3 Betrieb und Sicherheit vernetzter Systeme gewährleisten (Lernfeld 11b)



Darüber werden wir sprechen, kompetent und aktiv uns beteiligen, genauer im Arbeitsbuch folgende Lernsituationen/Lernarrangements bearbeiten:

Lernsituation 1: Wir erkennen Schutzbedarf und informieren uns über Informationssicherheit vernetzter Systeme.

Lernsituation 2: Wir ermitteln konkrete Schutzziele und Anforderungen an Informationssicherheit und benennen mögliche Risiken.

Lernsituation 3: Wir planen Maßnahmen zur Erhöhung der Sicherheit in vernetzten Systemen unter Beachtung betrieblicher Sicherheitsrichtlinien.

Lernsituation 4: Wir setzen Maßnahmen unter Berücksichtigung der technischen und organisatorischen Rahmenbedingungen um.

Lernsituation 5: Wir überprüfen die getroffenen Maßnahmen und erstellen eine Dokumentation der Risikoanalyse.

Lernsituation 6: Wir reflektieren den Arbeitsprozess und identifizieren mögliche Optimierungen.

Im ersten Ausbildungsjahr wurden bereits Gesetze, Standards und Maßnahmen zur Sicherstellung des IT-Grundschutzes, orientiert am Konzept des Bundesamtes für Sicherheit in der Informationstechnik (BSI), vorgestellt (siehe auch Jahrgangsband 1, Lernfeld 4). Im Fokus stand zunächst der eigene Arbeitsbereich. Viele dieser Grundlagen zur Schutzbedarfsanalyse finden sich in diesem Lernfeld 11b wieder. Zusätzlich werden hier der Betrieb und die Sicherheit der IT-Infrastruktur vernetzter Systeme anhand der Beispielkundin Rigudo GmbH in den Blick genommen. JIKU IT-Solutions soll die Rigudo GmbH bei der Planung, Umsetzung und Dokumentation von Schutzmaßnahmen und Schutzbedarf unterstützen.

Die Rigudo GmbH ist ein IT-Systemhaus, das eine Videokonferenzlösung entwickelt hat. Mit dieser Software bietet sie kundenspezifische Lösungen für mittelständische und kleine Unternehmen an. Die Rigudo GmbH möchte ihre IT-Infrastruktur nach ISO 27001 auf Basis des IT-Grundschutzes zertifizieren. Die Rigudo GmbH hat für sich erkannt, dass der reibungslose betriebliche Ablauf auf vielfältige Weise gestört werden kann. In solchen Fällen nimmt ein Unternehmen in aller Regel Schaden, der sowohl materiell (reale Kosten) als auch immateriell (Imageschaden) sein kann.

Für die Zertifizierung muss zunächst der Schutzbedarf ermittelt werden. Danach können die einzuführenden Schutzmaßnahmen geplant und umgesetzt werden. Abschließend werden die getroffenen Maßnahmen auf ihre Wirksamkeit überprüft.



Die Rigudo GmbH bittet die JIKU IT-Solutions GmbH, sie bei der Erarbeitung einer Risikoanalyse und der anschließenden Umsetzung geeigneter Maßnahmen zur Reduktion der identifizierten Risiken zu unterstützen. Hierzu gehört neben den Zugriffsrechten auf sensible Ressourcen auch die Sicherung von Zugängen im lokalen Netz. Darüber hinaus ist auch die Anbindung an das Internet zu berücksichtigen.

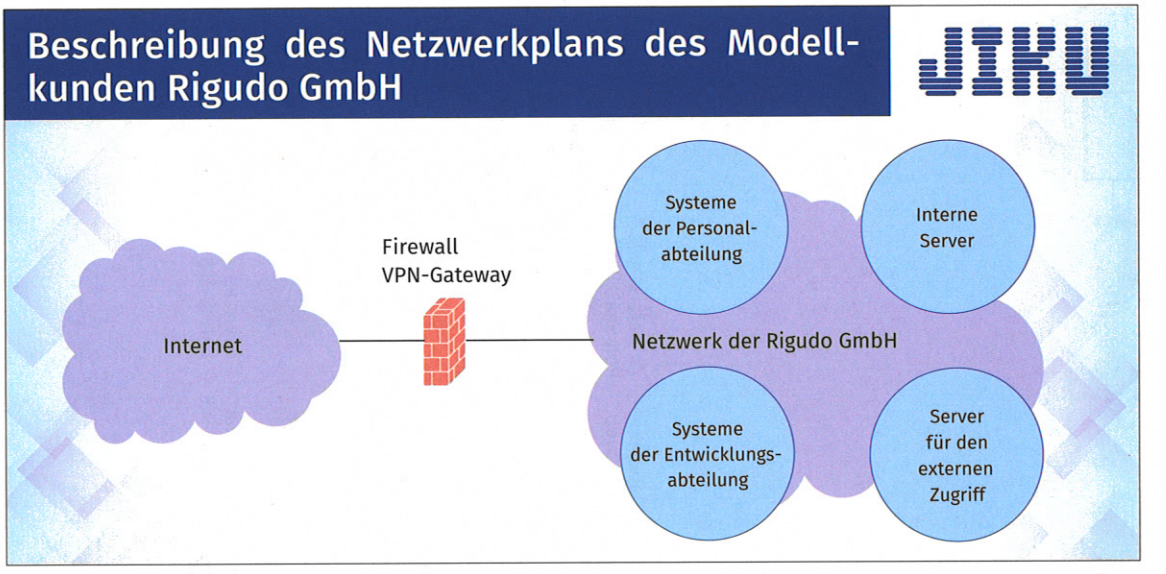
3.1 Schutzbedarf in vernetzten Systemen identifizieren

S **Sie sollen den Schutzbedarf vernetzter IT-Systeme erkennen und sich über die Informationssicherheit vernetzter Systeme informieren.**

Bevor das verantwortliche Team der JIKU IT-Solutions mit dem Projekt beginnen kann, muss es sich über die Gegebenheiten bei der Rigudo GmbH informieren. Während eines ersten Gesprächs werden die Fachleute von JIKU IT-Solutions über die bestehende IT-Infrastruktur der Rigudo GmbH aufgeklärt.



Das Netzwerk der Rigudo GmbH ist durch eine Firewall vor unberechtigtem Zugriff aus dem Internet geschützt. Innerhalb des Netzes lassen sich die IT-Endsysteme vier Bereichen zuordnen.



In den IT-Systemen der **Personalabteilung** werden die mitarbeiterbezogenen Daten bearbeitet. Hier werden beispielsweise die Lohnabrechnungen erstellt. Die Personalabteilung pflegt eine Datenbank mit den Daten aller Mitarbeiter.

Die **Entwicklungsabteilung** arbeitet an der Videokonferenzsoftware. Von dieser Abteilung wird die Software kundenunabhängig weiterentwickelt und gewartet. Die Abteilung verwendet dazu ein selbst betriebenes GitLab-System zur Verwaltung und Versionierung des erstellten Programmcodes. Fertige Softwareversionen (Releases) werden als installierbare Programme der Abteilung **Kundenlösungen** über einen gemeinsamen Dateiserver zur Verfügung gestellt.

Die Abteilung **Kundenlösungen** betreut die Projekte beim Kunden. Die Videokonferenzsoftware wird kundenspezifisch angepasst, dazu werden auch projektspezifische Daten der Kunden in den IT-Systemen der Rigudo GmbH verarbeitet. Die Abteilung Kundenlösungen pflegt die Kundendaten in einem eigenen Datenbanksystem. Außerdem werden die kundenspezifischen Lösungen auf einem Dateiserver abgelegt.

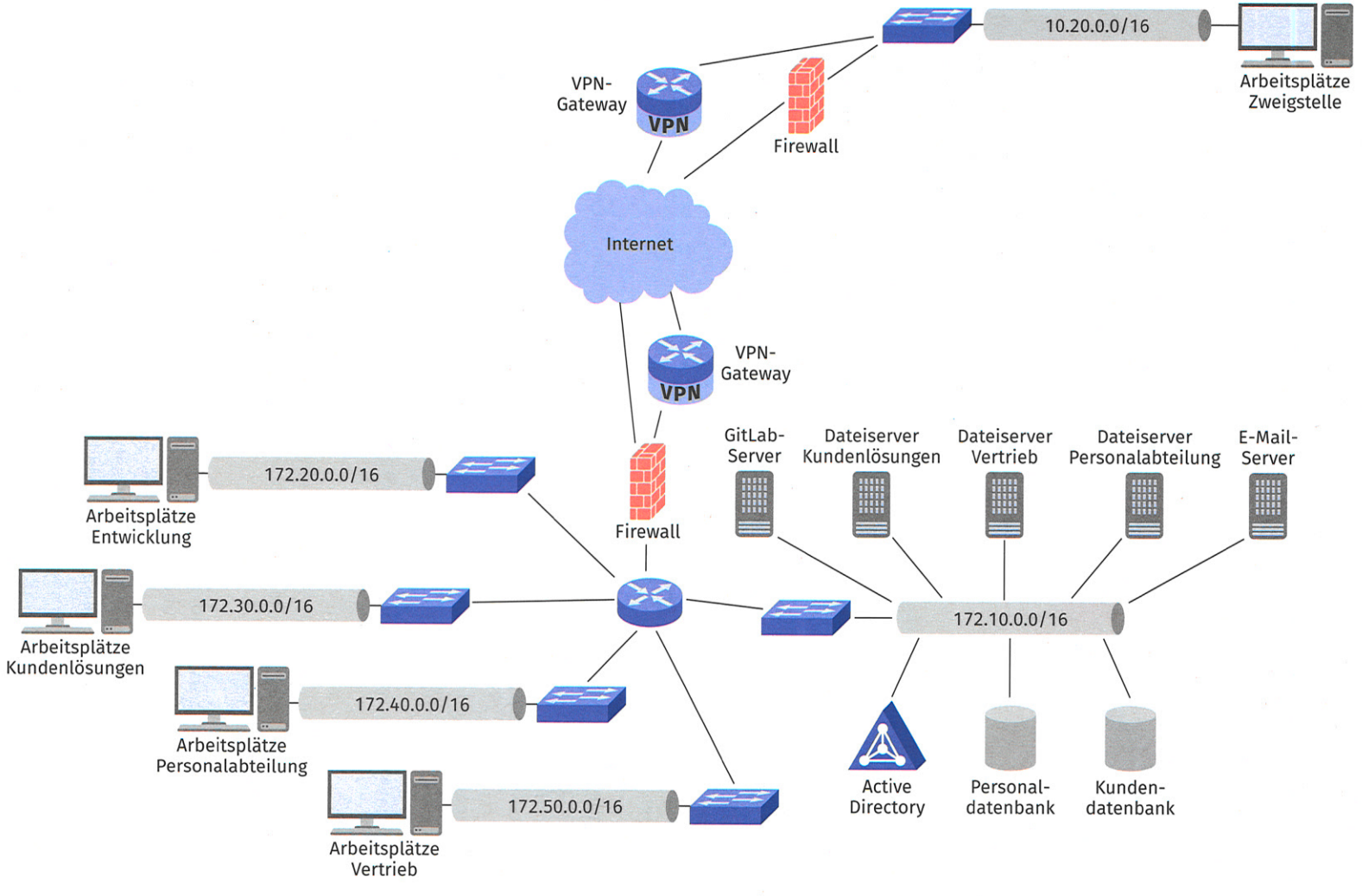
Für die Akquise neuer Kunden und als direkter Ansprechpartner für Bestandskunden ist die **Vertriebsabteilung** zuständig. Diese Abteilung verwendet als Datenbank ebenfalls die Kundendatenbank.

Alle Abteilungen haben separate abteilungsinterne Netzlaufwerke für die gemeinsame Bearbeitung von Daten.

Die Endsysteme aus Personal- und Entwicklungsabteilung greifen auf **interne Server** zu. Dazu gehören die Datenbankserver, das interne Git-Repository zur Versionierung und Pflege der zu entwickelnden Videokonferenzsoftware und die Dateiserver.

Alle Arbeitsplatzrechner und Server sind in einem Active Directory (AD) eingebunden. Beispielsweise wird die Anmeldung auf dem GitLab-Server über das AD verwaltet.

Innerhalb des Netzwerks der Rigudo GmbH gibt es zusätzlich **Server, die von außerhalb des Netzwerks** erreicht werden müssen. Dazu gehört beispielsweise der E-Mail-Server der Rigudo GmbH.



Netzwerkplan des Modellkunden Rigudo GmbH

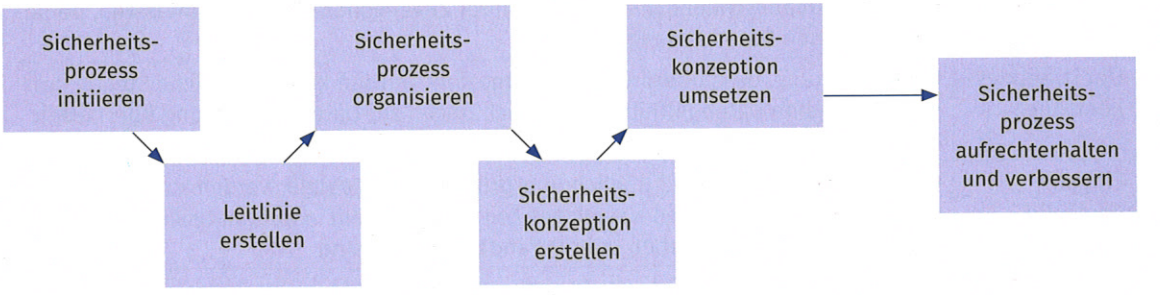
Die Mitarbeiter der Rigudo GmbH können während eines Einsatzes beim Kunden mittels VPN auf das interne Netzwerk der Firma zugreifen. Mitarbeiter im Homeoffice greifen ebenfalls auf das interne Netzwerk zu. Dazu steht ein VPN-Gateway zur Verfügung. Ein zweiter Standort der Rigudo GmbH wird ebenfalls mittels VPN an die Zentrale angebunden.

3.1.1 Schutzbedarf

S **Sie sollen den Prozess zur Ermittlung des Schutzbedarfs in vernetzten Systemen erläutern können.**

Bei der Schutzbedarfsfeststellung in vernetzten Systemen wird nicht der eigene Arbeitsbereich in den Fokus gerückt, sondern die IT-Infrastruktur als Gesamtsystem untersucht.

Der **Sicherheitsprozess nach dem BSI-Grundschutz** besteht aus klar definierten Phasen. Zunächst wird der Sicherheitsprozess initiiert. Dabei geht es um die Festlegung von Verantwortlichkeiten und die Planung des Ressourcenaufwands. Im nächsten Schritt wird die Leitlinie zur Informationssicherheit erstellt. In diesem Dokument werden alle Prinzipien, Ziele und Rahmenbedingungen festgehalten. Mit diesem Dokument wird das zu erreichende Niveau der Informationssicherheit im Unternehmen dokumentiert. Der dritte Schritt ist die Organisation des Sicherheitsprozesses. Dabei werden alle organisatorischen Maßnahmen, z. B. die Art der Kommunikation oder die Protokollierung von Ergebnissen, geplant. Im nächsten Schritt, der Erstellung einer Sicherheitskonzeption, werden die Maßnahmen beschrieben, mit denen die Ziele und Strategien der Informationssicherheit erreicht werden sollen. Dazu wird auch der Geltungsbereich des Sicherheitsprozesses festgelegt. Anschließend wird die Sicherheitskonzeption umgesetzt. Dazu werden die geplanten Maßnahmen realisiert. Der Sicherheitsprozess ist kein abschließbares Projekt, sondern muss stetig aufrechterhalten und verbessert werden. Der Sicherheitsprozess wird also weiterentwickelt.



Sicherheitsprozess nach dem BSI-Grundschutz

Zum Erstellen der Sicherheitskonzeption wird zunächst eine Strukturanalyse durchgeführt (siehe auch Jahrgangsband 1, Lernfeld 4 und Jahrgangsband 2, Lernfeld 9, Kapitel 4.4.2). Diese hat das Ziel, die gesammelten Informationen aus der Sicherheitskonzeption aufzubereiten. Auf Grundlage eines Netzwerkplans werden alle IT-Systeme und die darauf laufenden Anwendungen erhoben.

Ausgehend von der Strukturanalyse kann eine Schutzbedarfsfeststellung für jedes IT-System erstellt werden. Dabei wird geklärt, wie viel Schutz Informationen, Anwendungen, IT-Systeme und Infrastrukturkomponenten benötigen. Aus der Schutzbedarfsfeststellung resultiert, welche Systeme besonderen Schutz benötigen und welche Systeme nur grundlegenden Schutz brauchen.

3.1.2 Bedeutung von Datenschutz

S **Sie sollen die Bedeutung von Datenschutz in Unternehmen erläutern können.**

Teil der Informationssicherheit ist der Datenschutz, der durch die europäische Datenschutz-Grundverordnung (EU-DSGVO) geregelt wird. Artikel 24 und 32 der DSGVO verpflichten alle Unternehmen, die personenbezogene Daten verarbeiten, technische und organisatorische Maßnahmen (TOM) zum Datenschutz zu ergreifen. Die DSGVO beschreibt jedoch nicht detailliert, welche technischen und organisatorischen Maßnahmen das konkret sind. Hier wird das Bundesdatenschutzgesetz (BDSG) (Jahrgangsband 1, Lernfeld 4, Kapitel 4.2) deutlicher. Unter § 64 BDSG werden vierzehn konkrete technische und organisatorische Maßnahmen gelistet.

Anforderungen an die Sicherheit der Datenverarbeitung nach § 64 Bundesdatenschutzgesetz (BDSG)	
TOM	**Beschreibung**
Zugangskontrolle	Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte
Datenträgerkontrolle	Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern
Speicherkontrolle	Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten
Benutzerkontrolle	Verhinderung der Nutzung automatisierter Verarbeitungssysteme mithilfe von Einrichtungen zur Datenübertragung durch Unbefugte
Zugriffskontrolle	Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten, personenbezogenen Daten Zugang haben
Übertragungskontrolle	Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mithilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können
Eingabekontrolle	Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind
Transportkontrolle	Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden
Wiederherstellbarkeit	Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können
Zuverlässigkeit	Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden
Datenintegrität	Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können
Auftragskontrolle	Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können
Verfügbarkeitskontrolle	Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind
Trennbarkeit	Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können

Ein Unternehmen beschreibt mit den TOM, wie es mit den Daten umgeht und sie schützt. Beispielhaft sollen hier Maßnahmen für die Umsetzung der TOM Zugangskontrolle, Zugriffskontrolle, Übertragungskontrolle und Transportkontrolle beschrieben werden.

Maßnahmen für die Umsetzung der TOM		
Art	**Technische Maßnahmen**	**Organisatorische Maßnahmen**
Zugangskontrolle	Schließsystem zum Serverraum	Festlegung, wer Zugang zum Serverraum gewährt und wer ihn erhält; Verhaltensregel für Zugangsberechtigte zum Serverraum; Protokollierung der Zugänge; besondere Auswahl und Einweisung des Reinigungspersonals
	Absicherung alternativer Zugänge zum Serverraum, z. B. Notausgänge, Fenster, Oberlichter, Lüftungsschächte	Festlegung, wer alternative Zugänge öffnet und schließt; Verhaltens- und Aufsichtsregeln für Auftragsfirmen, die an den alternativen Zugängen Wartungs- und Reparaturarbeiten durchführen
Zugriffskontrolle	Benutzerkonten	Festlegung, wer Benutzerkonten verwaltet und wie die Vergabe stattfindet; rollenbasierte Zuordnung der Benutzerkonten
	Zugriffsrechte auf Daten festlegen	Festlegung, welche Benutzerkonten auf welche Daten zugreifen dürfen; über Rollen Zugriffe festlegen und Benutzerkonten den Rollen zuordnen; dabei das Minimalprinzip beachten, d. h., jeder Benutzer hat nur so viel Zugriff auf Daten wie nötig
	Protokollierung von Datenzugriff	Protokollierung, wer zu welcher Zeit auf Daten zugegriffen hat
	Ausmusterung von Hardware	Festlegung, wie Datenspeicher entsorgt werden, mit besonderer Beachtung, dass dadurch keine Daten unbeabsichtigt veröffentlicht werden
Übertragungskontrolle	Protokollierung der übertragenen Daten	Protokollierung durch die Software, welche Daten mit der Übermittlung übertragen wurden
Transportkontrolle	Einsatz von VPN	Einwahl von Außendienstmitarbeitern im Homeoffice in das Firmennetzwerk über verschlüsselte Verbindung mithilfe eines VPN; Vorgabe der zu verwendenden Software und Einstellungen durch IT-Abteilung; Vorgabe der zu verwendenden Endgeräte durch IT-Abteilung; Installation auf Endgeräten nur von durch IT-Abteilung zertifizierter Software
	E-Mail-Verschlüsselung	Übertragen von persönlichen Daten nur über Ende-zu-Ende-verschlüsselte E-Mails; Festlegung von Algorithmus und Schlüssellänge durch IT-Abteilung
	Verschlüsselter Zugang zu webbasierten Anwendungen	Eingabe der Arbeitszeiten durch Mitarbeiter über eine Webseite; Festlegung durch IT-Abteilung, welche Verschlüsselung als Mindestanforderung für den Zugang auf die Webseite nötig ist
	Verschlüsselung von USB-Sticks	Verwendung verschlüsselter USB-Sticks für den Austausch von Daten; Installation auf den Arbeitsplatzrechnern durch IT-Abteilung; Verwendung der USB-Sticks an den Arbeitsplatzrechnern nur mit verschlüsselten Containern

Mit den TOM dokumentiert ein Unternehmen die Maßnahmen, mit denen die Daten geschützt werden sollen. Im Fall eines Datenschutzverstoßes stellen die TOM die Grundlage dar, um festzustellen, ob ausreichende Maßnahmen für den Schutz der Daten ergriffen bzw. bestehende Maßnahmen richtig umgesetzt wurden.

3.1.3 Risikoanalyse und Risikokategorien

S **Sie sollen die Bedeutung von Vertraulichkeit, Integrität und Verfügbarkeit von IT-Systemen eines Unternehmens erläutern können.**

Die IT-Grundschutz-Bausteine des BSI beinhalten Hilfestellungen und Maßnahmen zum Schutz von IT-Systemen und Anwendungen, die einen normalen Schutzbedarf benötigen. Für die meisten IT-Systeme in einem IT-Verbund ist ein IT-Grundschutz ausreichend. Es gibt aber in fast jedem IT-Verbund Systeme mit erhöhtem Schutzbedarf.

IT-Verbund
Der Geltungsbereich eines Informationssicherheitskonzepts wird als IT-Verbund bezeichnet.

In der Schutzbedarfsfeststellung wurden die drei Schutzziele **Vertraulichkeit**, **Integrität** und **Verfügbarkeit** für jedes IT-System untersucht. Sollte eines der Schutzziele mit einem sehr hohen Schutzbedarf bewertet sein, muss das IT-System gesondert betrachtet werden. Das gilt auch, wenn es für ein IT-System keinen Baustein aus dem IT-Grundschutz gibt oder die Einsatzumgebung des IT-Systems untypisch ist.

Ein solches System wird einer Risikoanalyse unterzogen. Mit der Risikoanalyse wird untersucht, welche zusätzlichen Gefahren (vgl. Kapitel 3.2.3 elementare Gefährdungen) für das IT-System existieren, die im IT-Grundschutz für dieses IT-System noch nicht behandelt sind. Daraus folgend werden ergänzende Sicherheitsmaßnahmen geplant und umgesetzt.

Beispiel: Im Fokus steht ein Webserver. Der Grundschutz bietet für Webserver einen eigenen Baustein (vgl. BSI Baustein APP3.2 Webserver). Bei der Strukturanalyse wird ein sehr hoher Schutzbedarf festgelegt, da auf dem Webserver personenbezogene Daten verarbeitet werden. Es ist somit nötig, dass der Webserver explizit einer Risikoanalyse unterzogen wird. Dabei wird nun geprüft, ob die Sicherheitsrisiken angemessen betrachtet wurden.

Bei der Risikoanalyse wird eine Gefahr oder ein Ereignis, das eine Gefahr birgt, beschrieben. Zunächst wird die Eintrittshäufigkeit des Ereignisses festgelegt.

Eintrittshäufigkeit	Beschreibung
selten	Ereignis tritt höchstens einmal alle fünf Jahre ein.
mittel	Ereignis tritt einmal alle fünf Jahre bis einmal im Jahr ein.
häufig	Ereignis tritt einmal im Jahr bis einmal im Monat ein.
sehr häufig	Ereignis tritt mehrmals im Monat ein.

Quelle: BSI-Standard 200-3 – Risikoanalyse auf der Basis von IT-Grundschutz, Version 1.0, Bundesamt für Sicherheit in der Informationstechnik, Bonn, S. 26f. (verändert)

Anschließend wird betrachtet, was passiert, wenn das Ereignis eintritt. Diese Folge wird in der Schadenshöhe festgelegt.

Schadenshöhe	Schadensauswirkungen
vernachlässigbar	Die Schadensauswirkungen sind gering und können vernachlässigt werden.
begrenzt	Die Schadensauswirkungen sind begrenzt und überschaubar.
beträchtlich	Die Schadensauswirkungen können umfangreich sein.
existenzbedrohend	Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

Quelle: BSI-Standard 200-3 – Risikoanalyse auf der Basis von IT-Grundschutz, Version 1.0, Bundesamt für Sicherheit in der Informationstechnik, Bonn, S. 26f. (verändert)

Das BSI gibt nun eine Matrix zur Einstufung des Risikos vor. Diese Matrix stellt einen Zusammenhang zwischen der Auswirkung eines Ereignisses und der Eintrittshäufigkeit des Ereignisses her. Das Resultat ist die Einordnung eines Ereignisses in eine Risikokategorie.

Risikokategorien	
gering	Die [...] im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten einen ausreichenden Schutz. In der Praxis ist es üblich, geringe Risiken zu akzeptieren und die Gefährdung dennoch zu beobachten.
mittel	Die [...] im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen reichen möglicherweise nicht aus.
hoch	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung.
sehr hoch	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung. In der Praxis werden sehr hohe Risiken selten akzeptiert.

Quelle: BSI-Standard 200-3 – Risikoanalyse auf der Basis von IT-Grundschutz, Version 1.0, Bundesamt für Sicherheit in der Informationstechnik, Bonn, S. 26f.

Abschließend muss entschieden werden, wie das Unternehmen mit dem ermittelten Risiko umgeht. Dazu stehen verschiedene Möglichkeiten offen. Das Risiko kann vermieden werden, es kann reduziert werden, es kann verschoben werden oder akzeptiert werden. Für die verschiedenen Alternativen bietet das BSI Hilfestellung in Form von Leitfragen an.

Kompetenzcheck

1. Die Umsetzung der Schutzmaßnahmen soll ausführlich protokolliert werden, um eine spätere Überprüfung durchführen zu können. Sie wurden von Ihrem Ausbilder, Herrn Lübberstedt, aufgefordert ein Projektjournal anzulegen. Das Journal soll die täglich bzw. abschnittsweise durchgeführten Tätigkeiten enthalten. Dabei sind die Zeiten, Inhalte der Tätigkeiten sowie die möglichen Probleme und deren Lösungsansätze aufzuführen. Das Projektjournal kann in Tabellenform geführt werden. Am Ende des Kapitels werden diese Aufzeichnungen für eine Auswertung herangezogen.

2. Bearbeiten Sie die Aufgaben 1, 2 und 3 der Lernsituation 1 im Arbeitsbuch.

A1
A2
A3

3.2 Analyse des Schutzbedarfs in vernetzen Systemen

S **Sie sollen die Maßnahmen zur Erhöhung der Sicherheit in vernetzten Systemen unter Beachtung betrieblicher Sicherheitsrichtlinien planen.**



Für die Schutzbedarfsfeststellung werden zunächst Schadensszenarien festgelegt, aus welchen dann die Schutzbedarfskategorie für das IT-System bestimmt wird. Dabei wird in diesem Kapitel der Schutzbedarf nur auf die IT-Systeme und Netzwerkkomponenten reduziert.

Beispielsweise muss betrachtet werden, was passiert, wenn es zu einer unerlaubten Nutzung eines Arbeitsplatzes in der Abteilung „Vertrieb" kommt. Dabei könnten beispielsweise Kundendaten ausgelesen werden. Bei einer unerlaubten Veröffentlichung der Kundendaten oder bei einem illegalen Verkauf dieser Daten kommt es zu hohen Strafen und einem erheblichen Imageschaden.

Die Schutzbedarfskategorien reichen von „normal" über „hoch" bis hin zu „sehr hoch". Die Kategorie „normal" beschreibt, dass die Schadensauswirkungen begrenzt sind. Die Kategorie „sehr hoch" beschreibt, dass die Schadensauswirkungen existenziell für das Unternehmen sind.

Aus dem Schutzbedarf werden technische und organisatorische Maßnahmen abgeleitet. Sinnvollerweise werden dazu in einer Risikoanalyse die jeweiligen 47 elementaren Gefährdungen mit dem IT-System abgeglichen und analysiert, wie hoch die Eintrittswahrscheinlichkeit ist und wie stark die Auswirkungen der Gefährdungen sind.

Basierend auf dem Netzwerkplan der Rigudo GmbH (siehe S. 168) wurden für die IT-Systeme folgende Strukturanalysen durchgeführt.

Strukturanalysen JKU IT-Solutions

Nr.	Beschreibung	Plattform	Standort	Anzahl	Benutzer/Administrator
S01	GitLab-Server zum Management des Quellcodes der Videokonferenz-software	Linux	Serverraum R 0.13 Hauptgebäude	1	IT-Administration/ Benutzer Abteilung Entwicklung
S02	Dateiserver der Abteilung Kunden-lösungen	Linux	Serverraum R 0.13 Hauptgebäude	1	IT-Administration/ Benutzer Abteilung Entwicklung/Benutzer Abteilung Kunden-lösungen
S03	Dateiserver der Abteilung Vertrieb	Linux	Serverraum R 0.13 Hauptgebäude	1	IT-Administration/ Benutzer Abteilung Kundenlösungen/Benutzer Abteilung Vertrieb
S04	Dateiserver der Abteilung Personal	Windows Server	Serverraum R 0.13 Hauptgebäude	1	IT-Administration/ Benutzer Abteilung Personal
S05	AD-Server	Windows Server	Serverraum R 0.13 Hauptgebäude	1	IT-Administration/ alle Benutzer
S06	Server Personal-datenbank	Linux	Serverraum R 0.13 Hauptgebäude	1	IT-Administration/ Benutzer Abteilung Personal
S07	Server Kunden-datenbank	Windows SQL Server	Serverraum R 0.13 Hauptgebäude	1	IT-Administration/ Benutzer Abteilung Kundenlösungen/Benutzer Abteilung Vertrieb
S08	E-Mail-Server	Windows Exchange Server	Serverraum R 0.13 Hauptgebäude	1	IT-Administration/ alle Benutzer

Strukturanalysen					JIKU IT-Solutions
Nr.	**Beschreibung**	**Plattform**	**Standort**	**Anzahl**	**Benutzer/Administrator**
C01	Clients Abteilung Entwicklung	Windows 10	Räume R 2.01 bis R 2.10	20	IT-Administration/ Benutzer Abteilung Entwicklung
C02	Clients Abteilung Kundenlösungen	Windows 10	Räume R 1.10 bis R 1.20	10	IT-Administration/ Benutzer Abteilung Kundenlösungen
C03	Clients Abteilung Personal	Windows 10	Räume R 1.01 bis R 1.05	7	IT-Administration/ Benutzer Abteilung Personal
C04	Clients Abteilung Vertrieb	Windows 10	Räume R 1.06 bis R 1.09 und R 2.11 bis R 2.12	10	IT-Administration/ Benutzer Abteilung Vertrieb
N01	zentraler interner Router	RouterOS	Serverraum R 0.13 Hauptgebäude	1	IT-Administration/ alle Benutzer
N02	Switches	RouterOS	Serverraum R 0.13 Hauptgebäude/ Racks der strukturierten Verkabelung auf den Etagen	8	IT-Administration/ alle Benutzer
N03	Firewall-System	RouterOS	Serverraum R 0.13 Hauptgebäude	1	IT-Administration/ alle Benutzer
N04	VPN-Gateway	RouterOS	Serverraum R 0.13 Hauptgebäude	1	IT-Administration/ Mitarbeiter im Homeoffice/Mitarbeiter beim Kunden

Nach der Strukturanalyse wird ein Schutzbedarf für die einzelnen Systeme festgelegt. Dazu wird den drei Schutzzielen Vertraulichkeit, Integrität und Verfügbarkeit eine Schutzbedarfskategorie begründet zugewiesen.

