vier Methoden zur Durchsetzung der Sicherheitsrichtlinien und Zugriffskontrolle:

* + 1. Dienststeuerung: Diese Funktion steuert die Art der Internetdienste, auf die zugegriffen werden kann. Die Firewall filtert den Datenverkehr durch Überprüfung des ein- und ausgehenden Datenverkehrs auf IP-Adressen, Portnummern und Protokolle. Dies kann durch den Einsatz einer Proxy-Software erreicht werden, die (a) jede Dienstanforderung empfängt und interpretiert, und erst dann weiterleitet, oder (b) die Serversoftware hostet, wie z. B. einen Web- oder Maildienst.
    2. Richtungssteuerung: Damit wird die Richtung der Dienstanfrage, welche die Firewall passieren darf, geregelt.
    3. Nutzer-Steuerung: Nur autorisierte Nutzer:innen können auf den gewünschten Dienst zugreifen.
    4. Verhaltenssteuerung: Steuerung, wie bestimmte Dienste genutzt werden (z. B. der Abruf von E-Mails).

###### Firewall-Fähigkeiten und ‑Stärken

Bevor wir auf die verschiedenen Arten von Firewalls und ihre unterschiedlichen Konfigurationen eingehen, sollten wir zunächst definieren, was Firewalls leisten sollen.

Eine Firewall fungiert als zentraler Punkt, der verhindert, dass nicht autorisierte Nutzende auf das Netzwerk zugreifen. Sie verhindert, dass potenziell gefährdete Dienste ins Netzwerk hinein oder von dort hinausgelangen. Darüber hinaus bietet sie Schutz vor verschiedenen Arten von IP-Spoofing und Routing-Angriffen (Stallings & Brown, 2012).

Außerdem vereinfacht die Firewall die Sicherheitskontrolle (auf Erkennung und Prävention basierende Strategien), indem sie verschiedene Sicherheitsrichtlinien und ‑regeln in einem System oder einer Reihe von Systemen zusammenfasst. Darüber hinaus überwacht eine Firewall sicherheitsrelevante Ereignisse und ermöglicht die Implementierung von Alarmen und Audit-Indikatoren.

Eine Firewall ist für zahlreiche nicht sicherheitsrelevante Anwendungen nützlich, z. B. für eine Netzwerkverwaltung, welche über die Firewall die Internetnutzung überwacht. Ein weiteres Beispiel ist ein Netzwerkadressübersetzer, der über die Firewall lokalen Adressen Internetadressen zuordnet.

###### Beschränkungen und Schwachstellen von Firewalls

Firewalls haben die folgenden Beschränkungen:

* Firewalls setzen nur die konfigurierten Sicherheitsregeln und ‑richtlinien durch. Wenn diese also schlecht konzipiert sind, kann eine Firewall nicht alle Probleme verhindern.
* Firewalls setzen keine Passwortrichtlinien durch und verhindern nicht den Missbrauch von Passwörtern.
* Firewalls können nicht-technische Sicherheitsrisiken wie soziale Manipulation *(Social-Engineering-Angriffe)* nicht erkennen oder verhindern.
* Firewalls können nicht verhindern, dass autorisierte Nutzer:innen auf bösartige Websites zugreifen.
* Firewalls können interne Bedrohungen weder erkennen noch verhindern. Sie können zum Beispiel nicht verhindern, dass ein Mitarbeiter arglos oder absichtlich mit externen Angreifenden kooperiert.

###### Arten von Firewalls

Es gibt drei gängige Arten von Firewalls: paketfilternde Router, Gateways auf Anwendungsebene und Gateways auf Leitungsebene.

Paketfilternde Router

Ein paketfilternder Router leitet jedes ein- oder ausgehende IP-Paket gemäß einer Reihe von Regeln weiter oder verwirft es. Die Filterregeln werden auf der Grundlage der in einem Netzwerkpaket enthaltenen Informationen festgelegt. Es gibt mehrere wichtige Elemente für einen paketfilternden Router, darunter eine Quell-IP-Adresse, eine Ziel-IP-Adresse und die gewünschte Aktion. Eine Quell-IP-Adresse ist die Adresse des Systems, welches das IP-Paket verschickt hat (Absender). Die Zieladresse hingegen ist die Adresse, die der Absender zu erreichen versucht. Im Hinblick auf die gewünschte Aktion basieren die Regeln des Paketfilters auf dem Abgleich der IP-Header-Felder. Der paketfilternde Router kennt zwei Standardaktionen: Verweigern/Blockieren und Zulassen. Verweigern/Blockieren verbietet IP-Pakete, während Zulassen IP-Pakete passieren lässt.

Zur Verdeutlichung soll ein Beispiel dienen: Angenommen, jemand arbeitet in einer Organisation und verwaltet ein bestimmtes Projekt einer Universität. Das Projektnetzwerk ist 172.16.6.0, d. h. der IP-Adressbereich reicht von 172.16.6.0 bis 172.16.6.255. Die IP-Adressen der Universität sind 10.0.0.0-10.255.255.255. Die folgende Tabelle zeigt die drei Regeln für die Aufteilung von Paketen (Zwicky et al., 2000).

|  |  |  |  |
| --- | --- | --- | --- |
| Ein Beispiel für Sicherheitsregeln zur Paketfilterung | | | |
| Regel | Quelladresse | Zieladresse | Aktion |
| Α | 10.0.0.0/8 | 172.16.6.0/24 | Zulassen |
| B | 10.1.99.0/24 | 172.16.0.0/16 | Verweigern/Blockieren |
| C | Beliebig (\*) | Beliebig (\*) | Verweigern/Blockieren |

Die Regeln können folgendermaßen erklärt werden:

* Regel A erlaubt es der Universität, das Subnetz des Projekts zu erreichen.
* Regel B verhindert, dass die Universität das Netzwerk erreicht.
* Regel C blockiert jeden Internetzugang zum Netzwerk.

Die folgende Tabelle zeigt, wie eine Firewall die in der vorherigen Tabelle definierten Regeln (A, B und C) umsetzt.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Umsetzung der festgelegten Sicherheitsregeln aus der vorherigen Tabelle durch eine Firewall | | | | |
| Paket | Quell- adresse | Ziel- adresse | Gewünschte Aktion | Tatsächliche Aktion (nach Regel) |
| 1 | 10.1.99.1 | 172.16.6.1 | Zulassen | Zulassen (Regel A) |
| 2 | 192.168.3.4 | 172.16.6.1 | Verweigern/ Blockieren | Verweigern/Blockieren (Regel C) |
| 3 | 10.1.99.1 | 172.16.1.1 | Verweigern/ Blockieren | Verweigern/Blockieren (Regel B) |
| 4 | Beliebig | Beliebig | Verweigern/ Blockieren | Verweigern/Blockieren (Regel C) |

Die obige Tabelle zeigt Folgendes:

* Paket eins geht von einem Rechner der Universität zu einem Rechner im Subnetz des Projekts. Sie ist nach Regel A zulässig.
* Paket zwei wird von einem beliebigen (unbekannten) Rechner im Internet an einen der Projektrechner gesendet. Es wird durch Regel C verweigert (blockiert).
  + Paket drei geht von einem Universitätsrechner an eine zufällige Adresse im Netzwerk (nicht im Subnetz des Projekts). Sie wird durch Regel B verweigert.
  + Paket vier geht von einem beliebigen Rechner im Internet zu einem beliebigen Rechner im Subnetz des Projekts. Es wird durch Regel C verweigert (blockiert).

Eine detailliertere Tabelle könnte außerdem enthalten: (a) Quell- und Zielportnummern (so genannte „physische Schnittstellen“), (b) eine logische Schnittstelle mit virtuellen lokalen Netzwerkschnittstellen (VLAN), die erst nach der Konfiguration der physischen Schnittstelle konfiguriert werden können, und (c) ein IP-Feld mit der Definition des verwendeten Protokolls, wie zum Beispiel des Transmission Control Protocol (TCP) oder des User Datagram Protocol (UDP), über das erlaubte Protokolle herausgefiltert werden können. Das Protokollfeld ist im IP-Header lokalisiert.

Paketfilternde Firewalls haben drei wesentliche Vorteile (Bolar, 2020):

* + - 1. Sie können Pakete mit sehr hoher Geschwindigkeit verarbeiten.
      2. Die Sicherheit ist für Endnutzende transparent.
      3. Sie bieten Flexibilität bei der Implementierung von Sicherheitsrichtlinien (wie im obigen Beispiel gezeigt).

Trotz der Vorteile von paketfilternden Firewalls können sie Angriffe auf der Anwendungsschicht weder erkennen noch verhindern. Das liegt daran, dass Paketfilter-Firewalls die Daten der höheren Schichten nicht analysieren, weil sie den Inhalt der Datenpakete nicht betrachten. Außerdem unterstützen paketfilternde Firewalls keine Authentisierungsverfahren für Nutzer:innen und sind schwer zu kontrollieren.

Gateway auf Anwendungsebene

Im Gegensatz zu paketfilternden Firewalls filtern Gateways auf Anwendungsebene die Daten von Netzwerkanwendungen. Sie durchsuchen auch den Inhalt von Datenpaketen und analysieren so die Daten der Anwendungsschicht. Anhand eines realen Szenarios soll das Gateway auf Anwendungsebene erklärt werden: Eine Nutzerin versucht, auf eine bestimmte Anwendung oder einen bestimmten Dienst auf einem entfernten Host zuzugreifen. Sie greift auf das Gateway über eine Verbindung nach der Internet-Protokollfamilie (TCP/IP) zu, wie z. B. über das Dateiübertragungsprotokoll (FTP, engl. *File Transfer Protocol*). Bevor das Gateway die Anfrage bearbeitet, wird die Nutzerin authentifiziert, und nach erfolgreicher Authentifizierung kontaktiert das Gateway die Anwendung bzw. den Dienst auf dem entfernten Host.

Ein Gateway auf Anwendungsebene ist zwar sicherer als paketvermittelnde Firewalls, es benötigt aber mehr Verarbeitungszeit für die inhaltliche Prüfung von Datenpaketen und verursacht daher zusätzlichen Verarbeitungsaufwand (Bolar, 2020).

Gateway auf Leitungsebene

Gateways auf Leitungsebene überwachen das TCP-Handshaking zwischen den Paketen, um festzustellen, ob eine angeforderte Sitzung legitim ist. Angenommen, Nutzer:innen im lokalen Netzwerk möchten mit anderen Nutzern in einem externen Netzwerk kommunizieren. Das Gateway baut zwei TCP-Verbindungen auf, die erste mit den TCP-Nutzern auf dem lokalen Host, die andere mit den TCP-Nutzern auf einem externen Host. Sobald die beiden Verbindungen hergestellt sind, überträgt das Gateway TCP-Fragmente von einer Verbindung zur anderen über ein geschütztes Netzwerk. Daher verbergen Gateways auf Leitungsebene die Details des geschützten Netzwerks vor externem Verkehr. Die Sicherheitsfunktion der Gateways auf Leitungsebene besteht darin, festzulegen, welche Verbindungen zugelassen werden, und gleichzeitig Netzwerkinformationen vor externen Stellen zu verbergen.

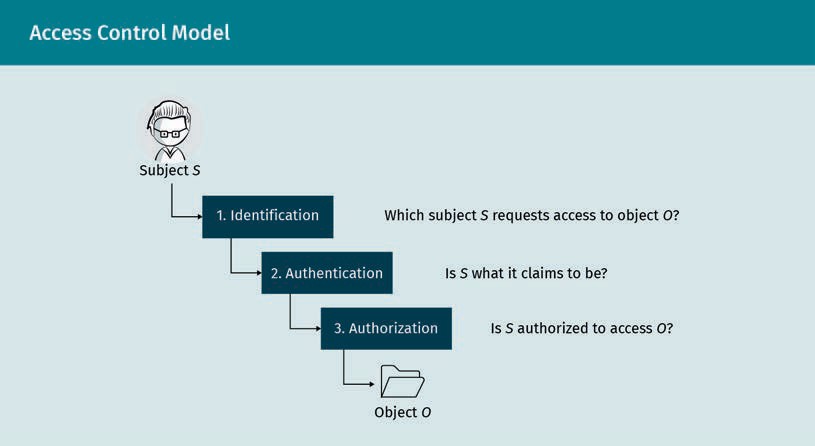
Allerdings filtern oder untersuchen sie keine einzelnen Pakete (Stallings & Brown, 2012). Gateways auf Leitungsebene werden in der Regel von Systemadministratoren eingesetzt, die den internen Nutzern vertrauen. Gateways auf Leitungsebene werden hauptsächlich für abgehende Verbindungen genutzt.

### Zugriffskontrolle

Über die Datenzugriffskontrolle wird der Zugriff auf sensible Daten oder Informationen (Dateien, Ordner usw.) in einer Organisation geregelt. Dabei wird das Prinzip der „geringsten Privilegien“ genutzt, d. h. die Verwaltung und Definition der Zugriffsrechte der Nutzenden (d. h. auf welche Daten oder Anwendungen sie Zugriff haben) basierend auf ihrer Rolle im Unternehmen.

Das bedeutet, dass jeder Nutzer bzw. jede Nutzerin durch ein Profil identifiziert wird, in dem die zulässigen Operationen und die Zugriffsrechte auf Dateien festgelegt sind. Das Betriebssystem überwacht die Einhaltung dieser Regeln. Ein allgemeines Zugriffskontrollmodell umfasst eine Zugriffsmatrix, wie in der folgenden Abbildung dargestellt. Die wesentlichen Elemente des Modells sind wie folgt:

* Subjekt: Dies ist die Entität, von der die Zugriffsanfrage ausgeht. Subjekte sind alle aktiven Parteien im System.
* Objekt: Dazu gehören alle Dinge, zu denen der Zugang geregelt ist. Objekte stellen die passiven Ressourcen eines Systems dar. Dazu gehören z. B. Dateien, Teile von Dateien, Programme und Speichersegmente.
* Zugriffsrechte: Die Arten möglichen Zugriffs einer Entität auf ein Objekt (z. B. lesen, schreiben oder ausführen).



Zugriffskontrollstrukturen sind Mechanismen zur Umsetzung von Zugriffsrichtlinien, wie z. B.:

* Zugriffskontrolltabellen,
* Fähigkeiten,
  + Zugriffskontrolllisten und
  + Zwischenkontrollen (Gruppen, negative Berechtigungen, Rollen und Schutzringe) (Zwicky et al., 2000).

|  |  |  |  |
| --- | --- | --- | --- |
| Ein Beispiel für eine Zugangsrichtlinie | | | |
|  | test.doc | test.exe | test.com |
| Alice | - | {Ausführen} | {Ausführen, Lesen} |
| Bob | {Lesen} | {Ausführen} | {Ausführen, Lesen, Schreiben} |

Anhand des Beispiels in der obigen Tabelle sollen drei Zugriffsrichtlinien betrachtet werden.

* + 1. Eine Zugriffskontrolltabelle ist ein grundlegender Kontrolldienst. Sie sorgt für eine klare Definition und einfache Verifizierung, ist aber schlecht skalierbar und kann nur schwer mit Änderungen umgehen.
    2. Eine Fähigkeit ist eine subjektbezogene Beschreibung von Zugriffsrechten. In diesem Fall hat Alice die Rechte (test.exe: Ausführen) und (test.com: Ausführen, Lesen), während Bob (test.doc: Lesen, Schreiben), (test.exe: Ausführen) und (test.com: Ausführen, Lesen, Schreiben) hat. Fähigkeiten erleichtern die Zugriffsrechte und definieren eindeutig die Eigentumsverhältnisse an den Daten. Allerdings machen sie die den Entzug der Rechte schwierig, ein Integritätsschutz ist erforderlich und es ist schwierig, die Zugriffsrechte für jedes Objekt einzusehen.
    3. Eine Zugriffskontrollliste (engl. *ACL, Access Control List*) ist eine objektzentrierte Beschreibung von Zugriffsrechten. In diesem Fall hat test.doc (Bob: Lesen, Schreiben), test.exe hat (Alice: Ausführen) und (Bob: Ausführen), während test.com (Alice: Ausführen, Lesen) und (Bob: Ausführen, Lesen, Schreiben) hat. Eine Zugriffskontrollliste macht es einfach, die Zugriffsrechte für Objekte zu sehen und erleichtert die Verwaltung durch Abstraktionen. Sie bietet jedoch nur einen unzureichenden Überblick über die Zugriffsrechte pro Subjekt. Auch der Entzug der Rechte sowie Freigabe sind bei ACLs schwierig.

### Angriffe im Zusammenhang mit Routern, Switches und Firewalls

Da offene Ports ein Sicherheitsrisiko darstellen, blockieren Firewalls manchmal Verbindungen, um das Netzwerk vor Angreifenden zu schützen. Daher sollte ein gut konfigurierter Router standardmäßig alle administrativen Schnittstellen/Ports zum Internet oder zu einem nicht vertrauenswürdigen Netzwerk blockieren. So sollten beispielsweise Dienste wie Telnet, Secure Shell Protocol (SSH), Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol Secure (HTTPS) und Simple Network Management Protocol (SNMP) nicht dem Internet ausgesetzt werden. Diese Dienste sind verschiedenen Angriffen ausgesetzt.

* Schwache Passwörter können es Angreifenden ermöglichen, über SSH auf physische Server zuzugreifen.
* Ransomware kann TCP-Ports öffnen und zur Weiterleitung bösartigen Datenverkehrs nutzen.
* Aufgedeckte Authentifizierungsdaten schaffen Möglichkeiten zur Umgehung der Schutzeinrichtungen (MTI Technology, 2018).

Manchmal können sich Angreifende zunächst den Zugriff zu einem Netzwerk verschaffen und dann die zulässigen Kommunikationspfade zwischen den Netzwerkgeräten durchqueren, um tieferen Zugriff zu erlangen. In diesem Fall können Angreifende ein angepasstes Firmware-Image auf den Router hochladen, das den Datenverkehr an einen Angreifer-Host weiterleitet oder einen Denial-of-Service-Angriff auslöst, indem es das Image neu konfiguriert (MTI, 2018). Programme auf einem Gerät werden mit Hilfe von Firmware ausgeführt.

Außerdem verfügen die meisten Router nicht über eine inkrementelle Patching-Funktion oder eine automatische Update-Funktion. Dementsprechend erfordern sie eine manuelle Installation des neuesten Firmware-Images. Das Herunterladen und Ausführen des neuesten Images erfordert es jedoch, dass der Router für kurze Zeit vom Netz genommen wird.

Anbieter nutzen dies, indem sie neue Firmware-Images nur registrierten Kunden zur Verfügung stellen, die für eine gültige Lizenz bezahlt haben oder noch über eine solche verfügen. Regelmäßige Updates oder Patches für die Netzwerkinfrastruktur sind daher ebenso wichtig wie Patches für Server und Workstations (MTI Technology, 2018).

###### Lösungen zur Entschärfung von Angriffen

Zur Eindämmung von Netzwerkangriffen können verschiedene Abwehrmaßnahmen eingesetzt werden. Dazu gehören die Abtrennung und Segmentierung von Netzwerken, die physische Trennung sensibler Daten, die virtuelle Trennung sensibler Daten, die Absicherung von Netzwerkgeräten und die Sicherung des Zugangs zu Infrastrukturgeräten.

Netzwerkabtrennung und ‑segmentierung

Angreifer, die den Host einer Organisation manipulieren, könnten versuchen, eine direkte Verbindung zu anfälligeren Hosts herzustellen. Wenn Angreifende den Kern des Netzwerks manipulieren, kann der Betrieb der Organisation erheblich gestört werden. Daher können Netzwerkabtrennung und ‑segmentierung dazu beitragen, solche Angriffe zu entschärfen. Bei der Netzwerksegmentierung wird das größere Netzwerk in kleinere Netzwerksegmente aufgeteilt. Dies kann durch den Einsatz von Firewalls, virtuellen lokalen Netzwerken (VLANs) und anderen Techniken erreicht werden. Bei der Netzwerkabtrennung werden die kritischen und sensibelsten Netzwerke (je nach Rolle und Funktionalität) vom Internet und anderen Netzwerken getrennt. Dementsprechend lauten die Empfehlungen wie folgt:

* Abtrennung von Hosts und Netzwerken, je nachdem wie kritisch diese für die Geschäftsabläufe des Unternehmens sind.
* Einsatz der besten Sicherheitspraktiken und ‑empfehlungen in allen Netzwerksegmenten und nicht nur auf der Netzwerkschicht (also von der Datenverbindungsschicht bis hin zur Anwendungsschicht).

Physische Trennung sensibler Informationen.

Normalerweise werden Router verwendet, um verschiedene LANs mit anderen Netzwerken zu verbinden. Sie sind so konzipiert, dass sie eine breite Netzwerkverbindung ermöglichen, Abgrenzungen schaffen und den Datenverkehr der Nutzer:innen filtern oder einschränken.

Mit diesen Abgrenzungen können Sicherheitsverletzungen minimiert werden, indem der Datenverkehr auf Netzwerksegmente beschränkt wird. Router können bei einem Sicherheitsverstoß sogar Netzwerksegmente isolieren, um Angreifende daran zu hindern, auf andere Segmente oder das Kernnetzwerk zuzugreifen (Cybersecurity and Infrastructure Security Agency, 2016). Dementsprechend wird empfohlen, bei den Konfigurationen aller Netzwerkschichten und ‑segmente bewährte Sicherheitsmethoden durchzusetzen.

Virtuelle Trennung sensibler Informationen

Die virtuelle Trennung ist ebenso wichtig wie die physische Trennung, da sie die Isolierung der Nutzerinnen und Nutzer, die Zugriffsrechte und den Zugriff auf logische Ressourcen umfasst. Dementsprechend lauten die Empfehlungen wie folgt:

* + Nutzung von Firewalls und VLANs, um nur berechtigten Nutzern den Zugriff auf die ihnen zugewiesenen Ressourcen zu ermöglichen und sensible Domänen von anderen Domänen zu isolieren.
  + Nutzung virtueller privater Netzwerke (VPNs) zum Tunneln von Hostverbindungen durch öffentliche Netze.

Härtung von Netzwerkgeräten

Zur Verbesserung der Sicherheit der Netzwerkinfrastruktur ist es wichtig, Netzwerkgeräte mit sicheren Konfigurationen zu schützen. Diese Konfigurationen sollten im Einklang mit Gesetzen, Vorschriften, Sicherheitsrichtlinien, Standards und bewährten Praktiken der Branche umgesetzt werden.

Dementsprechend lauten die Empfehlungen wie folgt:

* + Ausschließlich Nutzung gesicherter Protokolle für die Verwaltung der Netzwerkinfrastruktur (z. B. SSH statt Telnet und SCP (Secure Copy Protocol) anstelle von FTP).
  + Einführung strenger Passwortrichtlinien und Aktivierung der stärksten vom Gerät unterstützten Passwortverschlüsselung.
  + Einschränkung des physischen Zugangs zu Routern und Switches und Einsatz von Zugriffskontrolllisten für den Fernzugriff.
  + Überwachen und Protokollieren aller Zugriffsversuche auf Netzwerkgeräte.
  + Sichern der Konfigurationen und Offline-Speicherung
  + Verschlüsseln der Konfigurationsdateien beim Speichern und bei der Backup-Sicherung
  + Regelmäßiges Patchen aller Netzwerkgeräte (sobald ein neuer Patch veröffentlicht wird)
  + Regelmäßiges Testen der Sicherheitskonfigurationen durch Penetrationstests
  + Verschlüsseln der Konfigurationsdateien beim Speichern und bei der Backup-Sicherung
  + Beachten der Richtlinien von Grassi et al. (2020)

Sicherer Zugriff auf Infrastrukturgeräte

Normalerweise erlauben administrative oder Root-Zugriffsprivilegien (oder ‑rechte) auf Infrastrukturgeräten bestimmten Nutzerinnen und Nutzern (den sogenannten Admins oder Root-Nutzern) den vollen Zugriff auf die Infrastrukturgeräte. Sie können eine Reihe von Aktionen ausführen, die für andere nicht erlaubt sind. Wenn diese administrativen Rechte unsachgemäß definiert, in großem Umfang gewährt und nicht überprüft oder verifiziert werden, kann ein Eindringling diese Rechte ausnutzen, um vollen Zugriff auf und vollständige Kontrolle über den Netzwerkkern zu erhalten.

Die Durchsetzung einer angemessenen Sicherheitsrichtlinie kann den unbefugten Zugang zur Infrastruktur eindämmen (Cybersecurity and Infrastructure Security Agency, 2016). Dementsprechend lauten die Empfehlungen wie folgt:

* Implementierung der Multi-Faktor-Authentifizierung mit Hardware-Tokens und Passwörtern
* Speicherung des Zugriffs von Netzwerkgeräten mit Hilfe eines Autorisierungsservers (d. h. zur Verwaltung des privilegierten Zugriffs)
* Verwaltung der administrativen Anmeldeinformationen (oder, für Systeme, die keine Multi-Faktor-Authentifizierung implementieren und nutzen können: die Durchsetzung strenger Passwortrichtlinien)

Zusammenfassung

Diese Lektion vermittelte einen Überblick über die Funktionsweise und die Konstruktionsprinzipien von Firewalls und vertrauenswürdigen Systemen. Zuallererst wurden die verschiedenen Geräte der Netzwerkinfrastruktur detailliert beschrieben. Jedes dieser Geräte wurde spezifiziert und es wurde gezeigt, wie diese Geräte in einem gesicherten Netzwerk verbunden sind. Zweitens wurde die Sicherheit von Firewalls dargestellt und die Fähigkeiten, Einschränkungen sowie die unterschiedlichen Firewall-Arten erläutert. Zu jeder Firewall-Art wurden die Vorteile und Beschränkungen besprochen. Praktische Beispiele sollten verdeutlichen, wie die Sicherheitsrichtlinien einer Firewall funktionieren. Außerdem wurde in dieser Lektion ein allgemeines Modell für die Datenzugriffskontrolle entwickelt. Es wurden verschiedene Arten von Zugriffsrichtlinien vorgestellt und die Implementierung von Zugriffsrichtlinien beispielhaft gezeigt, einschließlich der Vor- und Nachteile jeder Richtlinie.

Schließlich ist das Verständnis der Bedrohungen für Netzwerkinfrastrukturen sowie die Lösungen zu ihrer Eindämmung sehr wichtig. In dieser Lektion wurden deshalb die Bedrohungen für die Netzwerkinfrastrukturgeräte und mögliche Abwehrmaßnahmen dagegen beschrieben, zusammen mit einer kurzen Erläuterung der einzelnen Abwehrmaßnahmen und den passenden Empfehlungen.



# Lektion 3

## Kryptographie

#### LERNZIELE

Nach Abschluss dieser Lektion werden Sie …

… die Grundlagen der Kryptographie und der Netzwerksicherheit verstehen.

… beschreiben können, wie Sie eine Nachricht über einen unsicheren Kanal auf   
verschiedene Weise sichern können.

… erklären können, wie die Vertraulichkeit und Integrität von Daten gewahrt wird.

DL-E-DLMCSEESN01\_E-U03

1. Kryptographie

### Einführung

Netzwerkprotokolle übertragen potenziell sensible Informationen zwischen verschiedenen Parteien in einem Netzwerk. Diese Informationen können Kreditkartendaten, Patienten-Gesundheitsdaten, vertrauliche amtliche Informationen oder andere Daten dieser Art sein. Folglich ist es unerlässlich, diese Informationen zu sichern. Beim Entwurf eines Systems oder Protokolls müssen deshalb viele Sicherheitsanforderungen berücksichtigt werden. Dennoch tauchen im Laufe der Zeit häufig Schwachstellen auf, insbesondere wenn ein Protokoll in öffentlichen Netzwerken genutzt wird, wo jeder am Datenverkehr Beteiligte es angreifen kann. Alle sicheren Protokolle sollten Folgendes leisten können (Zend Framework, o. D.):

* + Schutz der Daten vor dem Auslesen (Vertraulichkeit der Daten).
  + Schutz der Daten vor Änderungen (Datenintegrität).
  + Implementierung von Server- und Client-Authentifizierung, damit Angreifende sich nicht fälschlicherweise als Server oder Client ausgeben können.

In dieser Lektion werden verschiedene Sicherheitstechniken vorgestellt, die diese Anforderungen in den gängigen Netzwerkprotokollen erfüllen. Diese Techniken basieren auf der Kryptographie. Der Begriff kommt aus dem Griechischen und setzt sich aus *Krypto,* was geheim oder verborgen bedeutet und *Graphie* zusammen, was für Schreiben steht (Schneier, 2015).

Die folgenden zwei Methoden werden zum Schutz von Daten verwendet:

**Verschlüsselung**  
Hierbei handelt es sich um einen Vorgang, bei dem eine ursprüngliche Nachricht (Klartext) in eine verschlüsselte Form (Chiffretext) umgewandelt wird. So wird die Vertraulichkeit der Daten mit Hilfe einer Verschlüsselung und dem zugehörigen Schlüssel gewährleistet.

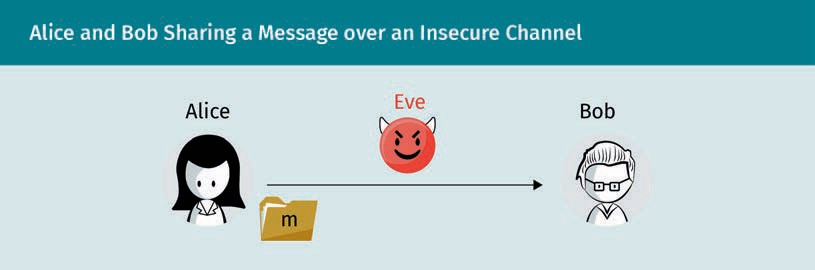
1. **Verschlüsselung (engl. Encryption)**. Dies gewährleistet die Vertraulichkeit der Daten.
2. Digitale Signatur und Hashing. Diese sorgen für Authentifizierung und Datenintegrität.

Obwohl Verschlüsselung und Signierung in vielen Netzwerkprotokollen verwendet werden, ist die korrekte Implementierung von Kryptographie meist nicht einfach. Fehler im Protokolldesign oder in der Hardware-Implementierung führen häufig zu Schwachstellen, welche die Korrektheit und Sicherheit eines Protokolls beeinträchtigen können. Daher ist bei der Analyse eines Systems oder Protokolls ein fundiertes Verständnis der beteiligten Algorithmen und Technologien erforderlich, um ernsthafte Schwachstellen oder mögliche Angriffspunkte zu erkennen.

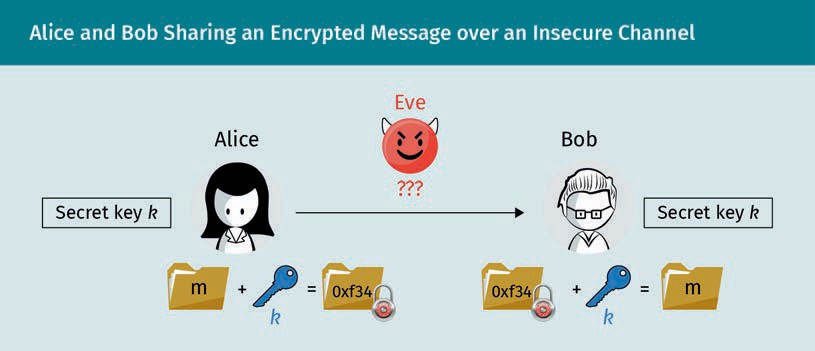
In dieser Lektion wird erläutert, wie die Vertraulichkeit mit zwei wichtigen Verschlüsselungsalgorithmen, der symmetrischen und der asymmetrischen Kryptographie, sichergestellt werden kann. Außerdem wird die Gewährleistung der Integrität und Authentizität von Nachrichten mit Hilfe von Hash-Funktionen und digitalen Signaturen erörtert.

### Verschlüsselungsalgorithmus

Zur Erklärung der Verschlüsselung sei angenommen, dass zwei vertrauenswürdige Parteien (Alice und Bob) eine Nachricht austauschen müssen. Ein Eindringling (Eve) lauscht auf dem unsicheren Kanal und will sich die Nachricht zu eigen machen (entweder durch lesen oder modifizieren), wie die folgende Abbildung zeigt.



Um zu verhindern, dass Eve die Nachricht für sich ausnutzt, sollte diese verschlüsselt werden. Die ursprüngliche Nachricht *m* wird von Alice an Bob gesendet. Sie ist unverschlüsselt und wird als **Klartext** *m* bezeichnet. Die Ausgabe des Verschlüsselungsalgorithmus ist eine verschlüsselte Nachricht, der sogenannte **Chiffretext** *"*. Die meisten Algorithmen benötigen auch einen Schlüssel für die Verschlüsselung *E* und Entschlüsselung *D,* wie in der folgenden Abbildung dargestellt.



Einige Verschlüsselungsalgorithmen funktionieren ohne komplexe Mathematik, weil sie lediglich die Struktur des Protokolls im Netzwerk verschleiern. Unter Datenverschleierung wird ein Vorgang zum Schutz von Daten verstanden, bei dem diese mit Sonderzeichen oder anderen Daten verändert werden. Die folgenden Lernzyklen erteilen einen Überblick über einige Standard-Verschlüsselungsalgorithmen. In dieser Lektion werden nur die verwendeten kryptographischen Algorithmen betrachtet, ohne dabei auf mathematische Beweise und Details der Algorithmenentwicklung einzugehen.

### Kryptographie mit symmetrischem Schlüssel

Bei der symmetrischen Kryptographie haben alle Parteien denselben Schlüssel für die Ver- und Entschlüsselung, wie es die folgende Abbildung zeigt.

**Klartext**

Die ursprüngliche Nachricht, die übermittelt werden muss.

**Chiffretext**

Die verschlüsselte Klartextnachricht.

**Entschlüsselung**

Der Prozess, bei dem eine verschlüsselte Nachricht (Chiffretext) mithilfe eines Entschlüsselungsschlüssels in ihr ursprüngliches Format (Klartext) zurückverwandelt wird.