Schutzbedarfsfeststellung				JIKU IT-Solutions	
Nr.	**Beschreibung**	**Grundwert**	**Schutzbedarf**	**Begründung**	
C01	Clients Abteilung Entwicklung	Vertraulichkeit	normal	Es werden keine personenbezogenen Daten verarbeitet. Die Entwicklung der Software ist in dieser Abteilung kundenunabhängig.	
		Integrität	normal	Fehler in der Entwicklung und den dazugehörigen Systemen werden meist schnell erkannt.	
		Verfügbarkeit	normal	Bei einem Ausfall eines Rechners kann auf den anderen Rechnern weitergearbeitet werden.	

Schutzbedarfsfeststellung				JIKU IT-Solutions
Nr.	**Beschreibung**	**Grundwert**	**Schutzbedarf**	**Begründung**
C02	Clients Abteilung Kunden-lösungen	Vertraulichkeit	sehr hoch	In der Abteilung werden Kundendaten erhoben und verarbeitet.
		Integrität	hoch	Im Falle einer Veränderung von Kunden-daten können ein erheblicher finanzieller Schaden und ein Imageschaden entstehen.
		Verfügbarkeit	normal	Bei einem Ausfall eines Rechners kann auf den anderen Rechnern weitergearbeitet werden.
C03	Clients Abteilung Personal	Vertraulichkeit	sehr hoch	Es werden personenbezogene Daten von Mitarbeitern verarbeitet.
		Integrität	normal	Eine Manipulation von Daten kann schnell erkannt werden.
		Verfügbarkeit	normal	Bei einem Ausfall eines Rechners kann auf den anderen Rechnern weitergearbeitet werden.
C04	Clients Abteilung Vertrieb	Vertraulichkeit	sehr hoch	In der Vertriebsabteilung wird auf Kunden-daten zugegriffen und diese werden verar-beitet.
		Integrität	sehr hoch	Im Falle einer Veränderung von Kunden-daten können ein erheblicher finanzieller Schaden und ein Imageschaden entstehen.
		Verfügbarkeit	normal	Bei einem Ausfall eines Rechners kann auf den anderen Rechnern weitergearbeitet werden.
N01	zentraler interner Router	Vertraulichkeit	sehr hoch	Über den Router werden alle Daten zwi-schen den Clients und dem Server über-mittelt. Der Datentransfer findet auch unverschlüsselt zwischen diesen Systemen statt. Die Daten ins Internet sind Ende-zu-Ende-verschlüsselt.
		Integrität	hoch	Durch Konfigurationsfehler können Daten-pakete falsch „geroutet" werden. Da der Router das zentrale Element des Netzwerks ist, kann ein unerlaubter Zugriff auf den Router auch zu unerlaubtem Zugriff auf die zu „routenden" Daten führen.
		Verfügbarkeit	hoch	Der Router ist ein „Single Point of Failure", da alle Datenpakete zwischen Client und Servern durch den Router weitergeleitet werden. Auch der Internetzugang hängt vom Router ab. Ein Ausfall ist nur kurzzeitig tragbar.

Schutzbedarfsfeststellung				JIKU IT-Solutions
Nr.	**Beschreibung**	**Grundwert**	**Schutzbedarf**	**Begründung**
N02	Switches	Vertraulichkeit	sehr hoch	Über die Switches werden alle Daten zwischen den Clients und den Servern übermittelt. Der Datentransfer findet auch unverschlüsselt zwischen diesen Systemen statt. Die Daten ins Internet sind Ende-zu-Ende-verschlüsselt.
		Integrität	normal	Durch das Switching-Verfahren „Store and Forward" werden nur fehlerfreie Daten übermittelt.
		Verfügbarkeit	hoch	Bei einem Ausfall eines Switches kann ein Teilbereich des Netzwerks nicht mehr ordnungsgemäß arbeiten. Ein Ausfall ist nur kurzzeitig tolerierbar.
N03	Firewall-System	Vertraulichkeit	normal	Alle Daten, die die Firewall passieren, sind verschlüsselt. Direkt auf der Firewall muss die Verschlüsselung aufgehoben werden.
		Integrität	sehr hoch	Nur durch eine fehlerfreie Konfiguration der Firewall kann die Sicherheit des internen Netzwerks und der darin arbeitenden IT-Systeme gewährleistet werden.
		Verfügbarkeit	hoch	Bei einem Ausfall der Firewall ist keine Verbindung mehr in externe Netzwerke möglich. Auch VPN-Verbindungen können nicht mehr aufgebaut werden. Ein Ausfall ist maximal 3 Stunden tolerierbar.
N04	VPN-Gateway	Vertraulichkeit	hoch	Die Daten, die aus dem externen Netzwerk am VPN-Gateway ankommen, sind verschlüsselt. Die Daten, die in das interne Netzwerk weitergeleitet werden, können auch unverschlüsselt sein. Die Schutzziele des VPN gelten nur bis zum VPN-Gateway.
		Integrität	hoch	Nur durch eine fehlerfreie Konfiguration des VPN-Gateways kann die Sicherheit des internen Netzwerks und der darin arbeitenden IT-Systeme gewährleistet werden.
		Verfügbarkeit	hoch	Bei einem Ausfall des VPN-Gateways sind keine VPN-Verbindungen von Mitarbeitern aus dem Homeoffice oder beim Kunden möglich. Ein Ausfall ist maximal 24 Stunden tragbar.

Schutzbedarfsfeststellung JKU IT-Solutions

Nr.	Beschreibung	Grundwert	Schutzbedarf	Begründung
S01	GitLab-Server	Vertraulichkeit	sehr hoch	Der Programmcode auf dem GitLab-Server stellt für die Unternehmung einen Kernunternehmenswert da. Alle Kundenlösungen basieren auf dem Programmcode. Die auf dem GitLab-Server gespeicherten Dateien müssen verschlüsselt sein.
		Integrität	normal	Eine unerlaubte Manipulation des Programmcodes kann schwere Schäden nach sich ziehen. Allerdings lässt sich eine Manipulation einfach erkennen und durch die Versionierung schnell rückgängig machen.
		Verfügbarkeit	hoch	Bei einem Ausfall des GitLab-Servers kann die Entwicklungsabteilung nur noch eingeschränkt weiterarbeiten, da nur die lokale Codevariante bearbeitet werden kann und eine Zusammenführung der Änderungen mehrerer Personen sehr aufwendig ist.
S02	Dateiserver Kundenlösungen	Vertraulichkeit	sehr hoch	Auf dem Dateiserver der Abteilung Kundenlösungen werden auch kundenspezifische Projekte abgespeichert.
		Integrität	normal	Fehler werden durch z. B. Prüfsummen erkannt und können korrigiert werden.
		Verfügbarkeit	hoch	Bei einem Ausfall des Dateiservers kann die Abteilung Kundenlösungen nur noch eingeschränkt weiterarbeiten, da auf die kundenspezifischen Projekte nicht zugegriffen werden kann.
S03	Dateiserver Vertrieb	Vertraulichkeit	sehr hoch	Auf dem Dateiserver der Abteilung Vertrieb werden auch kundenspezifische Daten, wie z. B. Rechnungen, abgespeichert.
		Integrität	normal	Fehler werden durch z. B. Prüfsummen erkannt und können korrigiert werden
		Verfügbarkeit	hoch	Bei einem Ausfall des Dateiservers kann die Abteilung Vertrieb nur noch eingeschränkt weiterarbeiten, da auf die kundenspezifischen Daten nicht zugegriffen werden kann.
S04	Dateiserver Personal	Vertraulichkeit	sehr hoch	Auf dem Dateiserver der Personalabteilung werden auch personenbezogene Daten der Mitarbeiter abgespeichert.
		Integrität	normal	Fehler werden durch z. B. Prüfsummen erkannt und können korrigiert werden
		Verfügbarkeit	normal	Ein Ausfall kann nicht langfristig toleriert werden. Allerdings spielt die Verfügbarkeit der Daten, wie Briefe oder Abrechnungen, eine untergeordnete Rolle.

Schutzbedarfsfeststellung				JKU IT-Solutions
Nr.	**Beschreibung**	**Grundwert**	**Schutzbedarf**	**Begründung**
S05	AD-Server	Vertraulichkeit	normal	Alle Passwörter sind verschlüsselt gespeichert und nicht zugänglich.
		Integrität	hoch	Bei Fehlern ist eine Authentifizierung von Benutzern u. U. nicht möglich. Neben der Benutzeridentifizierung wird auch die Zuweisung von Rollen und Rechten durch den AD-Server verwaltet.
		Verfügbarkeit	sehr hoch	Ein Ausfall kann nicht toleriert werden. Ohne diesen Server ist eine Anmeldung am IT-System nicht möglich.
S06	Personal-datenbank	Vertraulichkeit	sehr hoch	Personaldaten sind personenbezogene Daten und müssen besonders geschützt werden.
		Integrität	normal	Fehler in der Datenbank werden schnell erkannt und können entweder aus der Datensicherung eingespielt oder durch manuelle Eingabe korrigiert werden.
		Verfügbarkeit	normal	Ein Ausfall kann nicht langfristig toleriert werden. Ausfälle können zeitweise durch manuelle Verfahren überbrückt werden.

3.2.1 Schadenspotenziale in vernetzten Systemen identifizieren

S **Sie sollen mögliche Schadenspotenziale für vernetzte IT-Systeme identifizieren können.**

(1) Imageschaden identifizieren

Nach der Datenschutzgrundverordnung und dem Bundesdatenschutzgesetz drohen Bußgelder und sogar Freiheitsstrafen, wenn ein Unternehmen keine hinreichenden Maßnahmen umgesetzt hat, um den Anforderungen des Datenschutzes zu genügen. Verstöße gegen die DSGVO sind Ordnungswidrigkeiten und können bei unzureichenden TOM mit Bußgeldern bis zu 10 Millionen Euro oder bei Unternehmen mit bis zu 2 % des weltweiten Umsatzes belegt werden, je nachdem, welcher der Beträge größer ist (Artikel 83 DSGVO). Bei schweren Verstößen nennt die DSGVO einen maximalen Betrag von 20 Millionen Euro oder bei Unternehmen 4 % des weltweiten Umsatzes, je nachdem, welcher Betrag höher ist. Strenger ist das BDSG: Bei bestimmten Verstößen handelt es sich um Straftaten, die auch mit Freiheitsstrafen belegt werden können.

Man könnte zu der Ansicht kommen, dieser Mix aus nationalem und europäischem Recht erlaube es großen Firmen, sich durch die entsprechende Wahl des Standortes günstigere rechtliche Bedingungen zu verschaffen und bei entsprechender Größe des Unternehmens auch entspannter mit Strafen bei Verstößen gegen den Datenschutz umzugehen. Jedoch wirkt sich ein Verstoß auch auf das Image der Firma aus, was entsprechend geringeren Umsatz und damit auch sinkenden Gewinn zur Folge haben kann. Das führt dazu, dass der Imageschaden eine Motivation ist, den Datenschutz mit entsprechendem Aufwand umzusetzen.

Besonders betroffen sind hier Unternehmen, deren Geschäftsmodell auf der Sicherheit von Daten beruht, z. B. Banken, Steuerbüros oder Unternehmen, die Passwortmanager zur Verfügung stellen. Ein seriöser

Ruf ist zentral für diese Geschäftsmodelle. Strafen aufgrund des Verstoßes gegen den Datenschutz führen in diesen Geschäftsbereichen zu einem Imageschaden, der auch eine stärkere Auswirkung auf die Anzahl der Kunden hat als beispielsweise bei einer Social-Media-Plattform.

Ein Imageschaden tritt nicht nur bei Verstößen gegen den Datenschutz ein. Auch der Ausfall kritischer Prozesse durch den Ausfall von IT-Systemen führt zu einem Imageschaden. Als Beispiele sind etwa eine fehlerhafte Gepäckabfertigung am Flughafen oder ein Stellwerksausfall bei der Bahn zu nennen. Stehen alternative Anbieter zur Verfügung, kann der Imageschaden sich auch auf den Umsatz auswirken.

(2) Wirtschaftlicher Schaden

Ein wirtschaftlicher Schaden entsteht, wenn es durch den Ausfall von IT-Systemen zu Umsatzeinbußen kommt. Der Grund des Ausfalls ist hier nebensächlich. Entsprechende Maßnahmen sollten aufgrund der Eintrittswahrscheinlichkeit priorisiert werden. Ausfälle können durch einen Hackerangriff geschehen, aber auch Ausfälle durch andere Gefährdungskategorien sind möglich. Ein Stromausfall wird im Einzelhandel mit elektronischen Kassensystemen den Verkauf sofort stoppen. Eine Überflutung wird je nach Schwere den Betrieb eines Unternehmens unterbrechen. Durch Wasserschäden an Räumlichkeiten und der IT kann ein Betrieb auch weitaus länger beeinträchtigt oder unterbrochen sein, als die eigentliche Überschwemmung anhält.

Wichtig sind hier Strategien, die eine Sicherung und ein schnelles Rückspielen des Datenbestands möglich machen. Das BSI empfiehlt eine Speicherung der Daten an unterschiedlichen Orten (georedundante Speicherung), die mindestens 200 km voneinander entfernt liegen, um eine Auswirkung lokaler Katastrophen zu reduzieren. In Bezug auf Angriffe, die auf Verschlüsselung oder Zerstörung von Daten abzielen, ist es notwendig, dass Sicherheitskopien nicht ohne Weiteres von den Produktivsystemen erreicht werden, um vor einem Zugriff durch die Schadsoftware geschützt zu sein.

(3) Schaden durch Datenverlust

Beim Datenverlust sind zwei Aspekte zu betrachten. Grundsätzlich besteht für ein Unternehmen der Schaden erst einmal dadurch, dass die Daten nicht mehr für den Geschäftsprozess genutzt werden können. Darüber hinaus kann ein Imageschaden oder wirtschaftlicher Schaden entstehen.

Bei personenbezogenen Daten kommt es zudem auf die Art des Verlustes an. Sind die Daten nur für das Unternehmen verloren, entsteht dadurch kein Schaden für die betroffenen Personen. Wurden jedoch die Daten gestolen und stehen jetzt unberechtigterweise anderen zur Verfügung, entsteht dadurch auch ein Schaden für die betroffenen Personen. Ist das Unternehmen verantwortlich für diesen Datenverlust, droht ein Bußgeld und dadurch ein noch größerer wirtschaftlicher Schaden.

Kompetenzcheck ✓

1. Diskutieren Sie in Gruppen mögliche Schadenspotenziale für die folgenden Branchen: Apotheken, Einzelhandel und ÖPNV. Benennen Sie mindestens zwei Szenarien für jede Branche im Bereich
   a) Imageschaden,
   b) wirtschaftlicher Schaden,
   c) Schaden durch Datenverlust.

2. Notieren Sie wesentliche Aspekte aus diesem Abschnitt in Ihrem Projektjournal.

3. Bearbeiten Sie Aufgabe 1 der Lernsituation 2 im Arbeitsbuch. A1

3.2.2 Arten des Datenmissbrauchs

S **Sie sollen Datenmissbrauchsmöglichkeiten im Unternehmensumfeld erläutern können.**

(1) Social Engineering

Social Engineering

Social Engineering bezeichnet Angriffsszenarien, bei denen nicht das technische System direkt angegriffen wird, sondern indirekt über in die Irre geführte Menschen.

Beim Social Engineering wird der „Faktor Mensch" als schwaches Glied in der Sicherheitskette für einen Angriff verwendet. Es werden menschliche Eigenschaften ausgenutzt, um Informationen für einen Zugang oder einen Angriffsweg zu erhalten (Jahrgangsband 1, Lernfeld 4, Kapitel 4.1.5), z. B.:

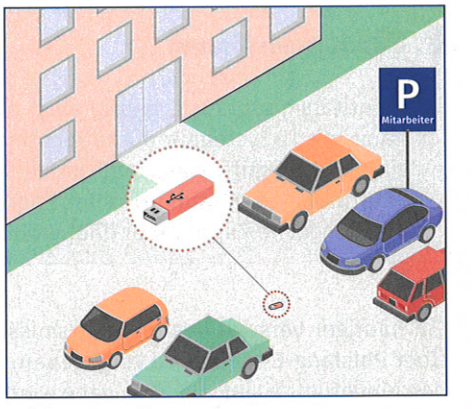
- Hilfsbereitschaft
- Vertrauen
- Angst
- Respekt
- Autorität
- Neugier

Eine einfache Art ist das „Über-die-Schulter-Schauen", um die Eingabe eines Passworts zu beobachten. Hier sollen folgende Arten detaillierter betrachtet werden:

- Baiting
- Phishing/Spear Phishing
- Dumpster Diving

Baiting

Baiting (dt. „Ködern") beschreibt eine Technik, bei der gezielt in der Umgebung einer Firma beispielsweise manipulierte USB-Sticks ausgelegt werden.



Baiting-Szenario

Ein für Angriffe konzipierter USB-Stick ist der sogenannte Rubber Ducky. Dabei handelt es sich nicht um ein klassisches Speichergerät. Wird der Stick in den Computer eingesteckt, agiert er als Tastatur und gibt voreingestellte Tastatureingaben ab. So kann etwa eine Konsole gestartet werden, über die dann Kommandos ausgeführt werden.

Ziel des Baiting ist, Neugier oder Hilfsbereitschaft der Mitarbeiter auszunutzen, um darüber einen gezielten Angriff durchzuführen.

Phishing, Spear Phishing

Das Wort Phishing setzt sich zusammen aus den Wörtern Phreaking (selbst eine Kombination aus Phone and Freak, bezeichnet das Hacking des Telefonsystems bereits in den 1950er-Jahren, um u. a. günstige Telefongespräche zu erreichen) und Fishing (dt. Fischen, Angeln). Phishing beschreibt eine Form des Social Engineering mit dem Ziel, vertrauliche persönliche Informationen wie Anmeldedaten oder Kreditkartennummern zu erhalten oder den Empfänger zur Ausführung einer für ihn schädlichen Handlung zu bewegen.

Während beim Phishing die Opfer in der Regel nicht bekannt sind, zielt das Spear Phishing ganz gezielt auf bestimmte Opfer ab. Dazu werden Informationen über das Opfer für einen Angriff gesucht. Ein Weg ist beispielsweise das Dumpster Diving.

Dumpster Diving

Beim Dumpster Diving wird der Abfall der anzugreifenden Person zur Gewinnung von gezielten Informationen genutzt.

Um einen gezielten Angriff, z. B. auf eine Firma, zu unternehmen, kann die Suche nach Informationen für einen Social-Engineering-Angriff zielführend sein.



Dumpster-Diving-Szenario

Beispiel: Die Bank50 soll angegriffen werden. Beim Dumpster Diving wurde im Papiermüll ein Motorradmagazin gefunden mit dem privaten Adressaufkleber von Alex Schmidt. Bekannt ist, dass die Bank50 für die Mitarbeiter die E-Mails nach dem Schema Vorname.Nachname@Bank50.de erstellt. Ein Spear-Phishing-Angriff wird mit einer gefälschten E-Mail von dem Motorradmagazin an Alex Schmidt@Bank50.de gesendet, mit dem Ziel, den Benutzer über einen in der E-Mail hinterlegten Link auf eine präparierte Webseite zu locken, von der Schadcode für einen Angriff auf die Computer der Bank50 geladen wird.

(2) Identitätsmissbrauch

Identitätsmissbrauch

Identitätsmissbrauch, häufig auch als Identitätsdiebstahl bezeichnet, beschreibt im Zusammenhang mit IT-Systemen die unrechtmäßige Aneignung von Daten und deren missbräuchliche Nutzung. Der Begriff „Diebstahl" ist häufig nicht zutreffend, da gewöhnlich nach einem Diebstahl der rechtmäßige Eigentümer keinen Zugriff mehr darauf hat. Im Zusammenhang mit IT-Systemen ist der ursprüngliche Zugriff aber häufig noch vorhanden.

Ein häufiger Versuch des Identitätsmissbrauchs ist es, die Zugangsdaten von Bankkunden zu erhalten. Über Phishing-E-Mails wird vorgegeben, dass z. B. der Zugang zur Bankwebseite gesperrt wurde und über den eingefügten Link dieser Zugang wieder entsperrt werden soll. Durch das Klicken auf den Link wird der Nutzer auf eine gefälschte Webseite umgeleitet, die der Bankwebseite sehr ähnlich sieht. Gibt der Nutzer dort seine Zugangsdaten ein, kann der Angreifer sie mitlesen, sich damit bei der richtigen Bankwebseite missbräuchlich anmelden und so Zugriff auf die Kontoinformationen des Nutzers erhalten.

Eine andere Form des Identitätsmissbrauchs ist es, im Namen eines anderen Menschen Konten, z. B. in sozialen Netzwerken, anzulegen und dann im Namen dieser Menschen zu handeln. Weitergeführt kann das auf Einkaufsplattformen zu Waren- oder Dienstleistungsbetrug kommen. Hier werden im Namen eines anderen Menschen Waren oder Dienstleistungen bestellt, die dann der Geschädigte bezahlen soll.

Der Identitätsmissbrauch ist aber nicht auf den direkten Angriff einzelner Zugangsdaten beschränkt. Lukrativ ist ein Angriff auf die Datenbank von Onlineplattformen, die auf den Servern der Anbieter liegen. Durch den Zugriff auf die Datenbank fallen den Angreifern sofort alle Nutzerdaten der Plattform in die Hände. Je nach Plattform sind das eventuell nur die E-Mail-Adresse und das „gehashte" Passwort,

gegebenenfalls noch eine Mobilnummer. Bei Einkaufsplattformen betrifft das aber möglicherweise auch Kontodaten, die für den Bezahlvorgang gespeichert wurden.

Über **Datenleaks** veröffentlichen Angreifer erbeutete Daten und machen sie dadurch auch einem weiteren Kreis für den Missbrauch verfügbar. Beim **Doxing** werden Daten aus verschiedenen Angriffen gesammelt veröffentlicht.

(3) Digitale Erpressung

Digitale Erpressung

Unter digitaler Erpressung versteht man die Erpressung von Lösegeld oder Handlungen mithilfe von entsprechenden Druckmitteln, die über das Internet gesendet werden.

Im privaten Bereich kann digitale Erpressung durch Androhung der Veröffentlichung privater Informationen geschehen. Die weit häufigere und vom finanziellen Aspekt gewinnbringendere Form ist im geschäftlichen Umfeld der Angriff mit **Ransomware** und die daraus resultierende Erpressung von Lösegeld (engl. Ransom). Der Ablauf eines Angriffs mit Ransomware folgt typischerweise dem folgenden Muster: Über eine manipulierte E-Mail, ein manipuliertes Dokument oder auf ähnliche Weise wird aus dem Internet die Schadsoftware geladen, die dann damit beginnt, bevorzugt Dokumente in Ordnern (z. B. auch über Netzlaufwerke angebundene Ordner) zu verschlüsseln. Je nach Ausgereiftheit der Software verbreitet sie sich weiter im Netzwerk auf andere Computer und setzt dort die Arbeit fort. Der für die Verschlüsselung verwendete Schlüssel wird auf einem Server der Hacker deponiert. Über eine Nachricht werden die Betroffenen informiert, dass ihre Daten verschlüsselt sind und sie nach einer Zahlung von Lösegeld den Schlüssel erhalten, um die Daten wieder zu entschlüsseln. Um der Echtheit Nachdruck zu verleihen, entschlüsseln die Täter beispielhaft eine Datei. In einer anderen Variante werden die verschlüsselten Daten auf die Server der Hacker übertragen. Daraus ergibt sich dann eine sogenannte Dreifacherpressung:

- Zahlung für den Schlüssel, um die Daten zu entschlüsseln
- Versicherung, dass die Daten nicht veröffentlicht werden
- Zusicherung, dass keine DDoS-Angriffe auf das Unternehmen durchgeführt werden (DDoS = Distributed Denial of Service)



Zahlungsaufforderung nach einem Ransomware-Angriff

Die massenhafte Verschlüsselung von Dokumenten führt zu wiederholten Schreiboperationen auf dem Dateispeicher, was von Schutzsoftware als Indikator für einen Ransomware-Angriff genommen und für Gegenmaßnahmen genutzt werden kann. Die Verschlüsselung kann auch fehleranfällig sein und nicht zum erhofften Erfolg führen. Eine Variante ist daher, nur die Daten zu übertragen und mit der Veröffentlichung zu drohen. Eine Erweiterung dazu ist, nach der Übertragung der Daten diese auf dem angegriffenen Rechner zu löschen. Dadurch ist eine Wiederherstellung nur durch Rückübertragung möglich.

Für forensische Untersuchungen werden nach einem Ransomware-Angriff alle Rechner heruntergefahren. Zum einen soll dadurch eine weitere Verbreitung unterbunden und zum anderen eine Analyse der Ransomware durchgeführt werden. Ziel der Analyse ist es, die Verursacher anhand der verwendeten Softwarestruktur zu identifizieren oder zumindest Anhaltspunkte zu sammeln, die die Angreifer mit anderen Angriffen in Verbindung bringen.

Eine Entwicklung macht diese Analyse schwieriger: Unter dem Begriff **Ransomware-as-a-Service (RaaS)** bieten spezialisierte Hacker die Nutzung ihrer Software als Dienstleistung an.

Kompetenzcheck

1. Beschreiben Sie die Begriffe „Baiting", „Phishing" und „Dumpster Diving" in eigenen Worten.
2. Erläutern Sie, wie ein Angriffsszenario zur Erlangung von personenbezogenen Daten mit anschließendem Identitätsmissbrauch innerhalb eines Unternehmens initiiert werden könnte.
3. Recherchieren Sie weitere Schadenspotenziale im Internet.
4. Notieren Sie wesentliche Aspekte aus diesem Abschnitt in Ihrem Projektjournal.
5. Bearbeiten Sie Aufgabe 2 der Lernsituation 2 im Arbeitsbuch.

A2

3.2.3 Gefährdungenv

S Sie sollen ausgewählte Gefährdungsmöglichkeiten für Unternehmen erläutern können.

IT-Sicherheit wird durch verschiedene Faktoren beeinflusst. Eine systematische Einteilung von Gefährdungen unterscheidet „Höhere Gewalt", „Fahrlässigkeit", „Vorsatz", „technisches Versagen" und „organisatorische Mängel". Daraus hat der BSI die elementaren Gefährdungen entwickelt.



(1) Ausgewählte Gefährdung – Sabotage

Die Sabotage ist nach dem BSI eine elementare Gefährdung. Das BSI beschreibt die elementare Gefahr der Sabotage unter G 0.41.

Sabotage

Der Saboteur hat das Ziel, dem Opfer Schaden zuzufügen. Dazu beschädigt oder manipuliert er ein System, indem er einen Gegenstand oder einen Ablauf absichtlich stört.

Ein Netzwerk kann an vielen verschiedenen Stellen sabotiert werden. Beispielsweise kann der Internetanschluss des Unternehmens von außen lahmgelegt werden. Dazu könnte ein Angreifer den Kabelverzweiger des Telekommunikationsanbieters sabotieren, z. B. die Glasfaser zerschneiden. Weitaus häufiger als Sabotagen von außen ist eine Sabotage von innen. Mitarbeiter können aus verschiedenen Gründen, z. B. aus Unzufriedenheit, den Betriebsablauf durch Sabotage des Netzwerks stören. Besonders ein unkontrollierter Zugriff auf Netzwerkelemente kann leicht zu einer Sabotage führen. So können z. B. Kabel einfach aus- oder umgesteckt werden. Eine Manipulation der Stromversorgung oder der Kühlung

wäre auch denkbar. Beides würde zu einem Ausfall der Netzwerkkomponenten führen. Es ist somit wichtig, den Zugang zu diesen Geräten separat abzusichern.

Nicht jede Sabotage findet direkt am Gerät oder in der unmittelbaren Umgebung statt. Oftmals führt eine Sabotage an einer anderen Stelle durch eine Verkettung von Systemen zu einem Stillstand des Gesamtsystems. Die Sabotage muss auch nicht immer am IT-System durchgeführt werden. Zum Schutz vor Sabotage ist es sinnvoll, dass ein Unternehmen verschiedene Maßnahmen durchführt. Die Einführung eines Zugangsschutzes zu Räumen und Geräten ist nötig. Beispielsweise durch ein gestuftes Schließsystem, mit dem der Zutritt zu Räumen organisiert und protokolliert werden kann. Sinnvoll ist auch die Verwendung von granularen Zugriffsrechten auf IT-Systeme. Auch hier muss eine Protokollierung erfolgen, um einen Zugriff nachvollziehen zu können. Eine nicht-technische Maßnahme ist beispielsweise die Förderung der Zufriedenheit der Mitarbeiter durch eine hohe Wertschätzung und einen respektvollen Umgang.

Durch eine umfangreiche Überwachung der IT-Infrastruktur kann eine Sabotage zeitnah bemerkt und die Folgen können abgeschwächt oder beseitigt werden. Eine erfolgreiche Sabotage beeinträchtigt vor allem die Verfügbarkeit der IT-Infrastruktur.

(2) Ausgewählte Gefährdung – Vandalismus

Vandalismus ist keine elementare Gefährdung nach dem BSI-Grundschutz. Allerdings wird Vandalismus als Folge der elementaren Gefährdung „Unbefugtes Eindringen in Räumlichkeiten" (G 0.44) genannt.

Vandalismus

Unter Vandalismus versteht man eine nicht zielgerichtete Zerstörungswut.

Bei einer Sabotage soll einem Unternehmen mit Absicht ein Schaden zufügt werden. Dazu wird beispielsweise ein IT-System geplant zerstört oder im Ablauf gestört. Eine Sabotage beinhaltet eine vorherige Planung und eine Auseinandersetzung mit dem zu sabotierenden System.

Beim Vandalismus steht die Zerstörung im Fokus. Meist geht dem Vandalismus ein unbefugtes Eindringen in die Räume des Unternehmens voraus. Dabei kommt es häufig auch zu Diebstahl.

Um Vandalismus entgegenzuwirken, ist ein sicherer Zutrittsschutz sinnvoll. Bei abgelegenen Räumlichkeiten kann zusätzlich eine Überwachung durch ein Videosystem und/oder einen Überwachungsdienst gerade am Wochenende dazu dienen, Vandalismus einzuschränken. Räumlichkeiten in belebten Gegenden wie Einkaufsstraßen, besonders im Erdgeschoss, können unter Umständen Ziel von Vandalismus sein. Da sind zum einen Protestaktionen, die in gewalttätige Ausschreitungen übergehen, oder aggressive Fangruppen, um nur zwei Beispiele zu nennen. Hier ist es sinnvoll, die IT-Infrastruktur so zu gestalten, dass Systeme mit wichtigen Daten nicht in den zugänglichen Räumlichkeiten, sondern in besonders geschützten Räumen stehen, wenn möglich sogar auf anderen Ebenen als dem leicht zugänglichen Erdgeschoss.

Die Schäden, die durch Vandalismus entstehen, sind oftmals von einer Versicherung gedeckt. Ein Konzept, um keine Daten dadurch zu verlieren oder den unbefugten Zugriff auf Daten zu verhindern, ist aber unbedingt nötig.

(3) Ausgewählte Gefährdung – Katastrophen

Der Begriff Katastrophe wird bei den elementaren Gefahren des BSI mehrfach aufgeführt. Das BSI erläutert, dass ein Feuer (G 0.1 Feuer) eine Schadenswirkung katastrophalen Ausmaßes haben kann. Die elementare Gefahr G 0.5 beschreibt das Thema Naturkatastrophen, z. B. Erdbeben oder Hochwasser.

Außerdem gibt das Kapitel „Katastrophen im Umfeld" (G 0.6) die Beschreibung und ein Beispiel für Katastrophen, die im räumlichen Umfeld einer Unternehmung vorkommen können.

Katastrophen

Eine Katastrophe kann als schweres Unglück definiert werden. Es ist ein Ereignis mit verheerenden Folgen.

Im Gefährdungskatalog werden die Katastrophen unter dem Punkt „Höhere Gewalt" kategorisiert. Unter G 0.1 wird beschrieben, dass ein Brand etwa durch fahrlässigen Umgang mit Feuer, die unsachgemäße Verwendung elektrischer Einrichtungen oder technische Defekte an elektrischen Geräten entstehen kann. Ein sich ausbreitendes Feuer wird durch mangelnden Brandschutz begünstigt. Feuer beeinträchtigt die Verfügbarkeit der IT-Infrastruktur.

Naturkatastrophen können seismischen, klimatischen oder vulkanischen Ursprungs sein. Besonders Hochwasser ist in den vergangenen Jahren eine große Gefahr geworden. Die IT-Infrastruktur muss nicht direkt von der Katastrophe betroffen sein. Es kann auch zu einer Beeinträchtigung der Verfügbarkeit kommen, wenn z. B. der Stromlieferant betroffen ist.

Bei Katastrophen im Umfeld kommt es in der nahen räumlichen Umgebung der Unternehmung zu einem schweren Unglücksfall. Dadurch wird auch die Unternehmung indirekt betroffen. Beispielsweise kann es bei einem Brand in der Nachbarschaft zu starker Rauchentwicklung kommen. Die Frischluftzufuhr kann durch die Rauchentwicklung beeinträchtigt werden. Wegen mangelnder Kühlung wird ein IT-System heruntergefahren.

Kompetenzcheck

1. Erläutern Sie die Unterschiede zwischen Sabotage, Vandalismus und Katastrophen als Risiken für ein Unternehmen.
2. Diskutieren Sie in der Gruppe weitere Risiken für einen sicheren Betrieb innerhalb eines Unternehmens. Betrachten Sie dabei insbesondere Bereiche, die nicht unmittelbar mit IT-Systemen zusammenhängen.
3. Notieren Sie wesentliche Aspekte aus diesem Abschnitt in Ihrem Projektjournal.
4. Bearbeiten Sie Aufgabe 3 der Lernsituation 2 im Arbeitsbuch.

A3

3.3 Maßnahmen zur Erhöhung der Sicherheit in vernetzten Systemen planen

S Sie sollen die Maßnahmen zur Erhöhung der Sicherheit in vernetzten Systemen unter Beachtung betrieblicher Sicherheitsrichtlinien planen.

In Kapitel 3.1 dieses Lernfeldes wurden die Grundlagen wiederholt und ein Bezug zum Betrieb und zu der Sicherheit vernetzter Systeme gezogen (siehe auch Jahrgangsband 1, Lernfeld 4). In Kapitel 3.2 wurden die Struktur- und die Schutzbedarfsanalyse der Rigudo GmbH sowie zusätzlich verschiedene Gefährdungen für die IT-Infrastruktur beschrieben. In diesem Kapitel 3.3 soll es nun um die Planung von Maßnahmen gehen, die den sicheren Betrieb vernetzter Systeme gewährleisten. Diese Maßnahmen leiten sich zum Teil aus den entsprechenden Bausteinen des BSI ab. Bei der Planung sollten alle Planungsschritte dokumentiert werden. Die Dokumentation ist auch für eine spätere Zertifizierung nötig.

3.3.1 Grundschutz für Clients planen

S **Sie sollen den Grundschutz für Clients zur Erhöhung der Sicherheit planen.**

(1) Endpoint Security

Ein wesentlicher Teil des Betriebs und der Sicherheit von Systemen ist die Sicherheit der Endgeräte.

Endpoint Security

Endpoint Security umfasst den Schutz des Endgeräts vor vielfältigen Bedrohungen. Dieser Schutz wird durch sehr unterschiedliche Maßnahmen gewährleistet. Dazu gehören z. B. der Virenschutz oder der Schutz vor unbefugter Verwendung des Endgeräts.

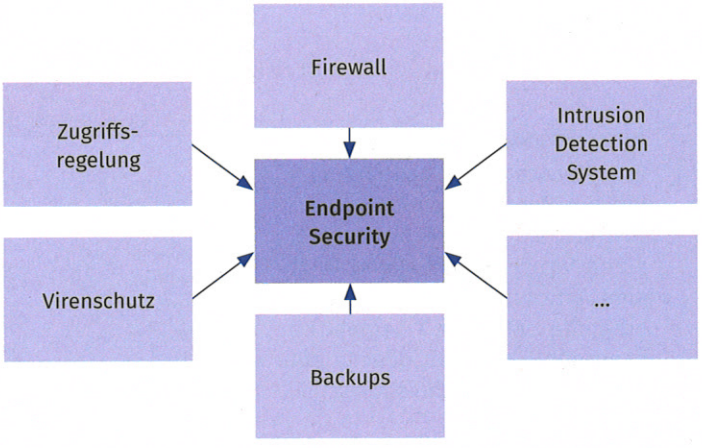
Neben der Absicherung des Netzwerks ist auch die des Endgeräts wichtig. Im Unternehmen werden immer mehr Geräte eingesetzt, die nicht nur mit dem firmeninternen Netzwerk verbunden sind, sondern auch mit anderen Netzwerken wie z. B. dem Internet oder dem Netzwerk im privaten Haushalt.

Gerade durch Verfahren wie „Bring your own device" (BYOD) wird diese Gegebenheit gefördert. Im Firmennetzwerk arbeiten diese eigentlich privaten Geräte mit Firmendaten. Hier sind sie vor externen Angriffen durch die firmeninterne Firewall geschützt. Der Schutz dieser Daten kann aber im privaten Netzwerk unter Umständen nicht gewährleistet werden. So gefährden beispielsweise Cyberangriffe die Endgeräte sowohl im Firmennetzwerk als auch im Netzwerk zu Hause. Es ist nicht ausgeschlossen, dass z. B. ein Trojaner über ein kompromittiertes Gerät im BYOD auch das Firmennetzwerk beeinträchtigt. Werden die Daten im Firmennetzwerk dann durch Ransomware verschlüsselt, kann ein existenzieller Schaden für das Unternehmen entstehen.

Für den Schutz des Endgeräts steht eine Vielzahl technischer und organisatorischer Maßnahmen zur Verfügung. Diese werden im Normalfall kombiniert, um Gegenmaßnahmen für möglichst viele Gefährdungen einzuleiten.

Zugriffsregelung

Bei jedem eingesetzten Endgerät sollte eine Zugriffsregelung existieren. Nur berechtigte Personen dürfen und können das Endgerät verwenden. Diese Zugriffsregelung ist nicht auf eine Benutzeranmeldung beschränkt, sondern kann auch den Zugriff auf die physische Hardware beinhalten. Eine einfache Umsetzung wäre beispielsweise ein automatisches Sperren des Gerätes nach einer bestimmten Zeitdauer der Inaktivität oder das Sichern eines Laptops durch ein Computerkabelschloss.



Backups

Das regelmäßige Erstellen von Backups ist ebenfalls eine Maßnahme, die für die Endgeräte und deren Daten durchgeführt werden sollte. Zur richtigen Backup-Strategie gehört die Wahl eines Backup-Verfahrens (Vollbackup, differenzielles Backup oder inkrementelles Backup) und die Überlegung, welche Backup-Medien wie oft verwendet werden (Stichwort Generationenprinzip). Der Sicherungsprozess und der Wiederherstellungsprozess sollten dokumentiert und getestet werden.

Verschlüsselung der Datenträger und Übermittlung

Die Verschlüsselung der Datenträger kann besonders bei mobilen Geräten sinnvoll sein. Wird beispielsweise ein Gerät entwendet und eine Benutzeranmeldung am System umgangen, z. B. durch den Ausbau des Speichers, schützt eine Verschlüsselung der Daten vor unerlaubtem Zugriff. Durch die Verwendung verschlüsselter Transportwege (z. B. VPN) kann auch ein unberechtigtes Mitlesen und Interpretieren der Daten unterbunden werden.

Firewall

Neben Firewalls, die an den (Sicherheits-)Zonenübergängen im Netzwerk den ein- und ausgehenden Datenverkehr überprüfen, kann es sinnvoll sein, auch hostbasierte Firewalls einzusetzen. Dieser Firewall-Typ sichert nur ein einzelnes Hostsystem ab. Hinsichtlich der grundlegenden Arbeitsweise unterscheidet sich eine hostbasierte nicht von einer netzbasierten Firewall. Beide prüfen meist anhand von Regeln, ob ein Datenpaket oder eine Verbindung erlaubt oder verboten ist. Ein bekanntes Beispiel für eine solche hostbasierte Firewall ist die Windows-Firewall.

IDS/IPS

Neben der Firewall kann beim Hostsystem auch ein sogenanntes Intrusion Detection oder Intrusion Prevention System (IDS/IPS) aktiviert sein. Ein hostbasiertes IDS/IPS arbeitet – wie die hostbasierte Firewall – grundlegend wie ein IDS/IPS, welches ein Netzwerk schützt (vgl. Kapitel 3.5.2).

Schulung

Eine wichtige Maßnahme zur Erhöhung der Sicherheit eines Endsystems ist die Schulung und Sensibilisierung von Mitarbeitern. Diese müssen informiert werden, dass nur durch ihre Mitarbeit eine sichere Arbeit mit dem IT-System gewährleistet werden kann. Beispielsweise müssen Mitarbeiter wissen, dass Phishing-E-Mails existieren und dass ein Klick auf den falschen Link oder das Ausführen eines Makros zu erheblichen Schäden im Netzwerk führen können. Schulungen zur IT-Sicherheit sollten regelmäßig stattfinden. Durch Phishing-Tests kann die Wirksamkeit dieser Maßnahme überprüft werden.

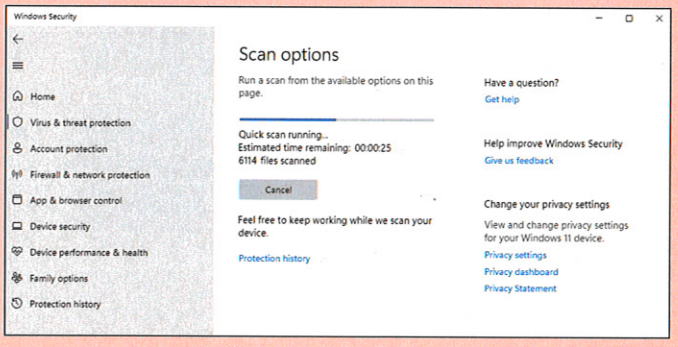
Virenscanner/Antivirus-Software

Ein Virenscanner wird fast immer im Bereich der Endpoint Security eingesetzt. Er prüft eingehende und vorhandene Dateien auf Viren. Moderne Virenscanner überprüfen auch das Verhalten von Prozessen, die bestimmte Systemdateien verändern. Wird hier ein bekanntes Angriffsverfahren identifiziert, wird es vom Virenscanner unterbunden.

Virenscanner und Antivirus-Software

Arbeitsweise von Virenscannern

Ein Virenscanner arbeitet in zwei Phasen. Zuerst erkennt und spezifiziert er eine Malware (z. B. einen Virus). Anschließend folgt eine Aktion. Eine Datei, die eine erkannte Malware beinhaltet, kann dabei gelöscht oder in ein Quarantäneverzeichnis verschoben werden.

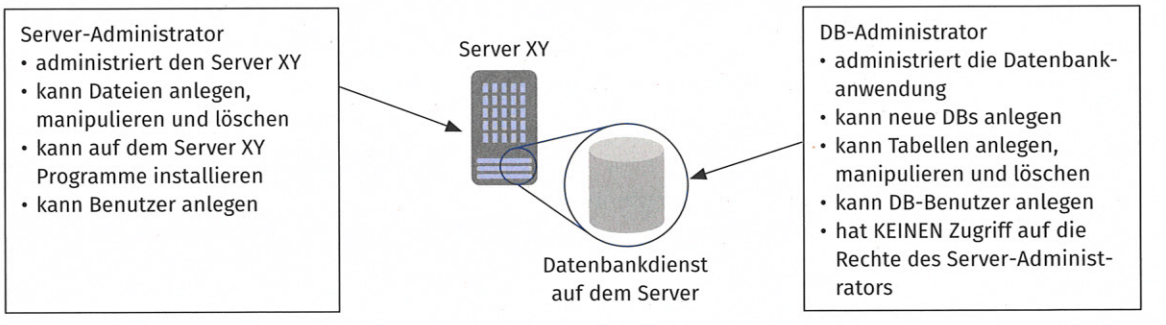


Kommen eine Datei oder allgemein Daten beim Hostsystem an, überprüft der Virenscanner, ob er in den Daten ein bestimmtes bekanntes Bitmuster finden kann. Dieses Bitmuster wird Signatur genannt. Viele Virenscanner arbeiten signaturbasiert. Neue Virensignaturen werden durch Updates in die Datenbank des Virenscanner eingepflegt.
Ein Signaturvergleich erlaubt eine schnelle Erkennung von Viren. Als Abwehrmaßnahme gegen aktuelle Schadsoftware muss der Virenscanner über möglichst aktuelle Signaturen verfügen. Das Scannen eines großen Datenbestands ist ressourcenintensiv und benötigt Zeit. Gerade auf älteren Endsystemen wird so ein Großteil der Systemressourcen zur Malware-Überprüfung benötigt – mit dem Effekt, dass das System sehr langsam auf Benutzereingaben reagiert.
Die Anwendung von mehreren Virenscannern verschiedener Hersteller sollte vermieden werden. Im schlimmsten Fall erkennen sich beide Virenscanner wegen der Signaturdatenbanken gegenseitig als Malware und behindern die ordnungsgemäße Ausführung des jeweils anderen Scanners. Das Endsystem kann vom Benutzer gegebenenfalls nicht mehr sinnvoll verwendet werden.

Arbeitsweise von Antivirus-Software
Zusätzlich zur Signaturerkennung kann eine Antivirus-Software mit einer heuristischen Erkennung arbeiten. Bei dieser Erkennungsart wird das Systemverhalten beim Laden und Ausführen von Dateien beobachtet und anormales Verhalten unterbunden. Eine heuristische Erkennung arbeitet regelbasiert. Eine Regel könnte z. B. unter Windows die Registry-Einträge beobachten. Wird hier beispielsweise ein Eintrag im „Autostart" vorgenommen, wird dieser unterbunden. Auch diese Regeln werden durch Updates auf dem aktuellsten Stand gehalten. Ein weiterer Vorteil ist die mögliche Ausführung von Software in einer sogenannten Sandbox. Dabei wird eine Datei automatisch in einer virtuellen Umgebung geöffnet. Diese Umgebung hat keinen Kontakt zur Produktivumgebung. Erst wenn innerhalb der Sandbox kein ungewöhnliches Verhalten festgestellt werden kann, wird die Datei an die Produktivumgebung weitergeben. Dieses Verfahren benötigt allerdings viel Zeit und Ressourcen und verlangsamt das Endsystem.
Im neuesten Trend verwenden Antivirus-Programme KI-Strategien zur Erkennung von Malware. Durch solche Strategien kann gegebenenfalls auch noch unbekannte Malware erkannt werden. Außerdem können problematische Dateien zur näheren Untersuchung automatisch an den Virenschutzhersteller gesendet werden. Hier muss allerdings darauf geachtet werden, ob eine automatische Weiterleitung von Daten datenschutzkonform ist.

(2) Trennung von OS- und DB-Benutzerverwaltung

Beim Betrieb eines Servers kann für die Benutzerverwaltung zwischen der Serververwaltung und der Datenverwaltung unterschieden werden.



Abgrenzung der Benutzerverwaltungsbereiche

Die Serververwaltung installiert und administriert den Server inklusive Betriebssystem und Dienste. Der Administrator installiert beispielsweise einen Windows-Server und fügt die Serverrolle „DHCP" hinzu. Anschließend konfiguriert er den DHCP-Scope und die zu verteilenden Optionen. Bei der Installation und dem Betrieb von Anwendungssoftware kann es sinnvoll sein, die Benutzer des Betriebssystems und die

der Anwendungssoftware zu trennen. Das ist besonders dann der Fall, wenn der Anwendungsdienst aus dem öffentlichen Netzwerk erreichbar sein soll oder muss.

Ein Beispiel dafür ist die Verwendung einer Datenbank. Der Administrator des Betriebssystems kann im Betriebssystem Ordner anlegen, Dateien löschen, Programme installieren, Benutzer anlegen oder den Datenbankdienst installieren. Der Administrator der Datenbank hat keinen Zugriff auf die Rechte des Administrators des Betriebssystems. Der Datenbank-Administrator kann innerhalb des Datenbankmanagementsystems (DBMS) Tabellen anlegen, Sichten konstruieren, Datensätze manipulieren und beispielsweise Datenbank-Benutzer anlegen. Für beide Systeme liegen unterschiedliche Konten mit unterschiedlichen Rechten vor. Kommt es in diesem Szenario zu eine Kompromittierung der Datenbank, ist das restliche Serverbetriebssystem vor unberechtigtem Zugriff immer noch geschützt.

Das BSI setzt eine Trennung zwischen den administrativen Schichten voraus und verweist im Baustein APP 2.2 darauf, dass die Rollen „Dienste-Administrator" und „Daten-Administrator" nur möglichst wenigen Personen zur Verfügung stehen sollten.

(3) Softwareinstallation/Updates planen

Jede zu nutzende Software durchläuft einen Lebenszyklus, der die Schritte Planung, Anforderungen ermitteln, Beschaffung, Software-Tests, Installation, Schulung, Betrieb, Updates und Änderungsmanagement, gegebenenfalls Migration sowie Außerbetriebnahme (Deinstallation) der entsprechenden Software umfasst (siehe auch Jahrgangsband 1, Lernfeld 4, Kapitel 4.4.1). Hier soll nun die Planung der sicherheitsrelevanten Aspekte von Softwareinstallation und Aktualisierung betrachtet werden.

Bei der Planung sind neben den rein technischen Maßnahmen vor allem die Zuständigkeiten zu regeln. Für jeden Abschnitt des Lebenszyklus müssen die Zuständigkeiten klar formuliert und nachvollziehbar protokolliert werden.

Bei der Softwareinstallation sowie im Aktualisierungsmanagement sind folgende Aspekte zu berücksichtigen:

Aktualisierungsmanagement
Bezugsquellen (online) prüfen Quellen bzw. Download-Pakete auf Echtheit prüfen; Zertifikate prüfen; SHA2-Prüfsummen der Software prüfen; bei Linux: PPA-Quellen überprüfen
Regressionstest durchführen Vor dem produktiven Einsatz von Updates Tests einplanen, damit keine betriebsrelevanten Systeme gestört werden
Informationsmanagement sicherstellen Aktive Verfolgung von Nachrichten zu Sicherheitslücken der eingesetzten Software, z. B. durch Abos von Newslettern der Hersteller bzw. Sicherheitsforen; sicherheitskritische Updates müssen umgehend priorisiert durchgeführt werden
Hardware-Anforderungen prüfen Updates können die ursprünglichen Hardware-Anforderungen ändern; Überprüfung muss daher vor produktivem Einsatz erfolgen
Änderungen im Umgang Updates können die Bedienung der Software maßgeblich ändern; Schulungsbedarf prüfen, gegebenenfalls Mitarbeiter informieren; komplizierte Sicherheitsmechanismen können dazu führen, dass die Mitarbeiter diese umgehen bzw. ignorieren; gegebenenfalls Alternativen suchen

Auf Linux-Systemen ist es üblich, Software aus sogenannten Repositories, also Software-Katalogen, zu installieren. Hier muss zwischen Distribution Repositories und freien Bezugsquellen unterschieden wer-

den. Die Distribution Repositories sind gut gepflegt und werden regelmäßig getestet. Sie gelten im Allgemeinen als sicher. Bei freien Bezugsquellen, die häufig als Personal Package Archive (PPA) angeboten werden, sollte man vorab prüfen, ob diese Bezugsquelle ähnlich vertrauenswürdig ist.

! Auf der Seite https://launchpad.net/ können viele dieser PPA-Pakete eingesehen werden.

Bei Maintainer bzw. Member sollte auf die Membership Policy geachtet werden. Diese sollte „Restricted Team" oder „Moderated" lauten, da nur Administratoren und validierte Nutzer eingeladen werden. Daten eines „Open"-Accounts sollten nicht eingebunden werden, da diese Accounts frei erstellt werden können und keinerlei Kontrolle unterliegen. Diese Accounts können keine PPA pflegen.

Bevor man eine derartige Quelle nutzt, müssen die Quellen per Schlüsselimport in der lokalen Paketverwaltung bekannt gemacht werden. Dies soll sicherstellen, dass die Autorenschaft der Software überprüfbar wird und sich die Person gegenüber einer vertrauenswürdigen Stelle ausgewiesen hat.

Microsoft hat dieses System mit der Einführung des „Microsoft Store" nachgebildet. Microsoft stellt durch Prüfung der eingereichten Software sicher, dass diese frei von Schadsoftware ist. Für den Einsatz in geschlossenen Systemen wie Unternehmen oder Bildungseinrichtungen hat Microsoft die Varianten „Microsoft Store for Business" bzw. „Microsoft Store for Education" im Angebot. Hier ist es möglich, das Angebot des öffentlichen Stores auf die in der eigenen Einrichtung freigegebene Software zu beschränken. Diese Varianten werden allerdings nach Microsoft-Ankündigungen in naher Zukunft zu einer freieren Variante umgestaltet.

Neben dieser Möglichkeit gibt es für Windows-Clients verschiedene Möglichkeiten, Anwendungen kontrolliert zu installieren:
- Windows Server Update Service (WSUS)
- Deployment-Software wie Deskcenter, Empirum oder Microsoft Endpoint Configuration Manager (MECM)
- Chocolatey for Business

Mit diesen Werkzeugen kann ein eigenes Repository aufgebaut werden. Vorteil dieser Lösung ist die Unabhängigkeit von externen Software-Repositories. Größter Nachteil ist der zusätzliche Verwaltungsaufwand, der mit steigender Zahl der zur Verfügung zu stellenden Software nicht zu unterschätzen ist. Es ist daher zu entscheiden, ob man externen Repositories vertraut und Aufwände reduziert oder alles in der eigenen Hand behalten will. In Kapitel 3.4.1 wird die Vorgehensweise zur Installation und Konfiguration eigener Repositories exemplarisch vorgestellt.

Kompetenzcheck

1. Nennen Sie mindestens drei Schutzmaßnahmen für die Endpoint Security. Erläutern Sie diese Maßnahmen kurz.
2. Erklären Sie, was unter Trennung von Betriebssystem- und Anwendungsbenutzerverwaltung zu verstehen ist.
3. Nennen Sie die Aspekte, die vom Aktualisierungsmanagement berücksichtigt werden sollten.
4. Notieren Sie wesentliche Aspekte aus diesem Abschnitt in Ihrem Projektjournal.
5. Bearbeiten Sie Aufgabe 1 der Lernsituation 3 im Arbeitsbuch.

A1

3.3.2 Zugriffsmöglichkeit auf vernetzte Systeme im lokalen Netz planen

S **Sie sollen den Zugriff auf vernetzte Systeme im lokalen Netz mit ausgewählten Techniken planen.**

(1) VLAN planen

Die VLAN-Technik wurde bereits in anderen Lernfeldern behandelt (siehe auch Jahrgangsband 1, Lernfeld 3, Kapitel 3.3.3 und Jahrgangsband 2, Lernfeld 9, Kapitel 4.5.2). Im Folgenden soll für die Rigudo GmbH die VLAN-Struktur geplant werden.

VLAN

Ein VLAN stellt eine abgeschlossene Broadcast-Domäne dar. Die Zugehörigkeit zu einem VLAN kann per Konfiguration definiert werden. Sie kann über verschiedene Kriterien wie den Anschluss (Port), die MAC- oder IP-Adresse vorgenommen werden.

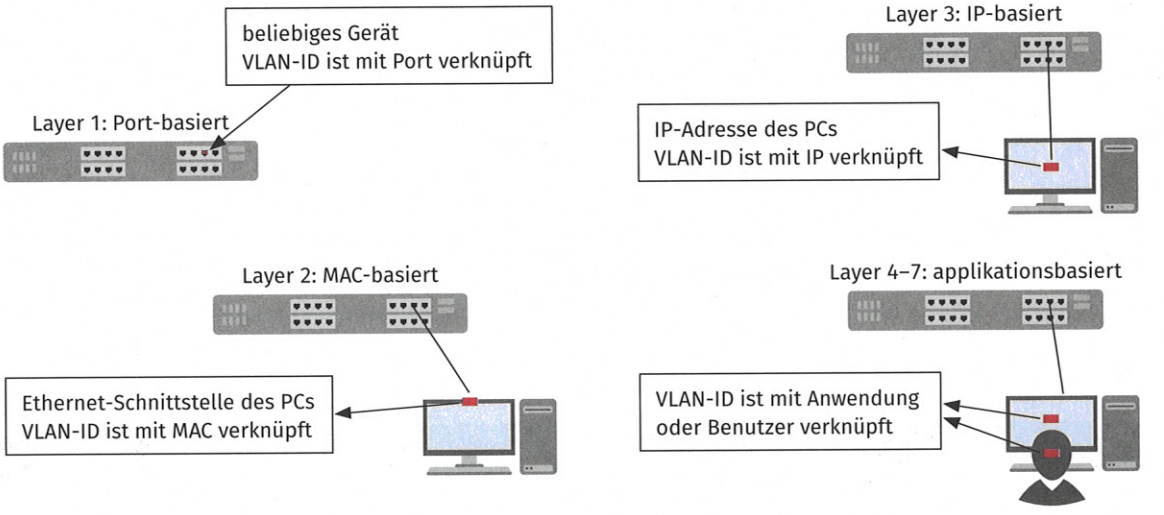
OSI-Schicht	Kriterium für VLAN-Zugehörigkeit	Sicherheit	Administrationsaufwand	Flexibilität
1	Zuordnung eines physikalischen Ports; portbasiert	mittel	niedrig	niedrig
2	Zuordnung einer MAC-Adresse; MAC-Adressen-basiert	mittel, MAC-Adresse kann geändert werden	höher, da MAC-Adressen ausgelesen werden müssen	höher, Arbeitsplatz kann am Switch geändert werden
3	Zuordnung einer IP-Adresse; IP-Adressen-basiert	mittel, IP-Adresse kann geändert werden	höher, da IP-Adressen verwaltet werden müssen	hoch, Arbeitsplatz kann im Subnetz geändert werden
4–7	Zuordnung über Anwendungen/Benutzer; applikationsbasiert	hoch, sofern Benutzer authentifiziert werden	höher, da Anwendungen/Benutzer verwaltet werden müssen	hoch, Arbeitsplatz kann im Unternehmen gewechselt werden

Die verschiedenen Kriterien sollten nach den drei Aspekten „Sicherheit", „Administrationsaufwand" und „Flexibilität" ausgewählt werden. Die einfachste Möglichkeit ist die fixe Zuordnung eines Ports zu einem VLAN. Hier kann der Nutzer dann beliebige Endgeräte nutzen. Darin besteht aber auch gleichzeitig ein Sicherheitsrisiko, wenn der Arbeitsplatz frei zugänglich ist, da Unbefugte über den betreffenden Port ebenfalls Zugang zu dem entsprechend VLAN erhalten. Die Flexibilität ist ebenfalls eingeschränkt, da ein Arbeitsplatz nicht ohne Rekonfiguration gewechselt werden kann (z. B. in einem Großraumbüro mit unterschiedlichen VLAN-Zugehörigkeiten).

Bei Kriterien wie MAC- oder IP-Adressen ist der Administrationsaufwand höher, da diese Informationen zusätzlich dokumentiert und verwaltet werden müssen. Unter Umständen müssen diese Informationen auf mehreren Switches hinterlegt werden. Dafür erhöht sich die Sicherheit leicht, da mögliche Angreifer zunächst die entsprechende Adresse ermitteln müssen, um diese dann am eigenen Gerät zu konfigurieren. Die Flexibilität erhöht sich, da in diesem Fall die feste Zuordnung zum Port entfällt.

Die größte Flexibilität erhält man bei Zuordnung über Anwendungen bzw. Benutzer. Die Administrationsaufwände sind leicht erhöht, da die Switche eine – idealerweise – zentrale Datenbank (z. B. ein Verzeichnisdienst wie ein Active Directory) abfragen müssen. Die Sicherheit ist ebenfalls erhöht, sofern eine Authentifikation vorgesehen ist (z. B. Single-Sign-On).

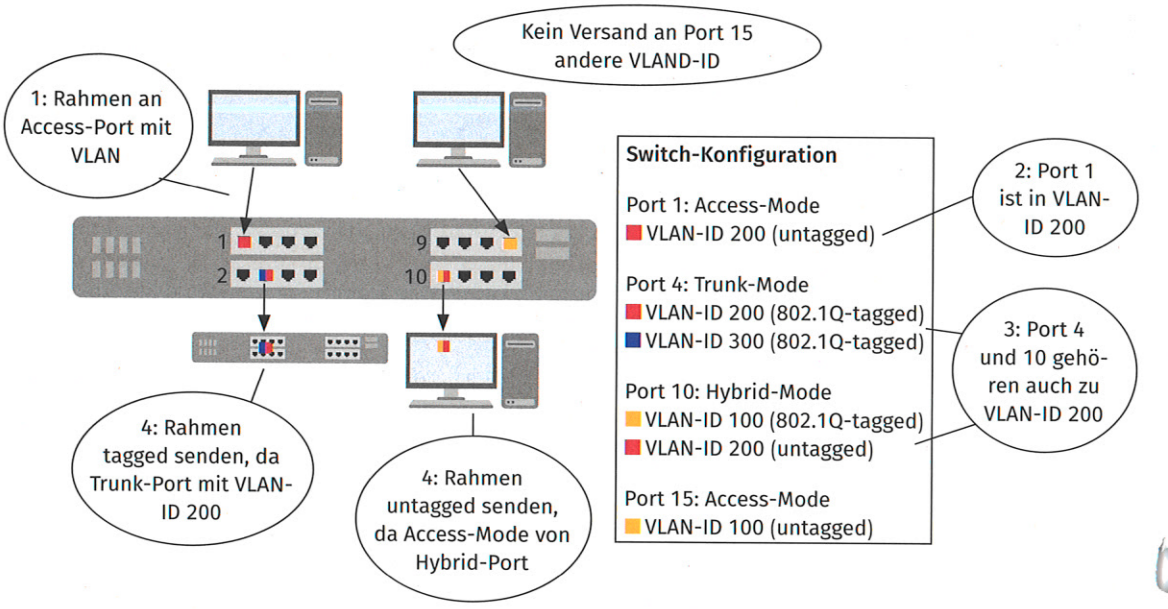
Die folgende Abbildung zeigt die unterschiedlichen Möglichkeiten der Zugehörigkeit. Die Umsetzung ist jeweils herstellerspezifisch, sodass bei der Auswahl der Switche nicht nur das „Feature VLAN" zu beachten ist. Meist ist damit zunächst die Unterstützung des Standards 802.1Q gemeint, der die Übermittlung von VLAN-IDs innerhalb des Ethernet-Frames (Ethernet-Rahmens) ermöglicht, das sogenannte VLAN-Tagging. 802.1Q stellt somit die Grundfunktion zum herstellerübergreifenden Einsatz von VLANs dar (siehe auch Erweiterung des Ethernet-Frames in Jahrgangsband 1, Lernfeld 3, Kapitel 3.3.3).



Kriterien für die VLAN-Zuordnung

Ein Switch arbeitet bei VLANs die **Zugehörigkeit** in vier Schritten wie folgt ab:

1. Prüfen, ob am Eingangs-Port VLAN konfiguriert ist.
2. Gemäß des Zugehörigkeitskriteriums (z. B. MAC-Adresse, Port-Nummer etc.) ermitteln, zu welcher VLAN-ID der angekommene Rahmen gehört.
3. Alle weiteren Mitglieder dieser VLAN-ID ermitteln.
4. Den Rahmen unter Berücksichtigung der Konfiguration des jeweiligen Ausgangsports an die Mitglieder senden.



VLAN-Varianten an Switch-Ports (Access, Trunk, Hybrid)

Ein Switch ist standardmäßig so konfiguriert, dass alle Ports untereinander kommunizieren können. Dabei sind die Ports im sogenannten **Access-Mode**. Daneben gibt es für VLANs nach 802.1Q den **Trunk-Mode** und den **Hybrid-Mode**.

Mode	Tagging	Beispiel
Access	nein	einfache PCs; Standard-Konfiguration
Trunk	ja, immer	Verbindungen zu anderen Switches oder Servern, die über eine Schnittstelle in mehr als ein VLAN kommunizieren
Hybrid	ein VLAN ohne Tagging; weitere VLANs mit Tagging	Administrator-Anschluss; ohne Tagging für Standard-anwendungen; mit Tagging für z. B. administrative Zugänge zu Servern

Bei der Planung von VLANs ist vor allem bei Servern und Rechnern, die mit Tagging betrieben werden sollen, die Unterstützung durch das Betriebssystem entscheidend. Unter Linux wird VLAN über ein einheitliches Modul direkt vom Kernel bereitgestellt, sodass im Prinzip jede von Linux unterstützte Netzwerkkarte auch mit VLAN-Tagging betrieben werden kann.