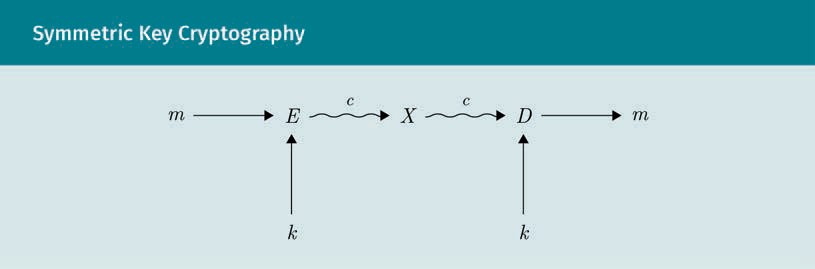
###### Definition

Um nach der Entschlüsselung des Chiffretextes (also der verschlüsselten Nachricht) wieder dieselbe Nachricht zu erhalten, muss die folgende Korrektheitseigenschaft für *∀m ∈ M*, *∀k ∈ K* gelten (Schneier, 2015):

*E*: *M*´*K* : *m*, *k " D*:´*K M* : *"*, *k m*

Hierbei gilt:

* *m* ist eine Klartextnachricht aus der Menge *M* aller möglichen Nachrichten,
* *k* ist der Schlüssel aus der Menge *K* aller möglichen Schlüssel, und *"* ist ein Chiffretext aus der Mengealler möglichen Chiffretexte, sowie
* *E* ist die Verschlüsselungsfunktion, *+* ist ein möglicher Lauscher auf dem unsicheren Kanal, und *D* ist die Entschlüsselungsfunktion.



Die Korrektheit der symmetrischen Verschlüsselung hängt vom Schlüssel ab. Es gibt also zwei Haupteigenschaften des Schlüssels (Schneier, 2015):

1. *k* wird zufällig und unterschiedslos aus *K* ausgewählt. Das bedeutet, jeder Schlüssel wird mit gleicher Wahrscheinlichkeit gewählt, und es ist nicht vorhersehbar welcher Schlüssel es sein wird.
2. *k* wird so geheim gehalten, dass der Gegner den Schlüssel nicht erfahren kann. Gleichzeitig kann der Schlüssel aber auch sicher zwischen den beiden Entitäten ausgetauscht werden (z. B. kann er durch einen vertrauenswürdigen Dritten ausgetauscht werden, ohne seine Geheimhaltung zu gefährden).

###### Moderne symmetrische Chiffren

Es gibt zwei Haupttypen von symmetrischen Chiffren: Block- und Stromchiffren. Jede hat ihre Vor- und Nachteile. Die Wahl der falschen Chiffre ermöglicht es Angreifenden, die Sicherheit der Kommunikation zu kapern (Schneier, 2015). Es ist wichtig, die folgenden Eigenschaften dieser Chiffren zu verstehen:

* Eine Stromchiffre besteht aus einem Datenstrom mit kleinen Datenpaketen, die ein einzelnes Bit, Byte oder Zeichen sein können und in der Regel 1 Byte groß sind. Sie werden eines nach dem anderen verschlüsselt.
* Eine Blockchiffre besteht aus in Blöcke fester Größe unterteilten Datenpaketen. Sie werden blockweise verschlüsselt. Die Blockgröße beträgt mindestens 64 Bit und bis zu 128 oder 256 Bit.

Nehmen wir zum Beispiel an, dass wir ein Buch verschlüsseln wollen. In diesem Fall verschlüsseln wir entweder einen Buchstaben oder ein Wort nach dem anderen (Stromchiffre) oder eine Seite nach der anderen (Blockchiffre). Jede der beiden Chiffren wurde für unterschiedliche Zwecke entwickelt, wie später noch erläutert wird.

Der *Advanced Encryption Standard* (AES) ist die gebräuchlichste Blockchiffre mit symmetrischem Schlüssel. Beim AES wird eine feste Blockgröße von 128 Bit als Eingabe und eine Schlüsselgröße von 128, 192 oder 256 Bit verwendet. AES löst den *Data Encryption Standard* (DES) ab, der mit einer Blockgröße von 64 Bit als Eingabe arbeitete (Schneier, 2015). AES arbeitet mit einem 4×4-Byte-Feld. Zum Beispiel werden 16 Bytes *,*0, *,*1, …, *,*15 dargestellt als:

*,*0 *• ,*12

*,*3 *• ,*15

Der AES arbeitet mit exklusivem ODER (XOR) und hat zwei Hauptoperationen, SubBytes (S-Box) und Shiftrows. S-Box mischt die Daten in nicht-linearer Weise, wohingegen Shiftrows die Bits um einen bestimmten Abstand (Offset) verschiebt.

AES funktioniert über die Kombination der Operationen S-Box und Shiftrows mit XOR, und würfelt so die Daten durcheinander. Dieser Vorgang findet mehrmals und über viele Durchgänge (Runden) statt. Die Anzahl der Runden hängt von der Schlüsselgröße ab (z. B. 10 Runden für die kleinste AES-Schlüsselgröße von 128 Bit). Angenommen, eine Nachricht soll mit *0* Bits (wobei *0* kleiner als 128 Bits ist) mit AES verschlüsselt werden. Wie bereits erwähnt, wird bei AES jedoch eine Blockchiffre von 128 Bit genutzt. Deshalb wird die Nachricht mit Nullen oder Einsen aufgefüllt, bis die erforderliche Länge erreicht ist. Das Auffüllen mit Nullen *(Zero Padding)* ist hierbei die einfachste Form (Schneier, 2015).

###### Blockchiffre-Betriebsarten

Der Algorithmus einer Blockchiffre beschreibt, wie die Chiffre die Datenblöcke verarbeitet. Allerdings leiden Blockchiffrieralgorithmen an einigen inhärenten Schwächen. Für eine höhere Sicherheit wird in einem realen Protokoll meist eine Blockchiffre mit einem anderen Algorithmus kombiniert, was als Betriebsart bezeichnet wird. Dies kann zum Beispiel geschehen, um den Chiffretext komplexer und damit weniger vorhersehbar zu machen. Die folgende Tabelle stellt einige der gebräuchlichsten Blockchiffre-Betriebsarten dar.

|  |  |  |
| --- | --- | --- |
| Blockchiffre-Betriebsarten | | |
| Modellname | Abkürzung | Betriebsart |
| Elektronisches Codebuch *(Electronic codebook)* | ECB | Block |
| Chiffrierte Blockverkettung *(Cipher block chaining)* | CBC | Block |
| Ausgaberückführung *(Output feedback)* | OF | Stream |
| Chiffrierte-Rückführung *(Cipher feedback)* | CFB | Stream |
| Stromzählung *(Stream counter)* | CTR | Stream |
| Galois-Zähler-Modus *(Galois counter mode)* | GCM | Strom mit Datenintegrität |

Blockchiffren haben unter anderem folgende Nachteile:

* + Langsame Verschlüsselung: Die Daten müssen in Blöcke aufgeteilt werden, bevor der Verschlüsselungsalgorithmus einsetzt. Außerdem müssen Klartexte zum Erreichen der Blocklänge meist aufgefüllt werden, wie auch bei AES.
  + Fehlerfortpflanzung: Ein Fehler in einem Symbol kann dazu führen, dass ein ganzer Block beschädigt wird.

###### Zufallszahlengeneratoren

Kryptografische Systeme sind in hohem Maße auf Zufallszahlen guter Qualität angewiesen. Wirklich zufällige Daten zu erhalten ist jedoch schwierig, denn Computer sind von Natur aus deterministisch, d. h., sie produzieren bei derselben Eingabe immer dieselbe Ausgabe. Deshalb verfügen kryptografische Bibliotheken über Pseudozufallszahlengeneratoren (PRNGs), die aus einem Anfangswert eine Zahlenfolge erzeugen, die theoretisch ohne Kenntnis des internen Zustands des Generators nicht vorhersehbar sein sollte (Forshaw, 2017).

###### Stromchiffren

Wie bereits erwähnt, verschlüsseln Stromchiffren kleine Datenpakete. Grundsätzlich erzeugt eine Stromchiffre aus einem anfänglichen Schlüssel einen pseudozufälligen Strom von Bits (genannt Schlüsselstrom), der dann arithmetisch mit einer Nachricht verknüpft wird. Der Chiffretext kann zum Beispiel durch eine XOR-Operation aus der Nachricht und dem Schlüsselstrom erzeugt werden. Stromchiffren sind also viel schneller als Blockchiffren, da sie jeweils nur ein Bit der Daten verschlüsseln und nicht ganze Blöcke. Außerdem ist einer der wichtigsten Vorteile von Stromchiffren gegenüber Blockchiffren, dass sie keine Auffüllung benötigen. Darüber hinaus sind Blockchiffren leistungsfähigere Objekte mit einer komplizierteren Schnittstelle.

### Schlüsselverteilung

Bei symmetrischen Chiffren verfügen alle beteiligten Parteien über denselben Schlüssel, der für die Ver- und Entschlüsselung genutzt wird. Wie bereits erwähnt, basiert die Korrektheit der Chiffre auf der Geheimhaltung des Schlüssels. Zur Kommunikation untereinander müssen die beteiligten Parteien denselben geheimen Schlüssel haben. Folglich muss dieser Schlüssel ohne Preisgabe an andere zwischen den Kommunikationsparteien ausgetauscht werden. Vor dem Aufkommen moderner Computer wurde dazu ein Codebuch verwendet, das physisch an die beteiligten Parteien verteilt wurde. Dies ist jedoch unpraktisch, da Codebücher gestohlen, kopiert oder manipuliert werden können. Heutzutage gibt es verschiedene Möglichkeiten zum Teilen eines sicheren Schlüssels.

###### Paarweise geteilte Schlüssel

Ein paarweise geteilter Schlüssel ist ein sicherer Schlüssel, der nur von zwei kommunizierenden Parteien verwendet wird. Das bedeutet, dass jeweils zwei kommunizierende Parteien einen anderen geheimen Schlüssel benötigen, selbst wenn sie Teil einer größeren Gruppe sind. Diese Art von Schlüssel ist sehr effizient, wenn nur wenige Kommunikationspartner beteiligt sind. Es wird jedoch aufwendig, wenn viele Parteien beteiligt sind, da die Anzahl der erzeugten Schlüssel steigt.

Gehen wir von *0* Personen aus. Die erste Person muss mit allen anderen (außer sich selbst) je einen geheimen Schlüssel erstellen. Folglich werden im ersten Schritt *0−* 1 Schlüssel erstellt. Als nächstes muss die zweite Person je einen geheimen Schlüssel mit allen anderen außer sich selbst und der ersten Person erstellen, weil dieser ja bereits existiert. Daher werden im zweiten Schritt, *0−* 2 Schlüssel erstellt. Entsprechend erstellen *0* Personen die erforderlichen Schlüssel. Insgesamt werden also *0−* 1 + *0−* 2 + *0−* 3 … + 3 + 2 + 1 Schlüssel erstellt. Durch arithmetische Umformung ist die Gesamtsumme der erstellten Schlüssel für *0* Personen also:

*0−* 1 i= n n *−* 1

*2* = 1 2

Beispiel:

Angenommen, wir haben ein Netzwerk mit 100 Personen (*0* = 100), die paarweise gemeinsame Schlüssel brauchen. Die Anzahl der erstellten Schlüssel ist also:

99 i= 100 100 *−* 1

= 4950

*2* = 1 2

Für eine Gruppe von109 Personen benötigen wir ungefähr 5,0 x 1017 unterschiedliche Schlüssel für je zwei Kommunikationspartner (Schneier, 2015).

###### Vertrauenswürdige Drittpartei

Eine vertrauenswürdige dritte Partei (Trusted Third Party, TTP) ist eine vertrauenswürdige Instanz, die verlässlich die geheimen Schlüssel der kommunizierenden Instanzen teilt. Die Kommunikationspartner könnten genauso gut einen von der TTP erstellten Schlüssel für ihre Kommunikation nutzen. Angenommen, die beiden Parteien *3* und *4* wollen miteinander kommunizieren. *3* kann den Schlüssel *k34* erzeugen und ihn über die TTP mit *4* teilen (indem *3* den Schlüssel an die TTP schickt und diese ihn dann sicher an *4* weiterleitet) oder auch umgekehrt. Genauso gut kann die TTP den Schlüssel *k34* erzeugen und ihn dann auf sichere Weise mit *3* und *4* teilen. Es gibt jedoch einige Nachteile bei der Verwendung einer TTP:

* Die TTP hat Zugriff auf *k34* und kann daher alle Nachrichten zwischen *3* und *4* über den unsicheren Kanal abhören.
* Die TTP kann zu einem Man-in-the-Middle-Angreifenden werden, der sich bei der Kommunikation mit *4* als *3* ausgibt, oder umgekehrt.

Daher ist das Verfahren mit einer TTP nicht besonders sicher.

###### Diffie-Hellman-Schlüsselaustausch

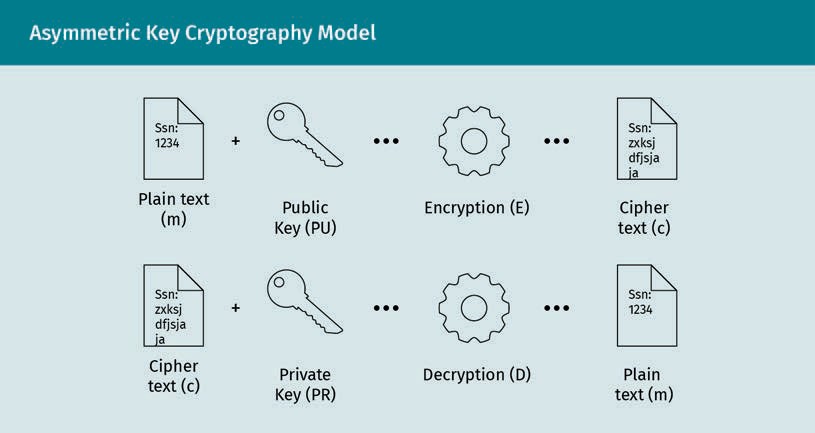
Das Verfahren nach Diffie-Hellman (DH) ermöglicht zwei Teilnehmenden in einem Netzwerk den Schlüsselaustausch und verhindert zugleich, dass jemand, der das Netzwerk belauscht, diesen Schlüssel herausbekommt. Allerdings ist DH nicht perfekt. Diese Basisversion des Algorithmus ist beispielsweise nicht in der Lage, Angreifende abzuwehren, die einen Man-in-the-Middle-Angriff auf den Schlüsselaustausch durchführen (Schneier, 2015).

Wollen sich beispielsweise Alice und Bob für Ihren Nachrichtenwechsel auf einen gemeinsamen Schlüssel einigen, so hängt die Geheimhaltung des gemeinsamen Schlüssels von den öffentlichen Schlüsseln von Alice und Bob ab. Eve (eine eindringende Person) kann jedoch den öffentlichen Schlüssel von Alice abfangen und ihren eigenen öffentlichen Schlüssel an Bob senden. Auf ähnliche Weise kann Eve Bobs öffentlichen Schlüssel abfangen und einen eigenen Schlüssel an Alice senden. Eve einigt sich also auf einen gemeinsamen Schlüssel mit Alice und auf einen weiteren gemeinsamen Schlüssel mit Bob. Alice und Bob glauben jedoch, dass sie denselben Schlüssel haben. Alice verschlüsselt also arglos jede gesendete Nachricht mit dem Schlüssel, den sie mit Eve teilt. Eve entschlüsselt dann die Nachricht und verschlüsselt sie erneut über den mit Bob geteilten Schlüssel.

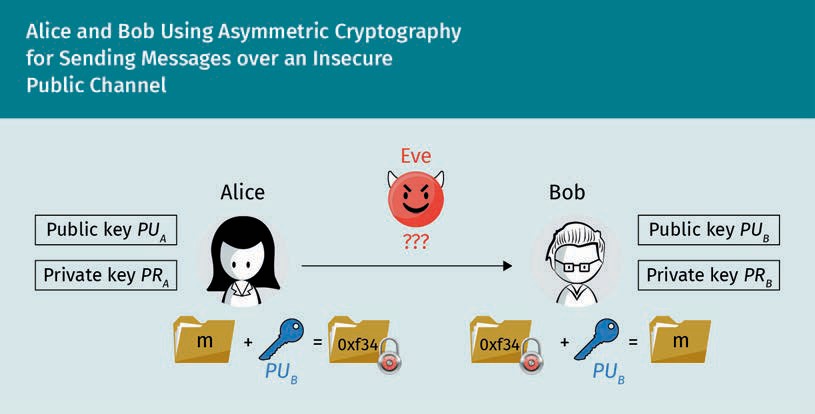
Eve kann nicht nur auf alle Nachrichten zwischen Alice und Bob zugreifen, sondern auch ihre eigenen Nachrichten im Namen von Alice oder Bob versenden. Diese Sicherheitslücke kann auftreten, weil DH die beteiligten Parteien nicht authentifiziert. Um dieses Problem zu lösen, können digitale Signaturen verwendet werden.

### Kryptographie mit asymmetrischem Schlüssel

Bei der asymmetrischen Kryptographie gibt es unterschiedliche Schlüssel für die Ver- und Entschlüsselung. Die Nachricht wird mit dem öffentlichen Schlüssel *5U* (der nicht geheim ist) verschlüsselt und mit dem privaten Schlüssel *5R* (der geheim bleiben sollte) entschlüsselt, wie in der folgenden Abbildung gezeigt. Asymmetrische Kryptosysteme sind auch als Public-Key-Kryptosysteme bekannt.



Angenommen, wir haben zwei Parteien, Alice und Bob. Alice möchte eine vertrauliche Nachricht über einen unsicheren Kanal an Bob senden. Alice und Bob teilen keinen geheimen Schlüssel, aber Alice hat den öffentlichen Schlüssel *5 R4* von Bob, und Bob hat seinen privaten Schlüssel *5 R4*, der geheim ist und zum öffentlichen Schlüssel *5U4* gehört. Nachrichten, die mit Bobs öffentlichem Schlüssel *5U4* verschlüsselt wurden, können nur mit Bobs privatem Schlüssel *5 R4* entschlüsselt werden, wie in der folgenden Abbildung dargestellt.



Alice sendet also eine mit Bobs öffentlichem Schlüssel *5U4* verschlüsselte Nachricht, und Bob entschlüsselt die Nachricht mit seinem privaten Schlüssel *5 R4*. Im umgekehrten Fall, wenn also Bob eine Nachricht an Alice senden möchte, sendet er die Nachricht verschlüsselt mit dem öffentlichen Schlüssel von Alice *5U3*, und Alice entschlüsselt die Nachricht mit ihrem eigenen privaten Schlüssel *5 R3*.

Die Korrektheitseigenschaft ist also (Schneier, 2015):

*D5 R4 E5 U4 m* = *m*

Hierbei gilt:

* *m* ist eine Klartextnachricht aus der Menge *M* aller möglichen Nachrichten.
* *5U4* ist der öffentliche Schlüssel von Bob, *5 R4* ist Bobs privater Schlüssel, und *"* ist ein Chiffretext aus der Mengealler möglichen Chiffretexte: *"* = *E5 U4 m.*
* *E* ist die Verschlüsselungsfunktion, und *D* ist die Entschlüsselungsfunktion: *D5 R4 "* = *m.*
* *5U3* ist der öffentliche Schlüssel von Alice, und *5 R3* ist der private Schlüssel von Alice.

###### RSA-Kryptosysteme

RSA, die Abkürzung für Rivest, Shamir und Adleman, ist das am häufigsten für die sichere Datenübertragung verwendete (asymmetrische) Public-Key-Kryptosystem. Die symmetrische Verschlüsselung funktioniert mit einem schnelleren Algorithmus als die asymmetrische, weil die Erstellung eines Paares aus öffentlichem und privatem Schlüssel mehr Zeit kostet. Deshalb wird RSA zur Verschlüsselung von Nutzerdaten nur selten eingesetzt. RSA wird häufig zur Übertragung von gemeinsamen geheimen Schlüsseln in der symmetrischen Kryptographie verwendet.

### Signaturalgorithmen

Die Verschlüsselung einer Nachricht wahrt die Vertraulichkeit der Daten, indem sie Angreifende daran hindert, die über das öffentliche Netzwerk gesendeten Daten zu erkennen. Die Identität der sendenden Partei wird jedoch nicht überprüft. In einem symmetrischen Kryptosystem reicht der Besitz des geheimen Schlüssels nicht aus, um die Identität des Senders oder Empfängers zu überprüfen. Außerdem kann in einem asymmetrischen Kryptosystem jeder Netzwerkteilnehmer den öffentlichen Schlüssel eines anderen Teilnehmers besitzen. Der Besitz eines öffentlichen Schlüssels verifiziert also nicht die Identität des Absenders. Dieses Problem wird mit Hilfe von Signaturalgorithmen gelöst, bei denen eine eindeutige Signatur für eine Nachricht erzeugt wird. Zunächst soll die reguläre physische Signatur beschrieben werden, bevor die digitale Signatur erklärt wird.

Physische Signaturen werden zur Authentifizierung von Dokumenten verwendet. Wenn ein Dokument von einer Person unterzeichnet wird, bedeutet dies, dass der Unterzeichner für den Inhalt des Dokuments verantwortlich ist. Darüber hinaus kann das Eigentum an dem Dokument durch die eindeutige Unterschrift des Unterzeichners verifiziert werden. Physische Signaturen sind jedoch für das Signieren digitaler Dokumente nicht sicher genug, weil eine Signatur kopiert oder ein Dokument nach dem Signieren verändert werden kann.

Eine digitale Signatur funktioniert anders: Sie erzeugt mit Hilfe der Nachricht einen Code (oder eine Signatur), welcher der Nachricht vor dem Sendevorgang hinzugefügt wird. Wenn ein Buchstabe in der Nachricht geändert wird, sollte sich auch die Signatur ändern, was die Datenintegrität gewährleistet. Bevor das Signaturverfahren näher beleuchtet wird, sollen zunächst kryptographische Hash-Algorithmen beschrieben werden. Alle Signaturalgorithmen basieren auf einer Hash-Funktion.

###### Kryptographische Hash-Funktion

Kryptographische Hashing-Algorithmen *H* sind Funktionen, die für jede Nachricht " = *H m* einen eindeutigen Wert mit fester Länge erzeugen (Streuwertfunktion). Hierbei ist *m* die Nachricht, und " ist der gehashte Ausgabewert. Mit Hashing wird also zur Überprüfung der Integrität einer Nachricht ein eindeutiger Wert erzeugt, weil jede Nachricht idealerweise genau einen Hash-Wert hat. Eine Hashing-Funktion muss die folgenden Bedingungen erfüllen:



1. Schwierige Rückgewinnung des Eingabewerts: Es sollte schwierig sein, eine Nachricht aus dem Hash-Wert wiederherzustellen.
2. Schwacher Kollisionsschutz: Für ein gegebenes " = *H m*  ist es schwer, ein anderes m′ zu finden, sodass *H m*′ = " gilt.
3. Starker Kollisionsschutz: Es sollte schwierig sein, aus zwei unterschiedlichen Nachrichten denselben Hash-Wert zu erzeugen. Es ist schwer, zwei Nachrichten *m*1 und *m*2 zu finden, sodass *H m*1 = *H m*2 gilt.

Zu den gängigsten Hash-Algorithmen gehören *Message Digest* (z. B. MD5) und der sichere Hash-Algorithmus (*Secure Hashing Algorithm*, SHA-1, SHA-2). MD5 gilt jedoch nicht mehr als sicher und wird daher nur noch selten genutzt. Auch SHA-1 wird kaum mehr verwendet. Derzeit ist SHA-2 die sicherste Hash-Funktion. Sie gibt entweder 256 Bits (SHA-256) oder 512 Bits (SHA-512) aus.

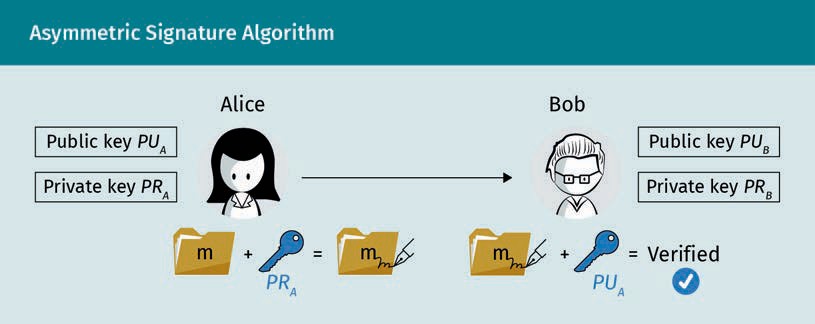
###### Asymmetrische Signaturalgorithmen

Asymmetrische Signaturalgorithmen erzeugen Signaturen mit Hilfe der Eigenschaften der Public-Key-Kryptographie. Dazu wird die zu signierende Nachricht gehasht, und aus dem Hashwert wird eine Signatur erzeugt. Weitere Einzelheiten sind im praktischen Beispiel im nächsten Lernzyklus zu finden.

Zuvor wurde gezeigt, dass RSA als Verschlüsselungsmethode eingesetzt werden kann. Dabei wird mit dem öffentlichen Schlüssel verschlüsselt und mit dem privaten Schlüssel entschlüsselt. Bei Signaturen wird der RSA-Signaturalgorithmus verwendet, bei dem es umgekehrt funktioniert: Die Nachricht wird mit dem privaten Schlüssel verschlüsselt (signiert) und dann mit dem öffentlichen Schlüssel verifiziert.

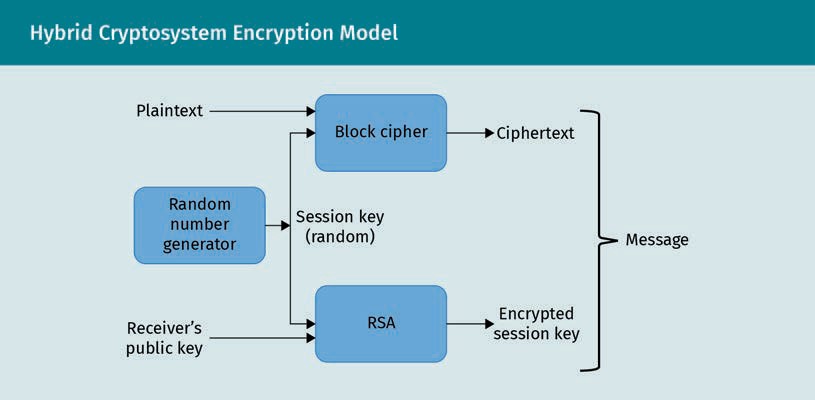
Als Beispiel dienen erneut Alice und Bob, wie in der folgenden Abbildung dargestellt. Alice signiert eine Nachricht und sendet sie an Bob. Dieser soll die Nachricht lesen können und wissen, dass diese wirklich von Alice stammt. Das bedeutet, dass Alice die Nachricht *m* hasht und die gehashte Nachricht dann mit ihrem privaten Schlüssel *5 R3* (der nur ihr bekannt ist) verschlüsselt.

Dieser verschlüsselte Hash ist die Signatur. Jeder, der über den öffentlichen Schlüssel *5 K3* von Alice verfügt (einschließlich Bob), kann die Nachricht entschlüsseln und überprüfen, ob sie wirklich von Alice gesendet und nicht verändert wurde.



###### Hybride Kryptosysteme

Hybride Verschlüsselungssysteme nutzen sowohl symmetrische als auch asymmetrische Kryptographiemethoden. Bei diesem Ansatz werden die Schlüssel per asymmetrischer Schlüsselkryptographie sicher getauscht und Nachrichten über symmetrische Verschlüsselung verschlüsselt. Der Hybridmodus kann in Mehrbenutzerszenarien eingesetzt werden, in denen die Entschlüsselung auf bestimmte Nutzende beschränkt werden soll. Wenn Alice eine Nachricht mit einem hybriden Kryptosystem an Bob schicken möchte, muss sie Folgendes tun (Zend Framework, o. D.):

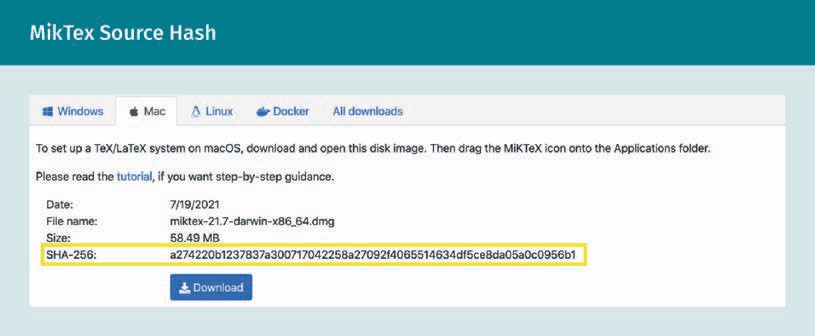
* 1. Bobs öffentlichen Schlüssel abrufen.
  2. Generieren eines zufälligen Sitzungsschlüssels (eine Einmalverschlüsselung, *One-Time-Pad*, OTP).
  3. Verschlüsseln der Nachricht mit einer symmetrischen Chiffre und dem o. g. Sitzungsschlüssel.
  4. Verschlüsseln des Sitzungsschlüssels mit Bobs öffentlichem Schlüssel.
  5. Senden der verschlüsselten Nachricht und des verschlüsselten Sitzungsschlüssels an Bob. Ein Schema der Verschlüsselung ist in der folgenden Abbildung dargestellt.

### Praktische Beispiele

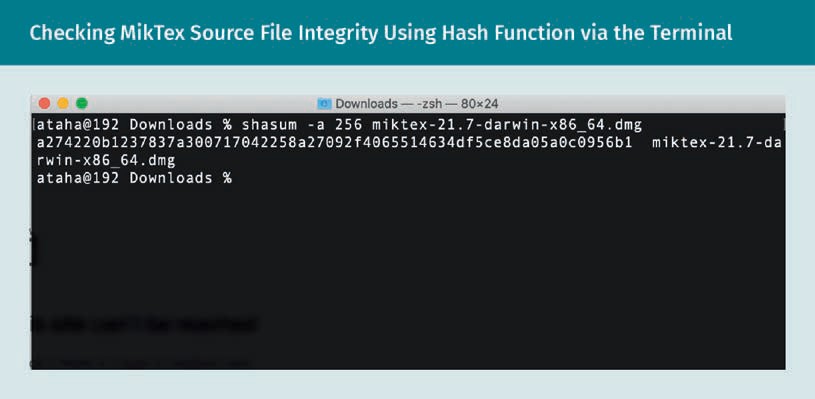
In diesem Lernzyklus finden sich praktische Szenarien zum Verständnis der oben vorgestellten Algorithmen.

###### Hashing-Algorithmus

Angenommen, Sie möchten eine Software herunterladen (z. B. MiKTeX) und dabei sicherstellen, dass die richtige Software und keine bösartige installiert wird. Einige Softwarehersteller veröffentlichen einen Software-Hash, mit dem die Integrität der Software überprüft werden kann, wie die folgende Abbildung zeigt.



Nach dem Herunterladen der Software kann durch Eingabe des Befehls shasum ‑a 256 [Speicherort der Datei] im Mac-Terminal die Integrität der Datei überprüft werden, wie in der folgenden Abbildung dargestellt. Die Entsprechung bei Windows ist certutil-hashfile [Dateispeicherort] SHA256 und bei Linux sha256sum [Dateispeicherort].

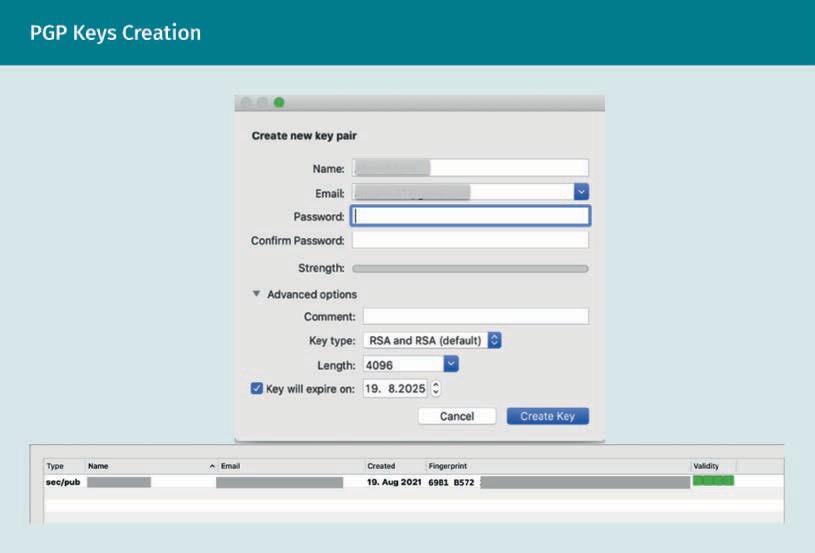


Durch Hashen der Software ergibt sich der genaue Wert, der die Software als authentisch und unverfälscht validiert.

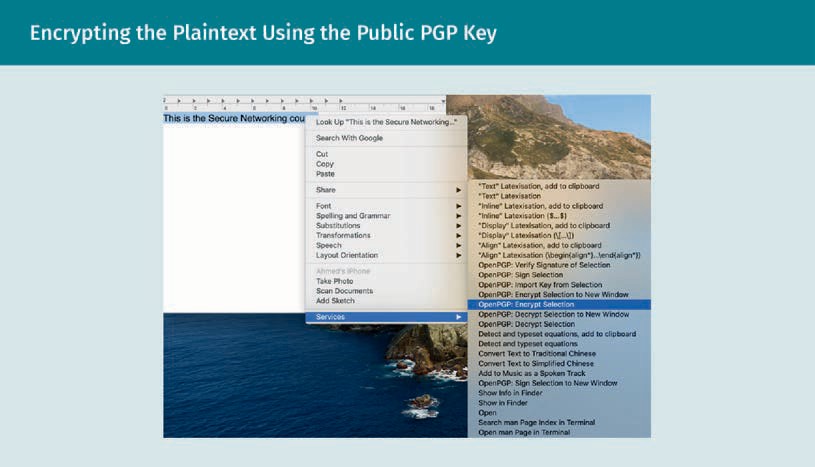
###### Verschlüsselung

Dieser Lernzyklus widmet sich *Pretty Good Privacy* (PGP), einem Verschlüsselungsprogramm, das kryptografische Vertraulichkeit und Authentifizierung für die Datenkommunikation gewährleistet.