MacOS unterstützt VLAN-Tagging ebenfalls direkt. Bei Windows ist VLAN-Tagging Bestandteil des jeweiligen Netzwerkkartentreibers und damit herstellerabhängig. Hersteller wie Intel und Realtek bieten diese Funktionalität für ihre Netzwerkkarten in ihren Treibern an. Allerdings ist auch hier ein Blick in das Datenblatt der Netzwerkkarte hilfreich. Jeder Hersteller arbeitet mit einer eigenen Umsetzung, wodurch eine einheitliche Planung erschwert wird.

Bei der Planung muss darauf geachtet werden, dass gemäß des Zonen- und Sicherheitskonzeptes Zugriffe nur dort möglich sind, wo sie zwingend erforderlich sind.

Für die Rigudo GmbH wurde ein solches Zonen-Konzept vorgestellt. Hiermit wird eine Zugriffsordnung vorgegeben, die definiert, welche Verbindungen zwischen den unterschiedlichen Netzbereichen erlaubt sind.

Zugriffsordnung des Modellkunden Rigudo GmbH

	Zone		Entwicklung 172.20.0.0/16	Kundenlösung 172.30.0.0/16	Personal-abteilung 172.40.0.0/16	Vertrieb 172.50.0.0/16
			2	3	2	3 ← Zone
Server-Netz	1	172.10.0.0/16	ja	ja	ja	ja
Gitlab	1	172.10.20.20/16	ja	nein	nein	nein
Dateiserver-KD-Lösungen	1	172.10.30.100/16	nein	ja	nein	ja
Dateiserver Vertrieb	1	172.10.50.100/16	nein	ja	nein	ja
Dateiserver Personal	1	172.10.40.100/16	nein	nein	ja	nein
Active Directory (AD)	1	172.10.0.1/16	ja	ja	ja	ja
Personal-DB	1	172.10.40.200/16	nein	nein	ja	nein
Kunden-DB	1	172.10.30.200/16	nein	ja	nein	ja

Zugriffsordnung des Modellkunden Rigudo GmbH

Hieraus können die VLAN-IDs und die notwendigen Betriebsmodi festgelegt werden.

Festgelegte Betriebsmodi in Zugriffsmatrix des Modellkunden Rigudo GmbH

	Zone		VLAN-ID → / VLAN-ID ↓	20 Entwicklung 172.20.0.0/16	30 Kundenlösung 172.30.0.0/16	40 Personal-abteilung 172.40.0.0/16	50 Vertrieb 172.50.0.0/16
				2	3	2	3 ← Zone
Server-Netz	1	172.10.0.0/16	10, 20, 30, 40, 50	ja	ja	ja	ja
Gitlab	1	172.10.20.20/16	10 20	ja	nein	nein	nein
Dateiserver KD-Lösungen	1	172.10.30.100/16	10, 30, 50	nein	ja	nein	ja
Dateiserver Vertrieb	1	172.10.50.100/16	10, 30, 50	nein	ja	nein	ja
Dateiserver Personal	1	172.10.40.100/16	10 40	nein	nein	ja	nein
Active Directory (AD)	1	172.10.0.1/16	10, 20, 30, 40, 50	ja	ja	ja	ja
Personal-DB	1	172.10.40.200/16	10 40	nein	nein	ja	nein
Kunden-DB	1	172.10.30.200/16	10, 30, 50	nein	ja	nein	ja

untagged
tagged
VLAN-ID 10 → Administration

Festgelegte Betriebsmodi in Zugriffsmatrix des Modellkunden Rigudo GmbH

Zusätzlich zu den anwendungsbezogenen Zugriffen soll der IT-Support auf alle Geräte zugreifen können. Die administrativen Zugänge zu den Servern und der Infrastruktur werden in einem eigenen VLAN mit der VLAN-ID 10 abgebildet.

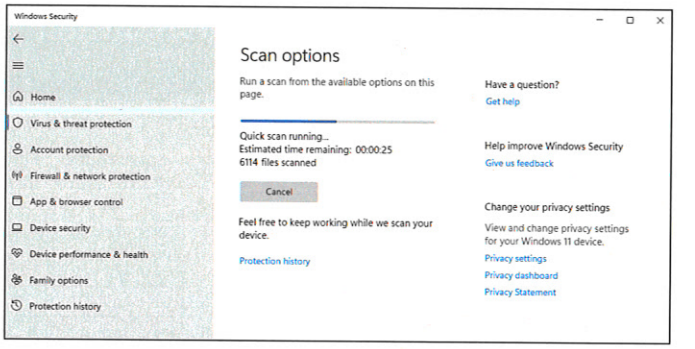
(2) Firewall planen

Eine Firewall ist für den Betrieb und die Sicherheit eines Netzwerkes unerlässlich. In den meisten Unternehmen kommt eine Firewall-Architektur zum Einsatz.

Auch das BSI klassifiziert die Firewall als eine Kernkomponente bezüglich der Sicherheit des Netzwerks und unterstützt den Betreiber eines Netzwerks mit dem Baustein „NET.3.2: Firewall".

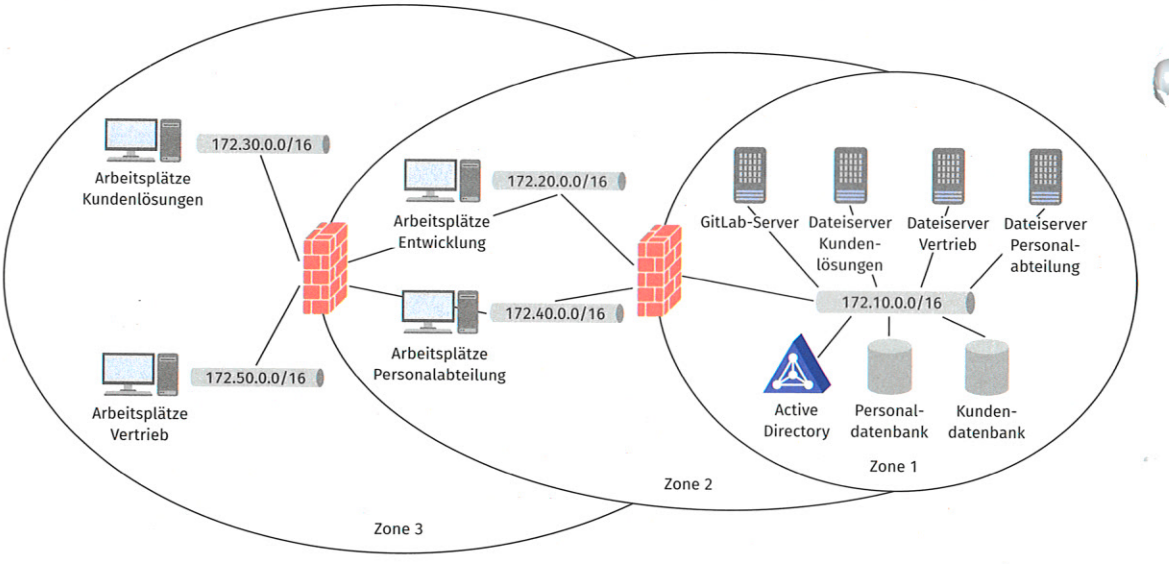
Eine Firewall kann als **hostbasierte Firewall** zum Schutz eines einzelnen Hostsystems eingesetzt werden.

Ein bekanntes Beispiel dafür ist die Windows-Firewall. Diese ist integrativer Bestandteil aktueller Windows-Betriebssysteme.



Firewall-Einstellungen unter Windows

In Unternehmen kommen **netzbasierte Firewalls** zum Einsatz. Diese Art von Firewall sichert Netzübergänge ab. Diese müssen nicht zwangsläufig zwischen dem internen Netzwerk und dem externen Netzwerk liegen. Ein sinnvoller Einsatz kann auch zwischen unterschiedlichen Sicherheitszonen innerhalb eines Netzwerks liegen.

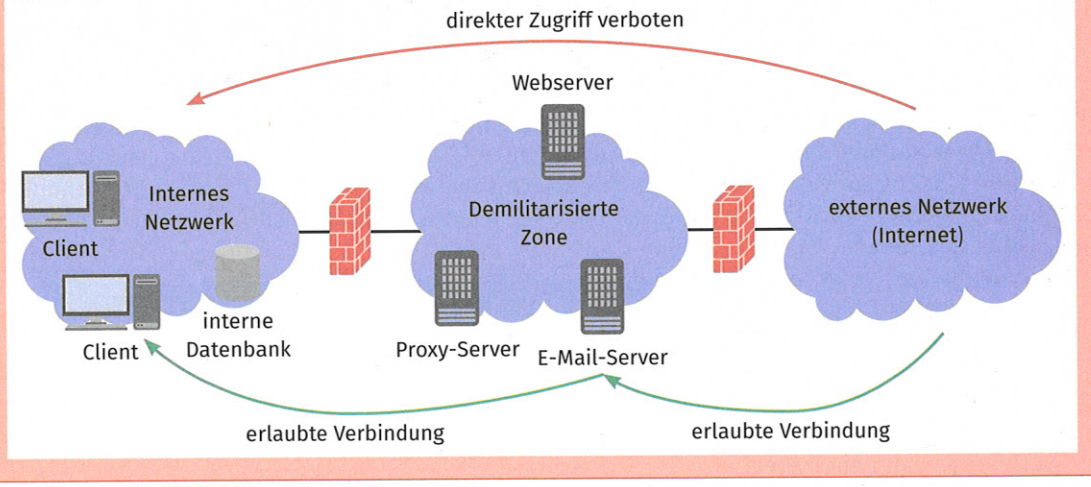


Beispielhaftes Zonenmodell der Rigudo GmbH

Sicherheitszonen

Das Einteilen eines Netzwerks in Sicherheitszonen ist ein Konzept, welches vom BSI im Baustein „NET.1.1: Netzarchitektur und -design" vorgeschlagen wird. In einem Gesamtnetzwerk werden einzelne Bereiche anhand der umzusetzenden Sicherheit definiert. Dabei müssen alle IT-Systeme berücksichtigt und analysiert werden. Zu untersuchen ist, welche Personen und Systeme auf welche Systeme Zugriff benötigen. Ausgehend von den Systemen und Berechtigten werden die Zonen gebildet.
Die Zonen werden logisch klar voneinander getrennt. Dazu wird z. B. die VLAN-Technik verwendet, um eine Trennung auf OSI-Schicht 2 zu erhalten.
Das minimale Zonenkonzept besteht aus drei Zonen und arbeitet mit einer sogenannten demilitarisierten Zone (DMZ). Das interne Netzwerk beinhaltet alle Systeme und Dienste, die nur aus dem internen Netzwerk erreichbar sein sollen. Das sind z. B. Clients oder eine nur firmenintern verwendete Kundendatenbank. Das Netzwerk zwischen internen und externen Netzwerken wird DMZ genannt. In der DMZ werden alle Dienste und Systeme installiert, auf die aus dem externen Netzwerk zugegriffen werden muss. Ein solcher Dienst kann z. B. ein E-Mail-Server sein, der aus dem externen

Netzwerk E-Mails empfangen kann. Ein anderes Beispiel ist ein Webserver, der eine Website zur Verfügung stellt, die aus dem externen Netzwerk abgerufen werden kann. Eine direkte Verbindung zwischen dem externen und dem internen Netzwerk ist nicht erlaubt. In der nachfolgenden Netzwerkskizze wird die beschriebene DMZ dargestellt.

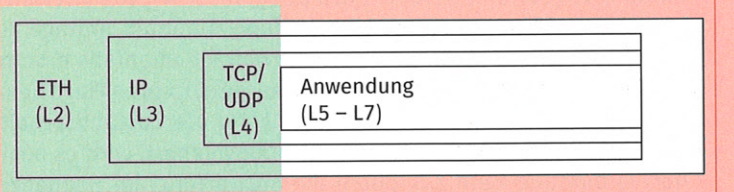


Für den Einsatz von Firewalls macht das BSI weitere Vorgaben. Die Firewalls müssen bestimmte Anforderungen erfüllen. Eine dieser Anforderungen beschreibt die einzusetzenden Firewall-Arten. Am Netzübergang zwischen externem Netzwerk und DMZ muss mindestens eine Paketfilter-Firewall mit Stateful Packet Inspection (SPI) eingesetzt werden. Am Netzübergang zwischen DMZ und internem Netzwerk sollte ein Application Layer Gateway (ALG) eingesetzt werden (siehe auch Jahrgangsband 2, Lernfeld 9, Kapitel 4.4.2)

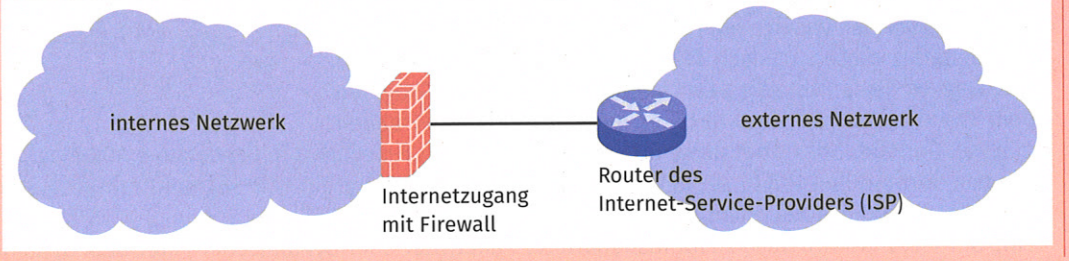
Firewall-Arten

Paketfilter-Firewall

Eine Paketfilter-Firewall arbeitet auf den OSI-Schichten 3 und 4 (Vermittlungs- und Transportschicht). Als Filterkriterien werden meist die Quell- und Ziel-IP-Adresse eines IP-Pakets und die UDP/TCP-Quell- und Ziel-Ports des Segments verwendet. Dazu müssen die Daten bis zur vierten OSI-Schicht analysiert werden. Die einzulesenden Daten werden in der obigen Grafik dargestellt.



Neben dem IP-Paket wird auch der Schicht-4-Protokoll-Header, der UDP-Header oder der TCP-Header eingelesen. Der Ethernet-Header (Schicht 2) wird von der Firewall ebenfalls eingelesen, aber es ist nicht sinnvoll, auf die MAC-Adresse zu filtern, da der administrative Aufwand bei einem Austausch der Hardware sehr hoch ist.



Bei einer typischen Netzwerkinstallation im privaten oder im Firmenumfeld ist das Netzwerk an einen Router des Internet-Service-Providers (ISP) angeschlossen. Auf diesem Gerät oder – direkt dahinter – am Netzübergang wird eine Firewall betrieben.
Im Netzwerksegment findet die Adressierung über die MAC-Adresse statt. Die Daten, die aus dem externen Netzwerk bei der Firewall ankommen, tragen immer die gleiche MAC-Adresse, nämlich die MAC-Adresse des Routers des Internet-Service-Providers.
Ein Paketfilter kann ein Paket auch auf andere Schicht-3-Protokolle untersuchen und dadurch die Pakete auf zusätzliche Informationen überprüfen. Ein Beispiel für ein Schicht-3-Protokoll ist das „Internet Control Message Protocol (ICMP)". Durch dieses Protokoll wird der „ping"-Befehl realisiert. Wenn A die Erreichbarkeit von B mittels „ping"-Befehl überprüfen möchte, sendet A eine ICMP-Nachricht an B. Diese Nachricht ist eine ICMP-Type-8-Nachricht und wird „ICMP Echo Request" genannt. Das System B antwortet mit einer ICMP-Type-0-Nachricht. Diese Nachricht heißt „ICMP Echo Reply".

Die Abbildung zeigt einen Wireshark-Mitschnitt eines „pings" zwischen den IP-Adressen 192.168.178.62 und 192.168.178.1.

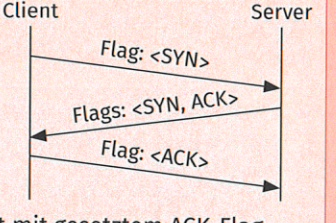
Source	Destination	Protocol	Info
192.168.178.62	192.168.178.1	ICMP	Echo (ping) request
192.168.178.1	192.168.178.62	ICMP	Echo (ping) reply

```
Internet Protocol Version 4, Src: 192.168.178.62, Dst: 192.168.178.1
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
Internet Protocol Version 4, Src: 192.168.178.62, Dst: 192.168.178.1
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
```

Oftmals soll eine Firewall verhindern, dass ein System über das ICMP erreichbar ist. Das System selbst soll aber ICMP-Requests senden können. Dazu kann eine Paketfilter-Firewall eingehende ICMP-Echo-Request-Nachrichten verwerfen. Jeder andere ICMP-Verkehr wird aber erlaubt.
Paketfilter-Firewalls sind weit verbreitet. Die meisten Betriebssysteme haben eine solche integriert. Da nicht alle Schichten, sondern nur die Schicht-3- und Schicht-4-Header untersucht werden, kann die Paketfilter-Firewall ressourcenschonend und schnell arbeiten.

Stateful Packet Inspection (SPI)

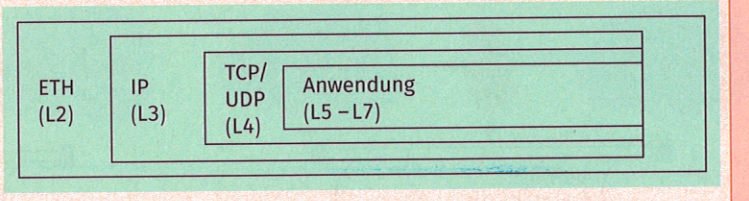
Ein großer Nachteil einer Paketfilter-Firewall ist, dass jedes Paket einzeln betrachtet wird. Eine Zuordnung eines Pakets zu einer Verbindung ist nicht möglich. Eine SPI-Firewall kann Informationen über Pakete abspeichern. Aufgrund dieser Informationen können weitere Pakete einer Verbindung zugeordnet werden. Dazu pflegt diese Art von Firewall einen Zustandsspeicher. Somit ist es möglich, dass die Firewall nach einer erlaubten Anfrage aus dem internen Netzwerk in das externe Netzwerk die Antwort auf die Anfrage ebenfalls erlauben kann. Eine SPI-Firewall wertet TCP-Sitzungen aus und analysiert die ausgetauschten Flags beim Verbindungsaufbau und -abbau. Durch diese Verbindungsauswertung kann die Zustandstabelle gefüllt werden. Wenn ein TCP-Segment zu einer aufgebauten Verbindung gehört, wird es auch erlaubt. Die Zugehörigkeit zu einer Verbindung kann z. B. durch die Auswertung der Sequenznummer des Segments in Verbindung mit der Quell- und Ziel-IP-Adresse vorgenommen werden.
Das Transmission Control Protocol (TCP) ist ein verbindungsorientiertes Protokoll. Vor dem Austausch von Nutzdaten wird eine Verbindung zwischen den Kommunikationspartnern aufgebaut. Während dieses Verbindungsaufbaus werden die Zählerstände für Sequenznummern und Quittierungsnummern ausgetauscht.



Die Grafik zeigt den Verbindungsaufbau (auch 3-Way-Handshake genannt) zwischen einem Client und einem Server. Der Client sendet ein TCP-Segment mit gesetztem SYN-Flag. Damit signalisiert er dem Server den Wunsch eine Verbindung aufzubauen. Der Server bestätigt diesen Wunsch mit einer Antwort mit gesetztem ACK-Flag. In dieser Antwort setzt er zusätzlich das SYN-Flag, um dem Client zu zeigen, dass auch er eine Verbindung aufbauen möchte. Der Client bestätigt diese Nachricht mit einem TCP-Segment mit gesetztem ACK-Flag.
Für den Verbindungsabbau sendet ein Kommunikationspartner ein TCP-Segment mit gesetztem FIN-Flag. Auch diese Nachricht muss bestätigt werden.
Eine SPI-Firewall wird auch zustandsbehafteter Paketfilter oder dynamischer Filter bzw. dynamische Firewall genannt.

Circuit-Level-Gateway
Ein Circuit-Level-Gateway arbeitet auf der vierten OSI-Schicht, der Transportschicht. Diese Firewall-Art hat die Aufgabe, Verbindungen zwischen Sender und Empfänger aufzutrennen. Wie ein Proxy-Server teilt es die TCP-Verbindung in zwei Verbindungen auf: eine Verbindung zwischen dem System im internen Netzwerk und der Firewall und eine Verbindung zwischen der Firewall und dem System im externen Netzwerk. Das bietet den Vorteil, dass die internen Systeme zusätzlich geschützt werden, da es keine direkte Verbindung (Ende-zu-Ende) zwischen internem und externem Netzwerk gibt. Zusätzlich können fragmentierte Pakete an der Firewall zusammengesetzt und untersucht werden. Eine Circuit-Level-Gateway-Firewall ist eine Erweiterung eines bestehenden Proxys um die Funktionalität einer Firewall.

Application-Layer-Gateway
Ein Application-Layer-Gateway (ALG) arbeitet, wie der Name es sagt, bis zur siebten OSI-Schicht – der Anwendungsschicht. Dadurch kann eine Application-Layer-Gateway-Firewall das komplette Paket inklusive der Inhalte auf der Anwendungsschicht analysieren.



Neben dem IP-Header und Header auf Schicht 4, dem TCP- oder UDP-Header, werden auch die höheren Schichten untersucht. Eine ALG-Firewall muss also mehr Daten einlesen und überprüfen als eine Paketfilter-Firewall. Dazu benötigt sie mehr Zeit und mehr Ressourcen, z. B. Speicherplatz und Rechenleistung.
Damit diese Art von Firewall ein Schicht-7-Protokoll und dessen Nutzdaten überprüfen kann, benötigt die Firewall Informationen über das zu filternde Protokoll.

```
▾ Session Initiation Protocol (INVITE)
 ▾ Request-Line: INVITE sip:user1@192.168.54.67 SIP/2.0
    Method: INVITE
   ▾ Request-URI: sip:user1@192.168.54.67
      Request-URI User Part: user1
      Request-URI Host Part: 192.168.54.67
```

Die Struktur und Arbeitsweise des zu filternden Protokolls müssen der Firewall vorliegen. Soll beispielsweise bei der Signalisierung eines VoIP-Telefonats mittels Session Initiation Protocol (SIP) ein bestimmter Empfänger, z. B. eine Telefonnummer, herausgefiltert werden, muss das Schema des SIP-Headers in der Firewall hinterlegt sein. Der Screenshot eines Mitschnitts eines SIP-Datenpakets zeigt, dass die Firewall z. B. Informationen darüber haben muss, dass der Empfänger in der Request-Line bzw. Request-URI hinterlegt ist, und welche Datenbytes diese Angaben repräsentieren.
Durch die Möglichkeit, auf Inhalte zu filtern, kann ein ALG z. B. als URL-Filter oder Content-Filter verwendet werden. Für einen URL-Filter werden die HTTP(S)-Requests nach dem Wert des Feldes „Host:" durchsucht. Bei der Verwendung als Content-Filter können die Pakete beispielsweise auf bestimmte Wörter geprüft werden.

Next-Generation-Firewall
Die Next-Generation-Firewall (NGFW) vereint im Gegensatz zur herkömmlichen Firewall mehrere Funktionen. Sie untersucht, genau wie ein ALG, Pakete und deren Inhalt, darüber hinaus ist oftmals ein IDS oder IPS integraler Bestandteil der Firewall. Die Firewall kann als Router arbeiten und bietet eine Network Address (Port) Translation an. Für eine Absicherung bezieht die Firewall nicht Informationen aus den angelegten Regeln, sondern kann z. B. mit der Virenschutzsoftware oder dem Netzwerk-Monitoring zusammenarbeiten.

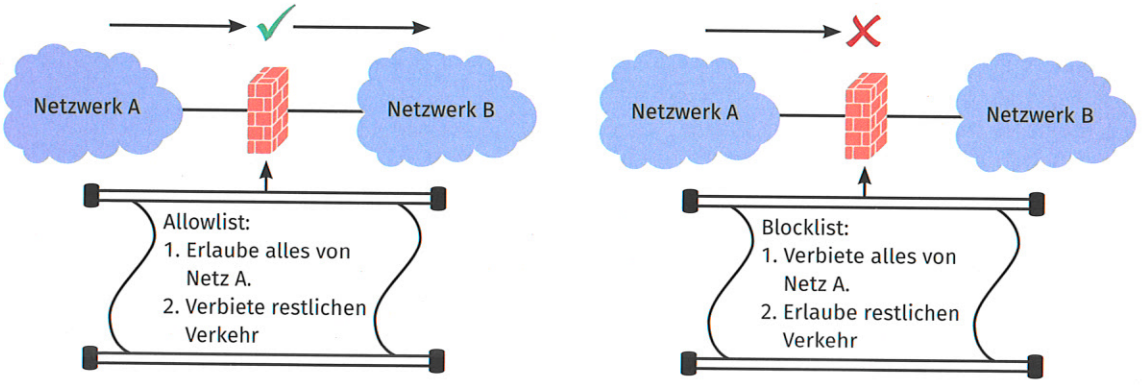
Nach der Planung der Architektur und der eingesetzten Firewall-Arten ist der nächste Schritt die Planung der Regeln einer Firewall. Die Gesamtheit der Regeln einer Firewall wird als Regelwerk bezeichnet. Das Regelwerk folgt einem von zwei möglichen Prinzipien.

Allowlist

Alles, was bei einer Allowlist (ehemals Whitelist) nicht explizit erlaubt ist, ist verboten.

Blocklist

Alles, was bei einer Blocklist (ehemals Blacklist) nicht explizit verboten ist, ist erlaubt.



Prinzip von Allowlist und Blocklist im Vergleich

Die Verwendung einer Allowlist ist für eine Firewall sinnvoll. Dazu werden nur die Verbindungen angegeben, die erlaubt sind, alle anderen Verbindungen werden verboten. Eine Blocklist wird beispielsweise beim Filtern von URLs eingesetzt. Alle nicht erwünschten URLs werden explizit angegeben, alle anderen URLs sind erlaubt. Das Prinzip einer Firewall wird durch die Standardregel („Default Policy") umgesetzt. Diese Default Policy ist eine Regel, die auf jedes Paket angewendet wird, für die es keine andere passende Regel gibt. Bei einer Allowlist werden diese Pakete verworfen.

Die Regeln im Regelwerk einer Firewall werden von oben nach unten abgearbeitet. Sobald eine Regel auf das zu untersuchende Paket passt, wird die Aktion der Regel angewendet und das Regelwerk verlassen. Alle weiteren Regeln werden für dieses Paket nicht mehr überprüft. Aus diesem Grund ist es wichtig, die Reihenfolge der Regeln zu beachten.

Das folgende Beispiel zeigt ein Regelwerk mit drei Regeln.

Nummer	Aktion	Protokoll	Ziel-IP	Quell-IP	Ziel-Port	Quell-Port
1	drop	IP	any	any	443	> 1023
2	allow	IP	144.155.166.177	10.0.0.99	443	> 1023
3	drop	any	any	any	any	any

Die erste Regel verbietet jeden IP-Verkehr mit dem Protokoll HTTPS (Port 443). Die zweite Regel erlaubt HTTPS-Verkehr von der IP-Adresse 10.0.0.99 zur IP-Adresse 144.155.166.177. In der dritten Regel wird jeglicher Verkehr verboten. Dies entspricht der Default-Policy für eine Allowlist.

Die zweite Regel wird in diesem Regelwerk niemals angewendet, da der auf die zweite Regel passende Verkehr schon durch die erste Regel behandelt bzw. verworfen und das Regelwerk anschließend verlassen wird.

Es kann sinnvoll sein, mit mehreren Regelwerken zu arbeiten. Das Regelwerk einer Firewall kann umfangreich sein, besonders wenn es für einzelne Protokolle viele erlaubte Ausnahmen gibt. Wenn alle Regeln aufgelistet sind, kann das Regelwerk unübersichtlich werden. Außerdem müssen gegebenenfalls viele

Regeln geprüft werden. Das benötigt Rechenzeit. Oftmals ist es bei einer Firewall möglich, die Regeln in mehrere Regelwerke zu gruppieren und nur bei Bedarf die jeweiligen Regeln zu prüfen.

Regelwerk ausgehender Verkehr	
1	wenn es sich um SSH-Verkehr handelt, springe in Regelwerk SSH
2	erlaube VoIP-Steuerverbindung
3	erlaube VoIP-Datenverkehr
4	verbiete jeden Verkehr

Regelwerk SSH	
1	erlaube Quell-IP 10.0.0.13
2	erlaube Quell-IP 10.0.0.14
3	erlaube Quell-IP 10.0.0.15
4	verbiete jeden Verkehr

Im nebenstehenden Beispiel wird im Standard-Regelwerk für den ausgehenden Verkehr geprüft, ob es sich um SSH-Verkehr handelt. Wenn das der Fall ist, wird in das Regelwerk „SSH" gesprungen und dort werden die Regeln überprüft. Handelt es sich nicht um SSH-Verkehr, müssen die dort hinterlegten Regeln nicht geprüft werden. Dieses Vorgehen spart Rechenzeit.

Bei der Planung der Regeln muss die richtige Aktion gewählt werden, die ausgeführt werden muss, wenn die Regel auf den Datenverkehr passt. Der Datenverkehr kann erlaubt oder verboten werden. Beim Verbieten von Datenverkehr gibt es zwei Möglichkeiten: Unerwünschter Datenverkehr aus dem externen Netzwerk sollte verworfen werden. Ein möglicher Angreifer soll nicht erfahren, dass die Anfragen durch eine Firewall gefiltert und verworfen wurden. Im Gegensatz dazu sollte bei der Ablehnung von unerwünschtem Datenverkehr aus dem internen Netzwerk der Anwender eine Rückmeldung erhalten, dass der Datenverkehr von der Firewall nicht erlaubt wurde. Er kann nun mit der zuständigen Stelle Kontakt aufnehmen und gegebenenfalls um eine andere Regelung für den Datenverkehr bitten.

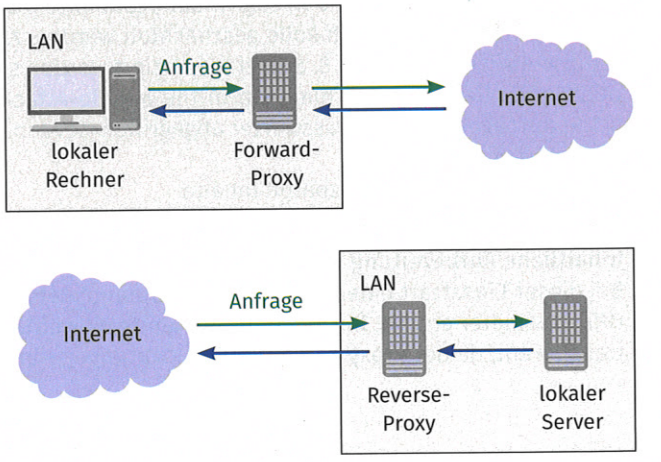
Wie für die meisten Dienste muss auch für eine Firewall die Protokollierung geplant werden. Alle relevanten Ereignisse, z. B. das Abweisen oder Verwerfen von Paketen, sollten protokolliert werden. Dazu müssen der Protokollierungsort, z. B. eine log-Datei oder ein log-Dienst, und die Menge der zu protokollierenden Daten festgelegt werden. Die Firewall muss vom firmeninternen Monitoring überwacht werden, um auf Systemfehler des Firewallsystems schnellstmöglich reagieren zu können (siehe auch Jahrgangsband 1, Lernfeld 3, Kapitel 3.8.3 und Jahrgangsband 2, Lernfeld 9, Kapitel 4.4.2)

(3) Proxy planen

Ein Proxy-Server (kurz: Proxy) kann als intelligenter NAT-Router verstanden werden. Ein NAT-Router reicht Anfragen vieler Clients aus einem lokalen/privaten Netz (LAN/PAN) in das öffentliche Netz (Internet) weiter. Die Antworten kann er anhand seiner NAT-Tabelle (Schicht 3 bis 4) wieder an den richtigen Client weiterleiten. Ein Proxy arbeitet ähnlich, allerdings mit dem Unterschied, dass dieser nicht nur Port und IP-Adressen beachtet, sondern auch die Protokollinhalte auf den höheren Schichten 5 bis 7.