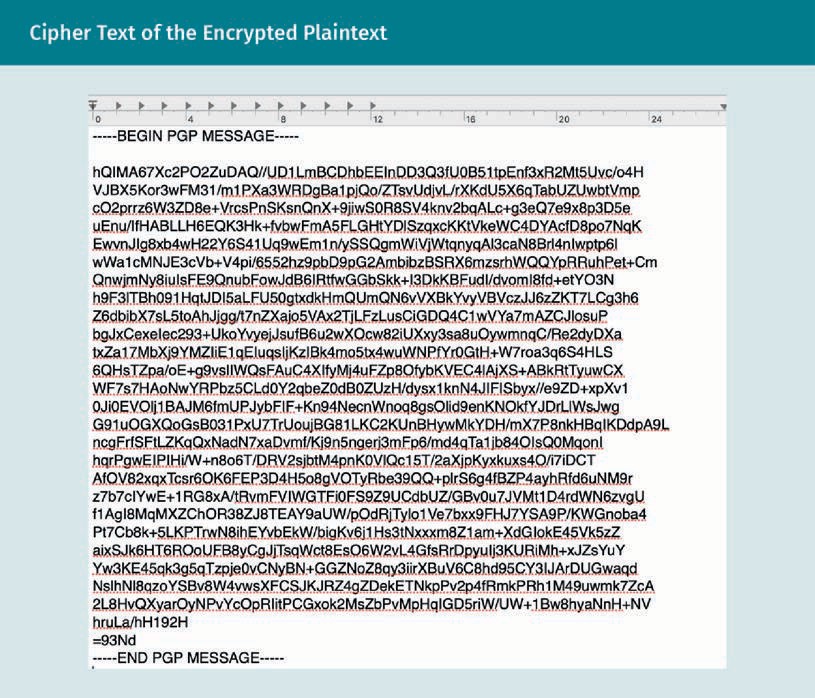
Erstellen Sie zunächst zwei Schlüsselpaare (öffentlicher und privater Schlüssel) unter Verwendung Ihrer E-Mail, wie in der folgenden Abbildung gezeigt.



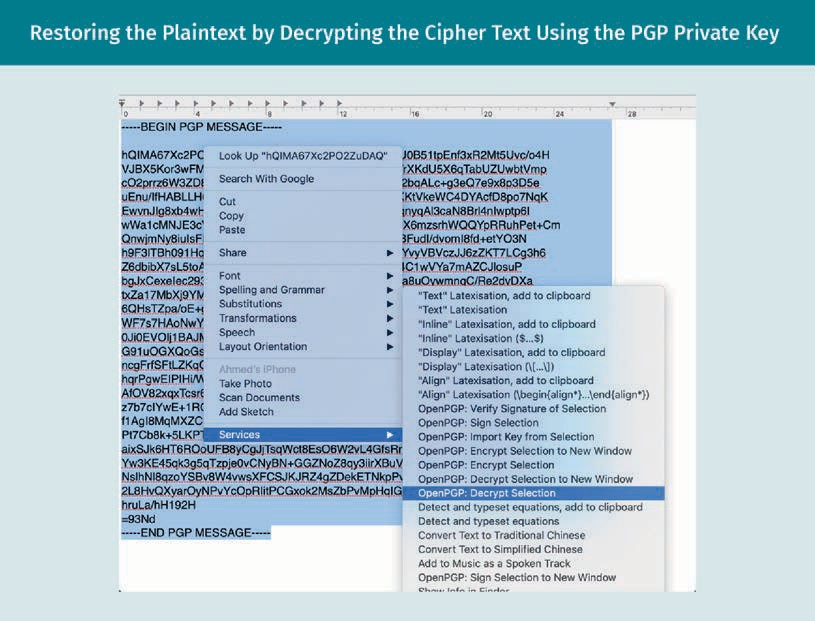
Öffnen Sie einen beliebigen Texteditor, z. B. Notes auf Windows oder TextEdit auf dem Mac, schreiben Sie einen beliebigen Text und verschlüsseln Sie die Nachricht mit dem erstellten öffentlichen Schlüssel, wie in der folgenden Abbildung gezeigt.



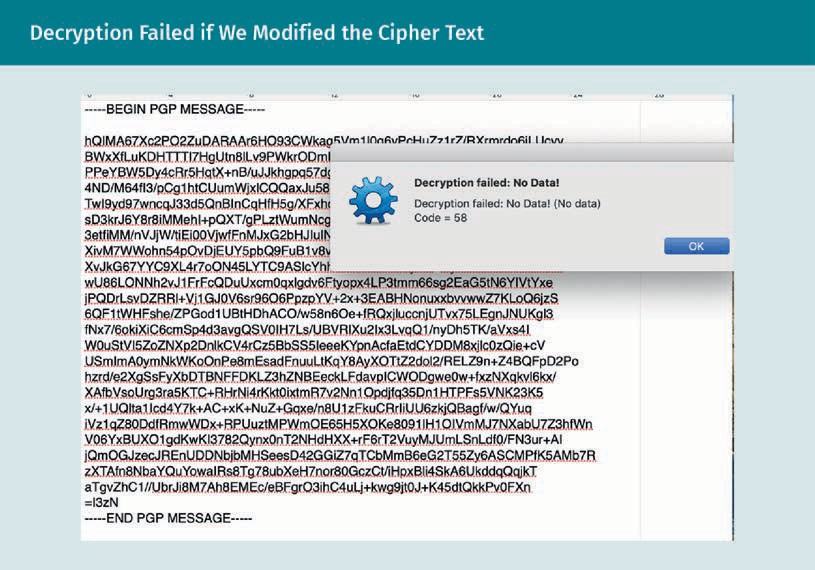
Die folgende Abbildung zeigt den erzeugten Chiffriertext.



Entschlüsseln Sie den Chiffretext dann mit dem privaten Schlüssel von PGP, um den ursprünglichen Text (Klartext) wiederherzustellen, wie in der unteren Abbildung dargestellt.

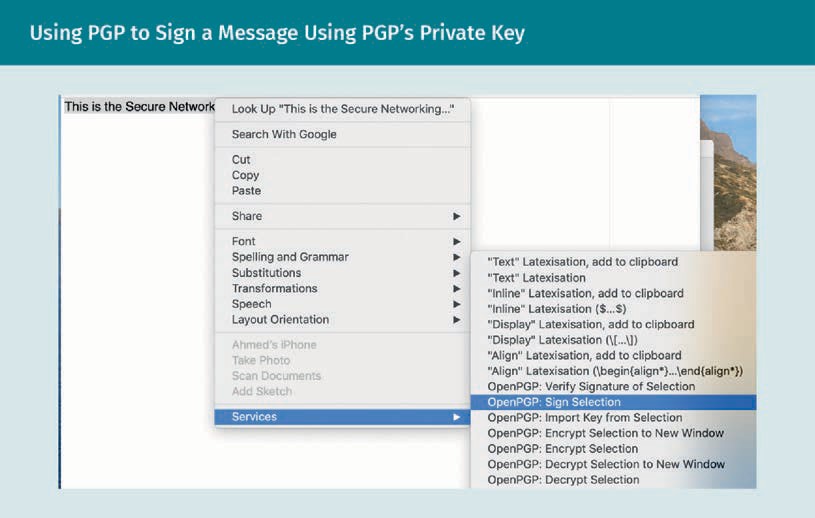


Wenn Sie die verschlüsselte Nachricht ändern (z. B. die letzten drei Zeilen in der obigen Abbildung entfernen) und dann versuchen, die Nachricht zu entschlüsseln, schlägt die Entschlüsselung fehl, wie es die folgende Abbildung zeigt.

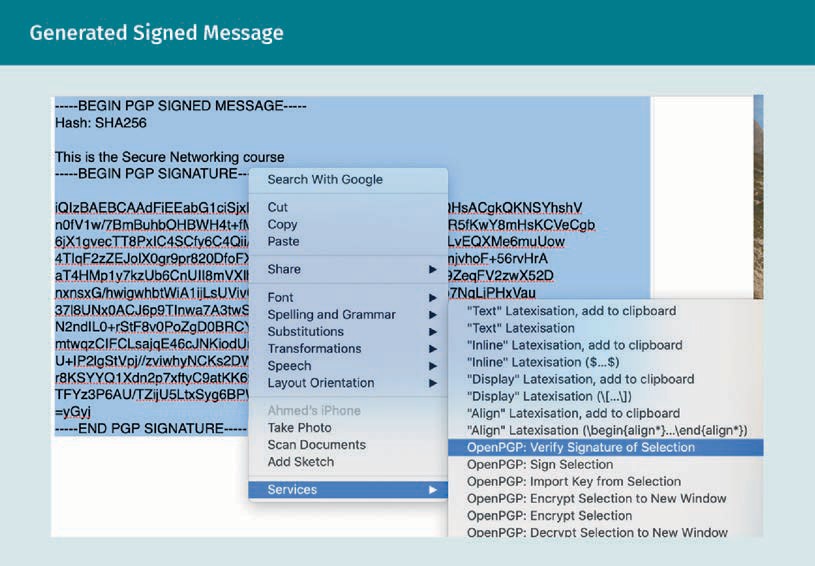


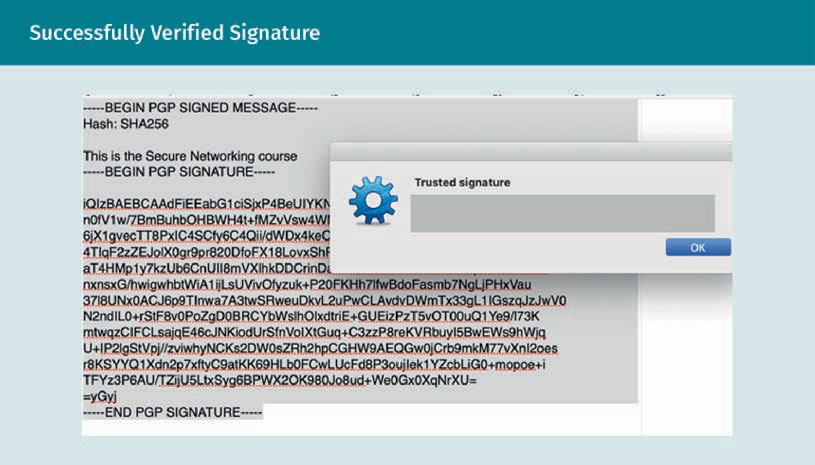
###### Signatur

Das untere Bild zeigt, wie mit Hilfe der PGP-Suite dieselbe Nachricht mit einem privaten Schlüssel signiert wird.

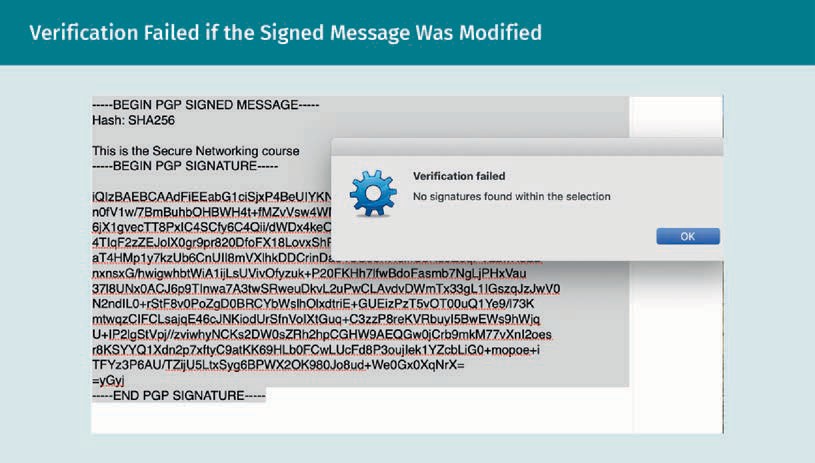


Die beiden folgenden Schaubilder zeigen die Schritte, die zur Überprüfung der erstellten Nachricht bzw. ihrer erfolgreichen Verifizierung erforderlich sind.





Wenn Sie nur einen Buchstaben aus dem signierten Text entfernen, würde die Verifizierung fehlschlagen, wie unten gezeigt.



Zusammenfassung

Diese Lektion konzentrierte sich auf die Grundlagen der Sicherheit und der kryptographischen Algorithmen. In unserem täglichen Leben nutzen wir verschiedene Anwendungen mit unterschiedlichen Sicherheitsprotokollen, z. B. für Online-Banking, Online-Einkäufe, VPN-Verbindungen und sicheres Surfen im Internet. Daher ist es wichtig, die Grundlagen dieser Protokolle zu verstehen, um bei einer Protokollanalyse möglicherweise auftretende Probleme zu erkennen.

Verschlüsselung und Signaturen sind die wichtigsten Techniken zum Schutz von Daten. Beide Techniken werden eingesetzt, um Datenverletzungen einzudämmen und Angreifende daran zu hindern, die über das Netzwerk übertragenen Nachrichten abzufangen. Bei der Verschlüsselung wird die Vertraulichkeit der Daten sichergestellt, indem normale Nachrichten (d. h. Klartext) in verschlüsselte Nachrichten (d. h. Chiffretext) umgewandelt werden. Signaturen stellen sicher, dass die übertragenen Daten nicht verändert wurden und gewährleisten somit Integrität und Authentizität Signaturen können auch zur Identitätsüberprüfung verwendet werden. Die Möglichkeit der Absenderverifizierung ist von Vorteil für die Authentifizierung von Nutzenden und Computern in einem nicht vertrauenswürdigen Netzwerk.

In dieser Lektion wurde zudem ein hybrides Kryptosystem betrachtet, das symmetrische Chiffren und Public-Key-Chiffren zusammen nutzt. Darüber hinaus wurden die vorgestellten Algorithmen anhand praktischer Szenarien veranschaulicht.



# Lektion 4

## Identitätsmanagement

#### LERNZIELE

Nach Abschluss dieser Lektion werden Sie …

… den Unterschied zwischen Identitätsmanagement und Authentifizierung verstehen können.

… die Nutzung, die Ausstellung und den Verifizierungsvorgang digitaler Zertifikate identifizieren können.

… Sie die Bedeutung der Authentifizierung erläutern können.

… beurteilen können, wie Authentifizierung umgesetzt werden kann.

… Bedrohungen für die Authentifizierung analysieren können.

DL-E-DLMCSEESN01\_E-U04

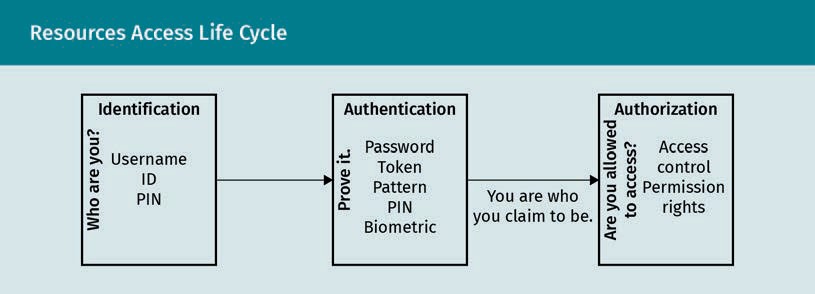
1. Identitätsmanagement

### Einführung

Die Identität einer Entität zu kennen, stellt ein strategisches Problem im virtuellen Raum (Cyberspace) dar. Die Verwendung statischer Identifikatoren (z. B. Namen oder E-Mails der Nutzerinnen und Nutzer) reicht nicht aus, um die Identität einer Person im digitalen Raum verlässlich zu bestimmen. Statische Identifikatoren können leicht gefälscht werden. Die entsprechenden Informationen können außerdem gestohlen und zur Verschleierung der wahren Identität einer Person verwendet werden. Unternehmer und IT-Abteilungen stehen unter wachsendem Druck durch Regulierungsbehörden und die eigene Organisation, den Zugang zu Unternehmensressourcen zu schützen. Deshalb sind heute fehleranfällige manuelle Abläufe nicht mehr ausreichend, um den Zugriff der Nutzenden zu überprüfen und ihre Berechtigungen zu verfolgen.

Zur Lösung dieses Problems wurde das Identitäts- und Zugriffsmanagement (IdM, oder engl.: *Identity and Access Management*, IAM) entwickelt. IdM bietet einen Rahmen, der die Zugriffskontrolle und die Überprüfung aller Unternehmensressourcen vor Ort und in der Cloud auf automatisierte Weise ermöglicht. Mit einem etablierten IdM-Rahmenwerk können IT-Manager den Zugriff der Nutzerinnen und Nutzer auf wichtige Informationen in ihrem Unternehmen regeln. IdM bietet die Möglichkeit, Daten und Datenkontrollfunktionen (engl. *Data Governance*) zu identifizieren und zu profilieren. So wird sichergestellt, dass nur notwendige und relevante Daten geteilt werden (Grassi et al., 2017; Schneier, 2015).

Die folgende Abbildung zeigt den Ablauf des Ressourcenzugriffs.



### 4.1 Digitale Identität

Eine digitale Identität ist die digitale Beschreibung von Informationen der Nutzer:innen. Sie ist immer einzigartig im Kontext eines digitalen Dienstes. Nehmen wir zum Beispiel an, ein Nutzer greift auf ein Dienstportal oder einen Online-Banking-Dienst zu. Eine digitale Identität ermöglicht die automatische Überprüfung von Informationen der Nutzer:innen ohne die Beteiligung von menschlichem Personal. Die interagierenden Informationen der Nutzerinnen und Nutzer sind die in Computersystemen gespeicherten und mit ihren Identitäten verknüpften Nutzerdaten (Grassi et al., 2017).

Derzeit wird diskutiert, ob digitale Identitäten für die Gesamtheit öffentlich zugänglicher, nicht anonymisierter und durch die Online-Aktivitäten einer Person erzeugten Informationen notwendig sind. Dazu gehören unter anderem Nutzernamen, Geburtsdatum, soziale Aktivitäten, Strafregister, Kaufhistorie und so weiter.

Trotz der zahlreichen Vorteile digitaler Identitäten von Nutzerinnen und Nutzern können Angriffe auch dazu führen, dass Identitäten nachgeahmt oder in betrügerischer Absicht ausgenutzt werden. Zur Entschärfung dieser Angriffe wird die digitale Authentifizierung eingesetzt. Bei diesem Vorgang wird festgestellt, ob ein Nutzer derjenige ist, der er zu sein vorgibt (Grassi et al., 2017).

###### Digitale Zertifikate

Digitale Identitäten können über digitale Zertifikate (Bescheinigungen) ausgestellt werden. Sie enthalten die Daten der zugehörigen Nutzer:innen und werden von juristischen Personen ausgestellt, die zuvor von einer Zertifizierungsbehörde oder einer **Zertifizierungsstelle** (CA) verifiziert wurden. In einer Public-Key-Infrastruktur (PKI) können Zertifikatsaussteller und Zertifizierungsstelle ein und dieselbe Entität sein. Das Zertifikat enthält Informationen über die Identität der jeweiligen Person („Subjekt“), den Schlüssel und die digitale Unterschrift der Entität („Aussteller“), die den Inhalt des Zertifikats verifiziert. Die Identität der Person wird durch die Aufnahme deren öffentlichen Schlüssels in das Zertifikat angegeben. Zur Bestätigung der Gültigkeit des Zertifikats werden das Ablaufdatum des Zertifikats und die Signatur des Ausstellers überprüft. Wenn beide gültig sind, ist das Zertifikat vertrauenswürdig und kann für die sichere Kommunikation mit dem entsprechenden Subjekt verwendet werden.

Außerdem können Nutzerinnen und Nutzer die Zertifikate des Servers vor der Verbindung überprüfen und so sicherstellen, dass die Verbindung sicher ist. Die Zertifikate können bösartige Entitäten umgehen, die sich als vertrauenswürdige Server ausgeben. Das bekannteste Format für Public-Key-Zertifikate ist ITU-T X.509 oder ISO/IEC/ITU 9594-8 (Housley et al., 1999).

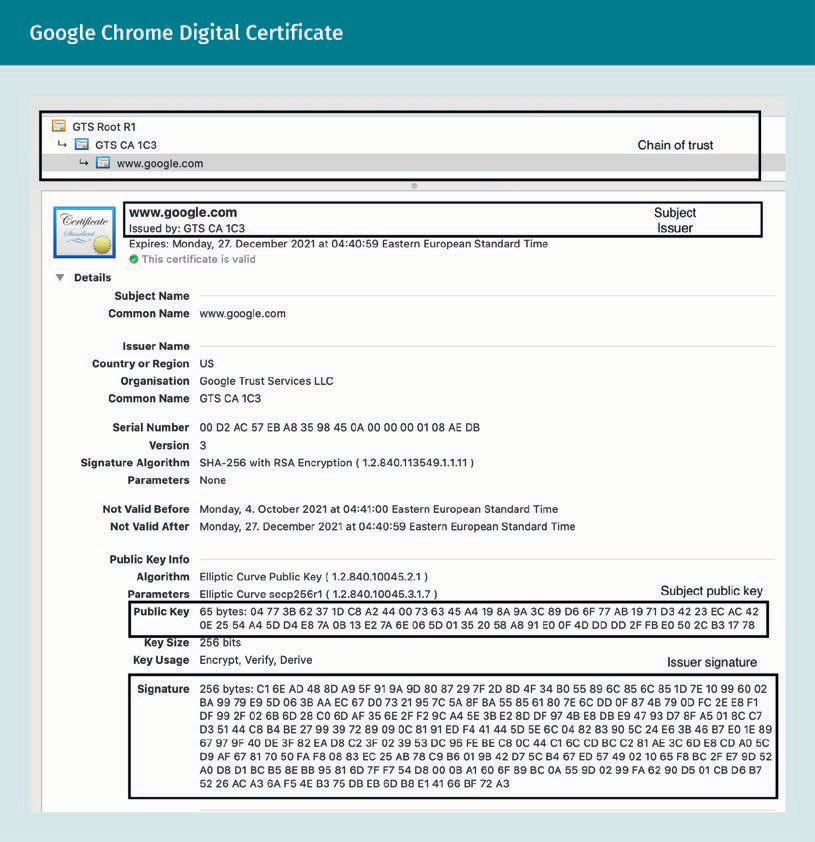
###### X.509-Zertifikate

X.509 ist ein Standard, der das Format von digitalen Zertifikaten definiert (Forshaw, 2017). Gültige Zertifikate müssen die folgenden Informationen enthalten (wie auch in der Abbildung weiter unten dargestellt):

* die Vertrauenskette, einschließlich der CA,
* den Namen und die Seriennummer des Emittenten,
* das Verfallsdatum,
* den öffentlichen Schlüssel des Subjekts, der dessen Identität spezifiziert,
* die Signatur des Ausstellers unter Verwendung seines privaten Schlüssels.

**Zertifizierungsstelle (engl. *Certificate authority*, CA)**

Eine Zertifizierungsstelle (CA) ist eine vertrauenswürdige Drittpartei, die   
digitale Zertifikate ausstellt.



Ein anderes Zertifikat kann das Stammzertifikat nicht signieren, weil dieses die höchste Hierarchie-Ebene in der Vertrauenskette ist. Das Stammzertifikat ist also selbstsigniert. Das bedeutet, dass der zum öffentlichen Schlüssel des Zertifikats gehörende private Schlüssel für die Selbstsignatur verwendet wird.

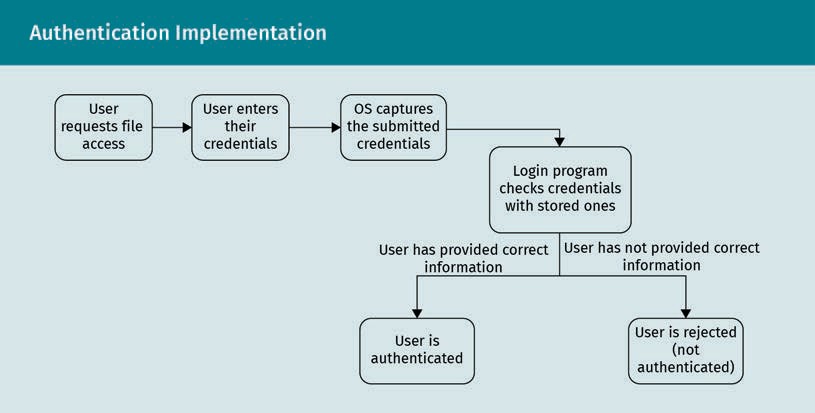
### Nutzer-Authentifizierung

Die Authentifizierung hilft dabei, die folgenden Fragen zu beantworten:

1. In wessen Auftrag läuft der Antragsprozess?
2. Wer möchte Zugriff auf die Systemressourcen erhalten?

Einfach ausgedrückt, stellt die Authentifizierung sicher, dass Nutzer:innen jeweils diejenigen sind, die sie zu sein vorgeben (Schneier, 2015; Tanenbaum & Wetherall, 2010). Zu den Authentifizierungsmethoden gehören die Vorlage eines Ausweises, die Übermittlung der erforderlichen Anmeldedaten (z. B. Passwörter), die Beantwortung vertraulicher Fragen, die Bestätigung des Besitzes der E-Mail-Adresse sowie biometrische Daten wie Fingerabdruck oder Gesichtserkennung (Stallings & Brown, 2012).

Mit anderen Worten: Die Authentifizierung bietet eine Zugriffskontrolle für Systeme. Damit wird geprüft, ob die Anmeldedaten der Nutzerin mit den Anmeldedaten in der Datenbank des Authentifizierungsservers übereinstimmen. Das Betriebssystem (BS oder engl. *Operating System*, OS) ist für die Verifizierung der Nutzer-Identität und die Authentifizierung bei Computersystemen verantwortlich.



Die Methoden zur Authentifizierung der Nutzer:innen basieren auf einer oder mehreren der folgenden Methoden:

* etwas, das ein Nutzer kennt (z. B. ein Passwort, eine geheime Frage oder eine persönliche Identifikationsnummer [PIN]),
* etwas, das ein Nutzer besitzt (z. B. eine ID-Karte, ein Sicherheits-Token oder ein Software-Token),
* etwas, das ein Nutzer ist (z. B. Fingerabdruck, Unterschrift oder Gesichtserkennung).

Wenn Nutzer:innen beispielsweise ihr Online-Bankkonto überprüfen, werden sie von der Bankanwendung durch Abfrage ihrer Anmeldedaten, die nur ihnen bekannt sind (z. B. die Kombination aus Benutzername und Passwort), authentifiziert. Einige Anwendungen haben strengere Authentifizierungsanforderungen, wie z. B. das Senden eines Einmalpassworts (engl. *One-time Password*, OTP), d. h. eines Codes mit begrenzter Lebensdauer, an das Smartphone oder die Anforderung einer biometrischen Bestätigung wie einem Fingerabdruck oder einem Gesichtsscan. Es gibt also folgende Authentifizierungsarten:

* Ein-Faktor-Authentifizierung mit nur einer der oben genannten Methoden, oder
* Multi-Faktor-Authentifizierung, also mit zwei oder mehreren der oben genannten Methoden.

Diese Authentifizierungsverfahren sollen kurz im Einzelnen beschrieben werden.

###### Nutzer-Authentifizierung mit einem Passwort

Die Nutzer-Authentifizierung mit einem Passwort ist die häufigste Form der Authentifizierung. Bei dieser Methode werden die Nutzer:innen aufgefordert, ihre Anmeldedaten einzugeben, d. h. ihren Benutzernamen/ID und ihr Passwort (Schneier, 2015; Stallings & Brown, 2012).

Die Speicherung aller Anmeldedaten in einer zentralen Liste ist die einfachste Implementierung der Nutzer-Authentifizierung. Immer wenn Personen ihre Anmeldedaten eingeben, sucht das Betriebssystem den eingegebenen Benutzernamen in der Liste und prüft dann, ob das eingegebene Passwort mit dem gespeicherten identisch ist.

Wenn die Passwörter übereinstimmen, wird die Person erfolgreich authentifiziert und für die Anmeldung in diesem System zugelassen. Wenn sie nicht übereinstimmen, wird der Nutzer abgelehnt und eine Fehlermeldung ausgegeben.

###### Bedrohungsmodell für ein sicheres Passwort

Einer Studie von ImmuniWeb (2019) zufolge nimmt die Zahl der Sicherheitsverletzungen aufgrund von schwachen Passwörtern rapide zu. Der Hauptgrund für diesen Anstieg sind Passwörter, die aus einfachen und naheliegenden Informationen bestehen, wie Namen oder Geburtsdaten. Außerdem verwenden Angestellte oft persönliche Passwörter für ihre beruflichen Konten. Nach Angaben von NordPass (2021) haben in den letzten 12 Monaten fast 2,5 Millionen Menschen „123456“ oder „123456789“ als Passwort verwendet.

Laut Cynet (2021) sind dies die häufigsten Passwortangriffe.

Phishing

Phishing wird als eine Art von sozialer Manipulation *(Social Engineering)* angesehen. Bei Phishing-Angriffen geben sich Angreifende als eine juristische Person oder Organisation aus und versenden eine betrügerische Nachricht, die vertrauenswürdig erscheint. Die Nachricht kann einen bösartigen Link enthalten, der zu einer gefälschten Anmeldeseite führt, auf der die Nutzerinnen und Nutzer aufgefordert werden, ihre Zugangsdaten einzugeben oder schädliche Software herunterzuladen und auf ihrem Computer zu speichern.

Wörterbuchangriff

Bei einem Wörterbuchangriff wird systematisch jedes Wort aus einer Wortliste oder einem Wörterbuch als Passwort verwendet, in der Hoffnung, dass das Passwort der Nutzer:innen ein beliebtes Wort ist. Viele haben Schwierigkeiten damit, sich mehrere Passwörter zu merken und verwenden daher leicht zu erratende Passwörter.

Methode der rohen Gewalt (Brute-Force-Angriff)

Dies ist eine Versuch-und-Irrtum-Methode, bei der alle möglichen Kombinationen von Anmeldeinformationen, Nutzernamen oder Passwörtern „erraten“ werden. So können Computer in etwa acht Stunden acht zufällige Zeichen (Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen) knacken. Zehn zufällige Zeichen erhöhen die benötigte Zeit auf fünf Jahre (Woodward, 2019).

Zur Abschwächung der beiden vorgenannten Angriffe sollte eine Sicherheitsrichtlinie durchgesetzt werden, die längere Passwörter mit verschiedenen Zeichentypen (d. h. Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen), häufige Passwortänderungen, das Verbot der Wiederverwendung alter Passwörter und eine Begrenzung der Anzahl der Anmeldeversuche vorsieht.

Zugriff auf die Passwortliste

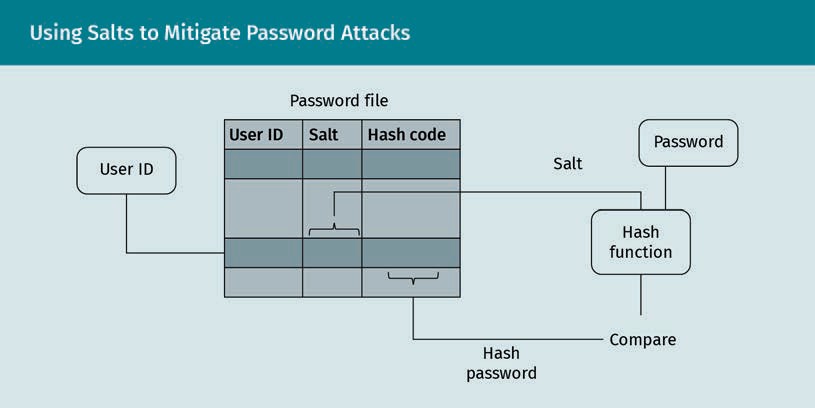
Wenn Passwörter als Klartext in Konfigurationsdateien gespeichert werden, können Angreifende bei einem Sicherheitsverstoß ggf. die Passwörter herausbekommen. Dieser Angriff kann entschärft werden, indem der Zugriff auf Konfigurationsdateien eingeschränkt und nur die aus Passwörtern erzeugten Hashes gespeichert werden (Wagner & Goldberg, 2000).

Angriff über eine Regenbogentabelle (engl. *Rainbow Table*)

Eine Regenbogentabelle enthält eine Liste von vorberechneten Hashes und den dazugehörigen Passwörtern. Bei einem Rainbow-Table-Angriff versuchen Angreifende mit Hilfe der Versuch-und-Irrtum-Methode die in einem Datenbanksystem gespeicherten Passwörter zu knacken. Der Unterschied zwischen Regenbogentabellen- und normalen Wörterbuchangriffen besteht in der unterschiedlichen Speicherung der Einträge. In der Regenbogentabelle werden sowohl Hashes als auch Passwörter gespeichert, aber sie ist im Grunde nur ein Wörterbuch (Avi, 2021).

Schauen wir uns ein Regenbogentabellen-Angriffsmodell an. Angenommen, Angreifende haben Ihnen eine lange Liste von Passwort-Hashes gestohlen. Sie prüfen dann, ob einer der Passwort-Hashes in der Regenbogentabelle enthalten ist. Wenn es eine Übereinstimmung gibt, enthält die Regenbogentabelle jedes Kennwort, das zu diesem Hash gehört (d. h. die Kennwörter, die gehasht wurden).

Zur Abwehr dieser Angriffsart wird vor dem Hashing ein Salt („Salz“ bzw. Zufallsdaten) hinzugefügt, wie in der folgenden Abbildung gezeigt wird. Das Salz wird dann zusammen mit dem gehashten Wert gespeichert.



Der gespeicherte Hash kann dann anhand des Salzes und dem eingegebenen Passwort überprüft werden.

###### Verbesserung der Passwortsicherheit

Die folgende Liste fasst die meisten Sicherheitsmaßnahmen zusammen, die von den Sicherheitsrichtlinien zum Schutz von Passwörtern eingefordert werden.

* + Längere Passwörter mit verschiedenen Zeichentypen,
  + ausschließlich Verwendung von Passwort-Hashes (erzeugt mit einem zufälligen Salt),
  + eingeschränkter Zugriff auf Passwort-Hashes,
  + begrenzte Anzahl an Anmeldeversuchen,
  + regelmäßiges Ändern von Passwörtern und keine Wiederverwendung alter Passwörter,
  + Verwendung von Single-Sign-On-Zertifikaten (wie z. B. X.509-Zertifikate),
  + Nutzung von Multi-Faktor-Authentifizierung.

###### Andere Authentifizierungsmethoden: Sicherheits-Tokens

**Physische Sicherheitstokens**   
Ein physisches Token ist ein Peripheriegerät, mit dem der Zugang zu einer elektronisch gesperrten Ressource ermöglicht wird.

**Software-Token**Ein Software-Token ist eine auf elektronischen Geräten wie Mobiltelefonen und Laptops installierte Software.

Eine weitere Möglichkeit der Authentifizierung stellt die Nutzer-Authentifizierung durch etwas Greifbares, das die Nutzer:innen besitzen, wie z. B. ein **physisches Sicherheitstoken**, dar. Das physische Objekt kann ein Armband, eine ID-Karte, ein Sicherheits-Token, ein Software-Token oder ein Mobiltelefon mit eingebautem Hardware- oder Software-Token sein. Im Gegensatz dazu ist ein Software-Token (oder Soft-Token) eine virtuelle Lösung (Software), die auf dem elektronischen Gerät der User:innen (z. B. einem Desktop-Computer, einem Laptop oder einem Mobiltelefon) installiert ist und dupliziert werden kann. Beide Token-Arten erzeugen einen einmalig verwendbaren Code für den Zugriff auf eine elektronisch eingeschränkte Ressource (z. B. auf eine Plattform).