Proxy

Ein Proxy ist ein „Stellvertreter-Server", der zwischen einem Endgerät und einem Dienst erbringenden Server geschaltet wird. Proxys werden darüber hinaus für weitere Dienste wie Datenkontrolle, Reduktion des Datentransfers, Protokollierung und Zugangsbeschränkung eingesetzt.



Einsatzgebiet Forward- und Reverse-Proxy

Im Normalfall arbeitet ein Proxy von innen (LAN) nach außen (Internet). Es werden also Anfragen der Clients aus dem lokalen Netz

über den Proxy stellvertretend an Server im Internet weitergeleitet. Ein solcher Proxy wird auch Forward-Proxy genannt. Meist wird aber nur von einem Proxy gesprochen.

Im Gegensatz dazu arbeitet ein Reverse-Proxy von außen nach innen und wird als Sicherheitskomponente vor lokale Server geschaltet. Da ein Proxy selbst keine Anwendungen bereitstellt, kann ein Reverse-Proxy unerwünschte Anfragen, wie sie durch einen DDoS-Angriff erfolgen, vom eigentlichen Anwendungsserver fernhalten.

Im Folgenden werden die weiteren Aufgabengebiete von Proxy-Servern vorgestellt. (Im Weiteren wird nur noch allgemein von Proxy gesprochen.)

Aufgabengebiete eines Proxys
Reduktion des Datentransfers Sofern der gesamte Traffic über einen Proxy geführt wird, kann dieser so konfiguriert werden, dass bereits angeforderte Dateien zwischengespeichert werden und bei nochmaliger Anforderung direkt vom Proxy statt aus dem Internet geliefert werden. Wenn also häufig dieselben Dateien heruntergeladen werden müssen, spart ein Proxy Übertragungskapazitäten auf der WAN-Schnittstelle. Ein mögliches Problem kann sein, dass sich die zwischengespeicherten Dateien häufig ändern und gegebenenfalls aus dem Cache eine ältere Version bereitgestellt wird. Vorteile: Reduktion der zu übertragenden Datenmenge Nachteile: Potenzielle Auslieferung veralteter Daten
Protokollierung des Datenverkehrs Da im Normalfall der gesamte Datenverkehr über den Proxy läuft, kann dieser sehr gut als Protokollierungswerkzeug eingesetzt werden. Hier sind auf jeden Fall Datenschutzrichtlinien einzuhalten. Es bedarf gegebenenfalls der Zustimmung des Datenschutzbeauftragten, wenn Verbindungsinformationen gespeichert werden sollen. Meist ist auch eine Anonymisierung notwendig.
Kontrolle des Datenverkehrs (Filterung) Da der Proxy alle ein- und ausgehenden Pakete filtert, kann er auch dazu eingesetzt werden, Clients in ihrer Übertragungsrate einzuschränken. Werden zu viele Daten gesendet, so werden auf dem Proxy oberhalb einer festgesetzten Übertragungsrate alle Pakete verworfen.
Zugangsbeschränkung im Sinne einer Application-Firewall Ein weiteres Einsatzgebiet für Proxys ist die Kontrolle des Datenverkehrs für bestimmte Protokolle. Man kann einen Proxy damit auch als Application-Firewall (vgl. AGL) verstehen. Das Filtern auf Applikationsebene ist relativ komplex, da hier nicht nur einfache Kriterien wie Port oder IP-Adressen zur Entscheidung herangezogen werden. Vielmehr wird innerhalb eines Protokolls höherer Schicht (z. B. HTTP) eine Entscheidung getroffen, ob die Pakete passieren dürfen oder nicht. Es gibt prinzipbedingt nicht für jedes Protokoll eine Proxy-Umsetzung. Dies wäre sehr aufwendig. Häufig wird in den Firmen ein Proxy dazu verwendet, den Zugriff auf bestimmte URLs zu unterbinden. Problematisch kann es werden, wenn diverse Protokolle geschachtelt werden, z. B. wenn eine HTTP-Anfrage über eine verschlüsselte-Verbindung (z. B. SSL) transportiert werden soll. Da der Proxy zwischen dem Client und dem Server liegt, könnten hier Man-in-the-Middle-Attacken (vgl. Jahrgangsband 1, Lernfeld 4, Kapitel 4.1.5) durchgeführt oder Passwörter abgegriffen werden. Um dies zu verhindern, sind gesonderte Maßnahmen vorzusehen. Vorteile: Kontrolle der nutzbaren Inhalte Nachteile: Probleme bei bestimmten Protokollen bzw. Schachtelung von Protokollen (z. B. HTTP über SSL)
Inhaltliche Aufbereitung der Daten Bei dieser Einsatzart eines Proxys werden Datenpakete inhaltlich geändert. Beispielsweise können URL-Parameter ersetzt, hinzugefügt oder entfernt werden. Für den Client geschieht das vollkommen transparent, da der Proxy dies für beide Richtungen durchführen kann.

Aufgabengebiete eines Proxys

Lastverteilung
Ein Proxy kann auch zur Lastverteilung (Load Balancing) eingesetzt werden. Wenn beispielsweise ein HTTP-Server nicht ausreicht, um alle eingehenden Anfragen abzuarbeiten, können weitere Server hinzugenommen werden. Um den Clients nicht unterschiedliche Ziele nennen zu müssen, wird ein Ziel genutzt (hier der Proxy). Dieser verteilt die eigentlichen Anfragen weiter an die HTTP-Server. Hier muss allerdings darauf geachtet werden, dass der Proxy über hinreichend Ressourcen verfügt, um die gesamte Anzahl an Anfragen verteilen zu können.

Gateway-Funktion
Wenn ein Proxy als Gateway eingesetzt wird, dann findet eine Übersetzung von einem Protokoll (z. B. HTTP) in ein anderes Protokoll (z. B. FTP) statt. Dies ist sehr aufwendig und bedarf in der Regel eines Spezial-Proxys. Ein Gateway ist allgemein eine Netzwerkkomponente, die Protokolle (z. B. HTTP zu FTP) oder auch Technologien (z. B. Ethernet zu Token Ring) konvertieren kann.

Für die Rigudo GmbH soll gemäß der Sicherheitsanalyse der Internetverkehr protokolliert werden. Darüber hinaus sollen kritische URLs gefiltert und blockiert bzw. mit einem Warnhinweis versehen werden.

Protokollierung des Datenverkehrs
Der Begriff „Protokollierung" ist sehr weit gefasst. Ein Proxy kann unterschiedliche Informationen protokollieren.

Protokollierungsarten eines Proxys

Protokollart	Erklärung
Zugriff	Anfragen auf z. B. Cache-Dateien, Server-Adressen oder administrativ
Ereignis	generelle Statusinformationen zum Proxy oder den Verbindungen
Fehler	auftretende Warnungen, Fehler und Störungen
Performance	Datendurchsatz (Schnittstellen), Speicherauslastung (Cache), Systemkomponenten (CPU/RAM)

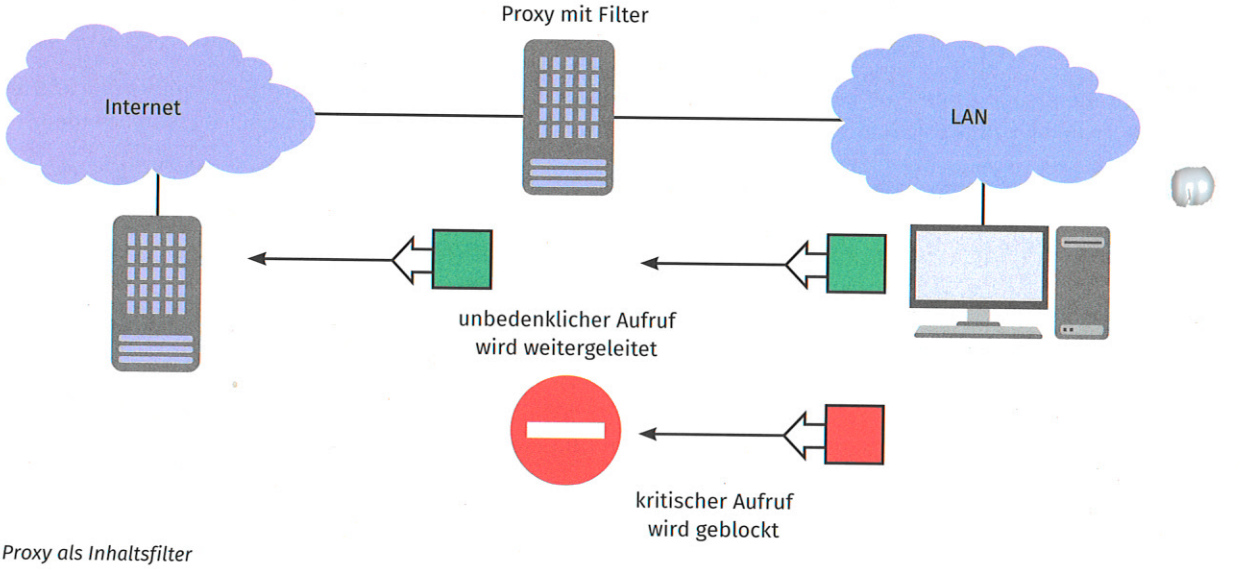
Bei der Protokollierung ist der Datenschutz der Mitarbeiter zu betrachten. Diese sind über die Art und den Umfang der Protokollierung zu informieren. Darüber hinaus muss die Verwendung der Protokolldaten an genau spezifizierte Zwecke gebunden sein. Der Zugriff auf die Protokolldaten muss geschützt sein und darf nur durch Mitarbeiter, die sich an die zuvor spezifizierten Zwecke halten, durchgeführt werden. Diese Maßnahmen sind organisatorisch zu verankern und durch entsprechende Unterweisungen zu kommunizieren. In größeren Unternehmen ist die Personalvertretung zu beteiligen. Die jeweils aktuell geltenden Datenschutzrichtlinien (vgl. DSGVO) sind dabei zu beachten. Eine Missachtung kann rechtliche Folgen haben.

Daher sollten diese Aspekte bereits in die Planung eines Protokollierungsdienstes einfließen. Die Zugriffsprotokolldaten können beispielsweise anonymisierte Hashwerte enthalten. Die Auflösung der Hashwerte in personenbezogenen Daten könnte dann durch Zugriffsbeschränkungen und Verschlüsselung der personenbezogenen Daten geschützt werden. Nur nach Eingabe von zwei Passwörtern (technischer Mitarbeiter und Personalvertretung) werden die Informationen lesbar (Vier-Augen-Prinzip).

Kommen mehrere Proxys zum Einsatz, dann ist der Speicherort der Protokolldaten zu betrachten. Diese können jeweils lokal auf dem jeweiligen Proxy abgelegt werden oder zentral auf einem eigenen Protokollserver. Bei einer zentralen Ablage ist zu betrachten, ob die Proxys aktiv jedes Ereignis an den zentralen Server melden. Dies hat eine erhöhte Netzauslastung zur Folge, aber liefert auch auf dem Protokollserver den jeweils aktuellen Status.

Alternativ können die Daten zunächst lokal auf den Proxys gespeichert und dann zu geplanten Zeitpunkten (z. B. nachts oder zu verkehrsschwachen Zeiten) an den zentralen Server übermittelt werden. Hier ist die Netzauslastung geringer. Allerdings ist der Stand auf dem Protokollserver nicht immer aktuell.

Zugangsbeschränkung im Sinne einer Application-Firewall
Ein Proxy ist in der Lage, bis in die Applikationsebene hinein Informationen zu analysieren und zu interpretieren. Ähnlich wie eine Application-Firewall kann ein Proxy nicht nur einzelne Pakete betrachten, sondern auch Bezüge zwischen Paketen herstellen. Darüber hinaus kann ein Proxy anders als eine reine Firewall auch Änderungen innerhalb der Pakete vornehmen, da er eine Stellvertreterfunktion hat. Auf diese Weise wird es möglich, bereits bei Aufruf kritische Begriffe oder Webseiten herauszufiltern. Der Proxy analysiert hierfür die Informationen des HTTP-Aufrufs (Schicht 5).



Proxy als Inhaltsfilter

Kompetenzcheck

1. Erklären Sie den Unterschied zwischen den Port-Typen „Access", „Trunk" und „Hybrid" im Zusammenhang mit VLAN in eigenen Worten.

2. Zählen Sie drei Firewall-Arten auf und beschreiben Sie die Unterschiede.

3. Geben Sie an, welche Server in der DMZ platziert werden müssen.
   a) E-Mail-Server für die Kommunikation mit dem Kunden
   b) Interner Dateiserver mit Versionierung
   c) Webserver mit der Internetpräsenz des Unternehmens
   d) Interner Webserver mit verschiedenen Anträgen und Formularen
   e) HTTPS-Proxy
   f) SIP-Proxy für die VoIP-Telefonie

4. Nennen Sie die Aufgaben eines Proxy-Servers.

5. Notieren Sie wesentliche Aspekte aus diesem Abschnitt in Ihrem Projektjournal.

6. Bearbeiten Sie Aufgabe 2 der Lernsituation 3 im Arbeitsbuch.

A2

3.3.3 Zugriffsmöglichkeit auf vernetzte Systeme am Internet-Anschluss planen

S **Sie sollen den sicheren Zugriff auf vernetzte Systeme am Internet-Anschluss mit ausgewählten Techniken planen.**

(1) Einsatz der Network Address Translation planen

IMEI (SIM-Steckplatz 2)
6122180110228276

IP-Adresse
10.161.116.47
2a02:3035:408a:1234::c3a2:4711

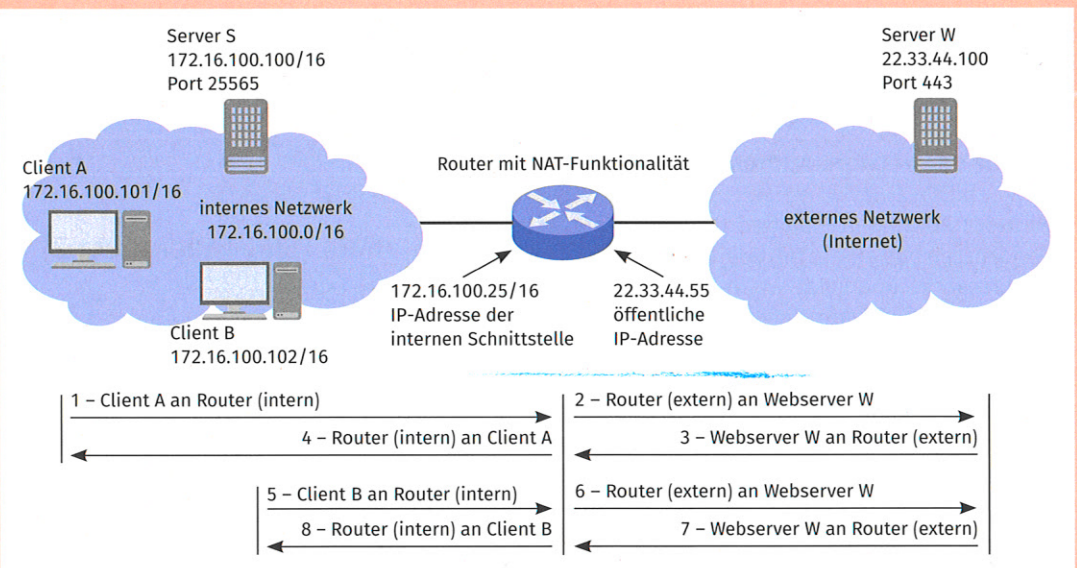
Die Network Address Translation (NAT) ist eine Technik, bei der IP-Adressen aus einem Netzwerk in IP-Adressen eines anderen Netzwerks übersetzt werden. Das eine Netzwerk ist meist das interne, private Netzwerk und verwendet IPv4-Adressen aus dem privaten IP-Adressraum, während das andere Netzwerk meist das öffentliche Netzwerk (Internet) ist. Bei vielen Anschlüssen im SoHo-Bereich (Small Office, Home Office) kommt die NAT-Technik zum Einsatz. Auch beim Anbinden von Mobilfunkgeräten, z. B. Smartphones, an das Internet durch den Mobilfunkbetreiber kann NAT verwendet werden. In der nebenstehenden Abbildung wird eine private IPv4-Adresse aus dem IP-Adressbereich 10.0.0.0/8 gezeigt, die dem Endgerät durch den Mobilfunkprovider zugewiesen wurde.

Das BSI beschreibt die NAT-Technik nicht als Maßnahme zur Erhöhung der Sicherheit der IT-Infrastruktur, trotzdem kommt sie in vielen Netzen zum Einsatz. Mit der NAT-Technik lässt sich die Struktur eines internen Netzwerks verschleiern. Ein Angreifer kennt nur die externe IP-Adresse des Netzwerks. Die Verwendung von NAT bietet, neben der Entkopplung der intern verwendeten IP-Adressen, auch den Vorteil, dass die Verschwendung von IPv4-Adressen reduziert wird. Im internen Netzwerk können IP-Adressen aus dem privaten Bereich verwendet werden. Private IP-Adressen werden im öffentlichen Netzwerk nicht geroutet, deshalb werden die internen Adressen in eine (oder mehrere) öffentliche IPv4-Adressen umgesetzt. Die internen Adressen treten öffentlich nicht in Erscheinung und können somit in einer Vielzahl von internen Netzwerken verwendet werden.

Network Address Port Translation (NAPT)

Beim Einsatz der NAT-Technik werden in den meisten Fällen nicht nur IP-Adressen ersetzt, sondern auch die TCP-Ports. Dieses Verfahren wird **Network Address Port Translation (NAPT)** oder **Port Address Translation (PAT)** genannt.

Die Übersetzung der Ports ist wichtig, damit mehrere Systeme aus dem internen Netzwerk mit der gleichen IP-Adresse im öffentlichen Netzwerk kommunizieren können. Die Netzwerkskizze zeigt ein internes Netzwerk mit zwei Endsystemen und einem Server. Die beiden Endsysteme sollen im internen Netzwerk auf den Webserver W zugreifen. Dieser erwartet auf dem Port 443 (HTTPS) eingehende Verbindungen. Der Server S im internen Netzwerk soll aus dem externen Netzwerk erreicht werden. Der interne Server erwartet auf Port 25565 eingehende Verbindungen.



Beide Endsysteme (Client A und Client B) sollen mit dem Webserver W kommunizieren. Dabei haben beide Systeme die gleiche öffentliche IP-Adresse. Wenn nun der Webserver W auf eine Anfrage der Clients antwortet, kann die Antwort ohne Port nicht eindeutig einer Verbindung zugewiesen werden. In der folgenden Tabelle werden die Nachrichten auf den jeweiligen Teilstrecken dargestellt.
Annahmen: Client A wählt als Quell-Port 50001 und Client B wählt ebenfalls Quell-Port 50001.

Nr.	Ziel-IP-Adresse	Quell-IP-Adresse	Ziel-Port	Quell-Port
1	22.33.44.100	172.16.100.101	443	50001
2	22.33.44.100	22.33.44.55	443	50001
3	22.33.44.55	22.33.44.100	50001	443
4	172.16.100.101	22.33.44.100	50001	443
5	22.33.44.100	172.16.100.102	443	50001
6	22.33.44.100	22.33.44.55	443	50002 **
7	22.33.44.55	22.33.44.100	50002	443
8	172.16.100.102	22.33.44.100	50001	443

Beide Clients haben sich in diesem Beispiel für denselben Quell-Port (aus dem Bereich der dynamischen Ports) entschieden. Bei der Umsetzung der IP-Adressen und der Ports ist es wichtig, dass die Kombination aus beiden Werten (sogenannter Socket) eindeutig ist. Deshalb wird beim NAT-Vorgang der Verbindung des zweiten Clients der Port geändert (gekennzeichnet durch **).
Der NAT-Router benötigt eine Zuweisungstabelle. Diese enthält die Zuordnung zwischen internem Socket und externem Socket. Dadurch kann der NAT-Vorgang durchgeführt und die IP-Adressen können umgeschrieben werden.

intern	extern
172.16.100.101:50001	22.33.44.55:50001
172.16.100.102:50001	22.33.44.55:50002

Das vorangegangene Beispiel verwendet die Methode **Source-NAT (SNAT)**, bei der die Quell-IP-Adresse ersetzt wird.

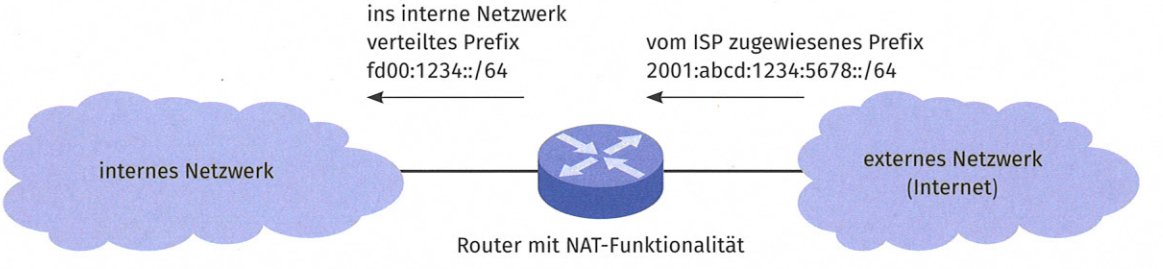
Damit der Server S im internen Netzwerk aus dem externen Netzwerk erreicht werden kann, ist es nötig, eine Port-Weiterleitung im NAT-Router einzugeben. Durch die Port-Weiterleitung kann der Router ankommende Daten dem richtigen internen Ziel zuordnen. Die Port-Weiterleitung ist ein manuell angelegter Eintrag in der NAT-Tabelle des Routers. Hierbei wird die Ziel-IP-Adresse eines IP-Pakets aus dem externen Netz ersetzt. Diese Verfahren wird **Destination-NAT (DNAT)** genannt. Die folgende NAT-Tabelle ist erweitert, sodass alle Datenpakete aus dem externen Netzwerk mit dem Ziel-Port 25565 an den Server S weitergeleitet werden.

intern	extern
172.16.100.101:50001	22.33.44.55:50001
172.16.100.102:50001	22.33.44.55:50002
172.16.100.100:25565	22.33.44.55:25565

Bei der Planung des NAT-Einsatzes gibt es verschiedene Aspekte zu beachten. Das Adressierungsschema, sowohl intern als auch extern, ist meist schon festgelegt. Für den NAT-Vorgang ist es aber wichtig zu planen, welche und wie viele externe bzw. öffentliche IP-Adressen zur Verfügung stehen. In großen Unternehmen können oftmals mehrere öffentliche IP-Adressen verwendet werden. Dann müssen die internen Adressen nicht auf eine externe Adresse umgesetzt werden, sondern die Kommunikation kann auf mehrere öffentliche IP-Adressen verteilt werden. Im SoHo-Einsatz ist die Schnittstelle zum Internet, das WAN-Interface, in den allermeisten Fällen vorgegeben. Beim Einsatz im Unternehmen kann es aber nötig sein, die passende Schnittstelle für das NAT festzulegen. Idealerweise wird eine Schnittstelle gewählt, die ständig erreichbar ist. Beim Einsatz der NAT-Technik muss die Zusammenarbeit mit der Firewall beachtet werden, damit ein sinnvolles Zusammenspiel möglich ist. Die Regeln der Firewall müssen an den NAT-Vorgang angepasst werden. Neben der Anpassung der Firewall muss auch definiert werden, welche Berechtigungen der NAT-Server haben darf.

Die Verwendung des NAT-Verfahrens hat einige **Nachteile**. Beim IP-Protokoll hat im Normalfall jedes System im Netzwerk eine IP-Adresse. Durch diese IP-Adresse ist das System erreichbar. Bei der Network Address Translation werden mehrere Systeme durch eine IP-Adresse repräsentiert. Das VPN-Protokoll IPsec hat beispielsweise Probleme im Zusammenspiel mit NAT. Während des NAT-Vorgangs wird der IP-Header verändert, da IP-Adressen ersetzt werden. Wenn durch IPsec über den IP-Header eine Prüfsumme gebildet wurde, stimmt diese nach dem NAT-Vorgang nicht mehr. Authentifizierte Pakete werden dann als verfälscht verworfen. Auch andere Protokolle, z. B. SIP, SMTP oder SNMP, haben Probleme mit der Umsetzung von IP-Adressen und Ports.

Durch eine Einführung von **IPv6** wird NAT bei vielen Anwendungsszenarien zunächst überflüssig. Durch den riesigen Adressraum ist es nicht nötig, Adressen zu sparen. Jedem System im Netzwerk kann eine eigene IPv6-Adresse zugewiesen werden. Dadurch fallen die durch NAT entstandenen Probleme weg. NAT kann aber weiterhin zum Einsatz kommen. Beispielsweise kann die interne Infrastruktur mit lokalen IPv6-Adressen (Unique Local Unicast Address – fc00::/7) betrieben werden. Am Netzübergang kommt nun ein NAT-Verfahren zum Einsatz.



NAT im IPv6-Netz

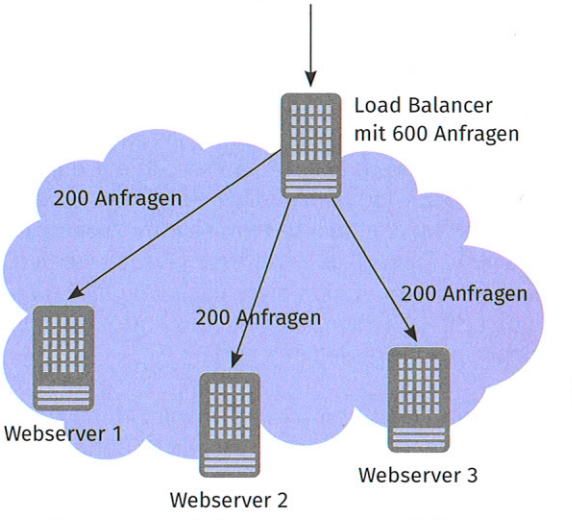
Im abgebildeten Netzwerk weist der Provider (ISP) dem Unternehmen das Präfix 2001:abcd:1234:5678::/64 zu. Das Unternehmen verwendet dieses Präfix für die Bildung einer öffentlichen IPv6-Adresse. Intern wird das Präfix nicht weitergegeben, sondern es werden IPv6-Adressen aus dem privaten Adressraum fd00:1234::/64 verwendet. Wenn das Unternehmen den Provider wechselt, muss an der internen Infrastruktur keine Änderung vorgenommen werden. Dadurch ist die interne Adressierung unabhängig vom IPv6-Präfix des Providers. Außerdem ist ein Mischbetrieb möglich. Die interne IT-Infrastruktur wird weiterhin mit IPv4 betrieben, nach außen wird mit einer öffentlichen IPv6-Adresse (Unique Glocal Unicast Address – 2000::/3) gearbeitet.

(2) Load Balancing als Sicherheitsaspekt planen

Das BSI führt das Element „Load Balancer", sowohl für die Software- als auch für die Hardware-Lösung, nicht als eigenen Baustein. Allerdings gibt es einen benutzerdefinierten Baustein (NET.bd.1). Dieser gibt, herstellerunabhängig, Hilfestellung für die Schutzbedarfsfeststellung, Maßnahmenplanung und -umsetzung. Die Aufgabe eines Load Balancers ist es, Anfragen an angeschlossene Systeme zu verteilen. Dazu ist es nötig, im Vorhinein abzuschätzen, wie viel Datenverkehr über den Load Balancer weitergeleitet wird. Dadurch lässt sich das Gerät ausreichend dimensioniert beschaffen.

Bei der Planung eines Load Balancers müssen die IP-Adressen, Portnummern und gegebenenfalls Dienstpfade zu den angeschlossenen Systemen vorliegen. Diese Parameter werden für die Konfiguration eines Load Balancers benötigt. Neben den oben genannten Konfigurationsparametern ist es sinnvoll, sich auf eine Verarbeitungsstrategie festzulegen (siehe auch Jahrgangsband 1, Lernfeld 4, Kapitel 4.1.3). Besonders in Umgebungen, in der bei einer hohen Auslastung weitere Server mit Diensten bereitgestellt werden können, ist z. B. das einfache Round-Robin-Prinzip nicht die ideale Wahl.

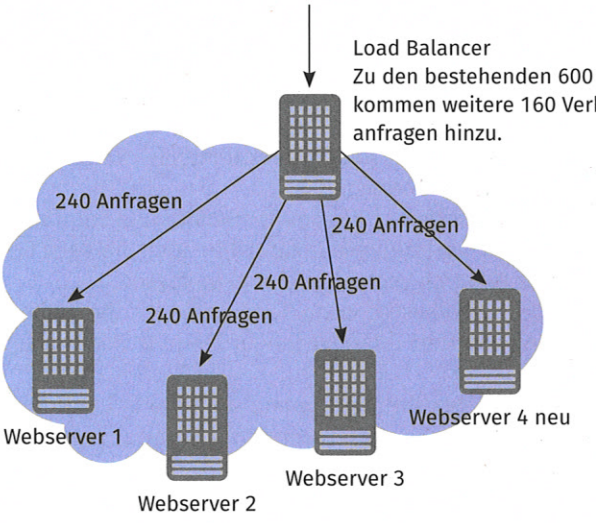
Beispiel: Die Abbildung zeigt einen Load Balancer, der eingehende Verbindungsanfragen gleichmäßig auf drei Server verteilt. Durch das Round-Robin-Verfahren wird die erste Anfrage an Webserver 1 weitergeleitet, die zweite Anfrage an den Webserver 2, die dritte Anfrage an den Webserver 3. Die vierte Anfrage bekommt wieder Webserver 1 usw. In einem Netzwerk, in dem nur die drei Webserver zum Bearbeiten von Anfragen zur Verfügung stehen, kann das Round-Robin-Verfahren zu einer fairen Verteilung der Last führen. Im Beispiel bekommt jeder Webserver 200 Anfragen zugewiesen.



Verteilung von Verbindungsanfragen auf drei Webserver durch einen Load Balancer

Wenn es in dieser Netzwerkumgebung dazu kommt, dass sehr viele Anfragen an die Webserver gestellt werden, ist es möglich, weitere Webserver in das Netzwerk zu integrieren, um eine Überlast des Webdienstes zu vermeiden. Bei der Verwendung des Round-Robin-Verfahrens würden weitere Verbindungen gleichmäßig auf alle Webserver verteilt werden. Die neuen Webserver werden dadurch nicht sinnvoll ausgelastet.

Im Beispiel wurde ein weiterer Webserver hinzugefügt. Unter der Annahme, dass zusätzliche 160 Verbindungen aufgebaut werden, verteilt der Load Balancer je 40 Verbindungen zusätzlich an alle Webserver. Wenn statt „Round Robin" beispielsweise „Least Connection" verwendet werden würde, würden die neuen Verbindungen alle dem neuen Webserver 4 zugewiesen werden, bis dieser eine ähnliche Auslastung wie die Webserver 1 bis 3 hat. Die Last wäre gleichmäßig verteilt.

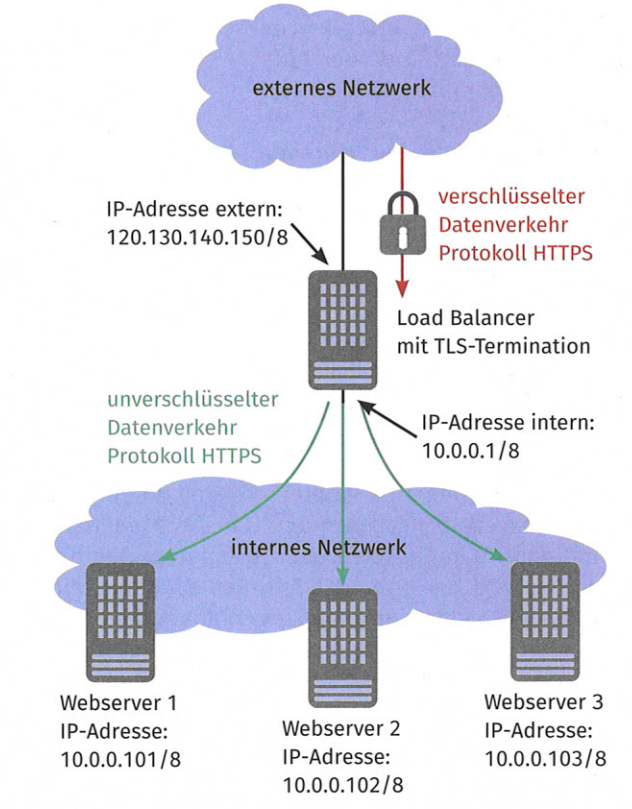


Integration eines weiteren Webservers

Im benutzerdefinierten Baustein des BSI wird zusätzlich eine Protokollierung vorgeschrieben. Eine Protokollierung ist immer an eine synchronisierte Zeit gebunden. Der Abgleich mit einem Zeitserver, intern oder extern, ist dazu sinnvoll. Ein weiteres zu planendes Verfahren ist das „SSL Offloading".