Bei den Sicherheits-Tokens kann es sich um Hardware- (d. h. physisch) oder **Software-Tokens** handeln. Tokens haben verschiedene Funktionen. Manche speichern Passwörter, andere kryptografische Schlüssel, die zur Erzeugung einer digitalen Signatur verwendet werden. Andere Tokens sind kleine Tastaturen zur Eingabe einer geheimen persönlichen Identifikationsnummer (PIN) und zur Generierung einer zufälligen, einmalig verwendbaren Nummer (dies war vor einigen Jahren der Standard bei Banking-Systemen).

Wieder andere Arten von physischen Tokens erfordern eine Verbindung zu einem Computer oder System. Daher basieren sie auf verschiedenen Technologien wie Universal Serial Bus (USB), Radiofrequenz-Identifikation (RFID) oder Bluetooth. Diese Tokens übertragen eine Schlüsselsequenz an den lokalen Client oder an einen nahe gelegenen Zugangspunkt. Manche Tokens verfügen auch über eine Audiofunktion für Menschen mit Sehbehinderung.

Eine andere Form des Sicherheitstokens nutzt die Kommunikation über einen anderen Kanal, z. B. über ein Mobiltelefon (entweder durch einen Anruf oder eine SMS mit einem eindeutigen Code). Software-Tokens werden heute am häufigsten verwendet. Dies sind auf elektronischen Geräten wie Mobiltelefonen installierte Anwendungen. Wie ein physischer Token generieren auch diese Anwendungen nach Eingabe der erforderlichen PIN eine einmalige Zufallszahl.

###### Andere Authentifizierungsmethoden: Biometrie

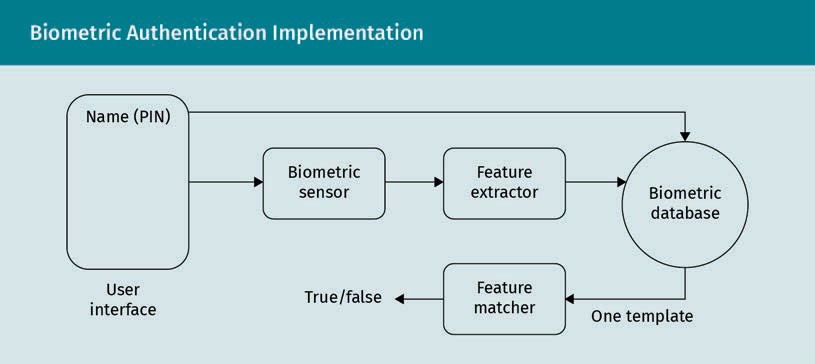
Als dritte Authentifizierungsmethode wollen wir uns die Nutzer-Authentifizierung mittels biometrischer Daten anschauen. Die biometrischen Daten aller Personen sind einzigartig. Daher können sie zur Identifizierung und Authentifizierung von Nutzern über persönliche und erkennbare Daten eingesetzt werden. Bei dieser Methode werden die physischen Merkmale der Nutzer gemessen, die nur schwer zu fälschen sind. Das typische biometrische System besteht aus zwei Teilen: Registrierung und Identifizierung (Ross & Jain, 2004; Singh et al., 2019).

Registrierung

In einem biometrischen System werden die Benutzereigenschaften (d. h. die Benutzermerkmale) während der Registrierung vermessen und die Ergebnisse digitalisiert. Dann werden die Merkmale der Nutzer:innen extrahiert und in einer biometrischen Datenbank (in einem eigenen Datensatz für jede Person) gespeichert.

Identifizierung

In diesem Fall versuchen Nutzer:innen, sich bei einem digitalen System anzumelden und geben dafür ihre Anmeldedaten (z. B. einen Namen/ID) ein. Das System verifiziert sie, indem es die Messung erneut erfasst. Wenn die neuen Messwerte mit den in der Anmeldephase ermittelten übereinstimmen, wird die Anmeldung akzeptiert. Andernfalls wird der Anmeldeversuch abgelehnt.



Biometrische Techniken bieten die folgenden Vorteile:

* Biometrische Merkmale sind einzigartig und unterscheiden sich deutlich von einer Person zur anderen.
* Sie sind dauerhaft, das heißt, sie werden im Laufe der Zeit nicht verändert.
* Sie sind messbar, was den späteren Vergleich ermöglicht.
* Sie sind fast unmöglich zu fälschen.

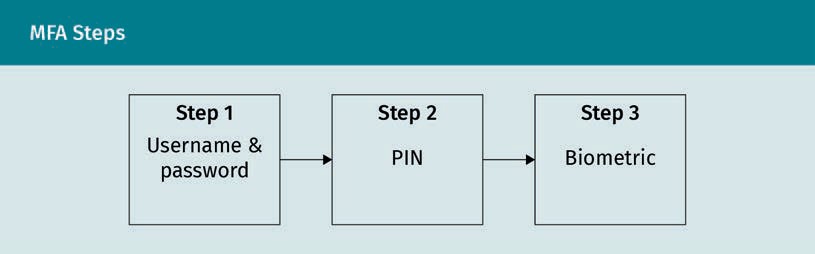
Obwohl die biometrische Authentifizierung zahlreiche Vorteile hat, leidet sie unter falsch-negativen und falsch-positiven Ergebnissen. Wenn das Gerät die biometrischen Daten der authentischen Nutzer:innen nicht identifizieren kann, handelt es sich um ein falsch negatives Ergebnis Dies kann z. B. vorkommen, wenn ein Mobiltelefon einen Fingerabdruck nicht erkennt. Wenn das Gerät andererseits die biometrischen Daten einer nicht authentischen Nutzerin akzeptiert, hat sie ein falsch positives Ergebnis erzielt. Dies kann z. B. passieren, wenn ein Telefon durch das Gesicht einer anderen Person entsperrt wird. Offensichtlich stellen falsch-positive Daten ein viel größeres Risiko für die Datensicherheit dar als falsch-negative.

###### Andere Authentifizierungsmethoden: Multi-Faktor-Authentifizierung

Bei der Multi-Faktor-Authentifizierung (MFA) werden zwei oder mehr Authentifizierungsmethoden verwendet (Lam & Gollmann, 1992). Bei dieser Methode müssen Nutzende zwei oder mehr Nachweise vorlegen, um Zugang zu einer App oder einem System zu erhalten. Dazu könnte die Eingabe eines Passworts gehören (das die Person kennt) und dann der Erhalt eines zeitlich begrenzten Einmalpassworts (OTP) per SMS auf das eigene Telefon. Eine wachsende Zahl von Diensten nutzt diese Art der Authentifizierung.

In diesem Fall müssen Angreifende beide Authentifizierungsmethoden umgehen, um das System zu manipulieren. Selbst wenn Angreifende das Passwort der User:innen manipulieren, reicht dies nicht aus, wenn für den Zugriff auf das gewünschte System auch ein Einmalpasswort (OTP) erforderlich ist.

Die folgende Abbildung zeigt ein Beispiel für eine MFA oder eine Drei-Faktoren-Kombination der Authentifizierung (Benutzername und Passwort + PIN + Fingerabdruck).



###### Andere Authentifizierungsmethoden: Einmalige Anmeldung (engl. *Single Sign-on*, SSO)

Single Sign-On (SSO) ist eine weitere in vielen Unternehmen eingesetzte Methode. SSO ermöglicht es, Anmeldedaten (z. B. Benutzernamen und Kennwort) einzugeben, um auf mehrere Anwendungen und Websites zuzugreifen. Stellen Sie sich eine Mitarbeiterin vor, der auf zwei verschiedenen Websites Zugriff auf die E-Mails und Anwendungen ihres Unternehmens erhalten möchte. Wenn die beiden Websites mit SSO verknüpft sind, haben die Nutzenden automatisch Zugriff auf die Anwendungen, nachdem sie sich beim E-Mail-Client angemeldet haben. SSO spart Zeit, da die User:innen ihre Passwörter nur einmal anstatt mehrfach eingeben müssen (De Clercq, 2002). Laut De Clercq (2002) „definiert die Open Group SSO als den Mechanismus, mit dem eine einzige erfolgreiche Nutzer-Authentifizierung und ‑Autorisierung den Nutzern den Zugriff auf alle angeschlossenen Computer und Systeme (auf denen sie eine Zugriffsberechtigung haben) ermöglichen kann, ohne dass sie mehrere Passwörter eingeben müssen“ (S. 40).

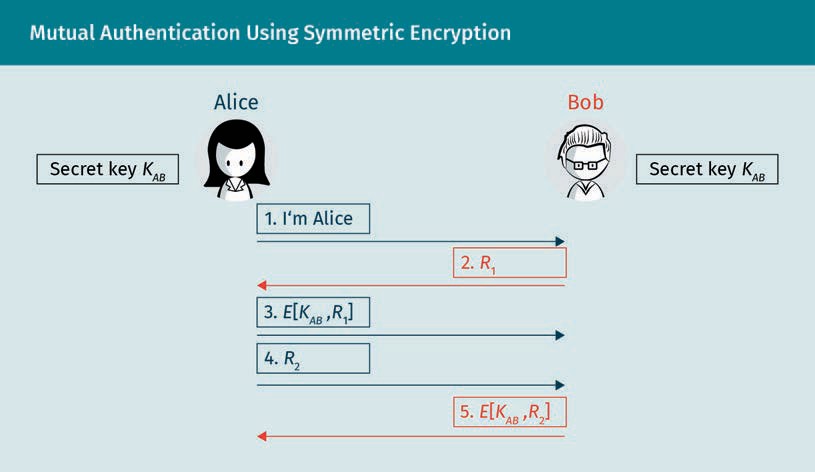
### Authentifizierungsprotokolle

Angenommen, Alice und Bob wollen sicher über das Internet kommunizieren, das von Natur aus nicht sicher ist. Sichere Kommunikation bedeutet in der Regel die Gewährleistung von Datenvertraulichkeit, Integrität, Authentizität und Identität beider Parteien. Daher werden kryptografische Algorithmen verwendet, um die erforderlichen Sicherheitsanforderungen zu erfüllen, wie z. B. symmetrische oder asymmetrische Verschlüsselungsalgorithmen und Hash-Funktionen. Für eine sichere Kommunikation zwischen zwei Parteien (in unserem Beispiel Alice und Bob), müssen diese sich zunächst gegenseitig authentifizieren, bevor sie Sitzungsschlüssel erstellen und austauschen und sich auf die zu verwendenden kryptographischen Algorithmen einigen.

Werfen wir einen Blick auf die Authentifizierung. Alice muss Bob beweisen, dass sie Alice ist, und Bob muss Alice beweisen, dass er Bob ist.

###### Gegenseitige Authentifizierung mit symmetrischer Kryptographie

Angenommen, Alice und Bob teilen sich einen geheimen Schlüssel *K34,* wie in der nachstehenden Abbildung gezeigt. Zuerst sendet Alice eine Nachricht, die ihre Identität enthält. Als Zweites stellt Bob Alice auf die Probe (Aufforderung), indem er ihr einen Zufallswert *R*1 sendet, um sicherzustellen, dass er mit Alice spricht. Alice verschlüsselt *R*1 dann unter Verwendung des gemeinsamen Schlüssels *K34* und sendet Bob den verschlüsselten Text (die so genannte Antwort). Wenn Bob die Antwort erhält, überprüft er den Zufallswert *R*1 durch Entschlüsseln der Antwort. Wenn *R*1 mit dem ursprünglich gesendeten Zufallswert übereinstimmt, dann weiß Bob, dass er mit Alice kommuniziert (erfolgreiche Alice-Authentifizierung), weil außer ihm nur Alice den gemeinsamen Schlüssel *K34* kennt. Ebenso möchte Alice Bob authentifizieren, um sicherzustellen, dass sie mit ihm kommuniziert. Sie stellt Bob mit einer Zufallszahl *R*2 auf die Probe. Schließlich verschlüsselt Bob *R*2 mit dem gemeinsamen Schlüssel *K34* und sendet den verschlüsselten Text an Alice. Diese wiederum entschlüsselt die Antwort und überprüft *R*2.



Falls nur eine einseitige Authentifizierung erforderlich ist, werden nur die ersten drei Schritte des Protokolls genutzt. Bei einer Client-Server-Kommunikation muss zum Beispiel nur der Server die Identität des Clients überprüfen (d. h. den Client authentifizieren).

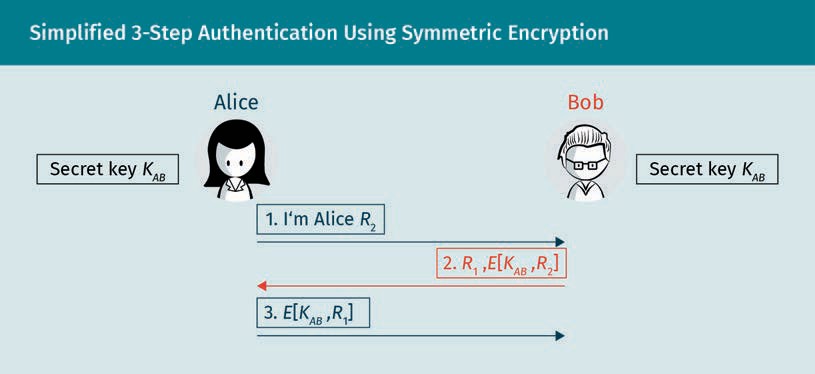
Es ist wichtig, dass die für die Aufforderung genutzten Zufallszahlen *R*1 und *R*2 nicht leicht wiederholbar oder vorhersehbar sind. Andernfalls kann eine Angreiferin (Eve) die Aufforderung und die Antwort zwischen Alice und Bob aufzeichnen und sie wiedergeben, um sich als eine der beiden Parteien auszugeben. Angenommen, Eve versucht, sich als Alice auszugeben, und Bob sendet *R*1 als Aufforderung, wobei Eve diese zuvor schon aufgezeichnet hat. Dann kann Eve die aufgezeichnete Antwort (d. h. den Chiffretext von *R*1) an Bob senden. In diesem Fall wird Bob ausgetrickst und glaubt, dass Eve Alice ist.

Nehmen wir als weiteres Beispiel an, dass die Werte der Herausforderungen immer und vorhersehbar zunehmen. In diesem Fall kann Eve sich zunächst als Bob ausgeben und als Probe eine größere Aufforderung *R*1 = 100.000 senden und dann die Antwort von Alice speichern. Gleichzeitig verwendet Bob einen kleineren Wert *R*1 = 90.0000.

Dann kann Eve sich irgendwann in der Zukunft als Alice ausgeben, wenn der echte Bob schließlich *R*1 = 100.000 verschickt. In der Praxis sollten *R*1 und *R*2 große Zufallswerte sein, damit sie unvorhersehbar sind und die Wahrscheinlichkeit einer Wiederholung minimiert wird (Stallings & Brown, 2012).

Eine weitere Sicherheitsvorkehrung betrifft den Schutz des gemeinsamen geheimen Schlüssels *K34*. Wenn Eve eine Kopie des Schlüssels von einem der beiden echten Kommunikationspartner stiehlt, kann sie sich entweder als Alice oder Bob ausgeben.

Wir können das Protokoll der gegenseitigen Authentifizierung in den folgenden drei Schritten zusammenfassen.



Zuerst sagt Alice „Hallo“ zu Bob und sendet zur Probe eine Aufforderung *R*2. Als zweite Antwort sendet Bob Alice den Chiffretext von *R*2 und seine Aufforderung, *R*1. Nach Erhalt dieser Antwort entschlüsselt Alice den verschlüsselten Text und überprüft, ob er mit dem an Bob geschickten Klartext *R*2 übereinstimmt. Falls ja, weiß sie, dass sie mit Bob kommuniziert. Drittens schickt Alice Bob einen verschlüsselten Text von *R*1. Bob entschlüsselt ihn und gleicht ihn mit dem Klartext von *R*1 ab, um so Alice zu authentifizieren.

**Reflection-Attacke** Dies ist eine Art Man-in-the-Middle-Angriff, bei dem das gleiche Protokoll in beide Richtungen verwendet wird.

Es gibt jedoch auch eine Art von Angriff, die sogenannte **Reflection-Attacke**. Hierbei handelt es sich um eine Art Man-in-the-Middle-Angriff. Das folgende Beispiel zeigt, wie es funktioniert.

Zuerst gibt sich Eve als Alice aus. Folgt man dem in der obigen Abbildung gezeigten Protokoll, bleibt Eve bei Schritt drei stecken, weil sie den Schlüssel *K34* nicht kennt. Sie wird jedoch zur Probe die Aufforderung erhalten *R*1. Eve öffnet dann eine weitere Verbindung mit Bob und gibt sich wiederum als Alice aus. Dieses Mal sendet Eve Bob die Herausforderung *R*1, die sie bei der ersten Verbindung gespeichert hat. Gemäß dem Protokoll antwortet Bob mit dem Chiffretext von *R*1 und einer weiteren Aufforderung *R*3.

Eve kann dann mit dem Chiffretext von *R*1 den Schritt drei der ersten Verbindung abschließen, indem sie einfach den Chiffriertext von *R*1 an Bob zurückschickt. Zu diesem Zeitpunkt ist die erste Verbindung erfolgreich beendet und Eve hat sich erfolgreich als Alice ausgegeben. Diese Art von Angriff ist als Reflection-Attacke bekannt, da Eve an Bob zurücksendet, was er ihr gerade über eine andere Verbindung geschickt hat.

###### Wie können Reflection-Attacken verhindert werden?

Eine Möglichkeit zur Verhinderung einer Reflection-Attacke besteht darin, zwei verschiedene gemeinsame Schlüssel zu verwenden. Einer davon sollte für die Urheberpartei der Verbindung (z. B. Alice) und der andere für die Antwortpartei (z. B. Bob) verwendet werden.

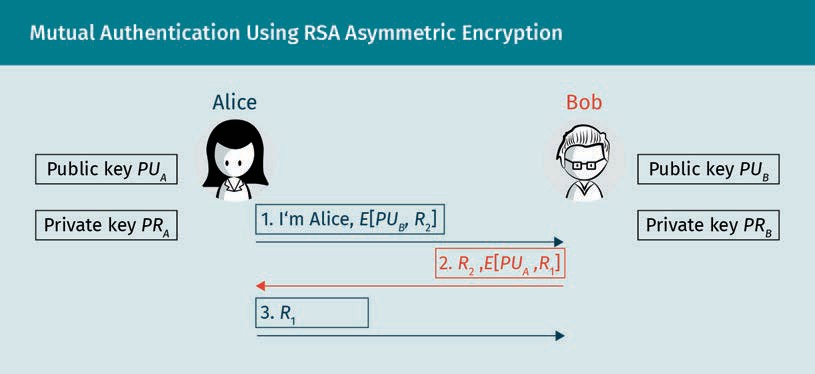
Wenn Alice in diesem Fall die Aufforderung *R*1 verschlüsselt, nimmt sie einen anderen Schlüssel als den, den Bob zur Verschlüsselung der Aufforderung *R*2 genutzt hat. Wenn Eve also den Chiffretext *R*2 von Bob erhält, kann sie ihn nicht einfach an Bob zurücksenden, weil er einen mit einem anderen Schlüssel erstellten Chiffretext erwartet.

Eine andere Möglichkeit besteht darin, die Aufforderungen für die Urheber- bzw. Antwortpartei zu variieren. Zum Beispiel könnte Alice eine gerade Zahl als Aufforderung verwenden und Bob eine ungerade Zahl. In diesem Fall kann Eve die Aufforderung *R*1 , die sie von Bob erhalten hat und die eine ungerade Zahl ist, nicht senden, weil Bob als Antwort eine gerade Zahl erwartet.

###### Gegenseitige Authentifizierung mit asymmetrischer Kryptographie

Angenommen, Alice und Bob verfügen über die öffentlichen Schlüssel des jeweils anderen, wie unten dargestellt. Zunächst sendet Alice eine mit Bobs öffentlichem Schlüssel *E 5U4* verschlüsselte Aufforderung *R*2 an Bob. Als Zweites entschlüsselt Bob mit seinem privaten Schlüssel *D 5 R4*, *E 5U4*, *R*2 den Chiffretext und sendet die Klartextaufforderung *R*2 zurück, zusammen mit seiner Aufforderung *R*1, welche mit dem öffentlichen Schlüssel von Alice *R*2, *E 5U3*, *R*1 verschlüsselt ist.

Wenn *R*2 mit dem von Alice zuvor gesendeten übereinstimmt, dann weiß Alice sicher, dass sie mit Bob kommuniziert, denn nur Bob hat den privaten Schlüssel, der zum öffentlichen Schlüssel gehört, mit dem sie *R*2 verschlüsselt hat. Entsprechend sendet Alice *R*1, womit Bob Alice authentifizieren kann, da nur sie den privaten Schlüssel besitzt, der zum öffentlichen Schlüssel gehört, mit dem *R*1 verschlüsselt wurde.



###### Sitzungsschlüssel

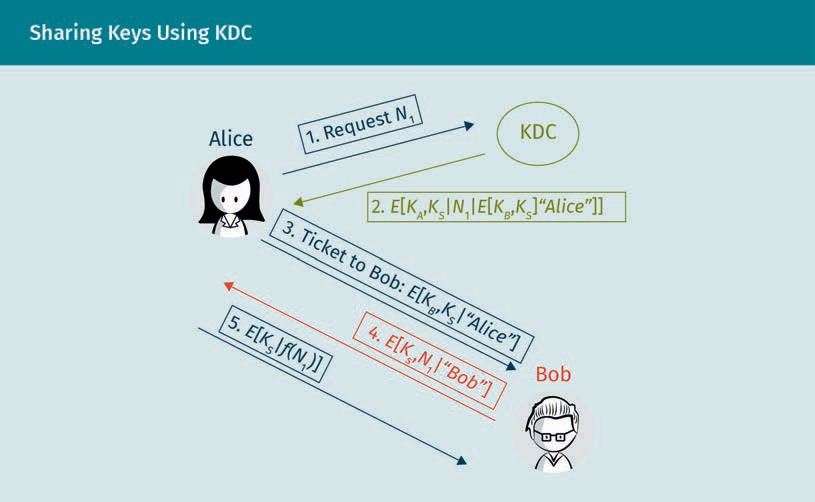
Nach der Authentifizierung teilen sich Alice und Bob einen langfristigen geheimen Schlüssel, den sogenannten Hauptschlüssel (engl. *Master Secret* oder *Master Key*). Der Hauptschlüssel kann von einem Passwort abgeleitet werden. Bei jeder Sitzung verwenden sowohl Alice als auch Bob den Hauptschlüssel, um sich gegenseitig zu authentifizieren und einen neuen Sitzungsschlüssel zu erzeugen. Dieser ist ein symmetrischer Schlüssel, der zur Ver- und Entschlüsselung der während der Kommunikation ausgetauschten Informationen und zur Überprüfung der Integrität der Nachrichten genutzt wird. Mit anderen Worten: Er wird verwendet, um Änderungen in den Daten zwischen dem Sende- und dem Empfangszeitpunkt zu erkennen (Schneier, 2015). Alle Nachrichten während der Sitzung werden dann mit dem Sitzungsschlüssel geschützt. Der Hauptvorteil eines Sitzungsschlüssels besteht darin, dass bei einem Leck des Sitzungsschlüssels nur die aktuelle Sitzung gefährdet würde, alle anderen Sitzungen aber wieder sicher wären. Je häufiger ein Hauptschlüssel verwendet wird, desto größer ist die Wahrscheinlichkeit, dass er durchsickert. Daher sollte der Langzeit-Hauptschlüssel so wenig wie möglich benutzt werden, z. B. nur zu Beginn einer Sitzung zur Authentifizierung und Festlegung des Sitzungsschlüssels.

Alice und Bob können auch über ihre öffentlichen Schlüssel einen gemeinsamen Sitzungsschlüssel austauschen. Alice kann Bob zum Beispiel einen Schlüssel schicken, der mit Bobs öffentlichem Schlüssel verschlüsselt ist, so dass nur Bob den Schlüssel entschlüsseln und nutzen kann. Dann kann sie das Ergebnis mit ihrem privaten Schlüssel signieren, sodass Bob sie authentifizieren und den Man-in-the-Middle-Angriff verhindern kann.

Ein Manko des paarweisen Schlüsselaustauschs auf der Basis von gemeinsamen geheimen Hauptschlüsseln ist die Skalierbarkeit. Jedes Kommunikationspaar muss einen gemeinsamen Hauptschlüssel haben. In der Praxis bedeutet das, dass Alice einen Hauptschlüssel mit Bob teilen muss, einen weiteren mit Carol und so weiter.

###### Key Distribution Center

Die Nutzung einer Schlüsselverwaltungszentrale (engl. *Key Distribution Center*, KDC) kann dieses Problem der Skalierbarkeit lösen. Alle Nutzer:innen haben einen Hauptschlüssel für das KDC. Das KDC hat viele Hauptschlüssel, einen für jeden Nutzer bzw. jede Nutzerin. Diese haben jedoch jeweils nur einen Hauptschlüssel, den sie mit dem KDC teilen, wie in der folgenden Abbildung dargestellt.



Nehmen wir nun an, dass Alice und Bob einen Sitzungsschlüssel erstellen müssen, wie oben dargestellt. Zunächst sendet Alice eine Anfrage an das KDC, z. B. „Ich brauche einen Schlüssel, um mit Bob zu sprechen“, zusammen mit einer Nonce *9*1, einem Zufallswert. Das KDC sendet dann eine verschlüsselte Nachricht mit dem zwischen Alice und dem KDC genutzten Hauptschlüssel *K3* . Diese Nachricht enthält (a) einen Sitzungsschlüssel *K:* , den das KDC für Alice und Bob erstellt hat, (b) eine Nonce *9*1, und (c) eine Nachricht, die als Ticket bezeichnet wird. Das Ticket wird mit dem zwischen Bob und dem KDC genutzten Hauptschlüssel *K4* verschlüsselt. Es enthält den Sitzungsschlüssel *K:* und die ID von Alice.

Alice entschlüsselt dann die vom KDC erhaltene Nachricht mit dem Hauptschlüssel *K3* und erhält so den Sitzungsschlüssel *K:*. Alice überprüft die Aktualität der Nachricht, indem sie die Aktualität der Nonce prüft, also um festzustellen, ob sie neu ist.

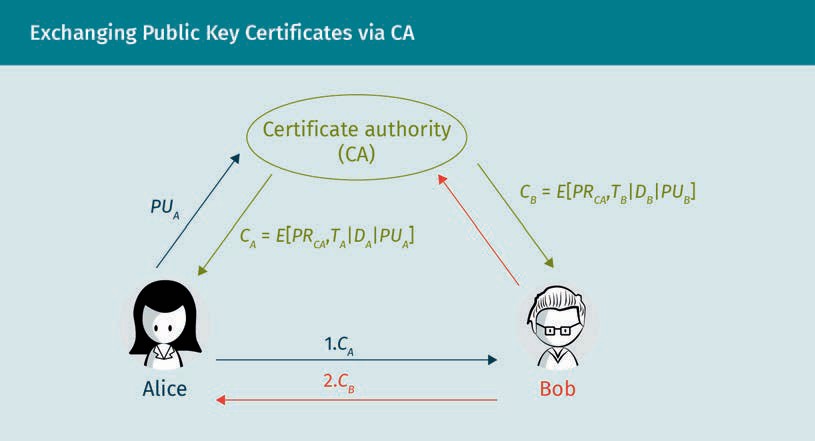
Alice sendet das Ticket daraufhin an Bob, der das Ticket mit dem zwischen ihm und dem KDC geteilten Hauptschlüssel *K4* entschlüsseln kann. Wenn Bob das Ticket entschlüsselt, stellt er sicher, dass es vom KDC erstellt wurde, da nur das KDC die ID von Alice verschlüsseln kann, und er weiß, dass der Sitzungsschlüssel *K:* vom KDC für die Kommunikation mit Alice erstellt wurde.

Bob sendet anschließend eine Nachricht an Alice, die eine Nonce *9*2 und seine mit dem Sitzungsschlüssel *K:* verschlüsselte ID enthält. Wenn Alice diese Nachricht erhält, weiß sie, dass sie mit Bob kommuniziert, weil *K:* nur zwischen ihnen genutzt wird. Alice führt dann eine vereinbarte Operation an *9*2 durch (zum Beispiel addiert sie 100 zu *9*2), verschlüsselt das Ergebnis mit *K:* und schickt es an Bob. Dies beweist Bob, dass er mit Alice kommuniziert, denn nur sie verfügt über den Sitzungsschlüssel *K:*.

###### Austausch von Public-Key-Zertifikaten

Öffentliche Schlüssel werden oft über eine Zertifizierungsstelle (CA) verteilt, wie nachfolgend dargestellt. Alice sendet ihren öffentlichen Schlüssel an die CA. Die CA verifiziert die Identität von Alice, erstellt ein Zertifikat ihres öffentlichen Schlüssels und sendet es an Alice. Das Zertifikat enthält den Zeitpunkt der Erstellung, die Gültigkeitsdauer, die ID von Alice und ihren öffentlichen Schlüssel und ist mit dem privaten Schlüssel der CA signiert.

Alice kann daraufhin ihr Zertifikat an beliebige Nutzer:innen senden oder es einfach veröffentlichen, so dass alle es einsehen können. Wir gehen davon aus, dass alle Nutzerinnen und Nutzer den öffentlichen Schlüssel der Zertifizierungsstelle kennen, so dass alle jeweils das Zertifikat von Alice mit dem öffentlichen Schlüssel der CA verifizieren und den öffentlichen Schlüssel von Alice erhalten können. Auf ähnliche Weise kann Bob sein Zertifikat erhalten und an Alice senden, wodurch sie seinen öffentlichen Schlüssel erhält.



Zusammenfassung

Diese Lektion betrachtete einseitige und gegenseitige Authentifizierungsprotokolle. Sie nutzen symmetrische und asymmetrische Verschlüsselungsalgorithmen unter Verwendung von geheimen Schlüsseln bzw. eines Paares aus privatem und öffentlichem Schlüssel. Es wurde die Bedeutung der Authentifizierung beleuchtet und die Frage, wie vertrauenswürdige Parteien die Authentizität von Nachrichten sicherstellen können. Darüber hinaus wurde gezeigt, wie wichtig es ist, mit zufälligen Aufforderungen andere Kommunikationspartner auf die Probe zu stellen, weil Angreifende das Challenge-and-Response-Verfahren durchbrechen und Imitationsangriffe starten können.

Zudem wurden Protokolle zur Erstellung von Sitzungsschlüsseln besprochen, die vorab oder über öffentliche Schlüssel ausgetauscht werden können, sowie die bei der Authentifizierung verwendete zufällige Aufforderung. Für die Erstellung und Verteilung von Sitzungsschlüsseln wird häufig eine Schlüsselverwaltungszentrale (KDC) genutzt. KDCs arbeiten hauptsächlich mit symmetrischer Schlüsselkryptographie und werden häufig in Systemen eingesetzt, die Nutzerinnen und Nutzern für eine bestimmte Zeit Zugang zu bestimmten Diensten gewähren. Eine Zertifizierungsstelle (CA) erzeugt digitale Zertifikate (d. h. Public-Key-Zertifikate).

Eine CA signiert auch digitale Zertifikate. Dazu nutzt sie ihren öffentlichen Schlüssel und ermöglicht so die Weitergabe und Verifizierung von Zertifikaten.



# Lektion 5

## Sicherheitsprotokolle

#### LERNZIELE

Nach Abschluss dieser Lektion werden Sie …

… die Verwendung, den Betrieb, die Architektur und die Modi der Internetprotokollsicherheit (IPsec) verstehen können.

… den Unterschied zwischen dem Tunnel- und dem Transportmodus in der IPsec identifizieren können.

… den durch *Encapsulating Security Payload* (ESP) und *Authentication Header* (AH) gewährleisteten Schutz der Vertraulichkeit und Authentizität erklären können.

… die Schichten der *Transport Layer Security* (TLS) bestimmen können, zu denen *Record Protocol*, *Handshake*, *Change Cipher Spec* und *Alert Protocols* gehören.

… Kerberos und seine Authentifizierungs- und Zugriffskontrolle, Tickets und Ticket Granting Tickets definieren können.

… *Pretty Good Privacy* (PGP) und *Secure/Multipurpose Internet Mail Extensions* (S/MIME) sowie deren Verwendung für die E-Mail-Sicherheit erörtern können.

DL-E-DLMCSEESN01\_E-U05

1. Sicherheitsprotokolle

### Einführung

Ein Netzwerkprotokoll ist ein festgelegter Satz von Regeln und Vereinbarungen für die Kommunikation zwischen verschiedenen Entitäten. Zusätzlich zu den Netzwerkprotokollen werden auch Sicherheitsprotokolle benötigt. Als Sicherheitsprotokoll kann eine Reihe von Regeln und Vereinbarungen für sichere Kommunikation verstanden werden. Folglich hat die Internet-Gemeinschaft Sicherheitsmethoden und ‑mechanismen in verschiedenen Anwendungsbereichen entwickelt, darunter E-Mail (z. B. Pretty Good Privacy [PGP] und Secure/Multipurpose Internet Mail Extensions [S/MIME]), Web-Zugang (z. B. Secure Sockets Layer) und Client/Server-Authentifizierung (z. B. X.509 Directory Authentication Service und Kerberos) und andere (Stallings & Brown, 2012). Durch die Implementierung von Sicherheit auf der Ebene des Internetprotokolls (IP) können Unternehmen ein sicheres Netzwerk für Anwendungen gewährleisten, die selbst über Sicherheitsmechanismen verfügen, ebenso wie für die vielen Anwendungen ohne integrierte Sicherheitsvorkehrungen (Stallings & Brown, 2012).

Authentifizierung, Integrität, Vertraulichkeit und Schlüsselverwaltung sind die vier wichtigsten Anforderungen und Mechanismen, die zur Gewährleistung und Durchsetzung von Sicherheit erforderlich sind. Der Authentifizierungsmechanismus beweist, dass eine empfangene Nachricht von der Partei gesendet wurde, die im Paketkopf als Quelle angegeben ist. Die Integritätsfunktion stellt sicher, dass die Nachricht während der Übertragung nicht verändert wurde. Vertraulichkeit gewährleistet die Geheimhaltung der Daten durch Verschlüsselung der Nachrichten, um das Abhören durch Angreifende oder nicht vertrauenswürdige Parteien zu verhindern. Zur Erfüllung der oben genannten Anforderungen ist schließlich ein Schlüsselverwaltungsmechanismus erforderlich, um den Austausch von Schlüsseln zu sichern (Stallings & Brown, 2012). In dieser Lektion werden verschiedene Bedrohungen sowie deren Abwehrmaßnahmen und Protokolle betrachtet.

### IP-Sicherheit (*IP Security*, IPsec)

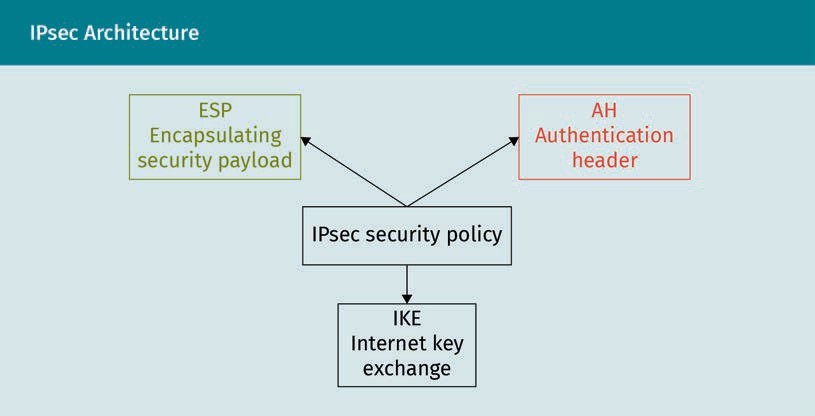
Eine der größten Schwächen des Internetprotokolls Version 4 (IPv4) ist, dass es die Authentifizierung von Quell-IP-Adressen nicht unterstützt. Wenn Bob zum Beispiel ein Paket empfängt, das die Quell-IP-Adresse von Alice enthält, kann er nicht sicher sein, dass die Nachricht von Alice stammt. Ein Mechanismus zur Authentifizierung der Quell-IP ist erforderlich, um die Echtheit der Nachricht zu gewährleisten.

Dieses Problem wird durch IPsec gelöst (Ferguson & Schneier, 2003). IPsec sorgt für die Authentifizierung von Quell-IP-Adressen, den Schutz der Vertraulichkeit und Integrität von Paketdaten sowie für die Authentizität von Paketdaten (und verhindert so das Wiederholen). IPsec ist eine Funktion, die mit jeder der aktuellen IP-Versionen (IPv4 oder IPv6) kombiniert werden kann, und die (durch zusätzliche Header) Sicherheitsfunktionen in den IP-Schichten bietet. Das Hauptmerkmal von IPsec, wodurch es unterschiedliche Anwendungen unterstützen kann, ist die Art und Weise, wie es alle Daten auf IP-Ebene verschlüsseln und authentifizieren kann (Ferguson & Schneier, 2003; Guttman et al., 2000; Stallings & Brown, 2012). Die Implementierung von Sicherheit auf der IP-Ebene kann allen Anwendungen ein sicheres Netzwerk garantieren, unabhängig davon, ob sie selbst Sicherheitsmechanismen bieten, weil alle Anwendungen auf der IP-Schicht laufen. So können alle verteilten Anwendungen gesichert werden, einschließlich Fernanmeldung, E-Mail, Dateiübertragung und Webzugriff.

###### IPsec Architektur

IPsec bietet Sicherheitsdienste auf der IP-Schicht, indem es einem System ermöglicht, die erforderlichen Sicherheitsprotokolle auszuwählen und die richtigen Algorithmen für die Dienste zu bestimmen (Ferguson & Schneier, 2003). Die Architektur umfasst Sicherheitsrichtlinien und Sicherheitsmechanismen, wie in der nachfolgenden Abbildung dargestellt. Die Sicherheitsrichtlinie legt fest, welcher Schutz auf der IP-Schicht erforderlich ist. Zu den Mechanismen, die zur Gewährleistung dieser Sicherheit eingesetzt werden, gehören das Internet Key Exchange Protocol (IKE) zur Aushandlung von Schutzparametern, einschließlich kryptographischer Algorithmen und Schlüssel, sowie die folgenden zwei Arten von Protokollen (Harkins, 1998; Perlman & Kaufman, 2001):

* 1. Authentifizierungs-Header (AH): Dieses Authentifizierungsprotokoll wird durch den Header des Protokolls bestimmt.
  2. Encapsulating security payload (ESP): Dabei handelt es sich um ein kombiniertes Verschlüsselungs- und Authentifizierungsprotokoll, das durch das Paketformat für dieses Protokoll gekennzeichnet ist.

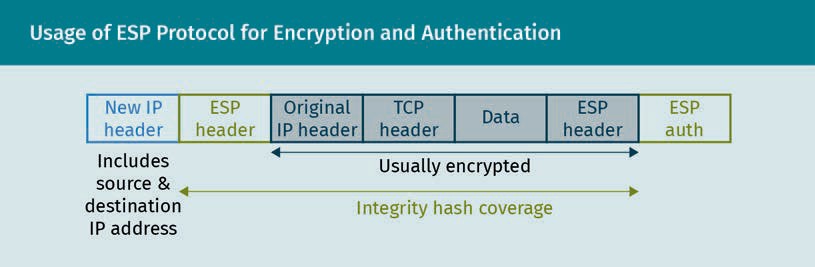


###### IPsec-Protokolle: Encapsulating Security Payload (ESP) und Authentifizierungs-Header (AH)

Die folgende Tabelle zeigt, welche Dienste die Protokolle AH und ESP bieten. Der AH sorgt für die Authentizität und Integrität der Pakete. ESP-Protokolle können mit oder ohne die Authentifizierungsoption sein. Wenn ein ESP genutzt wird, werden zum Schutz der Vertraulichkeit die Nutzdaten des Pakets verschlüsselt. Als zusätzliche Option kann die Nachrichtenauthentifizierung auf die verschlüsselten Nutzdaten und den IPsec-Header ausgeweitet werden.

|  |  |  |  |
| --- | --- | --- | --- |
| Von den Protokollen AH und ESP bereitgestellte Sicherheitsdienste | | | |
| Sicherheitsdienste | AH | ESP (nur Verschlüsselung) | ESP (Verschlüsselung und Authentifizierung) |
| Zugriffskontrolle | X | X | X |
| Integrität | X |  | X |
| Authentifizierung der Datenherkunft | X |  | X |
| Vertraulichkeit |  | X | X |

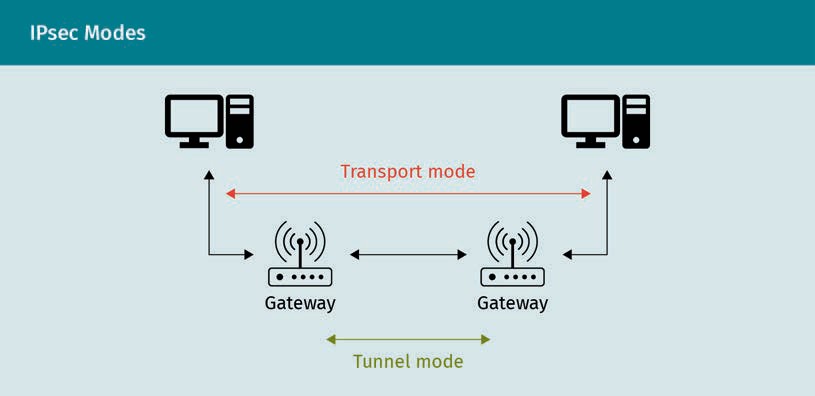
Ein ESP (Verschlüsselung und Authentifizierung) kann in einem IPsec-Tunnelmodus verwendet werden, wie in der folgenden Abbildung gezeigt. Neben dem neuen IP-Header wird ein ESP-Header hinzugefügt, und die Nutzdaten des Pakets werden verschlüsselt. Die Nutzdaten des Pakets enthalten die ursprünglichen IP-Header-Daten (d. h. die Quell- und Ziel-IP-Adressen), wie in der Abbildung gezeigt. Der Nachrichtenauthentifizierungscode wird über das erzeugte Gesamtpaket (das Originalpaket plus ESP-Header und Trailer) berechnet. Auf diese Weise wird sogar der Header der ursprünglichen IP authentifiziert (Perlman & Kaufman, 2001).



###### IPsec-Betriebsarten

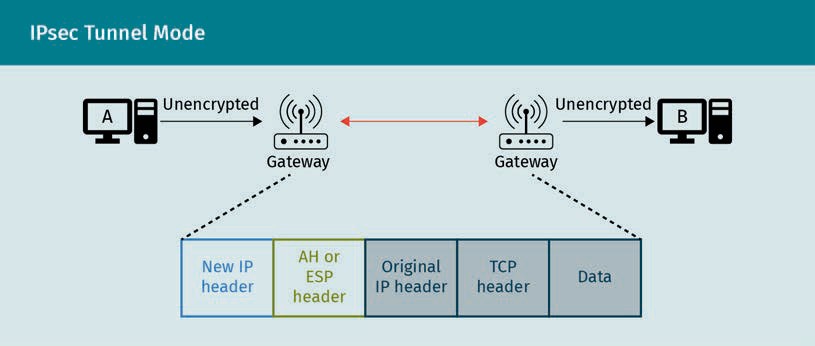
IPsec hat zwei Betriebsarten, Transport und Tunnel, wie die folgende Abbildung zeigt. Im Transportmodus sind die Quell- und Zielgeräte (also die beteiligten Endgeräte) für die Aushandlung der kryptographischen Grundlagen und die Aufrechterhaltung einer sicheren Verbindung verantwortlich. Aus diesem Grund wird sie auch als durchgängige Sicherheit (engl. *End-to-End*) bezeichnet. Im Tunnelmodus wird eine gesicherte Verbindung nicht nur von den Endgeräten, sondern auch von den Netzwerk-Gateways aufrechterhalten. Der Schutz des Datenverkehrs erfolgt über eine Reihe von Gateways (vom Gateway eines Netzwerks zum Gateway eines anderen Netzwerks), die somit Gateway-to-Gateway-Sicherheit bieten (Fruhlinger, 2021).

Auf diese Weise werden virtuelle private Netzwerke (VPNs) implementiert.



###### Tunnel-Modus

Angenommen, wir haben zwei Endhosts, *3* und *4*, die zum selben Unternehmen gehören, sich aber in zwei verschiedenen lokalen, über das Internet verbundenen Netzwerken befinden, wie in der folgenden Abbildung dargestellt. Wir nehmen einen IPsec-Tunnel zwischen den Gateways der beiden lokalen Netzwerke (LANs) an, so dass der Tunnel den Verkehr von *3* zu *4* schützt. Das bedeutet, dass *3* unverschlüsselte Datenpakete senden kann, das Gateway aber einen Schutz hinzufügt, bevor die Pakete das lokale Netzwerk verlassen. Es schickt die Pakete an das Netzwerk-Gateway von *4*, das sie entschlüsselt und an *4* weiterleitet.



Das Netzwerk-Gateway von *3* fügt einen neuen IP-Header und einen IPsec-Header hinzu. Der neue IP-Header enthält das Gateway von *3* als Quell-IP und das Gateway von *4* als Ziel-IP. Der neue IP-Header stellt sicher, dass das gesicherte Paket zuerst an das Gateway von *4* zugestellt wird. Der IPsec-Header enthält Informationen über den durch AH oder ESP gewährleisteten Schutz.

###### Internet-Schlüsselaustauschprotokoll (Internet Key Exchange, IKE)

Zur Nutzung von IPsec für sichere Verbindungen über das Internet müssen Endgeräte bzw. Gateways ein Sicherheitsprotokoll verwenden, das eine gegenseitige Authentifizierung und einen Schlüsselaustausch durchführt. Dieses Protokoll legt die Regeln fest, wie sich die beiden Parteien auf die zu nutzenden Sicherheitsmethoden einigen können. Dazu gehören unter anderem die Sicherheitsparameter (AH oder ESP) und die kryptografischen Algorithmen für Verschlüsselung oder Hashing. Dieses Sicherheitsprotokoll wird als IKE-Protokoll *(Internet Key Exchange)* bezeichnet (Harkins, 1998; Kaufman et al., 2010).

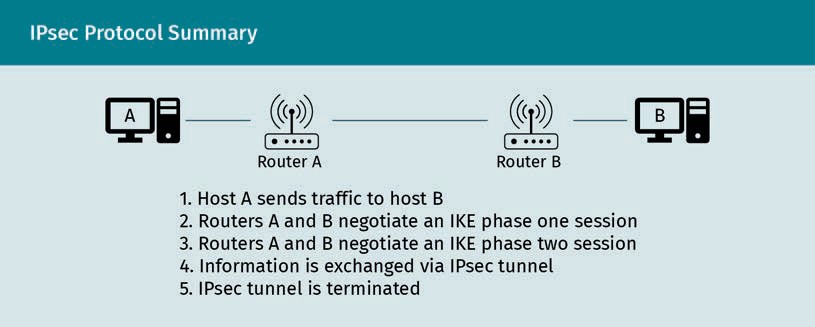
Mit anderen Worten: IKE wird zum Einrichten einer Sicherheitsverbindung (engl. *Security Association*, SA) in der IPsec-Protokollsuite genutzt. Eine SA spezifiziert die Sicherheitsparameter, die für eine sichere Kommunikation zwischen zwei Entitäten ausgetauscht werden. Zu den Sicherheitsparametern gehören unter anderem kryptographische Algorithmen, Verschlüsselungsschlüssel und Sitzungsschlüssel.

Wenn zwei Entitäten zum ersten Mal IPsec für die Kommunikation untereinander benötigen, müssen sie sich zunächst auf die zu verwendenden Sicherheitsparameter einigen, z. B. auf die Verschlüsselungs- und Authentifizierungsalgorithmen und Schlüssel. Sie müssen diese Parameter aushandeln und in einer SA speichern, und genau dafür wird IKE verwendet.

Das IKE-Protokoll besteht aus zwei Phasen. Die erste Phase umfasst die Einrichtung einer IKE-Sicherheitsverbindung (IKE-SA). Das liegt daran, dass die Aushandlung einer SA selbst geschützt werden sollte. Die IKE-SA kann das Aushandeln mehrerer IPsec-SAs absichern und dabei den SA-Aushandlungsverkehr von beiden Seiten (bidirektional) schützen (Kaufman et al., 2010).

In dieser ersten Phase eines IKE-Protokolls handeln beide Seiten den zu nutzenden Schutz (z. B. AH oder ESP) und die zu verwendenden Kryptoalgorithmen aus, wie z. B. Advanced Encryption Standard (AES) oder Hash-based Message Authentication Code (HMAC) mit Secure Hash Algorithm One (SHA-1). Sie erstellen dann ein gemeinsames Geheimnis. Zur Authentifizierung des gemeinsamen Geheimnisses können beide Seiten entweder einen gemeinsamen Schlüssel, digitale Signaturen oder die Verschlüsselung mit öffentlichen Schlüsseln verwenden. In der zweiten Phase eines IKE wird eine IPsec-SA eingerichtet. Es können mehrere IPsec-SAs ausgehandelt werden, um die in Phase eins eingerichtete IKE-SA abzusichern (Kaufman et al., 2010).

Die folgende Abbildung zeigt den typischen Ablauf, wenn zwei Entitäten sicher kommunizieren möchten.



Zuerst sendet der Host *3* Daten an den Host *4*. Zur Gewährleistung einer sicheren Verbindung greifen die Router oder Gateways von *3* und *4* auf das IKE-Protokoll zurück und handeln so die IKE-SA aus. Sie handeln dann mittels IKE-SA die IPsec-SAs aus und schaffen damit einen IPsec-Tunnel zwischen den beiden Routern. Dieser Tunnel schützt den Datenverkehr zwischen *3* und *4*. Die Paketdaten können verschlüsselt werden, und zusätzlich können auch die Header-Informationen (einschließlich der Quell-IP-Adresse und der Paketdaten) authentifiziert werden. Der IPsec-Tunnel zwischen den beiden Routern wird beendet, sobald eine der Parteien die Verbindung beendet (z. B., wenn *3* die Verbindung mit *4* abbricht).

### Transport Layer Security

Einer der am weitesten verbreiteten Sicherheitsdienste ist die Sicherheit auf der Transportschicht (engl. *Transport Layer Security*, TLS), die früher Secure Sockets Layer (SSL) genannt wurde. TLS hat mehrere Überarbeitungen durchlaufen, von SSL-Versionen 1.0–3.0 bis zu TLS-Versionen 1.0–1.3 (Dierks & Allen, 1999; Dierks & Rescorla, 2008). Obwohl TLS ursprünglich für das Hypertext Transfer Protocol (HTTP) entwickelt wurde, ist sie für jedes Übertragungssteuerungsprotokoll (*Transmission Control Protocol*, TCP) verwendbar.

TLS ist ein Allzweckdienst, der als eine Reihe von auf TCP basierenden Protokollen implementiert ist. Bei TLS authentifizieren sich beide Hosts (Clients und Server) vor der Verbindung mit digitalen Zertifikaten. Dazu findet zunächst ein gegenseitiger Identifizierungsprozess statt. Clients und Server tauschen ihre Zertifikate aus, um die Identität jeder Partei bei diesem Vorgang zu überprüfen. Das Server-Zertifikat (SSL-Zertifikat) authentifiziert die Identität des Servers. Es wird auf der Website installiert, damit der Webbrowser die Gültigkeit des Zertifikats überprüfen kann, bevor er sich mit der Website verbindet.

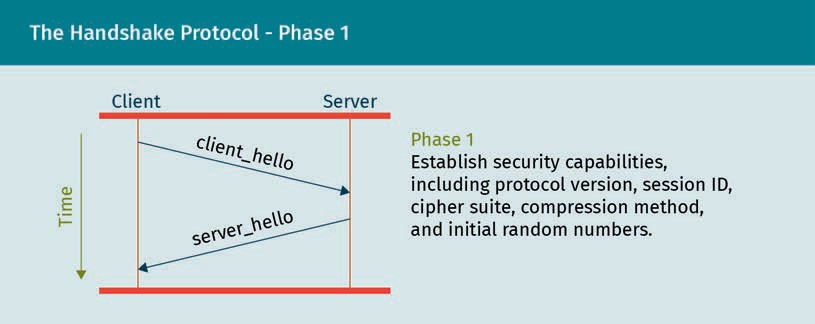
Auf dieser Ebene gibt es zwei Möglichkeiten zur Implementierung von TLS. Erstens kann TLS in spezielle Pakete eingebettet werden. Heute verfügen die meisten Browser über automatisch aktivierte SSL, und die meisten Webserver haben das Protokoll implementiert. Zweitens könnte TLS Teil der zugrundeliegenden Protokollsuite sein. Für Anwendungen ist es transparent.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TLS-Schichtenstruktur | | | | |
| Handshake-Protokoll | Protokoll zur Änderung der Chiffrierspezifikationen | Alert- Protokoll | HTTP | Heartbeat- Protokoll |
| Datensatzprotokoll | | | | |
| TCP | | | | |
| IP | | | | |

TLS ist dafür konzipiert, mit TCP einen zuverlässigen und sicheren durchgängigen Dienst (Ende-zu-Ende-Dienst) zu bieten. TLS verfügt über zwei Schutzschichten, wie die vorstehende Tabelle zeigt. Die Aufgabe des Datensatzprotokolls ist die Bereitstellung wesentlicher Sicherheitsdienste für verschiedene Anwendungsdaten (übergeordnete Protokolle) und die Überprüfung der Integrität und Herkunft. Ein HTTP-Protokoll kann zum Beispiel auf TLS aufbauen. Die Protokolle der höheren Schichten sind als Teil von TLS definiert. Dazu gehören das Handshake-Protokoll, das Protokoll zur Änderung der Chiffrierspezifikationen und das Alert-Protokoll (Dierks & Rescorla, 2008).

###### Das Handshake-Protokoll

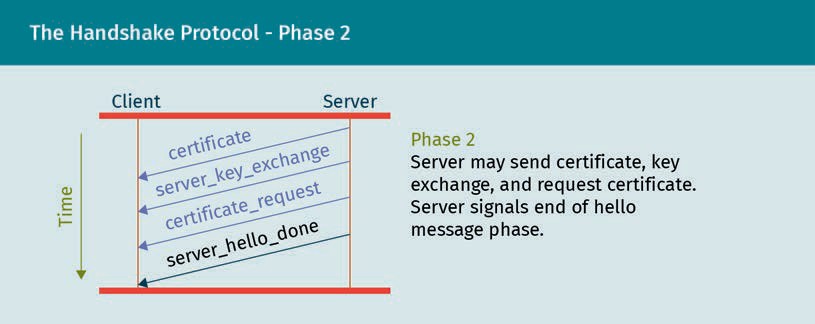
Über das TLS-Handshake-Protokoll werden die beteiligten Entitäten (Client und Server) authentifiziert, und es wird ausgehandelt, welche kryptografischen Protokollsuiten verwendet werden sollen. Das Handshake-Protokoll beinhaltet den Austausch von Nachrichten zwischen den kommunizierenden Teilnehmern (Dierks & Rescorla, 2008; Stallings & Brown, 2012). Die folgenden Abbildungen zeigen den anfänglichen Austausch, der für die Herstellung einer logischen Verbindung zwischen dem Server und dem Client notwendig ist. Das Handshake-Protokoll umfasst vier Phasen. In Phase eins wird eine logische Verbindung initiiert, um die Sicherheitsfunktionen auszuhandeln (d. h. Protokollversion, Sitzungs-ID, Cipher Suite, Kompressionsmethode usw.), wie in der folgenden Abbildung dargestellt.



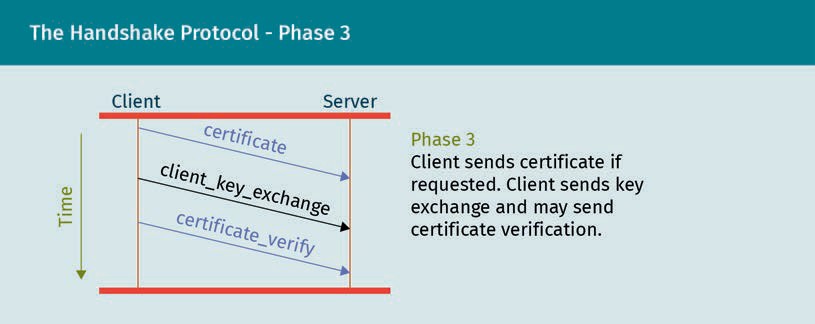
Der Client leitet eine Kommunikationsanfrage ein, indem er eine client\_hello-Nachricht mit den folgenden Parametern sendet:

* Version: Die höchste vom Client verwendete TLS-Version.
* Random: Eine zufällig generierte Zahl, die einen Replay-Angriff verhindern soll.
* Session ID: Eine Sitzungs-ID mit variabler Länge. Ein Wert ungleich Null bedeutet, dass der Client die Parameter einer bestehenden Verbindung aktualisieren oder eine neue Verbindung zu dieser Sitzung herstellen möchte. Der Wert Null bedeutet, dass der Client eine neue Verbindung in einer neuen Sitzung aufbauen möchte (Stallings & Brown, 2012).
* Cipher suite: Dies ist eine Liste mit den vom Client unterstützten kryptografischen Algorithmen.
* Compression method: Eine Liste der vom Client unterstützten Komprimierungsmethoden.

Die Einzelheiten der zweiten Phase (siehe Abbildung unten) hängen vom verwendeten Public-Key-Verschlüsselungsverfahren ab. Manchmal sendet der Server sein Zertifikat an den Client und wartet auf das Client-Zertifikat in der Antwort. Am Ende dieser Phase sendet der Server die Nachricht server\_done.

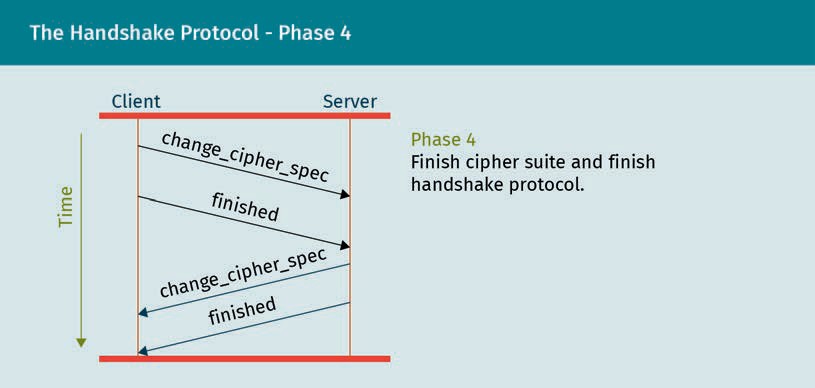


In Phase drei empfängt der Client die Nachricht server\_done und überprüft das Zertifikat des Servers (durch Prüfung des Ablaufdatums und der Zertifizierungsstelle). Außerdem prüft er, ob die server\_hello-Parameter in Ordnung sind, wie die folgende Abbildung zeigt. Je nach zugrunde liegendem Public-Key-Schema sendet der Client eine oder mehrere Nachrichten an den Server, wenn alles in Ordnung ist.



Die Einrichtung einer sicheren Verbindung wird in der vierten Phase abgeschlossen, wie unten gezeigt. Der Client sendet eine change\_cipher\_spec-Nachricht sowie die Abschlussnachricht mit den neuen Algorithmen und Schlüsseln. Am Ende wird eine Nachricht zur erfolgreichen Verifizierung gesendet. Diese zeigt den erfolgreichen Schlüsselaustausch und Authentifizierungsprozess an.

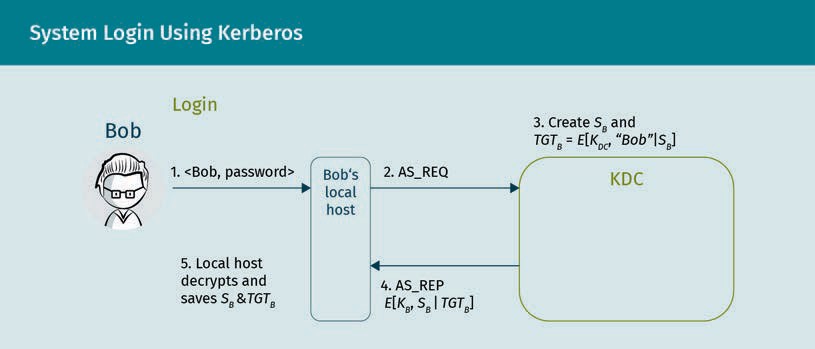
Als Antwort auf diese beiden Nachrichten sendet der Server seine Nachrichten change\_cipher\_spec und seine Abschlussnachricht. An diesem Punkt ist der Handshake abgeschlossen, und das Client-Server-Paar kann mit dem sicheren Datenaustausch beginnen.



### Kerberos

Kerberos ist ein Protokoll, das die Authentifizierung und Zugriffskontrolle zwischen vertrauenswürdigen Hosts in einer Netzwerkumgebung, in der Regel in einem Unternehmensnetzwerk, ermöglicht. Kerberos arbeitet auf der Grundlage von Tickets, um eine gegenseitige Authentifizierung zu ermöglichen, die es den Knoten erlaubt, ihre Identität gegenseitig auf sichere Weise nachzuweisen (Neuman & Ts'o, 1994; Steiner et al., 1988).

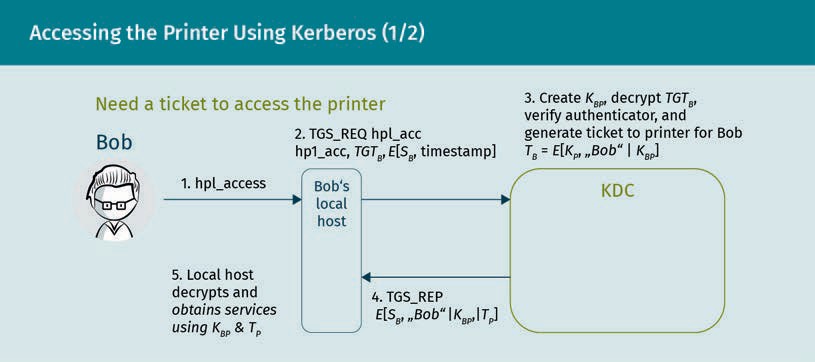
Die Hauptkomponente ist eine Schlüsselverwaltungszentrale (*Key Distribution Center*, KDC), in dem die geheimen Schlüssel aller Nutzer:innen und Dienste gespeichert sind. Sie bietet einen Authentifizierungsdienst (*Authentication Service*, AS) und eine Schlüsselverteilungsfunktionalität. Alle Nutzer:innen und Ressourcen im Netzwerk (z. B. Workstations und Drucker) haben also jeweils einen Hauptschlüssel, der mit den Kerberos-Servern geteilt wird. Alle Schlüssel werden sicher im KDC aufbewahrt.



Wie in der obigen Abbildung dargelegt, sendet der lokale Host des Nutzers Bob bei dessen Anmeldung eine Authentifizierungsanfrage (AS\_REQ) an das KDC. Das KDC erzeugt einen Tages-Sitzungsschlüssel *S4* und ein Ticket-Granting-Ticket mit *S4* sowie Bobs ID. Das KDC verschlüsselt das Ticket mit seinem Schlüssel *T=T4* = *E KD* , "Bob" *S4*.

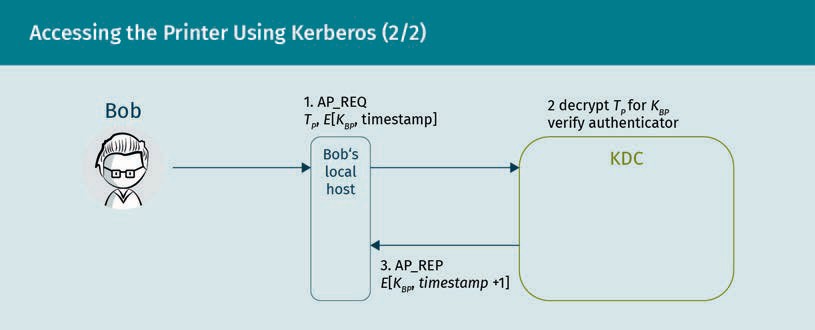
Das KDC sendet Bob daraufhin die mit dem Schlüssel *K4* verschlüsselte Nachricht mit dem Tages-Sitzungsschlüssel *S4* und dem Schlüssel *T=T4*. Da *K4* der zwischen Bob und dem KDC geteilte Hauptschlüssel ist, kann nur Bobs lokaler Host diese Nachricht entschlüsseln, und er speichert dann den Tages-Sitzungsschlüssel *S4* und *T=T4*. Bobs lokaler Host verwendet *S4* für anschließende Nachrichten mit dem KDC, so dass eine neue Anfrage an das KDC *T=T4* enthalten muss. Neue Tickets vom KDC müssen mit *S4* verschlüsselt werden.

Bei diesem Modell muss der lokale Host Bobs Passwort nicht speichern. Außerdem wird der zwischen Bob und dem KDC ausgetauschte Hauptschlüssel *K4* nur einmal pro Tag bei Bobs Anmeldung verwendet, was die Gefährdung des Hauptschlüssels begrenzt.



Angenommen, Bob möchte auf den Drucker namens hp1 zugreifen, wie in der obigen Abbildung zu sehen ist. Sein lokaler Host sendet eine Ticket-gewährende Dienstanfrage (*T=S*\_*REQ*) an das KDC. Die Anfrage enthält *T=T4* und ein weiteres Authentifikationselement, nämlich den mit Bobs Tagesschlüssel verschlüsselten aktuellen Zeitstempel *S4*.

Nachdem das KDC die Anfrage erhalten hat, entschlüsselt es *T=T4* und überprüft, ob der Zeitstempel gültig ist. Dies beweist, dass der Absender wirklich Bob ist, weil der zur Verschlüsselung des gültigen Zeitstempels verwendete Schlüssel *S4* nur Bob bekannt ist. Dann erstellt das KDC ein Ticket für Bobs Kommunikation mit dem Drucker. Der Drucker enthält einen Sitzungsschlüssel *K45* sowie Bobs ID, und er wird mit dem Hauptschlüssel des Druckers verschlüsselt. Ein Netzwerkgerät, wie z. B. ein Drucker, hat einen in der Konfiguration integrierten langen und zufälligen Hauptschlüssel, der in der Regel schwer zu erraten oder zu knacken ist. Daher wird das Ticket für diese Geräte mit ihren Hauptschlüsseln verschlüsselt.



Das KDC sendet die Antwort des Ticket-gewährenden Dienstes an Bobs lokalen Host. Sie enthält den Sitzungsschlüssel *K45*, Bobs ID sowie das Ticket für den Drucker, und sie wird mit Bobs Tagesschlüssel *S4* verschlüsselt. Daher kann nur Bobs lokaler Host diese Nachricht entschlüsseln und prüfen, ob sie vom KDC stammt, denn nur das KDC kann Bobs ID korrekt mit dem Schlüssel *S4* verschlüsseln. Es kann den Schlüssel *K45* und das Ticket für den Drucker protokollieren, wie in der obigen Abbildung dargestellt.

### Elektronische Post (E-Mail)

Elektronische Post (E-Mail) ist die am häufigsten genutzte netzwerkbasierte Anwendung, die auf allen Plattformen und Architekturen von einer Vielzahl von Nutzerinnen und Nutzern verwendet wird. Die Benutzer:innen erwarten, dass sie jederzeit E-Mails versenden oder empfangen können, unabhängig vom Standort oder der verwendeten Plattform (die heute meist ein Mobiltelefon ist; Schneier, 2015).

Angesichts der wachsenden Abhängigkeit von E-Mails im täglichen Leben sind Authentifizierungs- und Vertraulichkeitsdienste unerlässlich. Es gibt zwei Sicherheitsmodelle für die E-Mail-Übertragung: End-to-End (durchgängig) und Hop-to-Hop (Knoten zu Knoten). Pretty Good Privacy (PGP) und Secure/Multipurpose Internet Mail Extension (S/MIME) sind zwei Methoden, die eine durchgängige Verschlüsselung und digitale Signatur für E-Mails bieten. STARTTLS bietet Hop-to-Hop-Verschlüsselung (Knoten zu Knoten, mit TLS für E-Mail).

###### Pretty Good Privacy (PGP)

PGP ist eine quelloffene (Open-Source) Software für E-Mail, die von Philip Zimmermann entwickelt wurde (Garfinkel, 1995; Zimmermann, 1991). PGP gewährleistet die Vertraulichkeit und bietet Authentifizierungsdienste für elektronische Post und Dateispeicheranwendungen. PGP gewinnt zunehmend an Bedeutung und ist inzwischen weit verbreitet. Für ihr Wachstum können mehrere Gründe angeführt werden (Garfinkel, 1995):

* Es ist eine verfügbare, universelle Anwendung, die unabhängig von einem Betriebssystem und einem Prozessor ist und auf einem kleinen Satz einfacher Befehle basiert. PGP kann auf einer Vielzahl von Plattformen ausgeführt werden, darunter Windows, UNIX und Macintosh.
* Es basiert auf bekannten sicheren Algorithmen wie Rivest-Shamir-Adleman (RSA), Digital Signature Standard (DSS) und Diffie-Hellman für die Verschlüsselung mit öffentlichen Schlüsseln, Triple Data Encryption Algorithm (3DES) für die symmetrische Verschlüsselung und SHA-1 für das Hashing.
* Es ist vielseitig einsetzbar: Von Entitäten, die eine sichere Kommunikation erzwingen möchten, bis hin zu Nutzerinnen und Nutzern, die ihre persönlichen Daten verschlüsseln und sichere E-Mails versenden möchten.
* Das PGP-Paket mit Dokumentation, einschließlich des Quellcodes, sind frei verfügbar.
* Es wurde weder von einer Behörde- oder Normungsorganisation entwickelt noch jemals kontrolliert.