SSL-Offloading/TLS-Termination

Der Datenverkehr bei HTTPS ist verschlüsselt. Die Entschlüsselung des Datenverkehrs benötigt Zeit und erfordert Ressourcen. Bei ausgelasteten Webservern kann es sinnvoll sein, diese zusätzliche Arbeit auszulagern. Durch SSL-Offloading, auch TLS-Termination genannt, kann der Prozess der Ver- und Entschlüsselung vom Webserver auf ein anderes Gerät, z. B. den Load Balancer oder auch den Proxy, verschoben werden. Ein weiterer Vorteil dieser Technik ist, dass die unverschlüsselten Daten z. B. durch eine Firewall untersucht werden können.



(3) VPN planen

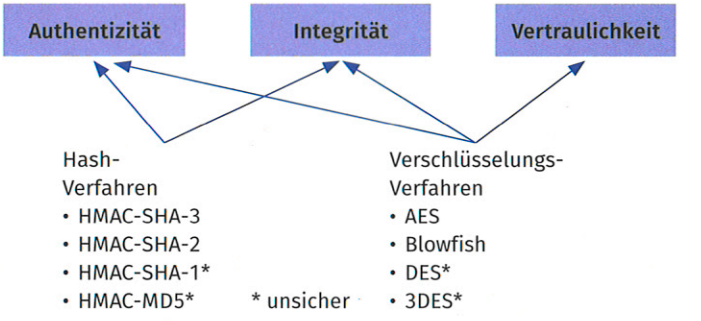
VPN-Tunnel

Ein VPN-Tunnel transportiert Daten über öffentliche Netze und kann dabei Vertraulichkeit, Integrität und Authentizität gewährleisten.
Die **Vertraulichkeit** verhindert, dass außer Sender und Empfänger Dritte die übertragenen Informationen lesen können. Vertraulichkeit kann hier auch die Verschleierung der eigentlichen Kommunikationspartner (z. B. durch Verschlüsselung) umfassen.
Die **Integrität** ist gewährleistet, wenn der Empfänger überprüfen kann, ob die Daten vom ursprünglichen Sender unverändert übertragen wurden (z. B. mit kryptografischen Hash-/Prüfsummenverfahren).
Die **Authentizität** ist gewährleistet, wenn die beteiligten Kommunikationspartner die Korrektheit der jeweiligen Identität überprüfen können (z. B. mit digitalen Signaturen).

Sowohl Verschlüsselung wie auch kryptografische Hash-Funktionen arbeiten mit Schlüsseln, die nur den Kommunikationspartnern zur Verfügung stehen. Die Sicherheit hängt vom eingesetzten Verfahren und der Länge der Schlüssel ab. Darüber hinaus ist ein regelmäßiger Wechsel der Schlüssel sinnvoll.

Würde ein Schlüssel einmal festgelegt und dann unverändert bleiben, so wäre für Angreifer die Möglichkeit gegeben, den Schlüssel durch zeitlich nahezu unbegrenztes Probieren (Brute Force) zu erraten.

Wird der Schlüssel hingegen täglich oder sogar stündlich gewechselt, wird die Zeitspanne für eine Brute-Force-Attacke stark reduziert bzw. der Aufwand für Angreifer durch Einsatz von leistungsfähiger Hardware erhöht. Ist der finanzielle Aufwand für Angreifer deutlich höher als der zu erwartende Gewinn, wird die Wahrscheinlichkeit für einen Angriff reduziert und ein System kann als sicher betrachtet werden.



VPN allgemein

Im IPsec-Protokoll wird die Sicherheit über das Unterprotokoll Encapsulation Security Payload (ESP) bzw. Authentication Header (AH) realisiert. IPsec wurde ursprünglich in RFC 2401 im Rahmen der Standardisierung von IPv6 vorgeschlagen. Da die Verbreitung von IPv6 allerdings nur schleppend vorankam, wurde es später ebenfalls in IPv4 integriert.

IPsec enthält neben den drei Hauptmerkmalen für einen VPN-Tunnel weitere Sicherheitsmechanismen. Um die Wiederholung von mitgeschnittenen Datenpaketen, z. B. für spätere Angriffszwecke, zu verhindern, wird bei IPsec der Anti-Replay-Schutz eingesetzt. Dabei werden die Pakete sinngemäß durchnummeriert und nur Pakete, die innerhalb eines aktuell gültigen Nummernbereichs liegen, werden weiterverarbeitet. Damit können Pakete aus einer früheren Übertragung direkt erkannt und bereits frühzeitig verworfen werden.



Realisierung von Sicherheit in IPsec

Diffie-Hellman-Verfahren (DH-Verfahren)
Bei einer sicheren Verbindung besteht das Grundproblem, die Schlüssel sicher bei beiden Kommunikationspartnern zu platzieren. Eine direkte Übertragung über eine ungesicherte Verbindung könnte von einem Angreifer ausgenutzt werden.

Das Diffie-Hellman-Verfahren ist ein sicherer Weg, um einen symmetrischen Schlüssel durch Generierung beiden Kommunikationspartnern zur Verfügung zu stellen. Das Verfahren nutzt hierfür den Modulo-Operator als sehr einfachen, aber dennoch sicheren „Falltür"-Algorithmus. Der Modulo-Operator berechnet den Rest einer Division.

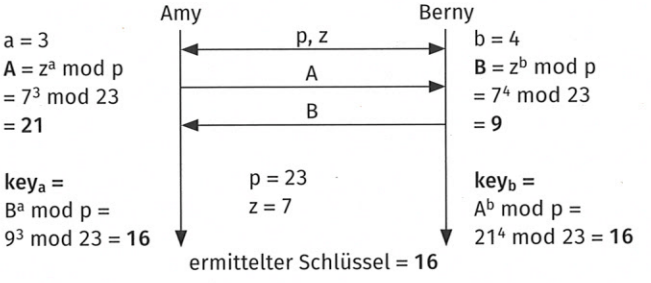
Beispiel: 17 mod 5 = 2
Die Falltür besteht darin, dass aus dem Ergebnis 2 nicht auf die Zahl 17 zurückgeschlossen werden kann. In diesem einfachen Beispiel ist die Menge der möglichen Ergebnisse wegen des sehr kleinen Divisors 5 allerdings sehr klein (0 bis 4). Das DH-Verfahren nutzt daher zur Erhöhung der Sicherheit sehr große Primzahlen (z. B. 2048-Bit) als Divisor, sodass die mögliche Menge der Ergebnisse sehr groß wird.

Für die Generierung des Schlüssels werden eine Primzahl p und eine Zufallszahl z als sogenannte modp-Gruppe definiert. Beide Kommunikationspartner wählen zusätzlich eine persönliche und geheime Zufallszahl a bzw. b.

Rechenbeispiel für DH-Verfahren	
Wert	**Beschreibung**
$p = 23$	vorab festgelegte Primzahl (modp-Gruppe)
$z = 7$	vorab festgelegte Zufallszahl (modp-Gruppe)
$a = 3$	geheime Zufallszahl Amy
$b = 4$	geheime Zufallszahl Berny
$A = z^a \bmod p = 7^3 \bmod 23 = 21$	öffentlicher Wert von Amy, der an Berny übermittelt wird
$B = z^b \bmod p = 7^4 \bmod 23 = 9$	öffentlicher Wert von Berny, der an Amy übermittelt wird
$key_a = B^a \bmod p = 9^3 \bmod 23 = 16$	geheimer Schlüssel von Amy mittels B errechnet
$key_b = A^b \bmod p = 21^4 \bmod 23 = 16$	geheimer Schlüssel von Berny mittels A errechnet

Beispiel: Beide Partner berechnen nun jeweils einen Modulo-Wert $A = z^a \bmod p$ bzw. $B = z^b \bmod p$. Da diese Restwerte keinen Rückschluss auf die geheimen Zufallszahlen ermöglichen, können sie über die unsichere Strecke transportiert werden.

Mit der zweiten Modulo-Rechnung $Key = B^a \bmod p$ bzw. $Key = A^b \bmod p$ wird der eigentliche Schlüssel berechnet.

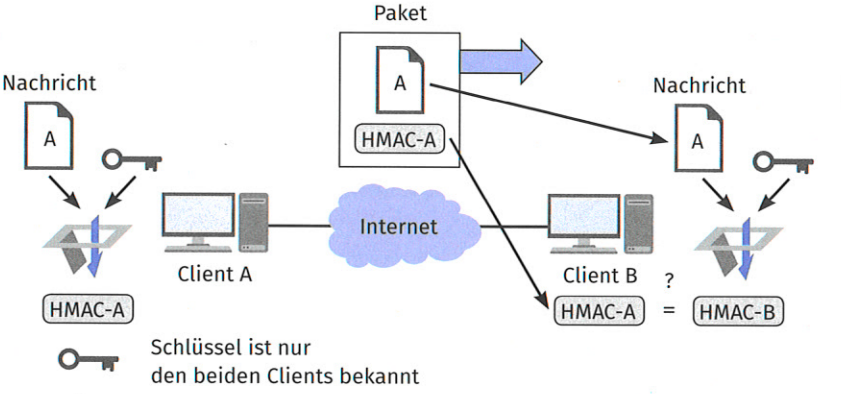


Das DH-Verfahren gilt als sicher (seit 1977). Nur durch einen Man-in-the-Middle-Angriff könnte der Schlüssel in unbefugte Hände gelangen. Das DH-Verfahren wird bei IPsec, SSH und TLS eingesetzt.

Verschlüsselungsverfahren	
Verfahren	**Bemerkung**
AES-128/AES-256	128/256-Bit-Blockcode; auch als „Rijndael" bezeichnet; muss von allen IPsec-Geräten unterstützt werden; RFC 3602
Blowfish	64-Bit-Blockcode; 32-448 Bit Schlüssellänge; gilt als sicher (bis auf „Geburtstagsangriff")
RC6	Ron Rivest Code; gilt als sicher; wird nicht von allen IPsec-Geräten unterstützt
DES	Data Encryption Standard; gilt als unsicher und sollte nicht mehr eingesetzt werden
3DES	Triple DES; gilt ebenfalls als unsicher und sollte nicht mehr eingesetzt werden

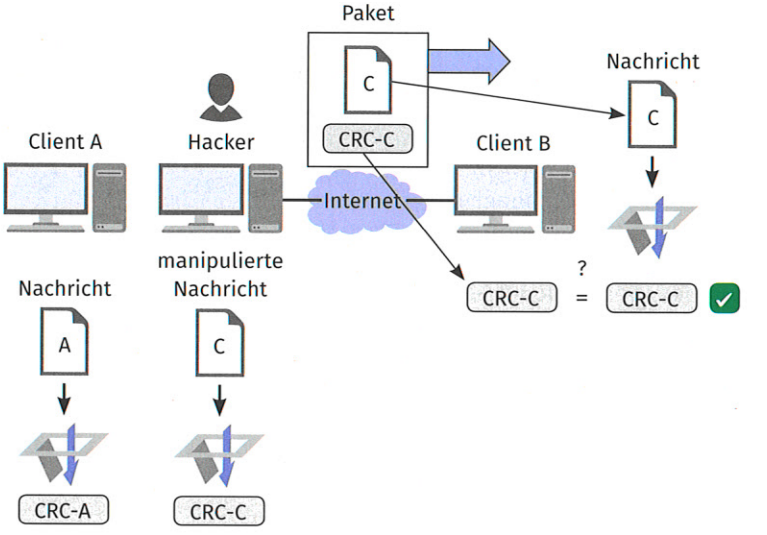
Kryptografische Prüfsummenverfahren

Prüfsummenverfahren (Hash-Verfahren) sind mit oder ohne Kryptografie verfügbar. Kryptografische Hash-Verfahren werden auch als Hash-based Message Authentication Code (HMAC) bezeichnet. Im Gegensatz zu nicht kryptografischen Hash-Verfahren (z. B. CRC) wird durch Verwendung eines gemeinsamen Schlüssels sichergestellt, dass überprüfbare Prüfsummen nur von den Kommunikationspartnern berechnet werden können. Eine Änderung der zu übermittelnden Daten ist durch einen Angreifer ohne diesen Schlüssel somit nicht mehr möglich.



Sichere Übertragung durch Einsatz eines kryptografischen Prüfsummenverfahrens

Würde ein einfaches CRC-Verfahren wie beim Ethernet-Rahmen (CRC-32) eingesetzt, so könnte ein Angreifer die Originalnachricht verändern und für die manipulierte Nachricht eine neue gültige Prüfsumme generieren. Der Empfänger wäre somit nicht mehr in der Lage, die Nachricht auf Integrität zu überprüfen.



Beispiel für einen erfolgreichen Angriff auf ein einfaches Prüfsummenverfahren wie CRC

Ein kryptografisches Prüfsummenverfahren generiert aus einer Informationsfolge und einem Schlüssel eine Prüfsumme, den sogenannten Hash-Wert.
Ein kryptografisches Prüfsummenverfahren muss folgende Kriterien erfüllen:

- **Fixe Hash-Wertlänge:** Sie verarbeitet eine beliebig lange Informationsfolge (Bits) und generiert daraus eine Prüfsumme (Hash-Wert) mit fester Länge.
- **Kollisionsfreiheit:** Es dürfen keine unterschiedlichen Informationsfolgen zu einer identischen Prüfsumme führen.
- **„Falltür"-Funktion:** Aus der Prüfsumme darf kein Rückschluss auf die zugrunde liegende Informationsfolge möglich sein (keine Möglichkeit der Rückrechnung).

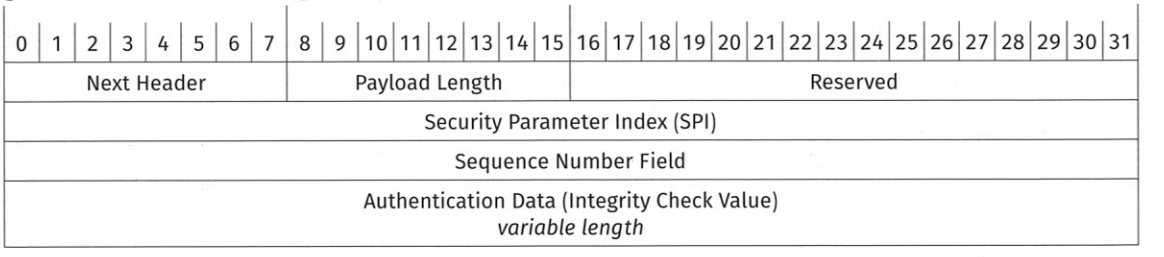
Kryptografische Hash-/Prüfsummenverfahren	
Verfahren	**Bemerkung**
HMAC-SHA-1	Secure Hash Algorithm; gilt als unsicher; wurde bei SSL, IPsec und S/MIME eingesetzt
HMAC-SHA-2	gilt grundsätzlich als sicher; arbeitet mit Hash-Längen von 224, 256, 384 und 512 Bit; SHA-224 wird als einziges SHA-2-Verfahren nicht mehr empfohlen
HMAC-SHA-3	gilt als sicher; Keccak-Verfahren wurde 2012 von NIST als SHA-3 zum Nachfolger für SHA-1 und SHA-2 gewählt
HMAC-MD5	gilt als unsicher; es existieren erfolgreiche Angriffe auf die Kollisionsfreiheit

Die möglichen IPsec-Protokollheader für ESP bzw. AH sehen wie folgt aus.

Authentication Header (AH)
Der AH ist für die folgenden Sicherheitskriterien zuständig:

- Authentifizierung der Datenquelle:
  Ist der Absender der korrekte Absender? Echtheit des Absenders
- Datenintegrität:
  Schutz gegen gezielte Verfälschung der Daten
- Anti-Replay Schutz:
  Schutz gegen das Ausspähen des Zielrechners mittels abgefangener Daten

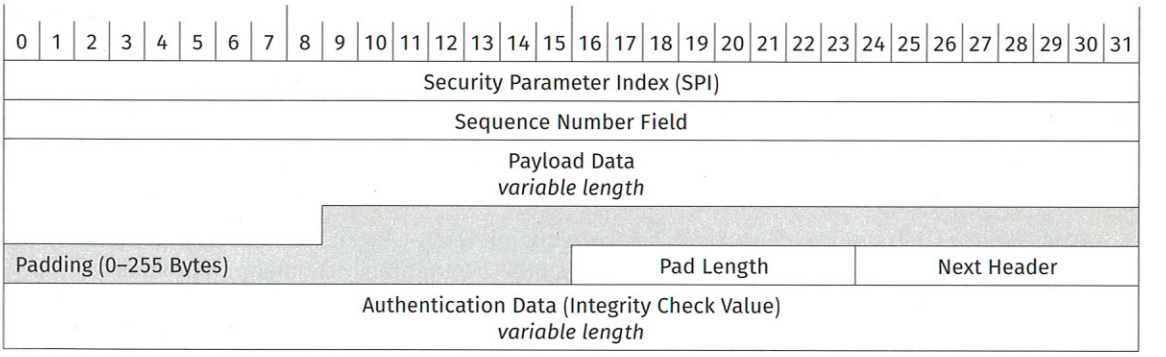
Wichtig: Die Vertraulichkeit wird aufgrund der fehlenden Verschlüsselung nicht gewährleistet. Erst mit ESP wird diese hergestellt. Das heißt, die Daten sind beim Einsatz von AH zwar gegen Manipulationen geschützt, können aber eingesehen werden.



Aufbau des Authentication Headers von IPsec	
Next Header	Header des nachfolgenden Protokolls, welches nach dem AH im IP-Paket folgt
Payload Length	Länge des AH (minus 2 in 32-Bit-Worten)
SPI	Referenz auf die SA in der SAD-Datenbank des Zielrechners
Sequence Number	zur „Durchnummerierung" der IP-Pakete (Anti-Replay-Schutz)
Authentication Data	kryptografische Prüfsumme, die mit geheimen Schlüsseln berechnet wird

Encapsulation Security Payload (ESP)
Der ESP besteht aus zwei Komponenten: Einem Header und einem Trailer (Anhang). Über den ESP werden die folgenden Sicherheitskriterien realisiert:

- Vertraulichkeit: Schutz vor Einsichtnahme in Daten durch Dritte
- Authentifizierung: wie AH
- Datenintegrität: wie AH
- Anti-Replay-Schutz: wie AH

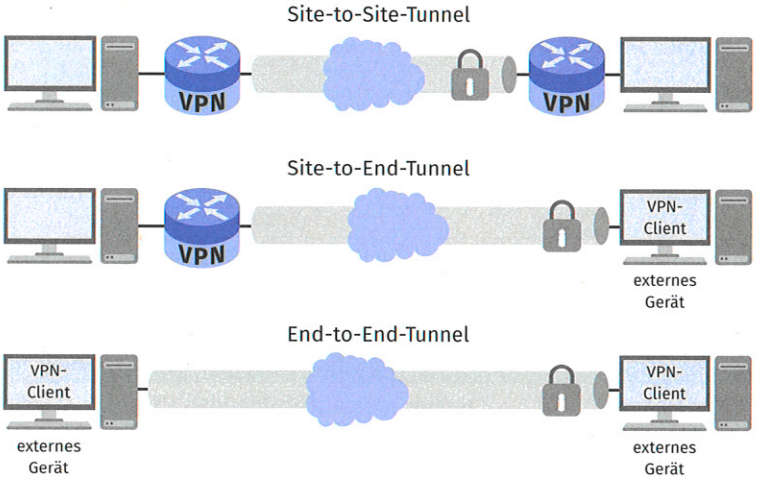


Aufbau des ESP-Headers von IPsec	
Payload Data	im Transport-Modus: Inhalt des eingebetteten IP-Paketes (ohne IP-Header) im Tunnel-Modus: das ganze IP-Paket
Padding	Fülldaten werden gegebenenfalls für Blockcodes mit fester Länge benötigt
Pad Length	Länge des Padding-Feldes

Die anderen Felder haben dieselbe Bedeutung wie im Authentication Header.

VPN-Verbindungen können in drei Grundstrukturen unterteilt werden (siehe auch Jahrgangsband 1, Lernfeld 3, Kapitel 3.2.2).

Site-to-Site planen
Die Rigudo GmbH plant, einen zweiten Standort zu eröffnen. Die Zweigstelle soll an das AD und den E-Mail-Server in der Zentrale angebunden werden. Zur Absicherung soll hier ebenfalls ein VPN-Tunnel zum Einsatz kommen. Damit die Kommunikation über den VPN-Tunnel funktioniert, müssen die IP-Adressbereiche in der Zweigstelle und der Zentrale unterschiedlich sein. Würde mit demselben IP-Netz gearbeitet werden, so würden die Clients jeweils im eigenen lokalen Netz die Zieladresse per ARP bzw. NDP suchen. Die VPN-Verbindung würde demnach nicht genutzt werden.



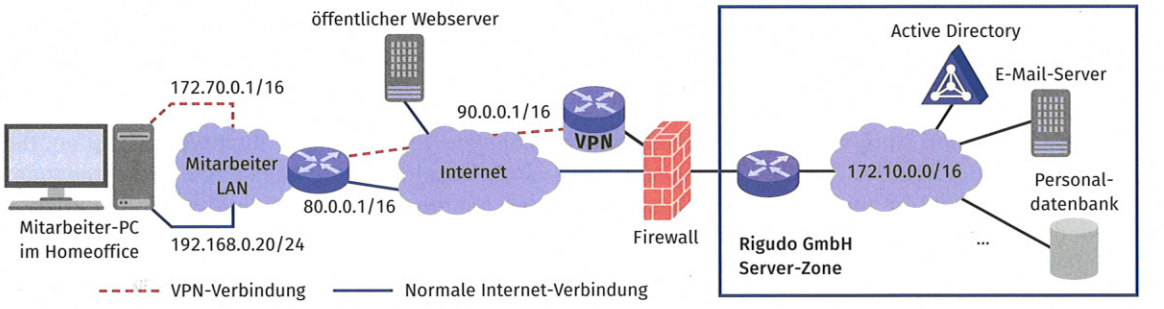
Grundstrukturen von VPN-Verbindungen

Eine solche Standortverbindung, wie sie die Modellkundin Rigudo GmbH benötigt, wird Site-to-Site genannt. Es sind jeweils drei Adressbereiche beteiligt und entsprechend zu planen.

1. Lokales Netz der Rigudo GmbH
2. Öffentliches Netz (hier können zwei unterschiedliche IP-Bereiche zum Einsatz kommen, da dies vom Provider vorgegeben wird)
3. Lokales Netz des zweiten Unternehmensnetzes der Rigudo GmbH

Site-to-End planen

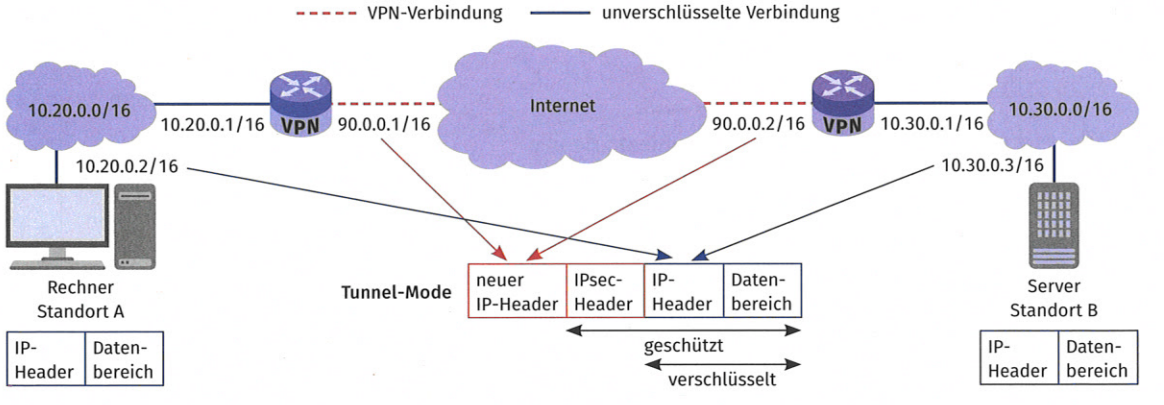
Der Zugriff für Mitarbeiter, die z. B. im Homeoffice einen sicheren Zugang zum Firmennetz benötigen, wird Site-to-End genannt. Hier bekommen Mitarbeiter über den VPN-Client eine IP-Adresse aus dem Firmennetz zugewiesen. Je nach Sicherheitsvorgaben wird bei aufgebauter VPN-Verbindung jeglicher Datenverkehr über das Firmennetz geleitet, um so die firmeneigene Sicherheitsstruktur zu nutzen. Dies hat allerdings zur Folge, dass das VPN-Gateway auf Firmenseite über hinreichende Ressourcen verfügen muss.



End-to-Site-VPN für den Zugriff auf das Firmennetz; normaler Internetverkehr unabhängig

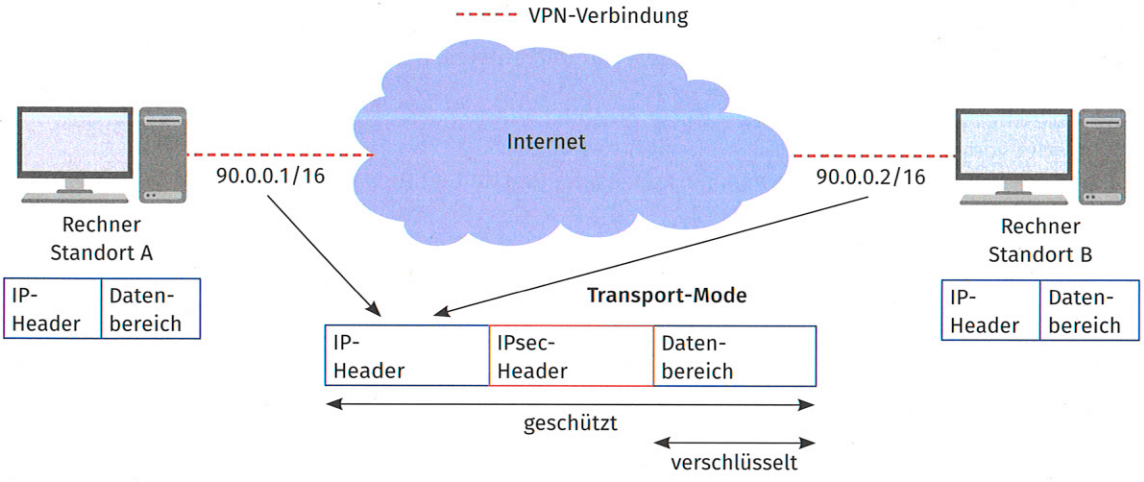
Neben der Struktur der VPN-Verbindung ist zu entscheiden, in welchem Modus die Verbindung betrieben wird. IPsec unterscheidet zwischen Tunnel- und Transport-Mode. Im Tunnel-Mode wird die VPN-Verbindung zwischen zwei Tunnelendpunkten aufgebaut. Die IP-Adressen dieser Tunnelendpunkte sind im öffentlichen Netz sichtbar. Die eigentlichen Kommunikationspartner befinden sich in den jeweiligen lokalen Netzen. Sowohl die Daten wie auch die IP-Adressen dieser Kommunikationspartner sind durch die Verschlüsselung des Tunnels im öffentlichen Netz nicht sichtbar.

Im **Tunnel-Mode** wird das ursprüngliche Paket eines Kommunikationspartners inklusive des IP-Headers verschlüsselt und mit einem neuen IP-Header für die VPN-Tunnelendpunkte versehen.



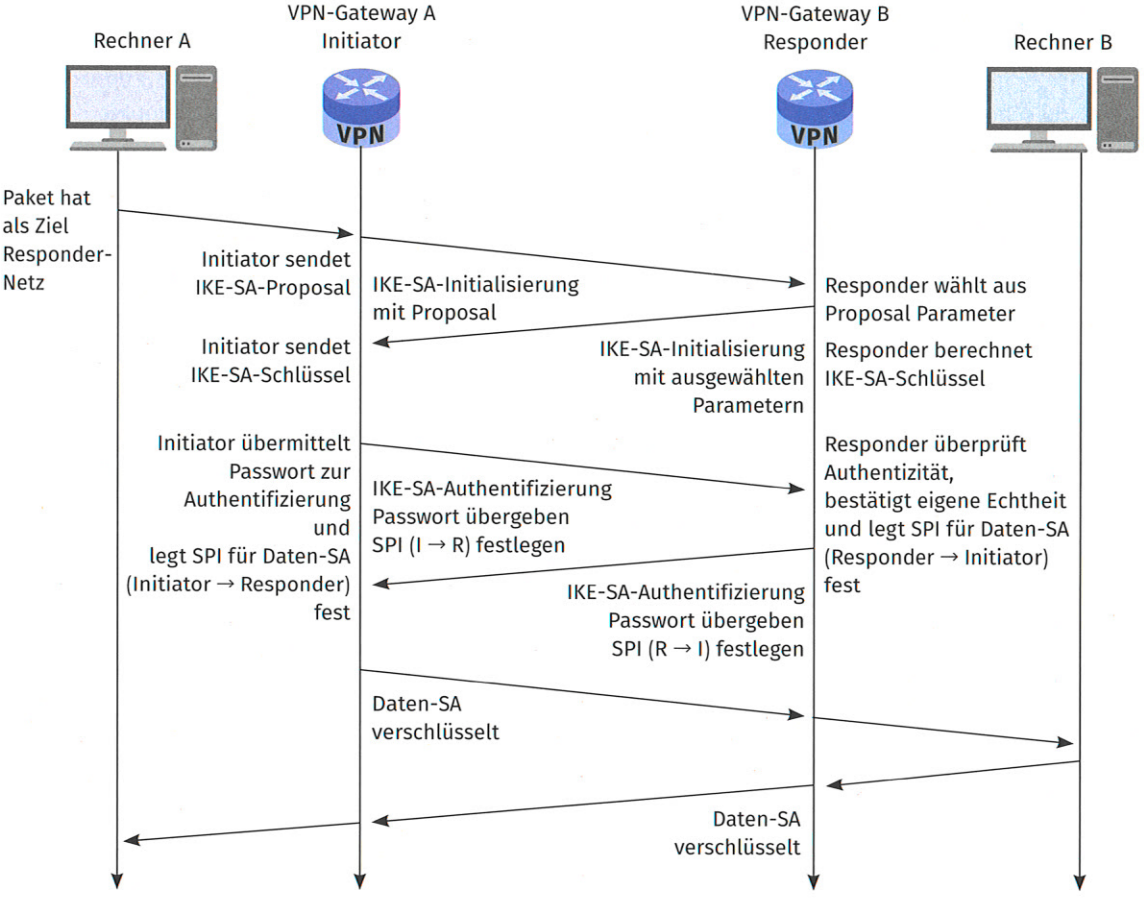
Tunnel-Mode

Im **Transport-Mode** wird der IPsec-Bereich hinter dem ursprünglichen IP-Header eingefügt. Die IP-Adressen der Kommunikationspartner sind die VPN-Endpunkte und können daher nicht verschleiert werden.



Transport-Mode

Ähnlich wie bei einer Routingtabelle wird bei IPsec ein Regelwerk definiert, bei dem ein Quell- und ein Zielnetz anzugeben sind. Diese Netze sind jeweils die lokalen Netze, die geschützt werden sollen. Die öffentlichen Adressen der VPN-Verbindung sind nicht verschlüsselt, da ansonsten das Transportnetz des Providers kein Routing im öffentlichen Netz durchführen könnte. IPsec entscheidet wie beim Routing anhand dieser Quell-/Zieladressenkombination, ob überhaupt IPsec angewendet werden soll und welche der konfigurierten IPsec-Verbindungen zu nutzen ist. Eine solche sichere Verbindung wird **Security Association (SA)** genannt.



VPN-Verbindungsaufbau mit IKEv2

Neben den IP-Adressen werden die Parameter für Verschlüsselung und Hash-Verfahren der eigentlichen VPN-Verbindung definiert. Dies wird mittels sogenannter Proposals umgesetzt.

Der Verbindungsaufbau mittels IKEv2 (Internet Key Exchange Protocol Version 2) läuft in zwei Phasen ab, bevor die eigentlichen Nutzdaten verschlüsselt übertragen werden.