Es gilt zu beachten, dass in der PGP-Dokumentation der Begriff „geheimer Schlüssel“ für einen privaten Schlüssel verwendet wird. Dieser wird mit einem öffentlichen Schlüssel in einem Public-Key-Verschlüsselungsverfahren gepaart. Um Verwechslungen mit dem für die symmetrische Verschlüsselung verwendeten geheimen Schlüssel zu vermeiden, wird stattdessen der Begriff privater Schlüssel genutzt.

###### Beschreibung der Funktionsweise

Die eigentliche Funktion von PGP besteht aus vier Hauptanforderungen: Authentifizierung, Vertraulichkeit, Komprimierung und E-Mail-Kompatibilität.

Authentifizierung

Die Authentifizierung erfolgt über ein digitales Signaturverfahren. Die Nachricht oder Datei enthält die digitale Signatur der Nutzerin bzw. des Nutzers, die mit dem öffentlichen Schlüssel der jeweiligen Nutzerin leicht verifiziert werden kann. Diese Signaturen werden als angehängte Signaturen bezeichnet, weil sie an die entsprechende Nachricht oder Datei angehängt werden. Eine andere Art von Signatur wird jedoch als losgelöste Signatur bezeichnet. In diesem Fall wird die Signatur der Nutzerin oder des Nutzers getrennt von der signierten Nachricht gespeichert und übertragen. Die abgetrennte Signatur kann verwendet werden, wenn mehr als eine Partei eine Datei oder ein Dokument unterschreiben muss, z. B. einen Vertrag. Die Unterschrift jeder Partei ist unabhängig und wird daher nicht nur dem Dokument beigefügt. Andernfalls müssten die Unterschriften ineinander verschachtelt werden, wobei der zweite Unterzeichner sowohl das Dokument als auch die erste Unterschrift unterschreibt und so weiter (Garfinkel, 1995).

Vertraulichkeit

Ein weiterer grundlegender Dienst von PGP ist die Vertraulichkeit. PGP gewährleistet Datenvertraulichkeit, weil es Datenverschlüsselung während der Übertragung (Verschlüsselung der übertragenen Nachrichten) und im Ruhezustand (lokal als Dateien gespeichert) bietet. Eines der Hauptprobleme ist die Schlüsselverteilung, d. h. wie die Schlüssel für die Verschlüsselung verteilt werden. In PGP wird für jede Nachricht ein neuer symmetrischer Schlüssel generiert (eine zufällige 128-Bit-Zahl). Obwohl dies in der Dokumentation als Sitzungsschlüssel bezeichnet wird, handelt es sich also in Wirklichkeit um einen einmaligen Schlüssel. Da die Sitzungsschlüssel nur einmal verwendet werden, sind sie an die Nachricht gebunden und werden zusammen mit der E-Mail-Übertragung und ‑Speicherung übertragen (Garfinkel, 1995; Zimmermann, 1991).

Komprimierung

PGP komprimiert die Nachricht nach der Signatur, aber vor der Verschlüsselung, um Platz für die E-Mail-Übertragung und die Speicherung zu sparen. Als Kompressionsalgorithmus wird ZIP genutzt (Garfinkel, 1995; Zimmermann, 1991).

E-Mail-Kompatibilität

Bei der Verwendung von PGP zur Verschlüsselung einer Nachricht werden verschiedene Optionen angeboten. Wenn nur der Signierdienst verwendet wird, wird der private Schlüssel des Absenders zur Verschlüsselung der Nachricht verwendet. Wenn der Vertraulichkeitsdienst verwendet wird, werden die Nachricht und die Signatur (falls vorhanden) mit einem Sitzungsschlüssel verschlüsselt, einem einmalig generierten symmetrischen Schlüssel (Garfinkel, 1995; Zimmermann, 1991).

###### Kryptographische Schlüssel und Schlüsselringe

**Passphrase**   
Eine Passphrase ist eine längere Version eines Passworts, die sicherer und schwieriger zu erraten ist.

PGP nutzt vier Arten von Schlüsseln, darunter symmetrische Schlüssel für einmalige Sitzungen, öffentliche Schlüssel, private Schlüssel und **passphrasenbasierte** symmetrische Schlüssel (die zum Schutz privater Schlüssel verwendet werden, wie nachfolgend erläutert). In Bezug auf diese Schlüssel können drei verschiedene Anforderungen identifiziert werden (Garfinkel, 1995):

1. Die Erzeugung unvorhersehbarer Sitzungsschlüssel ist notwendig.
2. Allen Nutzenden muss es erlaubt sein, mehrere öffentliche und private Schlüsselpaare zu besitzen, weil sie ihre Schlüsselpaare vielleicht von Zeit zu Zeit und aus verschiedenen Gründen ändern wollen. Sie können dies zum Beispiel zur Erhöhung der Sicherheit machen, indem sie die Menge der mit einem bestimmten Schlüssel verschlüsselten Daten begrenzen.
3. Jede PGP-Entität muss eine Datei mit ihren eigenen öffentlichen und privaten Schlüsselpaaren und eine Datei mit den öffentlichen Schlüsseln der Korrespondenten führen.

PGP verwendet eine Passphrase, um einen privaten Schlüssel auf einem Rechner zu verschlüsseln. Der private Schlüssel wird mit einem Hash der Passphrase als geheimem Schlüssel verschlüsselt. Außerdem kann die Passphrase zur Entschlüsselung und zur Verwendung des privaten Schlüssels genutzt werden. Eine Passphrase sollte schwer zu erraten sein.

Schlüsselverwaltung

Die gewünschten E-Mail-Kommunikationspartner müssen den öffentlichen Schlüssel kennen, damit eine verschlüsselte E-Mail-Kommunikation stattfinden kann. Daher ist es notwendig, sie entweder direkt an die jeweiligen Kontakte zu übermitteln oder sie auf einen externen Schlüsselserver hochzuladen. Zur Verschlüsselung aller E-Mails an den Schlüsselinhaber wird der öffentliche Schlüssel verwendet. Der Austausch von öffentlichen Schlüsseln ist eine wesentliche Komponente, ohne die PGP nicht funktionieren würde. Je nachdem, welche Form von PGP verwendet wird, erfordert dieser Prozess einige Zwischenschritte, die für jeden Kommunikationspartner durchgeführt werden müssen. Da es jedoch möglich ist, dass sich eine Person mit einem öffentlichen Schlüssel als jemand anderes ausgibt, muss die Authentizität dieses Schlüssels verifiziert werden (Garfinkel, 1995).

PGP verwendet einen dezentralen Ansatz zur Überprüfung der Authentizität von Schlüsseln, das sogenannte **Web of Trust**. Im Gegensatz zur Public-Key-Infrastruktur (PKI), die sich auf eine zentrale Zertifizierungsstelle stützt, basiert ein Web of Trust auf Teilnehmenden, die sich gegenseitig ihr Vertrauen schenken und durch ihre Unterschrift bestätigen, dass öffentliche Schlüssel zu bestimmten Eigentümern gehören. Jedes Mal, wenn ein Schlüssel signiert wird, wird ein Zertifikat erstellt. Je mehr Zertifikate ein Schlüssel erhält, desto größer ist die Sicherheit, dass der Schlüssel dem angegebenen Eigentümer gehört. All dies erfordert jedoch technische Vorkenntnisse bei den Nutzerinnen und Nutzern, weil es für weniger erfahrene Personen weder einfach noch intuitiv zu bedienen ist.

Widerruf von öffentlichen Schlüsseln

Es kann sein, dass Nutzende ihren aktuellen öffentlichen Schlüssel widerrufen möchten, entweder weil der Schlüssel möglicherweise aufgedeckt wurde oder um zu vermeiden, dass derselbe Schlüssel über einen längeren Zeitraum verwendet wird. Das Aufdecken würde aber voraussetzen, dass Angreifende eine Kopie des privaten Schlüssels zusammen mit der Passphrase oder einer unverschlüsselten Version des privaten Schlüssels besitzen. Um einen öffentlichen Schlüssel zu widerrufen, stellt der Schlüsseleigentümer ein Schlüsselwiderrufszertifikat aus, das mit dem entsprechenden privaten Schlüssel des Eigentümers signiert ist (Garfinkel, 1995).

Zu erwähnen sei hier, dass auch ein Angreifer, der den privaten Schlüssel eines Besitzers aufgedeckt hat, ein solches Zertifikat ausstellen kann. Dies würde jedoch dem Angreifer und dem rechtmäßigen Besitzer die Verwendung des öffentlichen Schlüssels verwehren und ist daher eine weit weniger wahrscheinliche Bedrohung als die böswillige Verwendung eines gestohlenen privaten Schlüssels.

**Web of Trust** **(Netz des Vertrauens)**

Ein PGP-Vertrauens­netzwerk und ein dezentraler Ansatz zur Überprüfung der Authentizität von Schlüsseln.

###### S/MIME

Das MIME-Protokoll (*Multipurpose Internet Mail Extensions*) hat das SMTP-Protokoll (*Simple Mail Transfer Protocol*) ersetzt. Es erweiterte das Format von E-Mail-Nachrichten und unterstützt so Text in anderen Formaten als dem American Standard Code for Information Interchange (ASCII). Es hat auch den Austausch von Multimedia-Dateien wie Audio, Video, Bilder und Dokumente erleichtert, denn das SMTP-Protokoll unterstützte keine Multimedia-Dateien (Freed & Borenstein, 1996).

S/MIME ist eine sicherheitserweiterte Version des MIME-Internet-E-Mail-Formats, das weithin für den Versand digital signierter und verschlüsselter Nachrichten verwendet wird. Es ist eine durchgehende Verschlüsselungslösung für E-Mail-Nachrichten mit asymmetrischer Kryptographie (d. h. für das Senden und Empfangen verschlüsselter E-Mails; Dusse et al., 1998; Ramsdell, 2004).

###### S/MIME-Funktionalität

S/MIME ist in Bezug auf die Funktionalität PGP sehr ähnlich. Beide bieten die Möglichkeit, Nachrichten mit bekannten sicheren Algorithmen wie RSA, DSS und Diffie-Hellman für die Public-Key-Verschlüsselung, 3DES für die symmetrische Verschlüsselung und SHA-1 für das Hashing zu signieren und zu verschlüsseln (Stallings & Brown, 2012).

Verschlüsselung

Jeder S/MIME-Nutzer hat einen öffentlichen und einen privaten Schlüssel. Die asymmetrische Verschlüsselung wird für den Austausch des Sitzungsschlüssels genutzt, der dann zur Verschlüsselung der Nachricht (E-Mail-Inhalt) mit einem symmetrischen Verschlüsselungsalgorithmus dient. Der Absender verschlüsselt die Nachricht mit einem Sitzungsschlüssel und verschlüsselt daraufhin den Sitzungsschlüssel mit dem öffentlichen Schlüssel des Empfängers. Der Empfänger entschlüsselt also den Sitzungsschlüssel mit seinem privaten Schlüssel und entschlüsselt dann die Nachricht mit dem extrahierten Sitzungsschlüssel. Da bei S/MIME sowohl symmetrische als auch asymmetrische Verschlüsselung genutzt wird, ist es eine hybride Verschlüsselung.

Wie zuvor erwähnt, basiert die S/MIME-Verschlüsselung auf der vorherigen Kenntnis des öffentlichen Schlüssels des Empfängers. Daher verwendet S/MIME Public-Key-Zertifikate, die dem Standard X.509 entsprechen und von Zertifizierungsstellen signiert werden.

Signaturen

Verschlüsselung allein reicht für eine sichere Kommunikation nicht aus. Ohne Prüfung der Absenderidentität können verschiedene Angriffe wie Phishing erfolgen. Daher unterstützt S/MIMIE die Signatur von E-Mails zur Authentifizierung der Absenderidentität. So kann der Empfänger überprüfen, ob die E-Mail von einer vertrauenswürdigen Partei stammt. Das Erstellen einer eindeutigen Signatur erfolgt mit dem privaten Schlüssel des Absenders. Außerdem prüft der Empfänger die Signatur mit dem öffentlichen Schlüssel des Absenders.

###### S/MIME Probleme

S/MIME leidet unter den folgenden Beschränkungen (Stallings & Brown, 2012).

Größenbeschränkungen für Anhänge

Manchmal enthalten die angehängten Dateien sensible Daten, die sicher übertragen werden müssen. Die Verschlüsselung der angehängten Dateien erhöht die Dateigröße. Wenn dadurch die Größe der Datei auf mehr als 25 MB ansteigt, kann sie nicht über die reguläre E-Mail-Infrastruktur übermittelt werden, weil sie für die beteiligten E-Mail-Server zu groß wäre. Daher können die Anhänge nur unverschlüsselt versendet werden. S/MIME bietet zusätzliche Module für die Übertragung großer Datenmengen, die allerdings mit einem Aufpreis verbunden sind.

Nutzung statischer Schlüsselpaare

Im Gegensatz zu PGP nutzen S/MIME-Lösungen statische Schlüsselpaare (öffentliche und private Schlüssel) über ihre gesamte Gültigkeitsdauer hinweg. Wenn also der private Schlüssel einer Nutzerin aufgedeckt wurde, werden alle mit dem aufgedeckten Schlüssel zu entschlüsselnden Daten zugänglich.

Unverschlüsselte Übertragung von Metadaten

Während S/MIME die übertragene Nachricht verschlüsselt, sind Metadaten (wie die Betreffzeile) von der Verschlüsselung ausgeschlossen. Oftmals enthalten die Metadaten aber auch schon Daten, die wertvolle Informationen über die Nachricht preisgeben können. Diese Informationen können z. B. für soziale Manipulation (Social-Engineering-Angriffe) missbraucht werden.

Erkennung bösartiger Anhänge

Im Prinzip verschlüsselt S/MIME den gesamten Inhalt einer E-Mail, was es Anti-Virus- und Anti-Malware-Scannern erschwert, bösartige Anhänge oder Links in einer E-Mail zu erkennen.

Keine Ad-hoc-Kommunikation mit Quittungen ohne S/MIME

Nur Nutzer:innen, die S/MIME verwenden, werden in die Ad-hoc-Kommunikation einbezogen.

###### Unterschiede zwischen PGP und S/MIME

Sowohl PGP als auch S/MIME gehören zu den Standards der Internet Engineering Task Force (IETF). Dennoch wurde S/MIME zum Industriestandard für den Einsatz in Unternehmen, während PGP für viele Nutzer:innen die erste Wahl für die persönliche E-Mail-Sicherheit bleibt. Dafür gibt es die folgenden Gründe:

* S/MIME ermöglicht den Versand von E-Mails mit Multimedia-Inhalten, während PGP reine Text-E-Mails verarbeitet.
* PGP ist viel billiger als S/MIME.
* Im Gegensatz zu PGP nutzt S/MIME eine zentralisierte Schlüsselverwaltung, die effizienter ist.

###### STARTTLS

Im Gegensatz zu PGP und S/MIME bietet STARTTLS (Hoffman, 2002) eine Hop-to-Hop-Verschlüsselung (Knoten zu Knoten). STARTTLS ist ein E-Mail-Befehl, der dem Mailserver mitteilt, dass der Inhalt einer E-Mail mit SSL/TLS verschlüsselt werden muss. Das bedeutet, dass der Nutzer eine bestehende unsichere Verbindung in eine sichere verwandeln möchte.

STARTTLS unterstützt sowohl TLS als auch SSL. Obwohl TLS Teil des Namens ist, muss nicht zwingend TLS genutzt werden, die Nutzenden können stattdessen SSL verwenden.

STARTTLS kann die übertragenen Nachrichten vor passiven Lauschangriffen schützen. Darüber hinaus verschlüsselt STARTTLS die Metadaten und verhindert so Datenverluste.

Zusammenfassung

In dieser Lektion wurden sicherheitsspezifische Mechanismen in verschiedenen Anwendungen erklärt. Dazu gehören die sichere Kommunikation über das Internet mit IP Security (IPsec) und Transport Layer Security (TLS), elektronische Post (S/MIME, PGP) und Client/Server-Authentifizierung (Kerberos).

Zunächst wurde die Implementierung von Sicherheit auf IP-Ebene mit Hilfe von IPsec besprochen, das mit jeder Version des Internetprotokolls (IPv4 oder IPv6) kombiniert werden kann. Für die Authentifizierungs-, Vertraulichkeits- und Schlüsselverwaltungsdienste werden zusätzliche Header verwendet.

Die IPsec-Architektur umfasst Sicherheitsrichtlinien und Sicherheitsmechanismen. Diese legen fest, welcher Schutz auf der IP-Schicht erforderlich ist und beziehen das Internet Key Exchange Protocol (IKE) zur Aushandlung von Sicherungsparametern ein.

Als Zweites wurden TLS betrachtet, ein Allzweckdienst, der als eine Reihe von auf TCP basierenden Protokollen implementiert ist. TLS bietet Vertraulichkeit durch symmetrische Verschlüsselung und Nachrichtenintegrität durch einen Nachrichtenauthentifizierungscode. Außerdem wurden Ziel und Zweck von Kerberos bewertet, einem Authentifizierungsdienst, der für den Einsatz in einer verteilten Umgebung konzipiert wurde. Das Kerberos-System wird verwendet, um Nutzende und Geräte in einem Netzwerk zu authentifizieren und Zugriffskontrollen durchzusetzen. Für jeden Zugang ist ein Ticket erforderlich, für dessen Anforderung ein Ticket-gewährendes Ticket verwendet wird. Schließlich wurden verfügbare Softwarepakete und Standard-Internetansätze zur E-Mail-Sicherheit besprochen, darunter PGP, S/MIME und STARTTLS.



# Lektion 6

## Sicherheit in drahtlosen Netzwerken

#### LERNZIELE

Nach Abschluss dieser Lektion werden Sie in der Lage sein, …

… drahtlose Netzwerktechnologien und Sicherheitsrisiken zu verstehen.

… verschiedene Wi-Fi Sicherheitsprotokolle zu beschreiben.

… die Bluetooth- und ZigBee-Standards sowie ihre Nutzung zu erklären.

… die Sicherheitsmerkmale von Bluetooth und Zigbee zu erörtern.

DL-E-DLMCSEESN01\_E-U06

1. Sicherheit in drahtlosen Netzwerken

### Einführung

Drahtlose Netzwerke sind Netzwerke ohne Kabelverbindungen, die es Nutzerinnen und Nutzern ermöglichen, sich von verschiedenen Standorten aus mit dem jeweiligen Netzwerk zu verbinden, wodurch Mobilität ermöglicht wird. Drahtlose Netzwerke gehören heute zu den am meisten verwendeten Technologien in unserem täglichen Leben. Sie werden für Anrufe, das Surfen im Internet, Sofortnachrichtendienste, das Abrufen von E-Mails und weitere Dienste genutzt. Wir können Online-Dienste unabhängig von Ort, Zeit oder anderen Umständen nutzen (z. B. im Zug, am Bahnhof oder mitten in der Nacht).

Angesichts der unterschiedlichen Anforderungen sind drahtlose Technologien für Anwendungen entstanden, die die Bedürfnisse sehr vieler Nutzer:innen erfüllen. Jede dieser Technologien ist für eine bestimmte Aufgabe ausgelegt und verfügt über ihre je eigenen Merkmale. Heutzutage werden zahlreiche drahtlose Technologien in unserem täglichen Leben eingesetzt, darunter Wi-Fi, Bluetooth, ZigBee, Near Field Communication (NFC), Long Term Evolution (LTE) und Satellitendienste, um nur einige zu nennen. Die Arten von drahtlosen Netzwerken lassen sich anhand der geografischen Reichweite veranschaulichen, wie die folgende Tabelle zeigt (Rawat et al., 2013).

|  |  |  |  |
| --- | --- | --- | --- |
| Arten drahtloser Netzwerke | | | |
| Typ | Reichweite | Anwendungen | Normen |
| Wireless personal area network (WPAN) | In Reichweite einer Person | Kabelersatz für Peripheriegeräte | Bluetooth,  ZigBee, NFC |
| Wireless local area network (WLAN) | Innerhalb eines Gebäudes oder Geländebereichs | Drahtlose Erweiterung eines kabelgebundenen Netzes | IEEE 802.11  (Wi-Fi) |
| Wireless metropolitan area network (WMAN) | Innerhalb einer Stadt | Drahtlose Verbindung zwischen Netzwerken | IEEE 802.15  (WiMAX) |
| Wireless wide area network (WWAN) | Weltweit | Drahtloser Netzwerkzugang | Mobiltelefonie (UMTS, LTE, etc.) |
| Datenrate | 11 Mbps | 250 kbps | 1 Mbps |
| Reichweite | Ca. 100m | Ca. 10–100m | Ca. 10 m |

Wi-Fi, Bluetooth und Zigbee sind die drei am weitesten verbreiteten Standards in der drahtlosen Technologie und werden in intelligenten Häusern und beim Internet der Dinge eingesetzt. Daher konzentriert sich diese Lektion auf die genannten Technologien und ihre Sicherheitsspezifikationen. Die wichtigsten Merkmale dieser drei Standards sind in der folgenden Tabelle aufgeführt.

|  |  |  |  |
| --- | --- | --- | --- |
| Technischer Vergleich von Wi-Fi, Bluetooth und Zigbee | | | |
| Standard | IEEE802.11b | IEEE 802.15.1 | IEE 802.15.4 und  Zigbee-Allianz |
| Spezifikation | Wi-Fi | Bluetooth | Zigbee |
| Frequenzband | 2,4 GHz | | |
| Datenrate | 11 Mbps | 1 Mbps | 250 kbps |
| Reichweite | Ca. 100m | Ca. 10 m | Ca. 10–100m |
| Knotenpunkte | 32 | 7 | 65.536 |
| Stromverbrauch | Hoch | Niedrig | Sehr niedrig |

### Wi-Fi

Auf den IEEE 802.11-Standards basierende drahtlose LANs sind die weltweit am meisten verbreiteten Computernetzwerke. Diese werden gemeinhin als Wi-Fi bezeichnet. IEEE 802.11 ist Teil der technischen Norm IEEE 802, die für die Definition von LAN-Protokollen (Local Area Network) verwendet wird und die Protokolle für die Implementierung von WLAN-Netzwerken vorgibt. Basierend auf IEEE 802.11 können verschiedene Geräte (z. B. Smartphones, Laptops und Drucker) über drahtlose Verbindungen kommunizieren und auf das Internet zugreifen (Rawat et al., 2013).

Trotz der wachsenden Bedeutung drahtloser Verbindungen in unserem täglichen Leben, von der Unterhaltung bis hin zum beruflichen Kontext, sind sie zunehmend anfällig für Angriffe. Der Grund dafür liegt darin, dass auf drahtlose Netzwerke von außerhalb eines Gebäudes oder Geländes zugegriffen werden kann, wo auch immer das Signal zu orten ist. Bei kabelgebundenen Netzwerken ist das anders: Unbefugter Zugriff wird verhindert, weil die Netzwerkzugangspunkte (APs) innerhalb von Gebäuden isoliert oder schlecht zugänglich verbaut sind. Bei drahtlosen Netzwerken müssen Zugangspunkte (APs) von anderen Netzwerken isoliert werden, sodass nur autorisierte Nutzer:innen sicheren Zugriff auf den AP haben. Die drahtlose Sicherheit, auch bekannt als Wi-Fi-Sicherheit, soll verhindern, dass Unbefugte auf ein bestimmtes drahtloses Netzwerk zugreifen können, so dass die Daten nur für befugte Nutzerinnen und Nutzer zugänglich sind.

###### Wi-Fi-Sicherheit

Wired Equivalent Privacy (WEP) und Wi-Fi Protected Access (WPA) sind die von der Wireless Alliance entwickelten Authentifizierungs-Sicherheitsprotokolle für die drahtlose Sicherheit. Heute gibt es vier drahtlose Sicherheitsprotokolle (Frankel et al., 2007; Rawat et al., 2013):

Wired equivalent privacy (WEP)

Im September 1999 wurde WEP offiziell als Wi-Fi-Sicherheitsstandard anerkannt. WEP sollte die gleiche Sicherheitsstufe bieten wie bei kabelgebundenen Netzwerken. WEP ist jedoch eine äußerst gefährliche Lösung, da dieser Standard leicht zu knacken ist. Deshalb wurde es 2004 von der Wi-Fi Alliance aufgegeben (Lashkari et al., 2009; Tews, 2007).

**Pre-Shared Key** Ein Pre-Shared Key (vorab vereinbarter Schlüssel) ist ein zwischen Nutzerinnen und Nutzern ausgetauschtes Passwort oder eine Passphrase, mit dem ein Netzwerk aktiviert wird.

Wi-Fi protected access (WPA)

Im Jahr 2003 wurde Wi-Fi Protected Access (WPA) als Ersatz für den anfälligen WEP-Standard von der Wi-Fi Alliance eingeführt. WPA verwendet einen **Pre-Shared Key** (PSK) zur Authentifizierung von Nutzerinnen und Nutzern in WLANs. Es wird daher auch WPA-PSK genannt. WPA nutzt ein zeitbasiertes Schlüsselintegritätsprotokoll (engl.: *temporal key integrity protocol*, TKIP) zur Verschlüsselung und Nachrichtenintegrität. TKIP nutzt ein paketbezogenes Schlüsselsystem, das sicherer ist als das bei WEP eingesetzte feste Schlüsselsystem. Die TKIP-Verschlüsselung wurde später durch die erweiterte Verschlüsselung (engl.: *advanced encryption standard*, AES) abgelöst (Lashkari et al., 2009; Tews & Beck, 2009).

Wi-Fi protected access 2 (WPA 2)

WPA2 hat WPA im Jahr 2006 offiziell abgelöst (Lashkari et al., 2009). WPA2 erzwang die Verwendung von AES-Algorithmen und führte als Ersatz für TKIP den Zählermodus mit dem CCMP *(Cipher Block Chaining Message Authentication Code Protocol)* ein. Die Hauptschwachstelle von WPA2 erfordert, dass Angreifende, die Zugriff auf das gesicherte WLAN-Netzwerk haben, auf bestimmte Schlüssel zugreifen. Anschließend verwenden Angreifende diese Schlüssel, um weitere Geräte im Netzwerk anzugreifen.

Wi-Fi protected access 3 (WPA 3)

Die Wi-Fi Alliance hat WPA3 2018 als Ersatz für WPA2 eingeführt. WPA3 nutzt im WPA3-Enterprise-Modus eine 192-Bit-Verschlüsselung (AES-256 im Galois/Counter-Modus [GCM] mit SHA-384 als hashbasiertem Nachrichtenauthentifizierungscode [HMAC]). Im WPA3-Personal-Modus wird der WPA2-Verschlüsselungsalgorithmus (CCMP-128; AES-128 im CCM-Modus) eingesetzt (Reddy & Srikanth, 2019).

Von WEP bis WPA3 (Reddy & Srikanth, 2019) hat jede neue Art von Sicherheitsprotokoll das vorherige verbessert und erweitert. Die nachstehende Tabelle zeigt, wie sich die vier Generationen von Wi-Fi-Sicherheitsprotokollen in jeder Hinsicht voneinander unterscheiden.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Wi-Fi-Sicherheitsprotokolle | | | | |
|  | WEP | WPA | WPA2 | WPA3 |
| Jahr der Veröffentlichung | 1999 | 2003 | 2004 | 2018 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | WEP | WPA | WPA2 | WPA3 |
| Verschlüsselungsmethode | Rivest-Chiffre 4 (RC4) | Temporal Key Integrity Protocol (TKIP) mit RC4 | CCMP und AES | AES |
| Größe des Sitzungsschlüssels | 40 Bit | 128 Bit | 128 Bit | 128 Bit 192 Bit |
| Chiffre-Typ | Stream | Stream | Block | Block |
| Datenintegrität | CRC-32 | Integritätscode für Nachrichten | CBC-MAC | Sicherer Hash-Algorithmus |

### Bluetooth-Sicherheit

Bluetooth ist ein offener Standard für die Funkkommunikation im Nahbereich. Es ist für einen geringen Stromverbrauch und eine kurze Reichweite ausgelegt (Gehrmann et al., 2004). Bluetooth wurde daraufhin entwickelt, die folgenden Anforderungen zu erfüllen:

* Eliminierung einer kabelgebundenen Verbindung zwischen den Nutzern und dem elektronischen Gerät und für eine Verbindung ohne direkte Aktion der Nutzer:innen.
* Kommunikation mehrerer Geräte miteinander durch gleichzeitige Verbindung.
* Für eine nahtlose lokale Konnektivität, bei der Bluetooth-Geräte einander automatisch erkennen, Verbindungen herstellen und herausfinden, wie sie zusammenarbeiten können.

Bluetooth ist ein Chip, der in elektronische Geräte eingesteckt werden kann, um die oben genannten Ziele zu erreichen. So wurde Bluetooth in viele Arten von elektronischen Geräten für den Geschäfts- und Privatgebrauch integriert, darunter Smartphones, Laptops, Drucker, Fernsehgeräte, Tastaturen, Türen, Headsets, medizinische Geräte und viele andere.

###### Bluetooth-Geräteklassen

Wie bereits erwähnt, wurde Bluetooth für einen geringen Stromverbrauch und eine kurze Reichweite entwickelt. Die Übertragungsreichweite hängt direkt von der Leistungsklasse ab. Die Palette der Bluetooth-Geräte wird durch drei Klassen charakterisiert, welche die Energieverwaltung definieren. Die folgende Tabelle fasst die Klassen zusammen, einschließlich ihrer Leistungsstufen und Reichweiten in Metern (Padgette, et al., 2017).

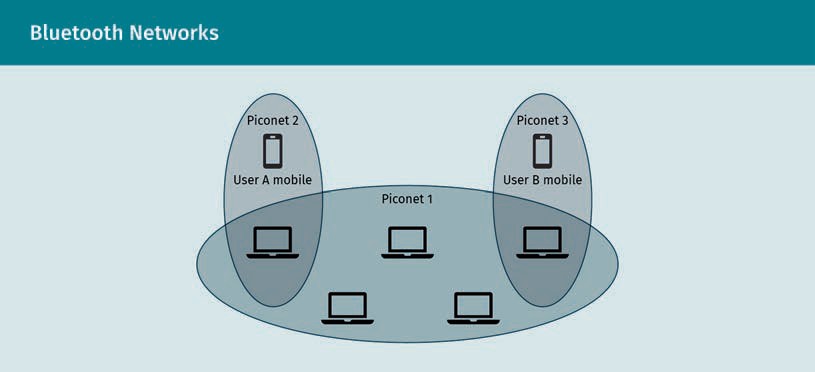
|  |  |  |  |
| --- | --- | --- | --- |
| Bluetooth-Geräteklassen | | | |
| Typ | Leistungsstufe | Vorgesehene Reichweite | Beispielgeräte |
| Klasse 1 | Hoch | Bis zu 100 m | USB-Adapter, Zugangspunkte (Access Points) |
| Klasse 2 | Mittel | Bis zu 10 m | Mobile Geräte, Bluetooth-Adapter, Chipkartenleser |
| Klasse 3 | Niedrig | Bis zu 1 m | Bluetooth-Adapter |

###### Bluetooth-Netzwerke: Piconets

**Piconet**   
Eine Verbindung zwischen einem Telefon und einem Headset mit Bluetooth-Technologie ist ein Beispiel für ein Piconet.

Ein Bluetooth-Netzwerk umfasst mindestens zwei Geräte und kann bis zu acht Geräte verbinden. Die Verbindung zwischen diesen Geräten wird als **Piconet** bezeichnet. Die Geräte können schnell, unmittelbar und sicher ein Piconet bilden und miteinander kommunizieren. Bei der Einrichtung eines Piconets und während der gesamten Dauer der Piconet-Verbindung fungiert ein Gerät als Master und die anderen als Slaves (Gehrmann et al., 2004; Padgette, et al., 2017). Ein Gerät kann Teil von mehr als einem Piconet sein, entweder als Slave oder als Master. Das bedeutet, dass ein Gerät als Master in einem Piconet und als Slave in einem anderen fungieren kann, wodurch eine Kette von Piconets, ein sogenanntes Scatternet, entsteht (Padgette et al., 2017).

So bilden mehrere unabhängige Piconets mit sich überschneidenden Versorgungsgebieten ein Scatternet. Ein Scatternet ermöglicht die Kommunikation zwischen Piconets. Die Bluetooth-Kernprotokolle bieten jedoch für Scatternet-Geräte keine Multi-Hop-Funktionen zum Netzwerk-Routing. In der folgenden Abbildung zum Beispiel kann die Kommunikation zwischen den Mobiltelefonen der Nutzenden A und B nicht stattfinden, weil sich beide in unterschiedlichen Piconets befinden. Ohne Aufbau eines zusätzlichen Piconets ist eine Übertragung nicht möglich (Padgette et al., 2017).



###### Verbindungsaufbau

Die folgenden Schritte müssen durchlaufen werden, damit Bluetooth-Geräte miteinander kommunizieren können.

Erkennung (engl. *discovery*)

Zur Verbindung eines Bluetooth-Geräts muss die Bluetooth-Funktion aktiviert sein und das Gerät sollte sich im Erkennungsmodus befinden. Sobald Bluetooth aktiviert ist, ist das Gerät im 2,4-GHz-Band sichtbar. Andere Bluetooth-Geräte können es dann erkennen und sich mit ihm koppeln und verbinden. Entsprechend verhindert die Einstellung des Bluetooth-Geräts auf den Modus „nicht sichtbar“ (engl. *un-discoverable*), dass andere Bluetooth-Geräte es identifizieren können.

Suche/Anfrage (engl. *search/inquiry*)

Wenn mehrere Bluetooth-Geräte auf den Erkennungsmodus eingestellt sind, können sie alle einen Suchlauf (Abfragescan) starten, um verfügbare, sich in Reichweite befindende Geräte zu finden. Mindestens zwanzig Geräte können von einem Anfragescanner entdeckt werden (Padgette et al., 2017). Die Scanning-Geräte lauschen auf bestimmten Frequenzen auf Anfragen. Wenn eine Anfrage eingeht, sendet das Scanning-Gerät dem anfragenden Gerät die notwendigen Informationen, um eine Verbindung herzustellen.

Zur Aufrechterhaltung der Sicherheit muss erkannt werden, welche Geräte verbunden werden können. Bluetooth nutzt einen einmaligen Passkey für die Geräteauthentifizierung. Ein Passkey ist wie ein Passwort oder PIN-Code, den beide Geräte für den Verbindungsaufbau akzeptieren müssen.

Koppeln (engl. *pairing*)

Koppeln der Geräte bedeutet, dass die Verbindung akzeptiert wird. Sobald der Passkey akzeptiert wird, werden die beiden Geräte gekoppelt. Das Koppeln erfolgt, nachdem die Identitäten der beteiligten Geräte authentifiziert wurden und eine verschlüsselte Verbindung hergestellt ist. Für die verschlüsselte Verbindung tauschen die beteiligten Geräte einen temporären Schlüssel (*temporary key*, TK) aus, der zur Erstellung eines kurzfristigen Schlüssels (*short-term key*, STK) zur Verschlüsselung der Verbindung verwendet wird. Dies gewährleistet eine sichere, vertrauenswürdige Verbindung (Gehrmann et al., 2004). Sobald Bluetooth-Geräte gekoppelt sind, wird eine gesicherte Verbindung hergestellt, und die Geräte können Informationen austauschen.

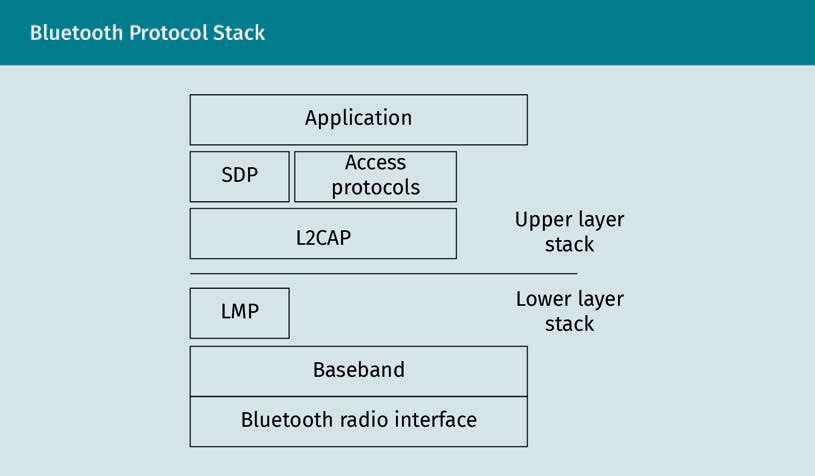
Bindung (engl. *bonding*)

Praktischerweise können sich Bluetooth-Geräte, die schon einmal verbunden waren, ohne manuellen Eingriff automatisch wieder verbinden, sobald sie sich in Reichweite befinden (d. h. ohne die vorherigen Schritte zu wiederholen). Dazu wird der Bindungsvorgang genutzt. Die Bindung (Bonding) ist ein Prozess, bei dem die bei der ersten Kopplung gesammelten Informationen (z. B. die Identitäten der Geräte) gespeichert werden, so dass bei wiederholten Verbindungen bekannter Geräte die Kopplung nicht jedes Mal wiederholt werden muss.

Mit anderen Worten: Sobald das Koppeln abgeschlossen ist, wird eine Verbindung zwischen den beiden Geräten hergestellt, die es ihnen ermöglicht, sich in Zukunft zu verbinden, ohne ihre Identitäten erneut zu bestätigen. Diese Bindung lässt sich bei Bedarf aufheben (Stirparo & Löschner, 2013).

###### Bluetooth Architektur und Protokollstapel

Die Bluetooth-Architektur (oder der Protokollstapel) besteht aus zwei Schichten. Diese spezifizieren das hardwarebasierte Funksystem (die untere Schicht) und die Verbindungen zwischen den Schichten (den Software-Stack der oberen Schicht), wie in der folgenden Abbildung dargestellt.



###### Untere Stapelschichten

Die Grundlage des Bluetooth-Protokolls ist die Bluetooth-Funkschnittstelle. Dies entspricht der physikalischen Schicht in einem TCP/IP-Protokoll. Die Funkschnittstelle spezifiziert die Übertragung von Funkwellen. Sie beschreibt die drahtlose Schnittstelle, Frequenzbänder, Frequenzsprungverfahren und Modulationstechniken.

Oberhalb der Funkschicht befinden sich das Basisband und das „Link Controller/Link Manager“-Protokoll (LMP). Das Basisband ist für die Datenformatierung zuständig. Es definiert die Anforderungen an die Übertragung, einschließlich Timing, Paketrahmenformat, Algorithmen zur Leistungssteuerung und Ablaufsteuerung der Verbindung. Mit LMP werden die logischen Verbindungen zwischen Bluetooth-Geräten hergestellt und die Kommunikationsverbindungen aufrechterhalten. Es wird für die Geräteauthentifizierung, die Nachrichtenverschlüsselung und die Aushandlung von Paketgrößen verwendet (Stirparo & Löschner, 2013).

###### Obere Stapelschichten

Unter Verwendung der Technologie der unteren Stapelschichten legen die oberen Stapelschichten die Spezifikationen fest, die für die Verbindung von Geräten und die Kommunikation zwischen ihnen erforderlich sind. Zunächst verfolgt das „Logical Link Control and Adaption Protocol“ (L2CAP) die Datenpakete und passt das Rahmenformat der oberen Schicht an die Basisbandschicht an. L2CAP bietet Unterstützung sowohl für verbindungsorientierte als auch für verbindungslose Dienste (Gehrmann et al., 2004).

Außerdem bietet das Service Discovery Protocol (SDP) die Schnittstelle zum Link Controller und ermöglicht die Interoperabilität zwischen Bluetooth-Geräten. Das SDP erledigt dienstbezogene Abfragen wie z. B. Geräteinformationen und stellt so eine Verbindung zwischen konkurrierenden Bluetooth-Geräten her (Gehrmann et al., 2004).

###### Bluetooth-Sicherheitsfunktionen

Wir betrachten im Folgenden die drei grundlegenden Sicherheitsanforderungen, die in den Bluetooth-Standards festgelegt sind:

1. Authentifizierung: Bluetooth bietet eine Geräteauthentifizierung und keine Benutzer-Authentifizierung. Mit anderen Worten: Bluetooth stellt die Authentifizierung sicher, indem es die Identitäten der kommunizierenden Geräte auf der Grundlage ihrer jeweiligen Bluetooth-Adressen verwendet.
2. Vertraulichkeit: Die Vertraulichkeit wird gewährleistet, indem verhindert wird, dass Unbefugte eine Verbindung herstellen, auf die übertragenen Daten zugreifen oder diese einsehen können. Wie bereits erwähnt, tauschen die Geräte nach dem Koppeln einen temporären Schlüssel (TK) aus. Mit diesem wird ein kurzfristiger Schlüssel (STK) erstellt, mit dem die eigentliche Verbindung verschlüsselt wird.
3. Autorisierung: Dadurch können nur autorisierte Geräte einen Dienst nutzen.

Auf der Grundlage der skizzierten Sicherheitsanforderungen legen die verschiedenen Bluetooth-Versionen vier Sicherheitsmodi fest. Jede Bluetooth-Version unterstützt einige, aber nicht alle der vier Modi. Außerdem muss jedes Bluetooth-Gerät in mindestens einem der vier unten beschriebenen Modi arbeiten:

* 1. Sicherheitsmodus eins ist ein unsicherer Modus, der die Sicherheitsfunktionen (Authentifizierung und Verschlüsselung) umgeht, wodurch das Gerät und die Verbindungen anfällig für Angreifende sind. Bluetooth-Geräte in diesem Modus verwenden keine Mechanismen, um andere bluetoothfähige Geräte daran zu hindern, Verbindungen herzustellen (Gehrmann et al., 2004).
  2. Im Sicherheitsmodus zwei steuert ein zentraler Sicherheitsmanager (wie in der Bluetooth-Architektur spezifiziert) den Zugriff auf bestimmte Geräte und Dienste (Gehrmann et al., 2004; Padgette et al., 2017). Der Sicherheitsmanager verwaltet verschiedene Zugriffskontrollrichtlinien, Schnittstellen und Vertrauensstufen mit anderen Geräten und Protokollen. Mit anderen Worten: In diesem und allen späteren Sicherheitsmodi gibt es ein Autorisierungskonzept.
  3. Im Sicherheitsmodus drei leitet ein Bluetooth-Gerät vor der Herstellung einer physischen Verbindung die Sicherheitsverfahren ein. Bluetooth-Geräte, die in diesem Modus arbeiten, erzwingen Verschlüsselung und Authentifizierung (unidirektional oder gegenseitig) für alle Verbindungen (Garg, 2007).
  4. Sicherheitsmodus vier verbessert die Sicherheit durch die Verwendung von Public-Key-Kryptographie zum Schutz vor passivem Abhören und Man-in-the-Middle-Angriffen (MITM) während der Kopplung (Padgette et al., 2017).

###### Dienststufen

Bluetooth legt drei Stufen der Dienstsicherheit fest (Gehrmann et al., 2004):

1. In der ersten Dienststufe (Service Level) sind sowohl die Autorisierung als auch die Authentifizierung erforderlich. Automatischer Zugriff wird nur vertrauenswürdigen Geräten gewährt, und für nicht vertrauenswürdige Geräte wird nur eine manuelle Autorisierung verwendet.
2. Dienststufe zwei erfordert nur einen Authentifizierungsprozess und keine Autorisierung.
3. In Dienststufe drei ist weder eine Authentifizierung noch eine Autorisierung erforderlich. Der automatische Zugriff wird gewährt.

### ZigBee-Sicherheit

ZigBee wurde als digitales Ad-hoc-Funknetz in den 1990er Jahren als Alternative zu kabelgebundenen Netzwerken entwickelt. Im Gegensatz zu Wi-Fi oder Bluetooth eignet sich ZigBee besser für Anwendungen in industriellen Automatisierungs- und Steuerungssystemen, bei denen die Endknoten eine geringe Datenmenge in regelmäßigen Abständen übertragen müssen, einen geringen Stromverbrauch (und eine lange Batterielebensdauer) haben und eine kurze Übertragungsdistanz zu einem zentralen Überwachungssystem aufweisen müssen. Deshalb wird Zigbee in drahtlosen Sensornetzwerken, der Haushaltsautomatisierung, der intelligenten Energiemessung und der Automatisierung im Gesundheitswesen eingesetzt (Rudresh, 2018; Silicon Labs, 2018).

###### Sicherheitsarten

Der ZigBee-Standard unterstützt die beiden Sicherheitsmodelle zentralisiert und verteilt.

Zentralisiertes Sicherheitsmodell

Ein einzelner Knoten, das sogenannte Trust Center, ist für die Aufrechterhaltung der gesamten Netzwerksicherheit verantwortlich (Silicon Labs, 2018). Das Trust Center agiert wie ein Netzwerkkoordinator, der für Folgendes verantwortlich ist:

* Konfiguration und Authentifizierung von Endgeräten und Routern, die dem Netzwerk beitreten.
* Erstellung eines Netzwerkschlüssels mit begrenzter Lebensdauer zur Verschlüsselung der Kommunikation über das Netzwerk.
* Ständiges Erstellen und Wechseln neuer Netzwerkschlüssel. So wird verhindert, dass Angreifende, die einen Netzwerkschlüssel erlangt haben, diesen lange nutzen können.
* Erstellen und Verteilen eines eindeutigen Verbindungsschlüssels zum Trust Center für jedes Gerät, sodass sicher mit dem Trust Center kommuniziert werden kann.

Verteiltes Sicherheitsmodell

Router bilden das verteilte Netzwerk. Im Gegensatz zum zentralisierten Modell ist keine bestimmte Entität für die Aufrechterhaltung der Netzwerksicherheit verantwortlich. Router ermöglichen es anderen Routern und Endgeräten, dem Netzwerk beizutreten. Sie generieren die Netzwerkschlüssel für neu hinzugekommene Endgeräte und Router, so dass alle Netzwerkknoten denselben Netzwerkschlüssel für die Verschlüsselung von Nachrichten verwenden.

###### Sicherheits-Schlüssel

ZigBee nutzt drei Arten von symmetrischen 128-Bit-Schlüsseln: Netzwerk-, Haupt- und Verbindungsschlüssel (Rudresh, 2018; Silicon Labs, 2018).

* Netzwerkschlüssel: Dieser wird für die Rundspruchkommunikation genutzt. Das Trust Center erstellt den Netzwerkschlüssel und verteilt ihn an alle Geräte, die berechtigt sind, dem Netzwerk beizutreten. Mit anderen Worten: Alle autorisierten Geräte im Netzwerk haben eine Kopie des Netzwerkschlüssels. Mit dem Netzwerkschlüssel können die Geräte sicher miteinander kommunizieren. Der Netzwerkschlüssel wird in regelmäßigen Abständen aktualisiert. Er ist daher mit einer Sequenznummer versehen, die es den Geräten ermöglicht, eine bestimmte Schlüsselinstanz zu identifizieren (Rudresh, 2018; Silicon Labs, 2018).
* Hauptschlüssel: Der Hauptschlüssel bildet die Grundlage für langfristige Sicherheit zwischen zwei Geräten.
* Verbindungsschlüssel: Mit einem Verbindungsschlüssel (auch Peer-to-Peer-Schlüssel genannt) wird die durchgängige (Ende-zu-Ende) Sicherheit gewährleistet, so dass zwei Geräte sicher Nachrichten über das Zigbee-Netzwerk senden können, ohne sie mit einem anderen Gerät zu teilen. Die Verbindungsschlüssel sind also nur den beiden Geräten bekannt. Die Verbindungsschlüssel minimieren die Sicherheitsrisiken im Zusammenhang mit der Verteilung des Hauptschlüssels (Rudresh, 2018; Silicon Labs, 2018).

###### Schlüsselverwaltung

Ein Gerät erwirbt Schlüssel mithilfe verschiedener Schlüsselherstellungsmechanismen (Silicon Labs, 2018):

* + Vorinstallation: Dies gilt nur für Hauptschlüssel. Der Hersteller baut während der Konfigurationsphase einen Hauptschlüssel in das Gerät ein.
  + Schlüsselerstellung: Dabei handelt es sich um eine lokale Methode zur Erstellung von Verbindungsschlüsseln auf der Grundlage des Hauptschlüssels. Die an der Kommunikation beteiligten Geräte müssen im Besitz des Hauptschlüssels sein, den sie durch die Vorinstallation, den Schlüsseltransport oder eine Eingabe durch die Nutzenden erhalten haben.
  + Schlüsseltransport: Hierzu fordert das Netzwerkgerät einen Verbindungsschlüssel vom Trust Center an. Das Trustcenter kann im Industrie- oder Heimmodus arbeiten (Silicon Labs, 2018).
    - Industriemodus: Das Trust Center führt eine Liste aller Geräte und Schlüssel (Haupt-, Netzwerk- und Verbindungsschlüssel).
    - Heimmodus: Das Trust Center bewahrt nur den Netzwerkschlüssel auf und steuert den Netzzugang, während alle anderen Informationen in den einzelnen Knoten gespeichert werden.

###### Sicherheitsmaßnahmen im ZigBee-Stapel

**AES-CCM**

Dies ist eine geringfügige Abwandlung des Advanced Encryption Standard (AES) mit einem modifizierten Zähler mit CBC-MAC-Modus (CCM).

Der ZigBee-Standard nutzt einen 128-Bit-**AES-CCM**-Verschlüsselungsalgorithmus für die folgenden Zwecke:

* Gewährleistung der Datenvertraulichkeit durch Verschlüsselung der übertragenen Pakete.
* Gewährleistung der Datenintegrität durch einen Message Integrity Code (MIC) oder Message Authentication Code (MAC).

Der ZigBee-Standard schützt vor Replay-Angriffen und bietet Geräteauthentifizierung (Rudresh, 2018).

Replay-Schutz

Jeder Knoten im ZigBee-Netzwerk enthält einen 32-Bit-Rahmen-Zähler, der bei jeder Paketübertragung um eins erhöht wird. Außerdem kennt jeder Knoten den Rahmen-Zähler der direkt verbundenen Knoten. Wenn also ein Knoten ein Paket von einem benachbarten Knoten empfängt, das den gleichen oder einen kleineren Wert hat als der eigene Zählerwert, wird das Paket verworfen. Der gleiche oder ein kleinerer Wert des Rahmen-Zählers bedeutet, dass dieses Paket schon einmal gesendet wurde (d. h. es wird erneut gesendet). Dieser Mechanismus gewährleistet einen Replay-Schutz, indem er Pakete verwirft, die der Knoten bereits empfangen hat (Rudresh, 2018).

Geräte-Authentifizierung

Der ZigBee-Standard unterstützt sowohl die Geräte- als auch die Datenauthentifizierung. Bei der Geräteauthentifizierung wird die Authentizität eines neuen, dem Netzwerk beitretenden Geräts, überprüft. Bei erfolgreicher Verifizierung erhält das neue Gerät einen Netzwerkschlüssel und eine Reihe anderer Attribute, damit es als authentifiziert gilt (Rudresh, 2018).

###### Schwachstellen von ZigBee

Die größte Sicherheitsschwäche von Zigbee ergibt sich direkt aus seiner Implementierung, denn die meisten ZigBee-Geräte sind batteriebetrieben, haben eine geringe Rechenleistung und verfügen über einen kleinen Speicher (Silicon Labs, 2018). So werden die im ZigBee-Netzwerk verwendeten Schlüssel im Speicher des Geräts abgelegt, was bedeutet, dass Angreifende (die physischen Zugriff auf das Gerät und eine spezielle Software haben) den Schlüssel direkt aus dem Speicher abrufen können. Ein Mikrocontroller für die sichere Authentifizierung kann diese Art von Angriff jedoch verhindern.

Zusammenfassung

Diese Lektion bietet einen Überblick über drahtlose Technologien und ihre Sicherheitsmerkmale. Es wurde gezeigt, warum drahtlose Netzwerke anfälliger sind als kabelgebundene Netze. Insbesondere die drei führenden Technologien Wi-Fi, Bluetooth und ZigBee wurden näher beleuchtet. Zunächst wurden die Wi-Fi-Sicherheitsprotokolle spezifiziert und zusammengefasst sowie die vier drahtlosen Sicherheitsprotokolle WEP, WPA1, WPA2 und WPA3 erläutert. Ferner wurden die Unterschiede zwischen den einzelnen Protokollen genauer betrachtet, darunter die Verschlüsselungsmethoden, die Größe der Sitzungsschlüssel und die Verschlüsselungsarten

Als Zweites stellte die Lektion die Topologie und Architektur von Bluetooth-Netzwerken vor. Dabei wurden der Verbindungsaufbau, der Protokollstapel und die Sicherheitsmerkmale besprochen. Außerdem wurde untersucht, wie die verschiedenen Versionen der Bluetooth-Spezifikationen vier Sicherheitsmodi und drei Sicherheitsdienststufen festlegen. Danach wurden die Sicherheitsmodelle von Zigbee (zentralisiert und dezentralisiert), die Sicherheitsschlüssel (Haupt-, Netzwerk- und Verbindungsschlüssel), die Schlüsselverwaltung und die kryptographischen Algorithmen erläutert. Abschließend wurden die Schwachstellen von ZigBee und die Sicherheitsmaßnahmen dagegen dargelegt.



# Lektion 7

## Cloud-Sicherheit

#### LERNZIELE

Nach Abschluss dieser Lektion werden Sie in der Lage sein, …

… die Terminologie des Cloud-Computing zu verstehen.

… den Unterschied zwischen den Cloud-Modellen zu erklären.

… verschiedene Cloud-Typen wie öffentliche, private und hybride Clouds zu identifizieren.

… die Bedeutung der Cloud-Sicherheit zu beschreiben.

… verschlüsselte Datenschemata zu analysieren.

DL-E-DLMCSEESN01\_E-U07

1. Cloud-Sicherheit

### Einführung

Heutzutage wird Datenverarbeitung als dienstleistungsbasiertes Modell angeboten („As-a-Service“). Bei diesem Modell werden erbrachte Dienstleistungen nach Nutzungsaufwand bezahlt (engl. *pay per use*), ähnlich wie bei der Abrechnung von Versorgungsleistungen wie Wasser, Gas und Strom. Cloud-Computing ist eine Technologielösung, bei der Ressourcen über das Internet von Cloud-Anbietern (engl. *Cloud Service Providers*, CSPs) angeboten werden. Die Ressourcen können hierbei sehr unterschiedlich sein. Die Bandbreite reicht vom reinen Datenspeicherangebot für Nutzer:innen bis hin zu umfangreichen Rechenkapazitäten, einschließlich Netzwerk- und IT-Infrastruktur. Derzeit kann jede Person Cloud-Dienste abonnieren und die Ressourcen je nach Bedarf nutzen, bezahlt wird nur für die Zeit der Ressourcennutzung

### Cloud-Dienstmodelle

Mit Cloud-Computing können Großunternehmen ihre Infrastruktur nach Bedarf skalieren und sie entsprechend ihren Geschäftsanforderungen dimensionieren. Darüber hinaus ermöglicht Cloud-Computing den Endnutzenden den Zugriff auf ihre Daten zu jeder Zeit, von jedem Ort und von jedem mit dem Internet verbundenen Gerät aus. Zur Kapazitätserweiterung ermöglicht Cloud-Computing außerdem die Integration neuer Funktionen oder zusätzlicher Ressourcen in die bestehenden Systeme (Buyya, 2013).

###### Cloud-Referenzmodell

Es gibt drei Hauptmodelle von Cloud-Diensten: Software as a Service (SaaS), Platform as a Service (PaaS) und Infrastructure as a Service (IaaS) (Buyya, 2013).

SaaS, auch bekannt als Cloud Application Services, liefert verschiedene Anwendungen und Software über das Internet. Dazu können Speicherdienste, Textverarbeitung, E-Mail und Software bzw. Anwendungen für die Zusammenarbeit gehören. Der Dienst wird von einem Drittanbieter verwaltet. SaaS ist die am meisten genutzte Option für Unternehmen auf dem Cloud-Markt, weil die Nutzenden damit ohne weitere Downloads oder Installationen Software und Anwendungen in ihrem Browser nutzen können (Buyya, 2013).

|  |  |  |  |
| --- | --- | --- | --- |
| Cloud-Dienstmodelle | | | |
| Parameter | SaaS | PaaS | IaaS |
| Akronym für | Software as a Service (Software als Dienstleistung) | Platform as a Service (Plattform als Dienstleistung) | Infrastructure as a Service (Infrastruktur als Dienstleistung) |

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter | SaaS | PaaS | IaaS |
| Modell | Hosting unterschiedlicher Software und Anwendungen als Kundenangebot. | Stellt die erforderlichen Werkzeuge für die Anwendungsentwicklung bereit. | Bietet unterschiedliche visualisierte Computing-Ressourcen im gesamten Internet. |
| Vorteile | * Verringert den Zeit- und Kostenaufwand für Verwaltungsaufgaben wie Installation, Herunterladen, Verwaltung und Patchen von Software. | * Einfache, kosteneffiziente Entwicklung und Bereitstellung von Anwendungen. * Reduziert den Zeitaufwand für die Programmierung. * Skalierbar. | * Einfacher und automatischer Einsatz von Speicher, Netzwerken, Servern und Verarbeitungsleistung. * Kauf von Hardware/Ressourcen nach Bedarf. * Nutzer:innen haben die vollständige Kontrolle über ihre Infrastruktur. * Hochgradig skalierbar. |
| Verwendung durch | Endnutzer:innen | Entwickler:innen | Netzwerkarchitektinnen und Architekten |
| Beispiele | * Google Workspace * Facebook-Apps * MS Office Web * Salesforce * Cisco WebEx * SAP Concur | * Amazon Web Services (AWS) Elastic Beanstalk * Azure-App-Dienst * Force.com * Google App Engine * OpenShift | * DigitalOcean * Rackspace * Amazon Simple Storage Service (Amazon S3) * Cisco Metacloud, * Google Compute Engine (GCE) |

PaaS bietet Entwicklern und Unternehmen eine Plattform zur einfachen und schnellen Erstellung von Anwendungen. Folglich können sich die Entwickler:innen auf die Entwicklung von Anwendungen konzentrieren, ohne sich um andere Infrastrukturanforderungen wie Patch-Verwaltung, Betriebssysteme und Speicher kümmern zu müssen (Buyya, 2013).

IaaS bietet über Virtualisierungstechnologien eine Cloud-Computing-Infrastruktur mit Servern, Netzwerken, Betriebssystemen und Speicherplatz. IaaS bietet Nutzenden die gleiche Erfahrung wie bei der Nutzung eines herkömmlichen Rechenzentrums, ohne dass dieses physisch gewartet oder verwaltet werden muss. IaaS-Nutzer:innen können über ein Dashboard oder eine nach der Content Security Policy (CSP) entwickelte und bereitgestellte Anwendungsprogrammierschnittstelle (API) auf ihre Server zugreifen und ihre Anwendungen nutzen. Dadurch erhalten IaaS-Nutzer die Kontrolle über die gesamte Infrastruktur. Über IaaS können Unternehmen Ressourcen auf Abruf und je nach Bedarf erwerben, anstatt die Hardware direkt zu kaufen (Buyya, 2013).

### Cloud-Arten

Es gibt verschiedene Arten von Cloud-Modellen, die jeweils unterschiedliche Möglichkeiten bieten, um die verschiedenen Bedürfnisse der Kundinnen und Kunden zu erfüllen. Die drei verschiedenen Cloud-Arten sind:

* Public Clouds (öffentliche Clouds): Diese Cloud-Dienste sind für jeden verfügbar.
* Private Clouds (private Clouds): In diesem Fall wird einer privaten Einrichtung eine Cloud zur Verfügung gestellt, auf die nur die Angehörigen der Einrichtung (oder ein bestimmter Teil davon) zugreifen können.
* Hybrid Clouds (hybride Clouds): Eine hybride Cloud ist eine Kombination aus öffentlicher und privater Cloud.

###### Öffentliche Clouds

Mit öffentlichen Clouds werden Cloud-Dienste für alle, von überall aus und zu jeder Zeit über das Internet verfügbar gemacht. Sie ermöglichen die Minimierung der IT-Infrastrukturkosten und dienen als praktikable Option zur Bewältigung von Lastspitzen in der lokalen Infrastruktur. Sie sind zu einer interessanten Option für kleine Unternehmen geworden, die ihre Geschäftstätigkeit ohne große Vorabinvestitionen aufnehmen können, indem sie sich für ihre IT-Bedürfnisse vollständig auf öffentliche Infrastrukturen verlassen. Öffentliche Clouds ermöglichen es Unternehmen, Infrastruktur zu mieten oder Anwendungsdienste zu abonnieren, ohne physische Hardware- und Software-Ressourcen kaufen oder installieren zu müssen. Sie bieten Unternehmen die Möglichkeit, ihre IT je nach Geschäftsbedarf zu vergrößern oder zu verkleinern. Derzeit werden öffentliche Clouds sowohl genutzt, um die IT-Infrastruktur von Unternehmen vollständig zu ersetzen als auch um sie bei Bedarf zu erweitern (Buyya, 2013).

Ein grundlegendes Merkmal öffentlicher Clouds ist die Mandantenfähigkeit. Damit kann eine Cloud viele Kundinnen und Kunden gleichzeitig bedienen, ohne dass sich die unterschiedlichen Dienste dabei gegenseitig stören. Jedem Kunden und jeder Kundin wird eine virtuelle Computer-Umgebung angeboten, die von anderen Kunden isoliert ist (Buyya, 2013). Daher ist die Verwaltung der Dienstgüte ein entscheidender Aspekt von öffentlichen Clouds. Ein erheblicher Teil der Software-Infrastruktur ist der Überwachung der Cloud-Ressourcen gewidmet, der Abrechnung gemäß den Verträgen mit den Nutzern und der Führung einer vollständigen Historie der Cloud-Nutzung für die gesamte Kundschaft.

Diese Funktionen sind für öffentliche Clouds von grundlegender Bedeutung, weil die Anbieter dadurch umfassende Rechenschaftsdienste anbieten können (Buyya, 2013).

Öffentliche Clouds bestehen in der Regel aus geografisch verteilten Rechenzentren, um möglichst viele Kundinnen und Kunden auf der ganzen Welt zu bedienen. Amazon Web Services hat zum Beispiel Rechenzentren in den Vereinigten Staaten, Europa, Singapur und Australien eingerichtet. So kann die Kundschaft zwischen drei verschiedenen Regionen wählen: us-west-1, us-ost-1 oder eu-west-1. Solche Regionen haben unterschiedliche Preise und sind außerdem in Verfügbarkeitszonen unterteilt, die bestimmten Rechenzentren zugeordnet sind (Buyya, 2013).

Eine öffentliche Cloud kann alle drei Arten von Diensten anbieten: IaaS, PaaS und SaaS. Amazon EC2 zum Beispiel ist eine öffentliche Cloud, die IaaS anbietet. Google AppEngine ist eine öffentliche Cloud, die PaaS anbietet, und SalesForce.com ist eine öffentliche Cloud, die SaaS anbietet (Buyya, 2013).

###### Private Clouds

Trotz der wirtschaftlichen und leistungsbezogenen Vorteile von öffentlichen Clouds werden diese Vorteile nicht allen Szenarien gerecht. Zu den Hauptproblemen in der Entwicklung der öffentlichen Cloud gehört der Kontrollverlust (Stallings & Brown, 2012). In öffentlichen Clouds steuert der Cloud-Anbieter (CSP) die Infrastruktur, demnach steuert er die Kernlogik und die sensiblen Daten der Kundinnen und Kunden. Auch wenn es ein regulatorisches Verfahren gibt, das eine ordnungsgemäße Verwaltung und den Schutz der Privatsphäre der Kundschaft garantiert, kann diese Bedingung immer noch als Bedrohung oder inakzeptables Risiko empfunden werden, das einige Unternehmen nicht eingehen wollen. Insbesondere sensible Entitäten wie Behörden und militärische Dienststellen vermeiden die Nutzung öffentlicher Clouds für die Verarbeitung oder Speicherung ihrer sensiblen Daten (Stallings & Brown, 2012). Darüber hinaus bestimmt der geografische Standort eines Rechenzentrums im Allgemeinen die Regeln und Vorschriften, die für die Verwaltung digitaler Informationen gelten.

Und schließlich ziehen bestehende Unternehmen, die über enorme Computerinfrastrukturen oder eine große Anzahl installierter Software verfügen, nicht gerne auf öffentliche Clouds um. Stattdessen nutzen sie ihre vorhandenen IT-Ressourcen und optimieren ihren Umsatz. Die genannten Aspekte erschweren die Nutzung der öffentlichen Computer-Infrastruktur in allen Szenarien. Zur Entschärfung dieser Probleme wurden spezielle Clouds entwickelt. **Private Clouds** sind wie öffentliche Clouds, allerdings beschränkt sich ihr Modell der Ressourcenbereitstellung auf die Grenzen eines Unternehmens.

###### Hybride Clouds

Obwohl die Option, sich vollständig auf eine öffentliche Infrastruktur zu verlassen, für Unternehmen attraktiv ist, leiden öffentliche Clouds unter Sicherheitsbedrohungen. Private Clouds sind die beste Lösung, wenn es notwendig ist, die Informationsverarbeitung innerhalb eines Unternehmens zu halten. Ein großer Nachteil privater Clouds ist jedoch die Unfähigkeit, nach Bedarf zu skalieren und Lastspitzen effizient zu bewältigen. In diesem Fall ist es von entscheidender Bedeutung, die Fähigkeiten der öffentlichen Clouds nach Bedarf zu nutzen, was als **Cloud Bursting** bekannt ist. Eine hybride Lösung nutzt die Vorteile von privaten und öffentlichen Clouds.

**Private Clouds** Eine private Cloud bezieht sich auf eine Cloud-Architektur, die im Rechenzentrum eines Unternehmens untergebracht ist.

**Cloud Bursting** Hierbei handelt es sich um die dynamische Bereitstellung von Ressourcen aus öffentlichen Clouds.

Eine hybride Cloud ist ein heterogenes verteiltes System, das aus der Nutzung einer privaten Cloud und der Integration zusätzlicher Dienste oder Ressourcen aus einer oder mehreren öffentlichen Clouds entsteht. Deshalb werden hybride Clouds auch als heterogene Clouds bezeichnet. Hybride Clouds ermöglichen es Unternehmen also, ihre sensiblen Informationen im Haus zu behalten, die vorhandene IT-Infrastruktur zu nutzen und bei Bedarf externe Ressourcen hinzuzufügen. Die Sicherheitsbedenken beschränken sich nur auf den öffentlichen Teil der Cloud, der für die am wenigsten sensiblen Vorgänge genutzt werden kann (Buyya, 2013).

### Cloud-Sicherheit

Auch wenn das Cloud-Computing zahlreiche Vorteile hat, bringt es auch Nachteile mit sich. Der mehr oder weniger große Mangel an Sicherheit, Vertrauen und Datenschutz behindert immer noch die Einführung von Cloud-Lösungen. Die fehlende Kontrolle über Daten und Prozesse sowie der Einsatz von Virtualisierungstechnologien haben zu neuartigen Bedrohungen geführt, die früher irrelevant waren. So können Cloud-Anwendungen beispielsweise auf vertrauliche Informationen zugreifen, was ein Sicherheitsrisiko darstellt (Stallings & Brown, 2012).

Unter Cloud-Sicherheit werden Maßnahmen zum Schutz digitaler, in der Cloud gespeicherter Vermögenswerte und Daten verstanden. Zu den Schutzmaßnahmen gehören u. a. Datenverschlüsselung, Daten-Hashing, die Nutzung virtueller privater Netzwerke (VPNs), Zugriffskontrolle und Sicherheits-Tokens, mehrstufige Authentifizierung und Autorisierung sowie Systeme zur Erkennung und Verhinderung von Eindringlingen.