In der ersten Phase wird zunächst mittels DH-Verfahren eine verschlüsselte Kommunikation zur Gegenstelle aufgebaut. Diese Verbindung ist die sogenannte IKE-SA. Da das DH-Verfahren mit unterschiedlichen Parametern genutzt werden kann, müssen sich die Kommunikationspartner zunächst auf einen Parametersatz einigen. Dies geschieht in den ersten beiden Nachrichten per Proposal (also Angebot) des Initiators und einer Antwort des Responders, in der er seine Wahl aus dem Angebot mitteilt. Damit sind Verschlüsselung, Hash-Verfahren und modp-Gruppe ausgehandelt und der initiale Schlüssel kann mittels DH-Verfahren generiert werden. Innerhalb dieser sicheren Verbindung können dann IKE-Nachrichten zur Steuerung der eigentlichen Nutzdatenverbindung (häufig als Child-SA bezeichnet) ausgetauscht werden. Hierzu gehört beispielsweise der zyklische Schlüsselaustausch zur Erhöhung der Sicherheit.

In der zweiten Phase werden dann die Parameter für die Nutzdatenverschlüsselung ausgetauscht. Diese sind zuvor durch den Administrator konfiguriert worden. Die Gegenstellen haben hierzu geschützte Datenbanken, in denen die SP (Security Parameter) für alle Verbindungen abgelegt sind. Somit müssen nur noch die Verweise in Form der SPI (Security Parameter Index) auf den genutzten Parametersatz angegeben werden.

Bei der Grundkonfiguration einer IPsec-Verbindung werden demnach folgende Parameter benötigt.

Parameter zur Grundkonfiguration einer IPsec-Verbindung
Lokaler/Remote-Adressbereich Jeweiliger privater Bereich; muss sich von Remote-Adressbereich unterscheiden, damit Routing möglich ist.
Öffentliche Adressen Tunnelendpunkt der VPN-Geräte
IKE-Proposal Parameterangebot für IPsec-Verbindungsaufbau
Nutzdatenproposal Parameterangebot für zu schützende Nutzdaten

Neben der hier ausführlich vorgestellten Möglichkeit, über IPsec einen VPN-Tunnel zu realisieren, gibt es eine große Anzahl an freien Open-Source- und proprietären Programmen.

Weitere VPN-Systeme	
VPN-System	**Beschreibung**
OpenVPN	Open-Source-Lösung; wird als eigenständige Software nachträglich installiert; arbeitet auf Layer 3 mit SSL/TLS; weit verbreitet und in viele Produkte integriert
Generic Routing Encapsulation Tunnel (GRE-Tunnel)	kein vollständiges VPN-System; kann als Trägerprotokoll für andere Protokolle genutzt werden
Layer 2 Tunnel Protocol (L2TP)	kein vollständiges VPN-System; arbeitet auf Layer 2; kann wie GRE als Trägerprotokoll für andere Protokolle genutzt werden
Multiprotocol Layer Switching (MPLS)	wird bei Providern als Ersatz für Standardfestverbindungen eingesetzt; kann als Trägerprotokoll für andere Protokolle genutzt werden; zeichnet sich durch hohen Durchsatz aus
Wireguard	relativ junges VPN-System für private Netze; einfache Konfiguration

(4) Öffentliche Cloud planen

Die Nutzung einer öffentlichen Cloud (Public Cloud) erfordert besondere Anforderungen, wenn personenbezogene Daten dort gespeichert werden sollen. Fallen Unternehmen unter die europäische Datenschutzgrundverordnung, müssen sie sicherstellen, dass der genutzte Cloud-Anbieter den Speicherort der Daten gewährleistet.

Soll die Cloud für eine eigene Produktentwicklung genutzt werden, ist es möglich, durch beispielsweise eine entsprechend verschlüsselte Ablage der Daten Einfluss auf die Datensicherheit zu nehmen. Wird die Cloud als Dateispeicher genutzt, stehen einerseits die Sicherheitsmechanismen der verwendeten Software zur Verfügung. Andererseits kann auch eine eigene Verschlüsselung unabhängig von der verwendeten Synchronisationssoftware verwendet werden, was aber die Nutzung komplizierter macht.

Im Zusammenhang mit Cloudspeicherlösungen gibt es einen Konflikt zwischen verschlüsselter Ablage und gemeinsamer Nutzung von Dateien. Wird eine Datei verschlüsselt abgelegt, muss der Schlüssel mit allen Nutzern geteilt werden. Damit muss aber für jede Datei ein extra Schlüssel erzeugt werden, da sonst ein Nutzer, der Zugriff auf eine geteilte Datei erhält, auch andere Dateien des teilenden Nutzers entschlüsseln könnte.

Auf der Serverseite bietet die Verschlüsselung der Daten Flexibilität bezüglich des Teilens von Dateien mit anderen Nutzern. Die Schlüssel werden jedoch auf dem Server abgelegt, wodurch ein Sicherheitsrisiko entstehen kann. Jedem, der auf die Schlüssel zugreifen kann, ist es möglich, auch die Daten zu entschlüsseln.

Auf der Clientseite bietet die Verschlüsselung der Dateien mehr Sicherheit. Allerdings muss sich hier der Nutzer um die Verwaltung der Schlüssel kümmern, wenn verschlüsselte Dateien mit anderen Nutzern geteilt werden sollen.

Die Absicherung der Konten mit Mehrfaktor-Authentifizierung bietet gegenüber Angriffen einen zusätzlichen Schutz.

Kompetenzcheck

1. Beschreiben Sie in eigenen Worten den Unterschied zwischen SNAT und DNAT.
2. Berechnen Sie den Schlüssel einer VPN-Verbindung, die mit dem DH-Verfahren gesichert wird. Das System verwendet die Primzahl p = 17 sowie die öffentliche Zufallszahl z = 20 und die beiden Geheimzahlen a = 4 und b = 5.
3. Nennen Sie mindestens zwei Verfahren, die bei der Verteilung von Paketen in einem Load Balancer eingesetzt werden. Erklären Sie die jeweiligen Verfahren kurz.
4. Unterscheiden Sie die Begriffe „Public Cloud“ und „Private Cloud“.
5. Notieren Sie wesentliche Aspekte aus diesem Abschnitt in Ihrem Projektjournal.
6. Bearbeiten Sie Aufgabe 3 der Lernsituation 3 im Arbeitsbuch.

A3

3.3.4 Technisch-organisatorische Maßnahmen planen

S **Sie sollen technisch-organisatorische Maßnahmen planen.**

In Kapitel 3.1 wurde das Firmenumfeld der Rigudo GmbH beschrieben. Im folgenden Abschnitt werden beispielhaft technisch-organisatorische Maßnahmen vorgestellt, die nach den Aspekten Vertraulichkeit, Integrität und Verfügbarkeit gruppiert sind.

Technisch-organisatorische Maßnahmen **Kundin: Rigudo GmbH**	JIKU IT-Solutions
Vertraulichkeit	
Zugangskontrolle	• *Die Server der Rigudo GmbH stehen im firmeneigenen Rechenzentrum am Hauptstandort.* • *Der Serverraum ist mit einem Schließsystem und einer Kameraüberwachung ausgestattet.* • *Die Serverschränke sind mit individuellen Schließsystemen versehen.* • *Der Zutritt zu den Servern ist nur einer kleinen Gruppe und besonders geschulten Mitarbeitern gestattet.* • *Handwerker, externe Servicetechniker oder Reinigungspersonal mit Zugriff zum Serverraum werden besonders unterwiesen und bei den Arbeiten im Serverraum begleitet.*
Zugriffskontrolle	• *Der Zugriff auf Datenträger wird durch verschlüsselte Dateisysteme abgesichert.* • *Mitarbeiter müssen administrativ explizit als Zugriffsberechtigte konfiguriert werden.* • *Berechtigungen sind nach entsprechendem rollenbasierten Zugriff modelliert (vgl. RBAC, Kapitel 3.3.5).*
Integrität	
Eingabekontrolle/ Verarbeitungskontrolle	• *Mitarbeiter sind verpflichtet, ihre Computerarbeitsplätze zu sperren, wenn sie den Platz verlassen.* • *Änderungen in Datenbanken mit personenbezogenen Daten werden protokolliert.*
Weitergabekontrolle	*Übermittlung der Daten zwischen dem Haupt- und dem Nebenstandort werden verschlüsselt übertragen.*
Verfügbarkeit	
Fail-Over	*Server sind im „Fail-over" geschaltet, der Storage für die Dateiserver wird mit gespiegelten Systemen realisiert.*
Geo-Redundanz	*Vom Storage werden Sicherheitskopien erstellt, die am Serverstandort und verschlüsselt am zweiten Standort abgelegt werden, der mehr als 200 km vom Hauptstandort entfernt liegt. Die Sicherheitskopien werden mit einer speziellen Software angelegt, die keinen direkten Netzwerkzugriff auf die gespeicherten Sicherheitskopien zulässt.*
Daten-Restore-Test	*Halbjährlich werden Daten-Restore-Tests durchgeführt und auf Vollständigkeit überprüft.*
USV	*Server werden mit einer unterbrechungsfreien Stromversorgung abgesichert, die einen Stromausfall von bis zu 30 Minuten überbrücken und dann die Server sicher herunterfahren kann.*

Kompetenzcheck

1. Ordnen Sie die entsprechenden Schutzziele den folgenden TOM zu.
   a) Der Serverraum kann nur von berechtigten Personen betreten werden.
   b) Das Serversystem ist als AP-Cluster installiert.
   c) Ein Druckjob kann nur nach Freigabe durch eine PIN durchgeführt werden.
   d) Bearbeitete Datensätze werden gezählt.
   e) Die Daten werden auf einem System mit RAID10 abgelegt.
   f) Im Formular können nur bestimmte Werte eingetragen werden.

2. Notieren Sie wesentliche Aspekte aus diesem Abschnitt in Ihrem Projektjournal.

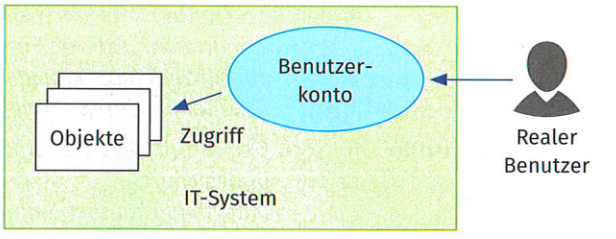
3. Bearbeiten Sie Aufgabe 4 der Lernsituation 3 im Arbeitsbuch. A4

3.3.5 Benutzerverwaltung planen

S Sie sollen die Benutzerverwaltung für vernetzte Systeme eines Unternehmens planen.

(1) Benutzer und Zugriffsrechte

Eine Grundlage der Informationssicherheit ist es, einem Benutzer nur so viel Rechte zu geben wie nötig. Um eine Rechtevergabe in einem IT-System durchzuführen, wird ein Benutzerkonto vergeben. Durch einen Benutzernamen und ein Passwort soll sichergestellt werden, dass nur die Person, der das Konto zugeordnet wurde, auch Zugriff auf das System und damit auf die Ressourcen darin erhält. Dem Benutzerkonto werden dann Zugriffsrechte auf die Ressourcen des Systems gegeben, die auch als Objekte bezeichnet werden. Objekte können physische Dinge wie Netzwerk, Drucker oder Speicher sein, aber auch logische wie Daten.

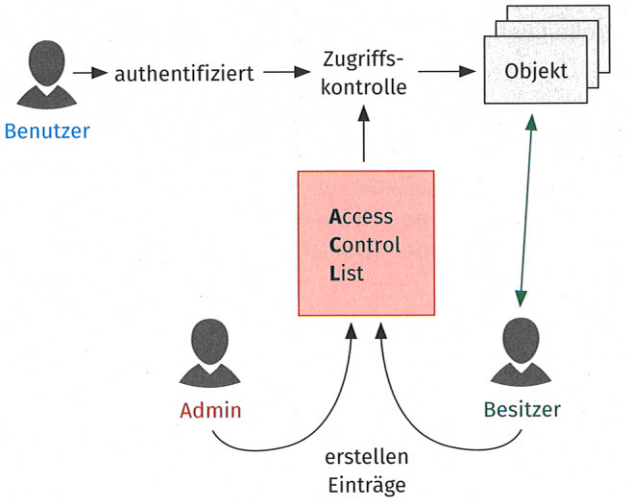


Zugriffssteuerung über Recht von Benutzerkonten

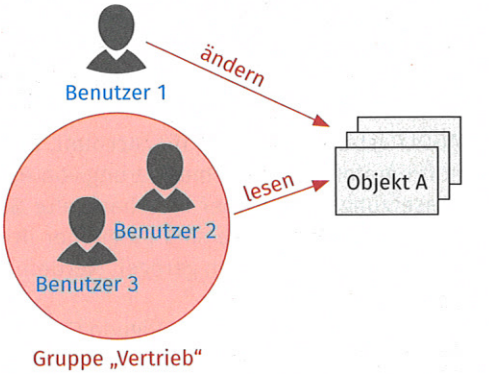
Je nach Größe eines Unternehmens oder einer Organisation können hunderte oder tausende Benutzer in einem System administriert werden. Der Aufwand, die Zugriffsrechte jedem Benutzerkonto einzeln zuzuordnen, wird bei einer Vielzahl von Benutzerkonten hoch und die Administration wird fehleranfällig.

(2) Access Control List planen

Die Access Control List (ACL) ist ein Weg, um Rechte zu vergeben. Die Vertrauenskette startet vom Objekt aus. Der Eigentümer des Objektes oder der Administrator legt in der ACL fest, welcher Benutzer auf ein Objekt zugreifen darf. Der Zugriff wird in der ACL festgelegt.



Prinzip der Access Control List (ACL)



Objekt	Benutzer/Gruppe	Berechtigung
A	Benutzer 1	ändern
A	Gruppe Vertrieb	lesen
	⋮	⋮

Zugriffsrechte basierend auf Benutzer und Gruppen

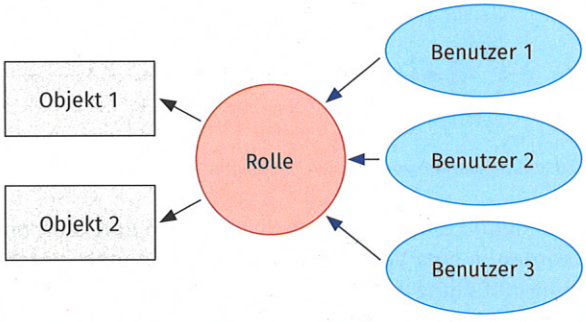
Wenn ein Benutzer auf ein Objekt zugreifen möchte, überprüft das System, ob er in der ACL mit den entsprechenden Berechtigungen aufgeführt ist. Ist das der Fall, wird der gewünschte Zugriff gewährt. Um nicht an jeden Benutzer, der zugriffsberechtigt ist, einzelne Rechte zu vergeben, gibt es die Gruppierung von Benutzern. Sie wird z. B. eingesetzt für:

- Netzwerkgeräte
- Router
- Proxy
- Firewall
- Wiki-Seite
- Dateizugriff

(3) Role Based Access Control planen

Role Based Access Control (RBAC) ist ein Modell, um Zugriffsrechte in komplexen Systemen effizient zu verwalten. Es wurde 1992 auf der 15th National Computer Security Conference vorgestellt und 2004 als ANSI-Norm 359-2004 verabschiedet.

Während bei der ACL der Fokus auf den Zielobjekten liegt, definiert das Role Based Access Control-Modell die Zugriffsrechte auf Basis der Struktur der Organisation.



Prinzip des rollenbasierten Zugriffs

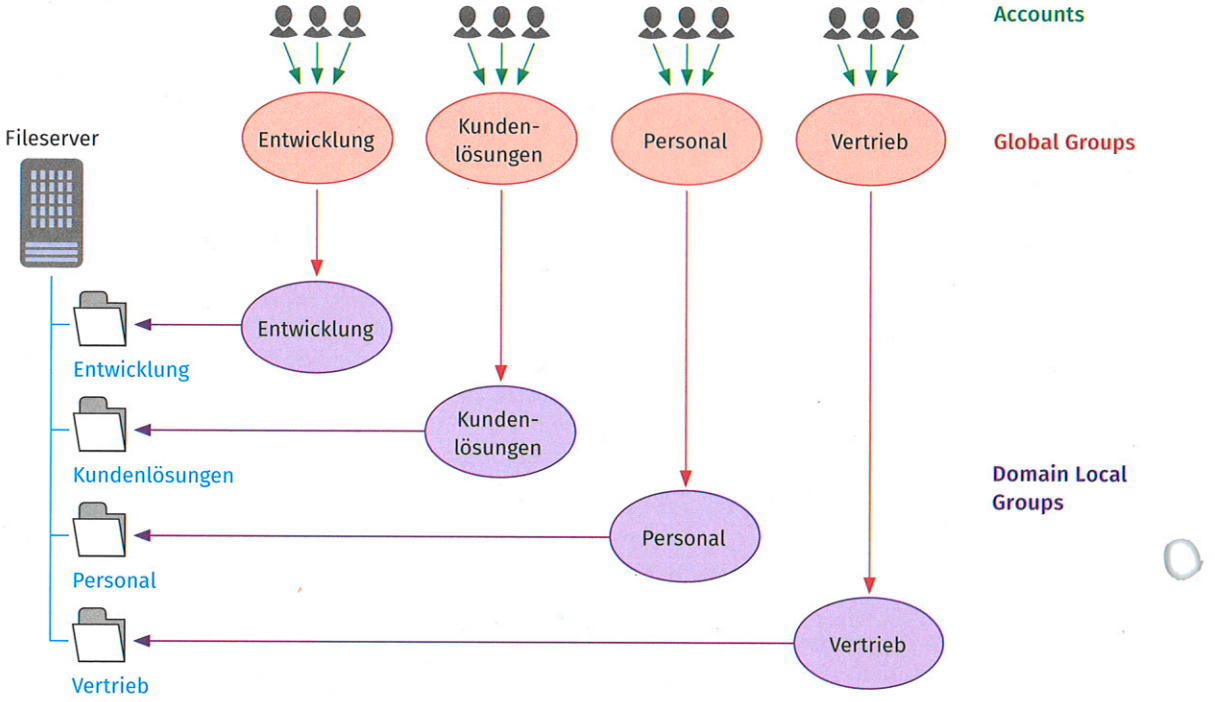
Es werden Rollen erstellt, die aus der Organisationsstruktur abgeleitet sind. Den Rollen werden ihrerseits Zugriffsrechte auf Objekte gegeben. Benutzern wiederum werden dann die entsprechenden Rollen zugeordnet. Der Vorteil dieses Systems besteht im Hinzufügen, Wechseln und Entfernen von Benutzern durch einfaches Administrieren der Rollenzugehörigkeit. Bei Benutzerverwaltungen ab einer Größe von Hunderten von Benutzern ist Role Based Access Control besser administrierbar als die einfache Zugriffsrechtevergabe über ACL.

Eine Weiterführung dieses Konzepts ist **Attribute Based Access Control (ABAC)**. Dieses Modell ermöglicht ein flexibleres Zuordnen von Zugriffsrechten in großen Benutzerverwaltungen.

(4) Windows-Rechtevergabe AGDLP planen

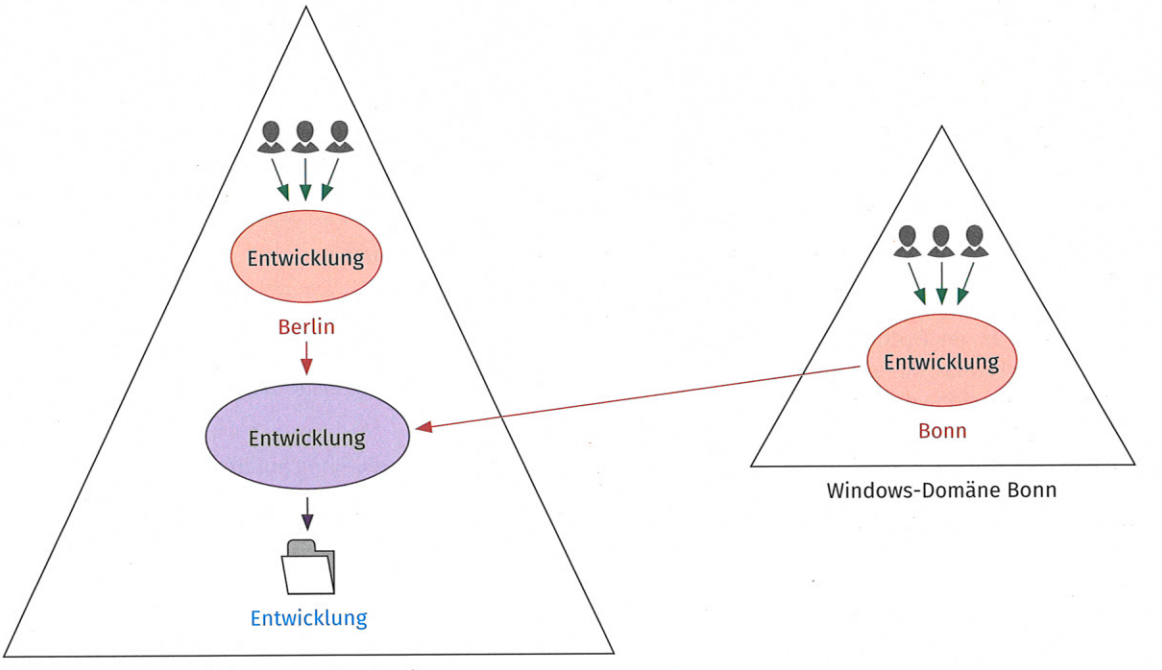
AGDLP ist die Abkürzung für „Account, Global, Domain, Local, Permission" und beschreibt die von Microsoft empfohlene Implementierung von Role Based Access Control (RBAC) in einer Windows-Domäne. Die Umsetzung erfolgt über verschachtelte Gruppen. **Globale Gruppen** (Global Groups) repräsentieren hier Geschäftsrollen. Diese sind Mitglieder in **domänenlokalen Gruppen** (Domain Local Groups), mit denen Zugriffe auf Ressourcen geregelt werden.

Als Beispiel dient die Firma Rigudo GmbH, die statistische Dienstleistungen erbringt. Sie hat die Abteilungen Entwicklung, Kundenlösungen, Vertrieb und Personal. Jede Abteilung erhält in der Windows-Domäne eine Netzwerkfreigabe, unter der die Dateien abgelegt werden. In der Windows-Domäne wird für jede Abteilung eine globale Gruppe erzeugt. Mitglieder der Abteilung werden diesen Gruppen zugeordnet. Auf dem Dateiserver werden domänenlokale Gruppen für jede Freigabe und für beispielsweise jeden Drucker erstellt. Die Zugriffsrechte auf die Freigaben werden über die jeweilige Gruppe geregelt. Die globale Gruppe für die jeweilige Abteilung wird den domänenlokalen Gruppen der Ressourcen zugeordnet.



Zusammenwirken von Global Groups und Domain Local Groups in AGDLP

Die Rigudo GmbH hat ihren Sitz in Berlin und kauft eine Firma in Bonn auf. Die beiden Windows-Domänen werden in eine Vertrauensstellung zueinander geschaltet. Damit die Projektgruppe der Bonner Entwicklungsabteilung auf die Daten in Berlin zugreifen kann, wird in der Bonner Domäne eine globale Gruppe „Entwicklung" erstellt, diese wird in der Berliner Domäne der domänenlokalen Gruppe „Entwicklung" zugeordnet. Damit haben auch die entsprechenden Benutzer aus Bonn Zugriff auf die Daten in Berlin.



Umsetzung von RBAC über verschiedene Domänen

(5) Modell der Rechteverwaltung unter Linux planen

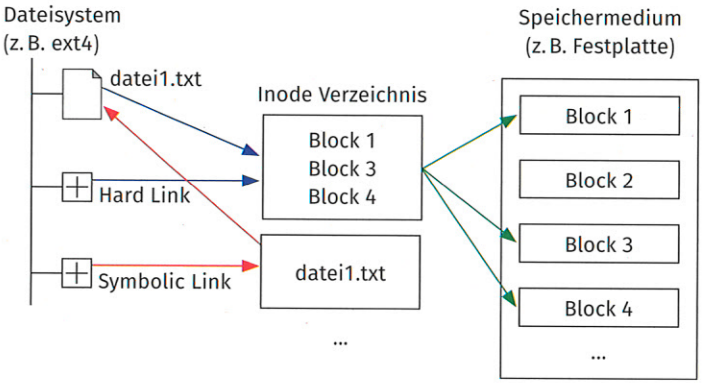
Die Entwicklungsabteilung der Rigudo GmbH benötigt für ihre Linux-Systeme geregelte Zugriffsrechte. Zur Planung der Rechteverwaltung werden zunächst die Möglichkeiten der Dateiverwaltung unter Linux betrachtet. Die Dateiverwaltung in einem Linux-Betriebssystem wird über sogenannte Inodes realisiert.

Inode

Inodes (Kurzvariante von Index nodes) speichern Metadaten zu den Dateien in einem virtuellen Dateisystem Virtual File System (VFS). Ein Inode trägt verschiedene Informationen.

Daten eines Inodes
Dateityp Normale Datei, Ordner, symbolische/harte Verweise (Links), block-/zeichenorientierte Gerätedatei, Pipes, Sockets
Zugriffsrechte Eigentümer, Gruppenzugehörigkeit, Ausführungsrechte
Größe Dateigröße
Zeitstempel Letzter Zeitpunkt des Zugriffs auf die Datei, die Inodes und deren Änderungen
Verweis auf Dateiinhalt Verweise auf die Dateiblöcke, in denen die eigentlichen Daten gespeichert sind; können direkt (üblich), indirekt oder zweistufig indirekt sein (indirekt eher unüblich)

Neben den normalen Dateien und Ordnern sind Verweise eine Besonderheit bei UNIX-Betriebssystemen. Verweise, sogenannte Links, können als symbolische oder harte Verweise ausgeführt werden. Ein symbolischer Verweis (Symbolic Link) enthält den Dateipfad zum eigentlichen Inode. Diese Art des Zugriffs wird häufig für Programme mit Versionsangaben im Dateinamen verwendet. Beispielsweise findet man im Ordner „/usr/bin" den Link „python3", der auf die aktuell installierte Version von Python 3 zeigt („/usr/bin/python3" → „python3.10").

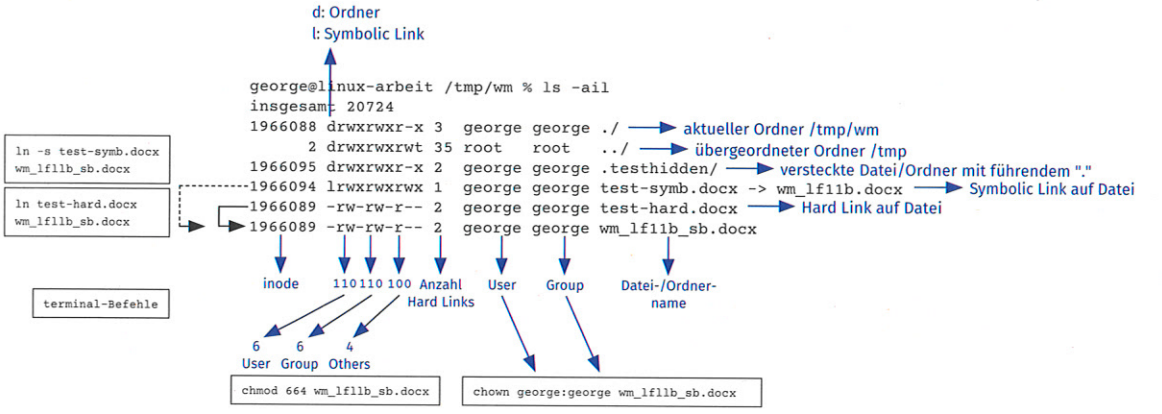


Zusammenhang zwischen Dateisystem, Inodes und Speichermedium

Wird ein solcher symbolischer Verweis gelöscht, dann hat dies keine Auswirkung auf die eigentliche Datei. Es wird lediglich der Inode, welcher den Dateipfad auf das eigentliche Ziel zeigt, gelöscht.

Bei einem harten Verweis (Hard Link) zeigen mehrere Einträge auf einen Inode, in dem die eigentlichen Daten verwaltet werden. Jeder dieser Links ist gleichberechtigt. Der Ziel-Inode zählt die Verweise auf ihn. Beim Löschen eines solches harten Verweises wird der Ziel-Inode erst dann aus dem Inode-Verzeichnis entfernt, wenn der letzte Verweis gelöscht wird.

Mit dem Befehl „ls -i" kann die Nummer des Inodes ausgelesen werden. Bei einem Hard Link wird auf den identischen Inode verwiesen. Man kann dies auch an der Dateigröße sehen. Ein Hard Link kann demnach nur auf Dateien und nicht auf Ordner gesetzt werden. Bei einem Symbolic Link wird lediglich eine Verknüpfung angelegt (erkennbar am „l" bei den Zugriffsrechten), die Dateigröße ist entsprechend klein.



Bedeutung der Inode-Informationen und Zugriffsbits

Die im Inode gespeicherten Metadaten können mit dem Befehl „stat" ausgelesen werden. Im Folgenden werden diese Daten für einen symbolischen Verweis und die eigentliche Datei gezeigt.

```
# Originaldatei wm_lf11b_sb.docx
george@linux-arbeit /tmp/wm % ls -i wm_lf11b_sb.docx
1966089 wm_lf11b_sb1.docx

george@linux-arbeit /tmp/wm% stat wm_lf11b_sb.docx
 Datei: wm_lf11b_sb.docx
 Größe: 4963616 Blöcke: 9696 EA Block: 4096 Normale Datei
Gerät: 10304h/66308d Inode: 1966089 Verknüpfungen: 2
Zugriff: (0664/-rw-rw-r--) Uid: ( 1000/ george) Gid: ( 1000/ george)
Zugriff: 2022-09-24 12:27:51.499790926 +0200
Modifiziert: 2022-09-24 12:27:42.343761525 +0200
Geändert: 2022-09-24 18:38:18.252220323 +0200
Geburt: 2022-09-24 12:26:16.531466778 +0200
```

Beim Hard Link auf die Datei ist die Anzahl der Verknüpfungen auf zwei erhöht worden. Die Inode-Kennung (1966089) ist dieselbe wie beim Original.

```
# Hard Link auf wm_lf11b_sb.docx
george@linux-arbeit /tmp/wm % ls -i test-hard.docx
1966089 test-hard.docx

george@linux-arbeit /tmp/wm % stat test-hard.docx
 Datei: test-hard.docx
 Größe: 4963616 Blöcke: 9696 EA Block: 4096 Normale Datei
Gerät: 10304h/66308d Inode: 1966089 Verknüpfungen: 2
Zugriff: (0664/-rw-rw-r--) Uid: ( 1000/ george) Gid: ( 1000/ george)
Zugriff: 2022-09-24 12:27:51.499790926 +0200
Modifiziert: 2022-09-24 12:27:42.343761525 +0200
Geändert: 2022-09-24 18:38:18.252220323 +0200
Geburt: 2022-09-24 12:26:16.531466778 +0200
```

Beim Symbolic Link auf die Datei ist die Anzahl der Verknüpfungen eins, da hier nur ein Inode mit einem Verweis genutzt wird. Der Link hat eine eigene Inode-Kennung (1966094).

```
# Symbolic Link auf wm_lf11b_sb.docx
george@linux-arbeit /tmp/wm % ls -i test-symb.docx
1966094 test-symb.docx@

george@linux-arbeit /tmp/wm % stat test-symb.docx
 Datei: test-symb.docx -> wm_lf11b_sb.docx
 Größe: 17 Blöcke: 0 EA Block: 4096 symbolische Verknüpfung
Gerät: 10304h/66308d Inode: 1966094 Verknüpfungen: 1
Zugriff: (0777/lrwxrwxrwx) Uid: ( 1000/ george) Gid: ( 1000/ george)
Zugriff: 2022-09-24 18:39:00.228282150 +0200
Modifiziert: 2022-09-24 18:38:59.700281373 +0200
Geändert: 2022-09-24 18:38:59.700281373 +0200
Geburt: 2022-09-24 18:38:59.700281373 +0200
```

Die Verwaltung der Inodes geschieht durch das Dateisystem, z. B. EXT4. Der Zugriff auf Dateien und Ordner wird über die User-ID (UID) und Group-ID (GID) geregelt. Die Namen werden diesen IDs entsprechend zugeordnet.