###### Cloud-Sicherheitslösungen

Zur Gewährleistung einer sicheren Cloud-Umgebung sollten die Cloud-Anbieter (CSPs) folgende Sicherheitsüberlegungen anstellen (Stallings & Brown, 2012):

* + Klassifizierung der Daten: Daten können bei der Erstellung in der Cloud nach ihrer Sensibilität klassifiziert werden (ob vertraulich, intern oder öffentlich). Klassifizierte und sensible Daten (einschließlich vertraulicher Informationen) wären somit nur für autorisierte Nutzende zugänglich, und ihr Eingang in den Cloud-Dienst bzw. das Verlassen des Dienstes kann verhindert werden.
  + Zugriff auf Cloud-Daten und ‑Anwendungen: Zu den typischen Kontrollen gehören die folgenden:
    - Zugriffskontrolle für Nutzende: Hierbei handelt es sich um ein Implementierungssystem und eine Zugriffskontrolle für Anwendungen, mit der die Nutzer:innen den Zugriff auf Cloud-Daten und ‑Anwendungen erhalten.
    - Zugriffskontrolle für Geräte: Dies blockiert den Zugriff, wenn ein persönliches, nicht autorisiertes Gerät versucht, auf Cloud-Daten zuzugreifen.
  + Verschlüsselung: Die Verschlüsselung der Daten in der Cloud gewährleistet die Vertraulichkeit und verhindert den unbefugten Zugriff auf die Daten.
  + Schutz vor Datenverlust (engl. *Data loss prevention*, DLP): Cloud-DLPs schützen Daten vor unberechtigtem Zugriff. Darüber hinaus deaktivieren sie nach dem Entdecken einer verdächtigen Aktivität automatisch den Zugriff auf Daten und deren Transport (Stallings & Brown, 2012).
  + Identifizierung von bösartigem Verhalten: Manipulierte Konten und Insider-Bedrohungen werden mit Hilfe von User Behaviour Analytics (UBA) erkannt, um so bösartige Datenverluste zu verhindern (Stallings & Brown, 2012).
* Schutz vor Malware: Das Eindringen von Malware in Cloud-Dienste wird durch bestimmte Techniken erkannt. Dazu gehören u. a. Datei-Scanning, die Erkennung von Malware durch maschinelles Lernen und die Analyse von Netzwerkverkehr.
* Einhaltung der Vorschriften (Compliance): Compliance stellt sicher, dass der Cloud-Dienst bestimmte Sicherheitsstandards (wie ISO27001) erfüllt, indem die erforderlichen Kontrollen und Verfahren entwickelt werden.
* Risikobewertung: Dazu gehört die fortlaufende Identifizierung von Cloud-Risiken und deren Eindämmung. Risiken müssen nach ihrem Schweregrad und der Wahrscheinlichkeit einer Verletzung eingestuft werden.
* Compliance-Bewertungen: Es ist von entscheidender Bedeutung, die Bewertungen zur Einhaltung der Zahlungskartenindustrie, des amerikanischen Sarbanes-Oxley-Gesetzes und anderer gültiger gesetzlicher Bestimmungen laufend zu überprüfen und zu aktualisieren (Stallings & Brown, 2012).

### Durchsuchen verschlüsselter Daten

Um das Problem des Durchsuchens verschlüsselter Daten zu verstehen, wird das folgende Beispiel herangezogen. Angenommen, ein Kunde verschlüsselt seine Dokumente und speichert diese auf dem Speicherserver des Cloud-Anbieters. Durch die Verschlüsselung dieser Dokumente kann der Kunde jedoch nicht mehr nach bestimmten Schlüsselwörtern suchen. Aus diesem Grund wird das Abrufen von Inhalten ineffizient. Um die gewünschten Daten zu einem bestimmten Stichwort abzurufen, muss der Kunde zunächst alle verschlüsselten Dokumente herunterladen und sie dann entschlüsseln, um die Stichwortsuche durchzuführen. Diese Lösung ist jedoch zeitaufwendig und unpraktisch. Außerdem verursacht das Abrufen aller Dateien unnötigen Netzwerkverkehr, was bei den heutigen nutzungsbasierten Cloud-Preismodellen unerwünscht ist.

Aus den oben genannten Problemen ergibt sich die Notwendigkeit eines effizienten Datenabrufsystems, mit dem die Kundinnen und Kunden verschlüsselte Daten direkt durchsuchen können. Eine Lösung stellt die so genannte durchsuchbare Verschlüsselung (engl. *searchable encryption*, SE) dar. Mit SE können Kunden ihre Daten so verschlüsseln, dass sie später Such-Tokens für Abfragen an den Cloud-Anbieter erstellen können. Mit diesen Tokens kann der Anbieter die verschlüsselten Daten durchsuchen und die gewünschten verschlüsselten Dateien abrufen.

Es gibt eine große Anzahl von SE-Verfahren, die entweder deterministisch oder randomisiert sind (Bellare et al., 2007; Boneh et al., 2004; Kamara et al., 2012; Song et al., 2000). Deterministische Verfahren verschlüsseln eine bestimmte Nachricht immer mit demselben Chiffretext (Bellare et al., 2007). Bei der deterministischen Verschlüsselung bleiben die Eigenschaften erhalten. Angenommen, wir haben zwei Verschlüsselungen wie folgt:

*"*1 = *E k*, *m*1 and *"*2 = *E k*, *m*2.

Dann sind die zugrunde liegenden Nachrichten gleich (d. h. *m*1 = *m*2), sofern *"*1 = *"*2 gilt. Eines der Hauptprobleme bei deterministischen Verschlüsselungssystemen sind Informationsverluste. Mit anderen Worten: In einem deterministischen Verschlüsselungsverfahren wird immer derselbe Schlüssel zur Verschlüsselung einer Nachricht verwendet. Das bedeutet, dass zwei ähnliche Nachrichten den gleichen Chiffretext haben. Wenn ein Server also zwei oder mehr gleiche Chiffretexte findet, weiß er, dass die gleiche Nachricht dahintersteckt.

Folglich kann der Server die Häufigkeit des Auftretens von Schlüsselwörtern in Erfahrung bringen, was die verschlüsselte Datenbank anfällig für Häufigkeitsanalysen macht.

Ein weiteres Problem tritt auf, wenn das deterministische Verschlüsselungsverfahren einen öffentlichen Schlüssel verwendet. In diesem Fall werden alle deterministischen Verschlüsselungen mit dem öffentlichen Schlüssel der Nutzer:innen verschlüsselt. Da dieser aber öffentlich ist, steht er auch dem Server zur Verfügung. Der Server kann eine Liste aller möglichen Schlüsselwörter mit dem öffentlichen Schlüssel der Nutzenden verschlüsseln und sie mit denen in der Datenbank vergleichen (d. h. ein Wörterbuchangriff). Wenn es einen Treffer erhält, kennt er das Schlüsselwort (Stallings & Brown, 2012).

Randomisierte Verfahren verhindern eine Häufigkeitsanalyse durch das „Salzen“ von Chiffretexten (Kamara et al., 2012; Song et al., 2000). Dies macht die Sicherheit robuster. Die Verwendung von Salzen erfordert jedoch die Kombination jedes Tokens mit jedem Salz, wodurch die Verarbeitungszeit parallel mit der Anzahl der Salze für jeden Token steigt. Wie in (Kamara et al., 2012) spezifiziert, ist ein SE-Verfahren sicher, wenn (i) der Geheimtext allein keine Informationen über die verschlüsselten Daten preisgibt, (ii) die verschlüsselten Daten zusammen mit einem Such-Token (d. h. Abfragen) höchstens das Ergebnis der Suche preisgeben und (iii) Such-Tokens nur mit demselben Chiffre-Schlüssel erzeugt werden können, der zur Verschlüsselung der Daten verwendet wurde.

Zusammenfassung

In dieser Lektion wurde die Bedeutung von Cloud Computing erläutert. In den letzten zehn Jahren haben Millionen von Unternehmen und Privatpersonen ihre Infrastruktur und Daten in Clouds verlagert. Trotz der wirtschaftlichen und leistungsbezogenen Vorteile von Clouds sind sie noch nicht in allen Szenarien einsetzbar. Der relative Mangel an Sicherheit, Vertrauen und Datenschutz steht einer stärkeren Cloud-Nutzung entgegen. Deshalb wurden verschiedene Cloud-Typen (öffentlich, privat und hybrid) entwickelt, um die Bedürfnisse aller Kundinnen und Kunden zu erfüllen. In dieser Lektion wurden außerdem Cloud-Modelle vorgestellt und der Unterschied zwischen IaaS, PaaS und SaaS erklärt.

Die Cloud-Sicherheit nimmt bei der Cloud-Kundschaft einen hohen Stellenwert ein. In dieser Lektion wurden Sicherheitsempfehlungen in Bezug auf Compliance, Auditing, Risikomanagement und Bedrohungsanalyse umrissen. Abschließend wurde das Durchsuchen verschlüsselter Daten mit deterministischen und randomisierten Ansätzen betrachtet. Obwohl randomisierte Schemata die Mängel der deterministischen Schemata beseitigen, führen sie dazu, dass die Verarbeitungszeit mit der Anzahl der Salze für jeden Token wächst.

# Lektion 8

## Erkennung von Eindringlingen und Prävention



#### LERNZIELE

Nach Abschluss dieser Lektion werden Sie in der Lage sein, …

… die grundlegenden Prinzipien und Anforderungen der Erkennung von Eindringlingen zu verstehen.

… die Schlüsselelemente der Host-basierten Erkennung von Eindringlingen zu erläutern.

… die wichtigsten Bestandteile der netzwerkbasierten Eindringlingserkennung zu beschreiben.

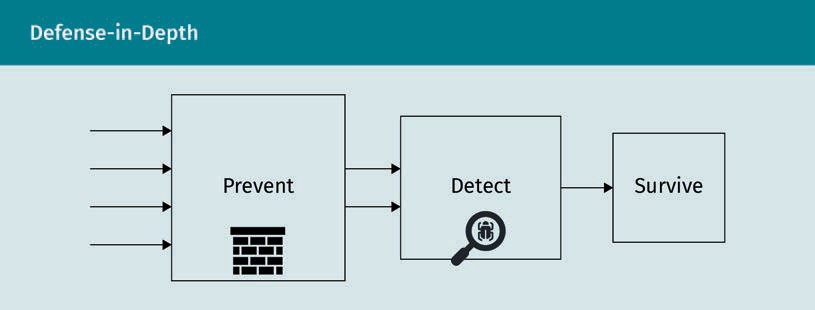
… die Bedeutung von Honigtöpfen (honeypots) zu erläutern.

DL-E-DLMCSEESN01\_E-U08

1. Erkennung von Eindringlingen und Prävention

### Einführung

Die Verteidigung in der Tiefe (engl. *Defense in Depth*) ist ein wesentlicher Grundsatz für die Abwehr von Angriffen. Dazu gehört der Einsatz mehrerer Schichten von Verteidigungsmechanismen, wie z. B. Präventionsmechanismen, Erkennungs- und Reaktionsmechanismen und angriffsresistente Technologien.



In der ersten Verteidigungslinie werden Präventionsmechanismen eingesetzt, um zu verhindern, dass Angreifer in die internen Netzwerke und Systeme gelangen. Allerdings können manche Angriffe diese Mechanismen aufgrund ihrer Anfälligkeiten und Schwachstellen überwinden. Ein Angriff kann zum Beispiel über ein JavaScript geführt werden, das nur zu einem bestimmten Zeitpunkt in der Zukunft ausgelöst werden kann (Stallings & Brown, 2012). Daher wäre es für das Präventionssystem nicht möglich, den Angriff sofort zu verhindern, weil es ihn erst bei seinem Auslösen erkennen würde.

Die zweite Verteidigungslinie umfasst Erkennungs- und Reaktionsmechanismen, die Aktivitäten auf Systemen und Netzwerken überwachen, um so Angriffe zu erkennen und Schäden zu beheben. Auch hier kann es Angriffe geben, die zumindest eine Zeit lang unentdeckt bleiben können. Dazu gehören zum Beispiel Angriffe, die sich in alltägliche Aktivitäten einfügen, wie ein bösartiges Browser-Plugin, das erst zu erkennen ist, wenn seine Auswirkungen eintreten – zum Beispiel bei Datenverlusten aufgrund gestohlener Zugangsdaten. Die dritte Verteidigungslinie sind angriffsresistente Technologien, aufgrund derer die Kernelemente (oder die wertvollsten Systeme) des Netzwerks Angriffe überleben und weiter funktionieren können (Stallings & Brown, 2012).

**Systeme zur Eindringlingserkennung** Ein System zur Erkennung von Eindringlingen ist ein passives Überwachungsgerät, das bei der Erkennung von Bedrohungen einen Alarm auslöst.

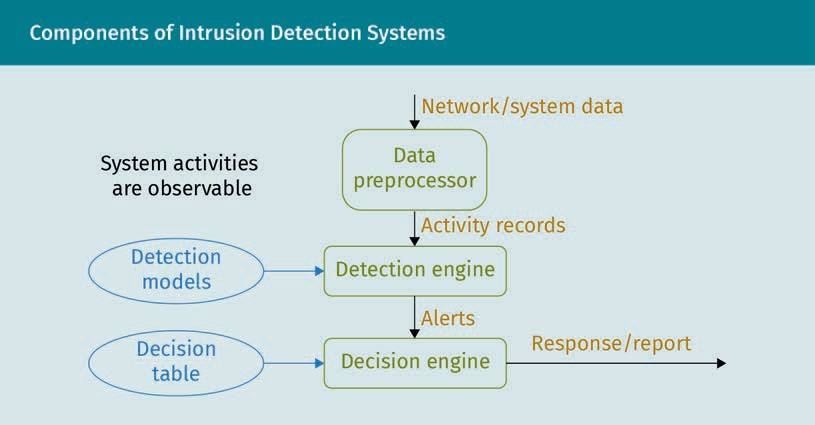
Diese Lektion konzentriert sich auf Erkennungsmechanismen, die sogenannten **Systeme zur Eindringlingserkennung** (engl. *Intrusion Detection Systems*, IDS).

### Grundlegende Konzepte von Systemen zur Eindringlingserkennung

Zunächst soll der Begriff „Eindringen“ (*intrusion*) definiert werden. Darunter fällt jeder Angriff, der darauf abzielt, die Sicherheit eines Unternehmens zu gefährden. Dazu zählen unter anderem die folgenden Dinge:

* + - Erraten von Passwörtern,
    - unbefugter Zugriff auf sensible Daten wie z. B. vertrauliche Dokumente oder Kreditkartennummern,
    - Erfassen von Benutzerdaten (Namen und Kennwörter) mithilfe von Hacking-Werkzeugen wie Packet Sniffer,
    - Aneignung von Administratorrechten,
    - Phishing-Angriffe.

Ein IDS ist darauf ausgelegt, diese Arten von Bedrohungen (und viele andere) zu erkennen. Für ein vollständig abgesichertes Netzwerk muss ein IDS Teil einer umfassenden Strategie zur Verteidigung in der Tiefe sein. Diese sollte Schemata zum ID-Zugriffsmanagement, die Verschlüsselung ruhender Daten (d. h. die Verschlüsselung sensibler, auf dem Server gespeicherter Informationen), starke Authentifizierungs- und Autorisierungsmechanismen sowie die Anwendungssicherheit umfassen (Scarfone & Mell, 2007).



Eine IDS-Architektur ist in der Abbildung oben dargestellt. Daten, welche die Systeme und Netzwerkaktivitäten beschreiben, werden als Input für das IDS verwendet. Durch die Datenaufbereitung werden zunächst Aktivitätsprotokolle extrahiert, die für die Sicherheit von Interesse sind. Als Zweites analysiert die Erkennungsmaschine die extrahierten Daten anhand der IDS-Erkennungsmodelle, die später beschrieben werden. Die Erkennungsmaschine gibt einen Alarm aus, sobald ein Eindringling entdeckt wird. Schließlich prüft die Entscheidungsmaschine den Alarm und entscheidet, wie darauf zu reagieren ist. Die Reaktion könnte das automatische Blockieren einer Netzwerkverbindung sein, oder auch ein an den Sicherheitsadministrator gesendeter Bericht (Scarfone & Mell, 2007; Stallings & Brown, 2012)

Für eine erfolgreiche Eindringlingserkennung sollten die Systemaktivitäten beobachtbar und Teil der Eingabedaten des IDS sein. Zu diesem Zweck umfasst ein IDS drei logische Komponenten (Stallings & Brown, 2012):

* + - * Sensoren: Diese erfassen Daten wie Netzwerkpakete, Protokolldateien und Daten zu Systemaufrufen. Nach der Erfassung der Daten leiten die Sensoren diese zur Analyse an das Analyseprogramm weiter.
      * Analyseprogramme: Diese erhalten Eingaben von einem oder mehreren Sensoren oder von anderen Analyseprogrammen. Das Analyseprogramm prüft die erfassten Daten und stellt fest, ob ein Eindringen stattgefunden hat. Wenn ein Eindringen erkannt wird, meldet das Analyseprogramm die Eindringlingserkennung und zeigt auf der Benutzeroberfläche Belege für diese Schlussfolgerung an. Das Analyseprogramm kann auf der Grundlage der Parameter des Eindringens bestimmte Maßnahmen vorschlagen. Die Sensordaten können auch zur späteren Analyse und Überprüfung in einer Speicher- oder Datenbankkomponente gespeichert werden.
      * Benutzeroberfläche: Damit können Nutzende die Systemausgaben sehen und das Systemverhalten steuern. Je nach Szenario kann die Benutzeroberfläche eine Manager-, Direktor- oder Konsolenkomponente sein.

###### IDS-Bewertung

Meist wird die Genauigkeit des Erkennungsalgorithmus anhand der folgenden Metriken beurteilt:

* + - * Erkennungsrate (engl. *Detection Rate* oder *True-Positive-Rate*): Diese Kennzahl gibt die Wahrscheinlichkeit darüber wieder, dass das IDS bei einem Eindringling tatsächlich eine Warnung ausgibt.
      * Falsch-positiv-Rate: Diese Kennzahl gibt die Wahrscheinlichkeit an, dass das IDS fälschlicherweise einen Alarm auslöst, wenn kein Eindringen vorliegt.
      * Bayessche Erkennungsrate: Diese gibt die Wahrscheinlichkeit wieder, dass nach der Alarmierung durch das IDS wirklich ein Eindringen stattgefunden hat.

### Ansätze zur Eindringlingserkennung

Mit den folgenden Ansätzen können die Sensordaten für die Eindringlingserkennung analysiert werden.

###### Anomalie-Erkennung

Der Ansatz zur **Erkennung von Anomalien** zielt darauf ab, normales oder erwartetes Verhalten zu definieren oder zu charakterisieren, um so bösartiges oder unbefugtes Verhalten zu identifizieren. Dabei werden über einen bestimmten Zeitraum Daten über das Nutzer-Verhalten gesammelt. Die Daten werden dann analysiert, um festzustellen, ob es sich um das Verhalten eines legitimen Nutzers bzw. einer legitimen Nutzerin oder eines Eindringlings handelt. Dabei wird zunächst ein Modell des legitimen Nutzer-Verhaltens entwickelt, indem in einer ersten Phase Daten aus dem normalen Betrieb des überwachten Systems gesammelt und verarbeitet werden (sogenannte Trainingsdaten). Dies kann zu verschiedenen Zeitpunkten geschehen, oder das Modell wird im Laufe der Zeit kontinuierlich überwacht und weiterentwickelt. Sobald dieses Modell existiert, wird das aktuell beobachtete Verhalten mit dem Modell verglichen, um es in der Erkennungsphase als legitim oder ungewöhnlich zu klassifizieren (Sample & Schaffer, 2013).

Zur Veranschaulichung soll ein Beispiel für ein System zur **Anomalie-Erkennung** dienen. Führen Sie zunächst ein Programm mehrere Male aus und zeichnen Sie jedes Mal Laufzeitmessungen wie CPU-Auslastung und Speichergröße auf. Analysieren Sie die gesammelten Messdaten durch Berechnen der Mittelwerte und Varianzen.

Sobald das Profil erstellt ist und das IDS feststellt, dass seine Messwerte bei der Ausführung des Programms über die zulässigen Schwellenwerte hinausgehen (d. h. die Werte liegen außerhalb der normalen Bereiche), gibt das IDS einen Alarm aus.

###### Erkennung von Missbrauch oder Signaturen

Die Missbrauchserkennung (oder signaturbasierte Erkennung) kann nur bekannte und öffentlich zugängliche Angriffe mit Mustern oder Regeln identifizieren, die zuvor von Schwachstellenanalyse-Teams identifiziert wurden. Dieser Ansatz vergleicht eine Reihe von bekannten bösartigen Datenmustern (Signaturen genannt) oder Angriffsregeln (Heuristiken genannt) mit dem aktuellen normalen Betriebsverhalten, um so zu entscheiden, ob ein Eindringen vorliegt. Die signaturbasierte Erkennung wird auch als Missbrauchserkennung bezeichnet (Stallings & Brown, 2012).

Signaturbasierte oder heuristische Techniken erkennen Eindringlinge über einen der folgenden Ansätze (Stallings, 2012):

Signatur-Ansätze

Signaturbasierte Ansätze (auch als Missbrauchserkennung bekannt) vergleichen eine Reihe bekannter bösartiger Datenmuster (Signaturen) oder Angriffsregeln mit dem aktuellen Verhalten, um dadurch einen Einbruch zu erkennen. Mit diesem Ansatz können nur bekannte Angriffe identifiziert werden, für die es Muster oder Regeln gibt. Dieser Ansatz ist in Antiviren-Produkten, Proxys zur Überwachung des Netzwerkverkehrs und netzwerkbasierten IDS (NIDS) weit verbreitet.

Regelbasierte heuristische Identifikation

Hierbei wird eine Sammlung von Regeln zur Identifikation von Eindringlingen genutzt, die bekannte Schwachstellen für Netzwerkangriffe ausnutzen. Diese Regeln werden durch die Analyse von Angriffswerkzeugen und Skripten entwickelt oder basieren auf den Angaben eines Sicherheitsexperten. Im letzteren Fall werden Systemadministratoren und Sicherheitsanalysten befragt. So lässt sich eine Reihe von bekannten Eindringszenarien und Schlüsselereignissen sammeln, welche die Sicherheit des Zielsystems bedrohen.

### Systeme und Implementierungsaspekte für den Einsatz von IDS

Ein IDS führt eine „passive“ Überwachung durch. Es zeichnet Daten über Systeme und Netzwerkaktivitäten auf und analysiert sie, bis es schließlich einen Alarm auslöst. Die Reaktionsstrategie schreibt eine direkte Maßnahme auf der Grundlage dieses Alarms vor, wie z. B. das Blockieren einer Verbindung oder das Beenden eines Programms. IDS können netzwerk- oder hostbasiert eingesetzt werden (Stallings & Brown, 2012).

###### Host-basierter Einsatz

Ein IDS kann auf einem End-Host zur Überwachung der Aktivitäten des Endsystems eingesetzt werden. Um beispielsweise das Verhalten eines Programms auf dem Endsystem zu überwachen, kann ein hostbasiertes IDS die Systemaufrufe des Programms beobachten. Systemaufrufdaten sind für die Sicherheitsüberwachung von Vorteil.

**Anomalie-Erkennung**   
Damit werden Verhaltensweisen, Ereignisse oder Beobachtungen identifiziert, die vom normalen Verhalten eines Datensatzes abweichen.

Immer wenn ein Programm eine Ressource anfordert (z. B. Speicherzuweisung, Zugriff auf das Lesesystem, Netzwerke oder Ein-/Ausgabegeräte), muss es einen Systemaufruf an das Betriebssystem (OS) richten, denn das OS verwaltet die Systemressourcen (Stallings & Brown, 2012). Nehmen wir zum Beispiel an, der Browser einer Nutzerin lädt eine Seite mit bösartigem JavaScript, das den Schutz des Browsers umgehen und die Windows-Registry überschreiben kann. In diesem Fall beobachtet das IDS einen „Schreib“-Systemaufruf in der Registry und entscheidet, dass es sich um eine Anomalie handelt. Neben Systemaufrufdaten sind gängige Datenquellen auch Audit-Aufzeichnungen (Logdateien) und Integritätsprüfsummen von Dateien (Stallings & Brown, 2012):

Audit-Aufzeichnungen (Protokolldateien)

Dies ist eine Software zur Buchführung über Benutzeraktivitäten, die in fast allen modernen Betriebssystemen eingesetzt wird. Durch die Verwendung von Daten wird keine zusätzliche Erfassungssoftware benötigt. Eindringlinge könnten jedoch versuchen, diese Protokolle zu manipulieren, um ihre Aktionen zu verbergen.

Datei-Integritätsprüfsummen

Wie bereits erwähnt, werden zum Finden manipulierter Dateien Integritätsprüfungen genutzt. Eine gängige Methode zur Erkennung von Eindringlingen in einem System ist das regelmäßige Scannen kritischer Dateien auf Veränderungen gegenüber den gewünschten Grundparametern. Dies geschieht durch die Überprüfung der kryptografischen Prüfsumme (String) dieser Dateien. Zu den Nachteilen dieses Ansatzes gehören die Erzeugung und der Schutz der Prüfsummen bekannter und geeigneter Dateien. Außerdem stellen sich im Normalbetrieb verändernde Dateien ein Problem dar.

###### Netzwerk-basierter Einsatz

Ein IDS kann am Rande eines Netzwerks oder Subnetzes zur Überwachung des Datenverkehrs in und aus dem Netzwerk eingesetzt werden. Diese Art von IDS wird als Netzwerk-IDS bezeichnet. Es erhält Daten zum Netzwerkverkehr über ein Paketüberwachungswerkzeug wie libpcap. Die Paketdaten enthalten vollständige Informationen über Netzwerkverbindungen. Angenommen, ein Nutzer verbindet sich über einen Browser mit einer Website. In diesem Fall enthalten die Paketdaten alle TCP-Handshake-Informationen (Transmission Control Protocol) zwischen dem Browser und dem Webserver, alle Anfragen des Browsers und die vom Server zurückgegebenen Seiteninhalte. Durch die Untersuchung der Paketdaten verfügt das IDS also über alle Daten, die vom Browser des Nutzers gesendet und empfangen wurden.

Ein netzwerkbasiertes IDS (NIDS) überwacht den Datenverkehr an ausgewählten Punkten in einem Netzwerk oder in einer Reihe miteinander verbundener Netzwerke. Eine typische NIDS-Konfiguration umfasst mehrere Sensoren zur Überwachung des Paketverkehrs. Das NIDS untersucht den Datenverkehr Paket für Paket und in Echtzeit, um Einbruchsmuster zu erkennen. Außerdem wird der Datenverkehr auf verschiedenen Ebenen des Protokollstapels untersucht, d. h. Aktivitäten auf Netzwerk-, Transport- oder Anwendungsebene. (Stallings, 2012)

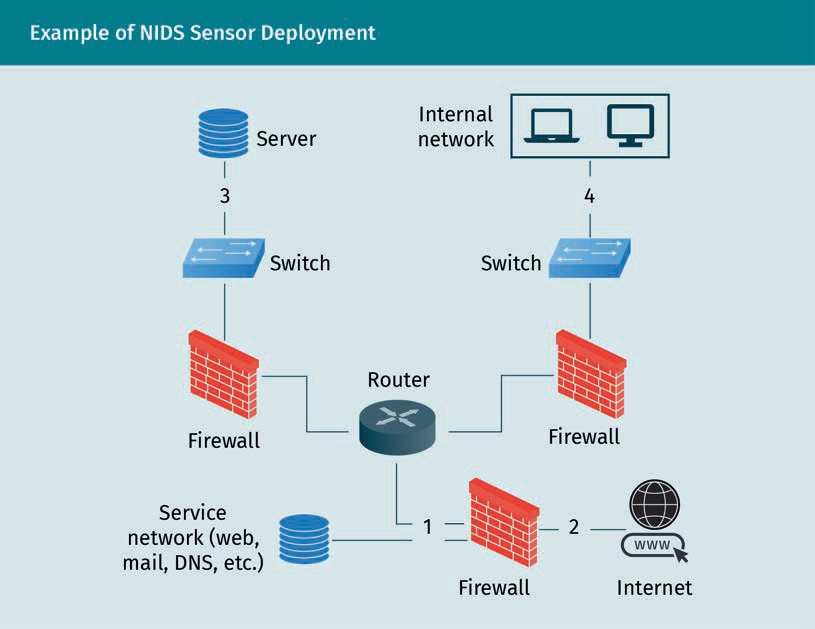
###### Arten von Netzwerksensoren

Die Sensoren können in zwei Modi eingesetzt werden: Inline oder passiv. Ein Inline-Sensor wird in ein Netzwerksegment eingefügt, so dass der überwachte Datenverkehr durch den Sensor laufen muss. In diesem Fall können Inline-Sensoren einen Angriff blockieren, sobald er entdeckt wird. Die Inline-Sensoren können also sowohl Funktionen zur Eindringlingserkennung als auch zur ‑verhinderung übernehmen (Stallings, 2012).

Ein passiver Sensor hingegen überwacht eine Kopie des Netzwerkverkehrs, so dass im Gegensatz zum Inline-Sensor der tatsächliche Verkehr nicht durch den passiven Sensor läuft. Aus Sicht der Leistung ist der passive Sensor effizienter, da er die tatsächlichen Daten nicht überprüft. Dieser zusätzliche Verarbeitungsschritt führt naturgemäß zu Paketverzögerungen und Leistungsdefiziten.

###### Einsatz von NIDS-Sensoren

Stellen wir uns ein Unternehmen mit mehreren Standorten vor, von denen jeder über ein oder mehrere lokale Netzwerke (LANs) verfügt, die über das Internet oder eine andere Wide Area Network (WAN)-Technologie miteinander verbunden sind. Für eine umfassende NIDS-Strategie werden an jedem Standort ein oder mehrere Sensoren benötigt. Innerhalb eines bestimmten Standorts ist die Platzierung der Sensoren eine wichtige Entscheidung für den Sicherheitsadministrator (Stallings, 2012, S. 286).



Die obige Abbildung veranschaulicht mehrere Möglichkeiten (nach Stallings und Brown, 2012). Im Allgemeinen wird der gesamte Internetverkehr durch eine externe Firewall geleitet, die das gesamte Unternehmen schützt. Der Verkehr von externen Quellen (z. B. Kunden und Lieferanten), die Zugang zu öffentlichen Diensten wie Web und E-Mail benötigen, wird überwacht. Die externe Firewall bietet auch einen gewissen Schutz für diejenigen Teile des Netzwerks, die nur für Nutzende von anderen Unternehmensstandorten zugänglich sein sollen. Mit internen Firewalls lassen sich bestimmte Teile des Netzwerks noch besser schützen.

Ein üblicher Standort für einen NIDS-Sensor ist direkt hinter der externen Firewall (Standort eins in der obigen Abbildung). Diese Position hat mehrere Vorteile. Erstens lassen sich dadurch die Angriffe von außen identifizieren, die den Schutz des Netzwerks zu durchdringen versuchen (die äußere Firewall). Zweitens lassen sich dadurch Angriffe auf den Webserver oder den FTP-Server (File Transfer Protocol) aufdecken.

Ein anderer Standort könnte zwischen der externen Firewall und dem Internet oder WAN liegen (Standort zwei in der obigen Abbildung). Von dort kann der Sensor den gesamten Netzwerkverkehr überwachen. Daher kann der Sensor die Anzahl und die Art der Angriffe aus dem Internet identifizieren, die auf das Netzwerk abzielen.

Standort zwei führt zu einem höheren Verarbeitungsaufwand als jeder andere Sensorstandort im Netzwerk. Außerdem können die Sensoren so konfiguriert werden, dass sie das Rückgrat des Netzwerks schützen. Dazu gehören interne Server und Datenbankressourcen (Position drei in der obigen Abbildung). An diesem Ort kann der Sensor eine große Menge an Netzwerkverkehr überwachen, um unbefugte Aktivitäten von autorisierten Nutzerinnen und Nutzern innerhalb der Sicherheitsgrenzen des Unternehmens zu erkennen. So kann ein Sensor an Standort drei sowohl interne als auch externe Angriffe überwachen (Stallings & Brown, 2012).

Schließlich können die Netzwerkeinrichtungen an einem Standort separate LANs umfassen, die Nutzenden-Arbeitsplätze und Server speziell für eine einzelne Abteilung verbinden (Stallings & Brown, 2012). Eine Firewall und ein NIDS-Sensor können damit so konfiguriert werden, dass sie zusätzlichen Schutz für alle kritischen Subsysteme wie Personal- und Finanznetzwerke bieten (Standort vier in der obigen Abbildung). An einem solchen Ort konzentriert sich der Sensor auf begrenzte Ressourcen und kann Angriffe auf die kritischen Subsysteme erkennen.

###### Honigtöpfe

Eine weitere Komponente von IDS sind Honigtöpfe (engl. *honeypots*). Diese sind Täuschungssysteme, die Angreifende von kritischen Systemen ablenken sollen (Stallings & Brown, 2012). Honigtöpfe sind für folgende Aufgaben konzipiert:

* Angreifer vom Zugriff auf kritische Systeme abhalten,
* Informationen über die Aktivitäten der Angreifenden sammeln,
* dafür sorgen, dass Angreifer so lange wie möglich im System bleiben, damit weitere Untersuchungen und Analysen durchgeführt werden können.

Honigtöpfe sind Systeme, die gefälschte oder nutzlose Informationen enthalten, die Außenstehenden wertvoll erscheinen sollen. Befugte Nutzer:innen des Systems würden wissen, dass diese Informationen uninteressant sind. Daher ist jeder Zugriff auf den Honigtopf verdächtig und wird als Eindringversuch eingestuft. Das System ist mit Sensoren ausgestattet, die Informationen über die Aktivitäten der Angreifenden erkennen und sammeln. Da jeder Angriff auf den Honigtopf als erfolgreich gilt, haben Administratoren genügend Zeit, die Angreifenden zu bewerten und zu verfolgen, ohne dass produktive oder wertvolle Systeme gefährdet werden (Stallings & Brown, 2012).

Zusammenfassung

In dieser Lektion wurden die Bedeutung der Verteidigung in der Tiefe und die Notwendigkeit von Systemen zur Eindringlingserkennung besprochen. Erkennungsraten und Falsch-positiv-Raten sind hierfür die gängigsten Leistungskennzahlen. Weiterhin wurden Ansätze zur Eindringlingserkennung vorgestellt sowie Anomalie-Erkennung und Erkennung von Missbrauch oder Signaturen erläutert. Zudem wurden die Vor- und Nachteile der einzelnen Produkte betrachtet. Der größte Nachteil von IDS zur Anomalie-Erkennung liegt zum Beispiel in der Erzeugung von Fehlalarmen. Signaturbasierte IDS haben den Nachteil, dass sie keine neuartigen Angriffe erkennen können, weil das System auf bereits entdeckte Muster programmiert wird.

Außerdem wurden die Schlüsselelemente der hostbasierten und netzwerkbasierten Eindringlingserkennung erläutert und dabei insbesondere den Einsatz von NIDS-Sensoren besprochen. Verschiedene Standorte für Sensoren wurden identifiziert und die jeweiligen Vor- und Nachteile aufgezeigt. Dabei erwies sich, dass die Standorte von den jeweiligen Bedürfnissen abhängen. Die Sensoren können zum Beispiel innerhalb der externen Firewall, zwischen der externen Firewall und dem Internet oder WAN, in internen Servern und Datenbankressourcen oder in der Nähe von internen Arbeitsplätzen platziert werden. Abschließend widmete sich die Lektion der Bedeutung und dem praktischen Nutzen von Honigtöpfen.