Die Zugriffsrechte ermöglichen es, administrative Vorgaben zu machen. Jeder Inode enthält 7 Bits, über die die Zugriffe geregelt werden. Die Bedeutung soll anhand des Beispiels der Datei „python3.10" und dem Link „python3" erläutert werden. Die Zugriffsrechte sind in vier Bereiche eingeteilt (ein Sonderrecht und drei Zugriffsrechte für Benutzer, Gruppe und Andere).

Bedeutung der Zugriffsrechte bei Dateien			
Sonderrecht	3 Bit	Set-UID-Recht s, Set-GID-Recht s, Sticky-Bit t	Bei ausführbaren Dateien werden diese immer im Kontext des Besitzers/der Gruppe ausgeführt. Dies kann ein Sicherheitsrisiko darstellen. Durch das Setzen der Set-UID kann für diese Datei ein anderer Kontext verwendet werden. Die mit dem t-Bit markierte Datei bzw. der Ordner kann nur noch vom Besitzer gelöscht bzw. umbenannt werden. Andere Benutzer können diese Dateien/Ordner nur noch lesen oder ausführen. Das t-Bit ergibt in Ordnern Sinn, auf die von mehreren Benutzern zugegriffen werden kann, z. B. /tmp. Dieses Merkmal wird auf darunter liegende Ordner weitergegeben. Der Besitzer des Hauptordners behält die Rechte zum Löschen und Umbenennen.
Zugriffsrechte Benutzer	3 Bit	r: read, w: write, x: eXecute	Werden diese Bits gesetzt, so erhält der Benutzer die entsprechende Berechtigung. Über das x-Bit wird entschieden, ob eine Datei ausgeführt werden darf oder nicht. Bei heruntergeladenen Skriptdateien muss das x-Bit aktiv gesetzt werden, damit die Datei ausgeführt werden kann. Unter Windows reicht hier in den meisten Fällen ein entsprechendes Suffix des Dateinamens (z. B. .exe oder .bat). Ein lesbarer Ordner hat immer das x- und r-Bit gesetzt. Das x-Bit hat hier die Bedeutung, dass der Ordner geöffnet („cd <Ordner>") werden darf.
Zugriffsrechte Gruppe	3 Bit	r: read, w: write, x: eXecute	Die Bits haben die gleiche Bedeutung wie beim Benutzer, sie gelten allerdings für die Gruppe, zu der die Datei gehört.
Zugriffsrechte Andere	3 Bit	r: read, w: write, x: eXecute	Die Bits haben die gleiche Bedeutung wie beim Benutzer/bei der Gruppe, sie gelten allerdings für alle anderen Nutzer/Gruppen (others).

Es gibt im Wesentlichen drei Darstellungen für die Zugriffsrechte: symbolisch, dezimal (0–7) oder binär (0–1).

Im Beispiel der Datei „/usr/bin/python3.10" kann dem Inode die folgende Rechtevergabe entnommen werden:

```
Zugriff: (0755/-rwxr-xr-x) Uid: ( 0/ root) Gid: ( 0/ root)
```

In der Klammer wird zunächst die dezimale Darstellung angezeigt. Bei 0775 hat jede Ziffer eine Bedeutung. In der ersten Ziffer wird das Sonderrecht „Sticky-Bit" abgelegt. Die weiteren drei Ziffern kann man als Dezimalwert für die drei Bits der Zugriffsrechte verstehen.

$7_{dezimal}$ = $111_{binär}$ -> r=1 w=1 und x=1 → Benutzer besitzt alle Rechte
$5_{dezimal}$ = $101_{binär}$ -> r=1 w=0 und x=1 → Gruppe und andere dürfen nur lesen und ausführen

Bei der symbolischen Schreibweise „-rwxr-xr-x" sind die Rechte direkt in der Reihenfolge „Benutzer – Gruppe – Andere" ablesbar. Der Benutzer und die Gruppe werden mit „Uid" und „Gid" angegeben. Normale Benutzer haben in der Regel eine ID ab 1 000.

Das System ist einfach strukturiert und ermöglicht, Zugriffe auf Dateien und Ordner gezielt zu steuern. Durch Anlegen von Gruppen und Zuordnen der Benutzer zu diesen Gruppen können Ordner nur den Mitgliedern einer solchen Gruppe zugänglich gemacht werden. Neben diesen beiden Darstellungsformen gibt es noch die sogenannte „umask". Diese arbeitet mit der entgegengesetzten Logik von „chmod", also dem Entzug von Rechten.

Die folgende Tabelle stellt die wesentlichen Werte gegenüber.

Rechtesystem von chmod und umask				
Rechte	**Symbolisch**	**Binär**	**chmod (dezimal)**	**umask (dezimal)**
Lesen, Schreiben, Ausführen	`rwx`	`111`	7	0
Lesen, Schreiben	`rw-`	`110`	6	1
Lesen, Ausführen	`r-x`	`101`	5	2
Lesen	`r--`	`100`	4	3
Schreiben, Ausführen (nur theoretisch)	`-wx`	`011`	3	4
Schreiben (nur theoretisch)	`-w-`	`010`	2	5
Ausführen (nur theoretisch)	`--x`	`001`	1	6
keine Rechte	`---`	`000`	0	7

Die Rechte „Schreiben" und „Ausführen" sind nur sinnvoll in Zusammenhang mit „Lesen" einsetzbar. Die Tabelle führt diese nur der Vollständigkeit halber auf. Die Standardeinstellung für die Erzeugung neuer Ordner oder Dateien wird für neu angelegte Benutzer in der Datei „/etc/login.defs" mit dem Parameter „UMASK" bzw. „HOME_MODE" festgelegt. Allerdings stößt das Prinzip an seine Grenzen, wenn die Freigaben für viele unterschiedliche einzelne Personen gelten sollen. Hier müsste man jeweils eine Gruppe mit zwei Personen erstellen und dann diese Gruppe der betreffenden Datei bzw. dem betreffenden Ordner zuordnen.

Als Alternative bietet sich hier die Access Control List (ACL) an. Mithilfe des Pakets „acl" können über „setacl" und „getacl" die Zugriffrechte für einzelne Benutzerebenen eingerichtet werden.

Das eXecute-Sonderrecht (s) kann kritisch sein, wenn die ausführbare Datei dem Benutzer „root" gehört. Hierdurch können alle Benutzer diese Datei mit root-Rechten, also vollem Zugriff auf das gesamte System, ausführen. Hat das betreffende Programm eine Schwachstelle, so kann diese in einem solchen Fall zur Übernahme durch einen Angreifer genutzt werden. Das s-Bit wird anstelle des x-Bits gesetzt.

Bekanntestes Beispiel ist der Befehl „sudo" mit den Zugriffsrechten „sudo: -rwsr-xr-x" sowie Benutzer: Gruppe „root:root". Bei einem Zugriff auf diese Programme fordert das Betriebssystem zur expliziten Authentifikation durch Eingabe des Passworts auf. Es wird dabei das persönliche Passwort des Benutzers abgefragt. Der Benutzer „root" hat standardmäßig kein eigenes Passwort. Bei Windows wurde dieser Mechanismus später durch User Account Control (UAC) übernommen.

Ordnerstruktur

In einem Linux-System werden Dateien hierarchisch abgelegt. So gibt es eigene Ordner, in denen zentral nur Konfigurationsdateien bzw. allgemeine Programme abgelegt werden, die jeder Benutzer aufrufen darf. Diese Ordnerstruktur wird vom Filesystem Hierarchy Standard (FHS) beschrieben. Hierdurch wird die Administration der Zugriffsrechte erleichtert.

In einem Windows-System gibt es ähnliche Strukturen. Hier wird allerdings im Bereich „Programme" keine weitere Unterscheidung zwischen administrativen und einfachen Programmen vorgenommen, sodass die Administration der Zugriffsrechte lückenhaft sein kann (siehe auch Kapitel 1.2.3).

Unter Linux hat der Systemadministrator die Möglichkeit, für jeden dieser Ordner einen eigenen Einhängepunkt (Mount-Point) zu definieren. So können die gemeinsamen Systemdateien („/usr") oder der Benutzerbereich („/home") beispielsweise auf einem Serverlaufwerk abgelegt werden, sofern die Datenrate der Netzanbindung hinreichend ist.

Die Dateien „/etc/passwd" und „/etc/shadow" enthalten alle Gruppen und Benutzer des Betriebssystems. Die Shadow-Datei enthält zusätzlich die Passwörter in gehashter Form, daher ist diese nur dem Root-Benutzer lesbar zugänglich. Ursprünglich waren auch die Passwörter in der Datei „/etc/passwd" gespeichert.

Netzwerkfreigaben im lokalen System einbinden

Linux verwendet für den Zugriff auf entfernte Serverfreigaben (Netzwerkfreigaben) standardmäßig NFS (Network File System). Bei Windows-Freigaben wird SMB (Server Message Block) genutzt. Der Befehl „mount -t <REMOTE-SERVER>:<REMOTE-PATH> <LOCALE-PATH>" kann genutzt werden, um entfernte Freigaben im lokalen System einzubinden.

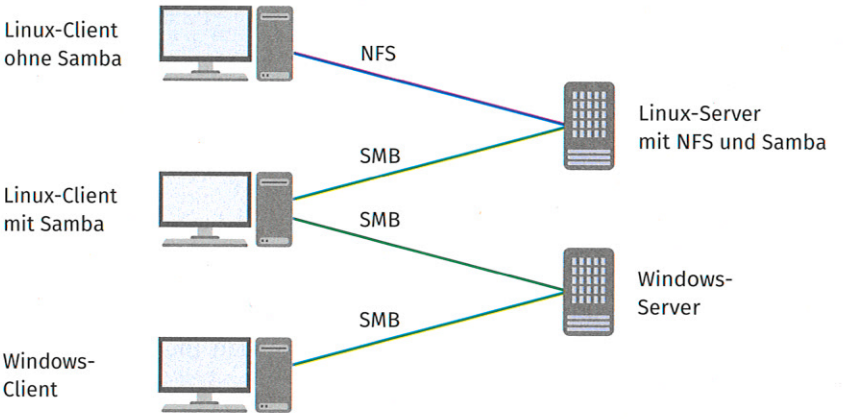
```
mount -t nfs server1:/nfs/public /mnt/public
```

Hier wird auf dem entfernten Server mit Namen „server1" der Ordner „/nfs/public" lokal unter dem Ordner „/mnt/public" eingebunden. Dieser Befehl gilt nur zur Laufzeit und wird nach einem Neustart zurückgesetzt. Eine dauerhafte Verbindung wird in der Datei „/etc/fstab" konfiguriert.

Beispieleintrag für NFS in „/etc/fstab"

```
server1:/nfs/public /mnt/public nfs default 0 0
```

Windows-basierte Freigaben werden in ähnlicher Weise eingebunden. Windows verwendet für Drucker- und Dateifreigaben das SMB-Protokoll. Unter Linux wird dies durch das Paket „samba" unterstützt. In diesem Zusammenhang wird auch von CIFS (Common Internet File System) gesprochen. Es handelt sich dabei um eine Implementierung des SMB-Protokolls. In einigen Konfigurationsdateien findet man daher CIFS statt SMB.



Zugriffsvarianten für NFS und SMB mit Windows- und Linux-Clients

```
mount -t smbfs //winserver1/nfs/public /mnt/public
oder
smbmount -t //winserver1/nfs/public /mnt/public
```

In der „/etc/fstab" können zusätzliche Angaben für einen bestimmten Benutzer angegeben werden. Hier sollte auf die direkte Angabe von Passwörtern verzichtet werden, da diese eingesehen werden können und darüber hinaus über den Administrator gepflegt werden müssen. Der bessere Weg ist es, über den Parameter „credentials" eine Datei anzugeben, die durch Dateirechte geschützt nur vom Benutzer eingesehen und gepflegt werden kann.

```
# Zu bevorzugende Variante
//server1:/nfs/public /mnt/public cifs credentials=/home/<BENUTZER>/.
smbcredentials 0 0

# NICHT empfehlenswert
//server1:/nfs/public /mnt/public cifs username=<BENUTZERNAME>,password
=<PASSWORT> 0 0
```

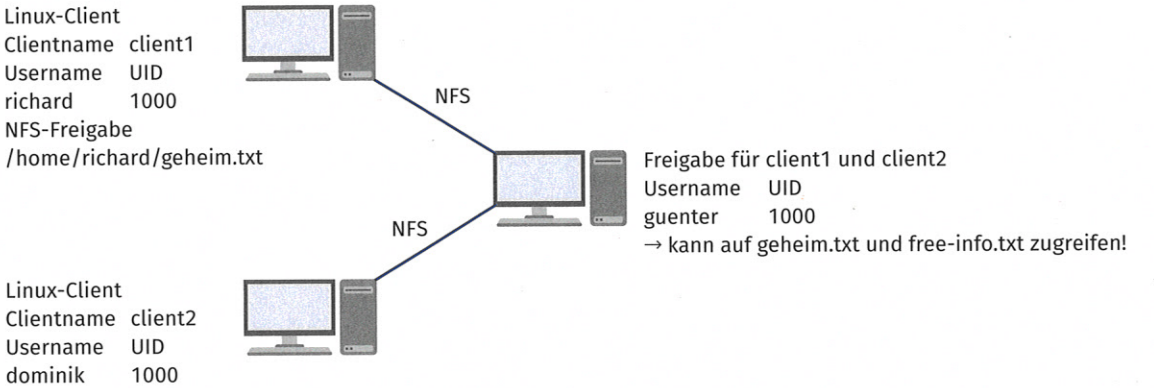
Netzwerkfreigaben bereitstellen

Die NFS-Freigaben werden in der Datei „/etc/exports" lokal gepflegt. Diese Datei wird vom rpc.nfsd und rpc.mountd ausgelesen, um die entsprechenden Freigaben bereitzustellen. Die Freigaben in „/etc/exports" sehen wie folgt aus:

```
/usr         *.rigudo.de(ro)
/home/user1  client01(rw)
/nfs/public  client02(ro)
```

Unter Linux werden, wie bereits beschrieben, die Zugriffsrechte über die UID und GID geregelt. Dies muss bei NFS-Freigaben berücksichtigt werden.

Es kann vorkommen, dass zwei unterschiedliche Benutzer auf getrennten Systemen dieselbe UID erhalten. Dies kann dazu führen, dass Zugriffe möglich werden, die eigentlich nicht gewünscht sind. Durch den Einsatz von Squashing kann dies unterbunden werden.



Beispiel für ungewollte Freigaben über UID

Kompetenzcheck

1. Beschreiben Sie, welches Schutzziel mit der Verwendung von Benutzername und Passwort umgesetzt werden kann.
2. Nennen Sie mindestens drei Einsatzbereiche von ACL.
3. Notieren Sie den Vorteil, der durch die Verwendung von Role Based Access Control (RBAC) entsteht.
4. Recherchieren Sie das sogenannte Prinzip der geringsten Rechte.
5. Erklären Sie den Unterschied zwischen einem Hard Link und einem Soft Link in einem Linux-Dateisystem.
6. Für zwei Dateien in einem Linux-Dateisystem werden die folgende Werte für die Zugriffsrechte angegeben: Datei 1 → 754 und Datei 2 → 740. Geben Sie an, welche Aktionen der Benutzer, die Gruppe und andere ausführen dürfen.
7. Notieren Sie wesentliche Aspekte aus diesem Abschnitt in Ihrem Projektjournal.
8. Bearbeiten Sie Aufgabe 5 der Lernsituation 3 im Arbeitsbuch.

A5

3.3.6 Identitätsmanagement planen

S **Sie sollen verschiedene Aspekte des Identitätsmanagements planen.**

(1) Verschlüsselung wie Pre-shared Key oder RADIUS planen

Die Rigudo GmbH möchte eine interne Zertifizierungsstelle betreiben, um z. B. Geräte und Benutzer mit Zertifikaten authentifizieren zu können und gegebenenfalls eine verschlüsselte Kommunikation zu ermöglichen.

Zertifikate können durch die Verwendung des Schlüsselpaares sowohl für die Sicherstellung der Authentizität als auch für das Herstellen der Vertraulichkeit verwendet werden. Die eigentliche Verschlüsselung findet meist über ein symmetrisches Verschlüsselungsverfahren statt, während für den Schlüsselaustausch des symmetrischen Schlüssels ein asymmetrisches Verfahren verwendet wird.

Verschlüsselungsverfahren

Symmetrische Verschlüsselung

Bei einer symmetrischen Verschlüsselung wird zur Verschlüsselung und zur Entschlüsselung derselbe Schlüssel verwendet. Ein leicht verständliches Beispiel dafür ist die sogenannte Caesar-Verschlüsselung. Jede Zahl wird durch einen Buchstaben repräsentiert. Die Buchstaben werden, beginnend mit A = 0 durchnummeriert. Zwei Personen, Alice und Bob, vereinbaren als gemeinsames geheimes Passwort eine Zahl zwischen 0 und 25. Wenn nun Alice an Bob einen Buchstaben versenden möchte, sucht Alice die entsprechende Zahl und addiert den Wert des geheimen Passworts. Das Ergebnis wird mit Modulo 26 berechnet, damit eine Verschiebung von z. B. dem Buchstaben Z nach B funktioniert. Bob erhält die Nachricht und subtrahiert den Wert des Schlüssels vom Ergebnis. Zu diesem Ergebnis wird die Zahl 26 addiert und dann wieder mit Modulo 26 berechnet.



Alice



Bob

gemeinsamer Schlüssel K_{PSK} —K_{PSK}→ gemeinsamer Schlüssel K_{PSK}

Nachricht N

K_{PSK} (N) = verschlüsselte Nachricht VN —VN→ K_{PSK} (VN) = Nachricht N

Beispiel: Alice hat mit Bob als Schlüssel den Wert 15 vereinbart. Alice möchte Bob das Wort „Hallo" senden.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Alice ersetzt die Buchstaben des Wortes „Hallo" durch die Werte aus der Tabelle. „Hallo" entspricht den Werten 7 0 11 11 14 . Alice addiert zu den Zahlen den Schlüssel. Es entstehen die Werte 22 15 26 26 29 . Abschließend werden die Werte mit Modulo 26 berechnet. Es entstehen die Werte 22 15 0 (26 mod 26 = 0) 0 3 (29 mod 26 = 3). Bob empfängt diese Werte. Als erstes zieht er von den Werten den Wert des Schlüssels ab. Es stehen die Zahlen 7 0 -15 -15 -12. Dann addiert er 26 hinzu. Das Ergebnis lautet 33 26 11 11 14. Diese Zahlen werden wieder mit Modulo 26 berechnet. Das Ergebnis lautet 7 0 11 11 14 . In der Tabelle können zu den Zahlen die Buchstaben abgelesen werden.

Die symmetrische Verschlüsselung ist schneller und ressourcenschonender als die asymmetrische Verschlüsselung. Das liegt daran, dass bei der symmetrischen Verschlüsselung kürzere Schlüssel zum Einsatz kommen können. In einer technischen Richtlinie empfiehlt das BSI mindestens 128 Bit Schlüssellänge. Ein modernes symmetrisches Verfahren ist der oft verwendete Advanced Encryption Standard (AES).

Das Problem der symmetrischen Verschlüsselung ist der Schlüsselaustausch. Alice und Bob teilen sich einen gemeinsamen Schlüssel. Dieser Schlüssel muss vorher ausgetauscht werden. Dieser wird als Pre-shared Key (PSK) bezeichnet. Zum Austausch des Schlüssels steht u. U. kein vertraulicher Kanal zur Verfügung. Das bedeutet, dass der Schlüssel über einen nicht vertraulichen Kanal übertragen wird, z. B. am Telefon oder via E-Mail. Idealerweise wird ein solcher Schlüssel persönlich ausgetauscht. Mit einem oder zehn Kommunikationspartner(n) ist ein persönlicher Austausch vorstellbar, mit 1 000 Kommunikationspartnern allerdings nicht mehr. Ein weiteres Problem ist das Management der Schlüssel. Mit jedem Kommunikationspartner muss ein eigener geheimer Schlüssel ausgetauscht werden. Die Zuordnung zwischen Kommunikationspartner und zugehörigem Schlüssel muss hinterlegt sein.

Asymmetrische Verschlüsselung

Bei der asymmetrischen Verschlüsselung hat jeder Teilnehmer einer Kommunikation zwei Schlüssel, das sogenannte Schlüsselpaar. Der eine Schlüssel heißt privater Schlüssel (Private Key) und ist geheim. Er darf niemandem mitgeteilt werden. Der andere Schlüssel wird öffentlicher Schlüssel genannt (Public Key) und darf jedem zugänglich gemacht werden.
Mit der asymmetrischen Verschlüsselung kann das Schutzziel „Vertraulichkeit" umgesetzt werden. Dazu verschlüsselt Alice die Nachricht N mit dem öffentlichen Schlüssel des Ziels, also Bob. Nur Bob kann die Nachricht mit dem eigenen privaten Schlüssel entschlüsseln.



Alice



Bob

gemeinsamer Schlüssel K_{PSK} von A: $K_{publicA}$ —K_{PSK}→ gemeinsamer Schlüssel K_{PSK}

K_{PSK} (N) = verschlüsselte Nachricht VN —VN→ K_{PSK} (VN) = Nachricht N

Schutzziel: Vertraulichkeit mit öffentlichen und privaten Schlüsseln

Neben der Vertraulichkeit kann auch die Authentizität erreicht werden. Dazu verschlüsselt Alice die Nachricht N mit dem privaten Schlüssel von A und versendet die verschlüsselte Nachricht an Bob. Jeder kann die Nachricht mit einem öffentlichen Schlüssel von Alice entschlüsseln. Da nur Alice den passenden privaten Schlüssel hat, ist nachgewiesen, dass die Nachricht von Alice kommt.



Alice



Bob

öffentlicher Schlüssel von A: $K_{publicA}$ —$K_{publicA}$→ $K_{publicA}$

$K_{privateA}$ (VN) = verschlüsselte Nachricht VN —VN→ verschlüsselte Nachricht N
$K_{publicA}$ (VN) = Nachricht N

Schutzziel: Authentizität mit öffentlichen und privaten Schlüsseln

Der Vorteil der asymmetrischen Verschlüsselung ist, dass der Schlüsselaustausch unproblematisch ist, da jeder den öffentlichen Schlüssel eines Kommunikationspartners haben kann. Allerdings benötigt die asymmetrische Verschlüsselung längere Schlüssellängen. Das BSI empfiehlt für langfristige Nutzung 3000 Bit beim asymmetrischen Verschlüsselungsverfahren RSA. RSA ist ein sehr bekanntes asymmetrisches Verfahren, das nach den Entwicklern Ron Rivest, Adi Shamir und Len Adleman benannt wurde.
Asymmetrische Verfahren benötigen mehr Zeit und mehr Ressourcen.

Im Folgenden wird die asymmetrische Verschlüsselung an einem vereinfachten Beispiel erklärt.

Beschreibung des Verfahrens	Beispiel
Alice wählt zwei Primzahlen P und Q.	P = 7 und Q = 11
Es werden die Werte X = P · Q und Y = (P – 1) · (Q – 1) berechnet.	X = 7 · 11 = 77 und Y = (7 – 1) · (11 – 1) = 60
Nun wird ein Wert Pub gewählt. Pub muss kleiner als X sein und darf keinen gemeinsamen Teiler mit Y haben.	Teiler von Y = 2 · 2 · 3 · 5; Pub < 77; z. B. Pub = 13 13 ist kein Teiler von 77
Jetzt wird ein Wert Priv gewählt. Priv muss ungleich Pub sein. Es muss weiterhin gelten Priv · Pub mod Y = 1 (Rest der Divison ist 1)	z. B. Priv = 37 Überprüfung: 37 · 13 mod 60 = 1
Der öffentliche Schlüssel besteht aus den Werten Pub = 13 und X = 77.	
Der private Schlüssel besteht aus den Werten Priv = 37 und X = 77.	
Bob möchte Alice das Wort „Hallo" verschlüsselt übersenden und ordnet jedem Buchstaben eine Zahl zu (beginnend bei A = 1).	H = 8, A = 1, L = 12, L = 12, O = 15
Bob verschlüsselt die einzelnen Buchstaben mit folgender Formel: $vZ = K^{Pub} \bmod X$. vZ ist hier das verschlüsselte Zeichen, K der Buchstabe als Zahl, Pub und X der öffentliche Schlüssel	$vZ1 = 8^{13} \bmod 77 = 50$ $vZ2 = 1^{13} \bmod 77 = 1$ $vZ3 = 12^{13} \bmod 77 = 12$ $vZ4 = 12^{13} \bmod 77 = 12$ $vZ5 = 15^{13} \bmod 77 = 64$ Die Ergebnisse der Potenzrechnung sind u. U. sehr große Zahlen. Verwenden Sie einen entsprechenden Taschenrechner, um die Ergebnisse zu berechnen.
Bob sendet die Werte an Alice.	
Alice entschlüsselt die Werte mit der Formel $K = vZ^{Priv} \bmod X$ vZ ist hier das verschlüsselte Zeichen, K der Buchstabe als Zahl im Klartext, Priv und X der private Schlüssel	$K\,1 = 50^{37} \bmod 77 = 8$ $K\,2 = 1^{37} \bmod 77 = 1$ $K\,3 = 12^{37} \bmod 77 = 12$ $K\,4 = 12^{37} \bmod 77 = 12$ $K\,5 = 64^{37} \bmod 77 = 15$
Alice ordnet den Zahlen Buchstaben zu (beginnend mit 1 = A).	8 = H, 1 = A, 12 = L, 12 = L, 15 = O

Hybride Verschlüsselung
Bei der hybriden Verschlüsselung wird ein symmetrischer Schlüssel über ein asymmetrisches Verfahren ausgetauscht. Damit wird das Problem des Schlüsselaustauschs umgangen. Außerdem wird hierbei das asymmetrische Verfahren nur für wenige Daten (den symmetrischen Schlüssel) verwendet, sodass der zusätzliche Zeitaufwand nicht ins Gewicht fällt.
Zum Schlüsselaustausch kommt oft das Diffie-Hellman-Verfahren zum Einsatz (vgl. Kapitel 3.3.3, Abschnitt [3]).

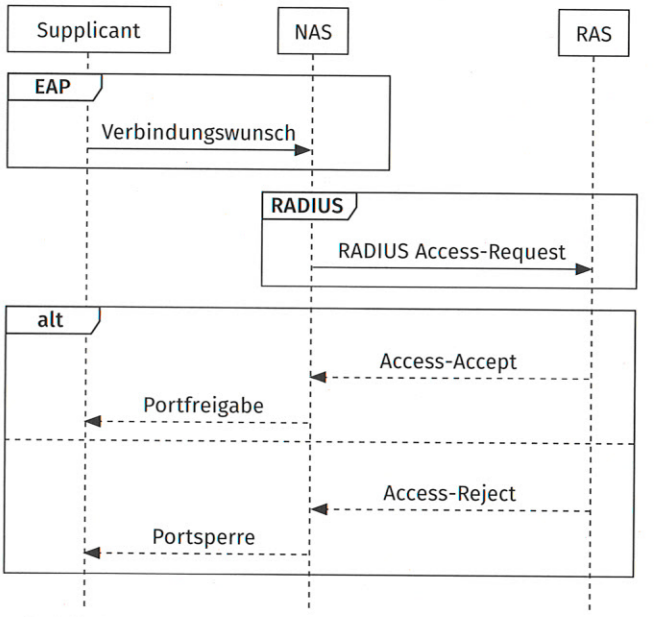
Bei der Arbeit mit Zertifikaten kommt ein asymmetrisches Verfahren zum Einsatz (siehe auch Kapitel 1.1.1, Abschnitt [7]). Für die Umsetzung des Schutzziels „Authentizität" im Unternehmensumfeld kann ein RADIUS-Server mit Zertifikaten eingesetzt werden, z. B. bei der Authentifizierung im WLAN.

Der **Remote Authentication Dial-In User Service (RADIUS)** bietet sogenanntes Triple-A an.

> **AAA (sprich: „Triple-A")**
>
> Die drei Buchstaben A stehen für „Authentication", „Authorization" und „Accounting". Die „Authentication" ist der Nachweis der richtigen Identität. Unter „Authorization" wird die Zuweisung von Rechten verstanden. „Accounting" umfasst die Protokollierung, welche Dienstleistungen verwendet werden.

Neben der Authentifizierung im WLAN kann RADIUS auch eingesetzt werden, um nur zugelassenen Geräten eine Verbindung über einen Switch-Port zu erlauben. Wenn ein Gerät nicht authentifiziert wird, wird der Switch-Port abgeschaltet.

Für ein solches Szenario gibt es bei IEEE 802.1X drei Rollen. Der Client, der sich authentifizieren möchte, wird **Supplicant** genannt. Der Switch, an dem der Client angeschlossen ist und der dem Client einen Port freigeben möchte, heißt **Network Access Server (NAS)** (bei WLAN in Verbindung mit IEEE 802.1X wird der AP „Authenticator" genannt). Der RADIUS-Server hat die Rolle des **Remote Authentication Servers (RAS)**.



Beispielhafter Nachrichtenaustausch bei RADIUS-Freigabe

Vor dem Austausch von Daten mit dem Netzwerk muss der Supplicant (z. B. ein Windows-Client) zunächst einen Verbindungswunsch an den NAS, im Beispiel den Switch, senden. Dabei kommt das Protokoll „Extensible Authentication Protocol" (EAP) zum Einsatz. Der NAS sendet die Daten an den RAS weiter. Der RAS kennt alle Supplicants und auch die entsprechenden Zertifikate der Zertifizierungsstellen. Mit dem NAS kommuniziert der RAS über das RADIUS-Protokoll. Diese Kommunikation ist über einen vorher geteilten Schlüssel gesichert. Der Administrator muss den Schlüssel im RAS und im NAS konfigurieren. Der RAS überprüft die Anfrage (RADIUS Access-Request) des Clients und kann sie erlauben (Access-Accept) oder ablehnen (Access-Reject). Entsprechend gibt der Switch den Port frei oder sperrt ihn.

(2) Planen einer Zertifizierungsstelle

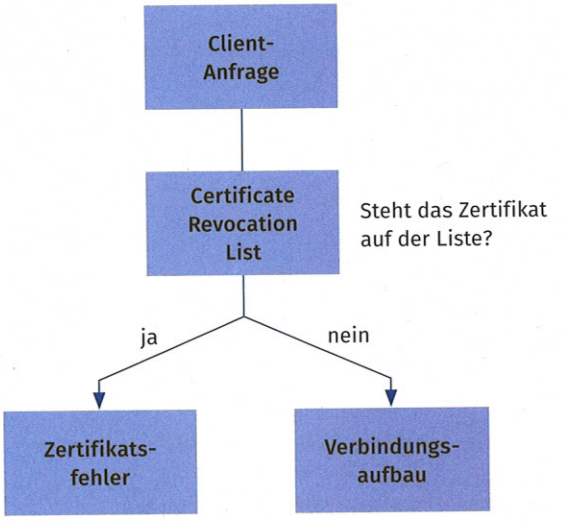
Vor der Planung der Zertifizierungsstelle müssen die Anforderungen an die Zertifikate und die Zertifizierungsstelle festgelegt werden. Die Rigudo GmbH möchte eine interne Zertifizierungsstelle installieren. Ziel ist es, eigene Geräte und gegebenenfalls Benutzer im Netzwerk zu authentifizieren. Außerdem soll eine WLAN-Anmeldung über Zertifikate möglich sein.

Bei der Planung der eigenen Zertifizierungsstelle (Certificate Authority, CA) muss zunächst die Entscheidung getroffen werden, ob eine öffentliche oder eine private Zertifizierungsstelle benötigt wird. Die Voraussetzungen sind hoch, eine öffentlich anerkannte Zertifizierungsstelle zu werden, z. B. für Web-Dienste. Ein Anwärter für eine öffentliche Zertifizierungsstelle muss einen Katalog von grundlegenden Anforderungen erfüllen. Dazu gehört beispielsweise die Planung der Authentifizierung der Zertifikatsanfragen, das Erstellen eines Planes, wie lange ein Zertifikat gültig ist oder wie es für ungültig erklärt werden kann. Es müssen aber beispielsweise auch physische Zutrittskontrollen nachgewiesen werden. Außerdem ist nachzuweisen, dass ein Konzept zur sicheren Entsorgung von Datenträgern vorliegt. Des Weiteren erfolgen regelmäßige Sicher-

heitsüberprüfungen. Über die Aufnahme einer Zertifizierungsstelle in die gängigen Browser (damit ein Zertifikat von gängigen Internet-Browsern als valide erkannt wird, siehe auch Kapitel 1.1.1), entscheidet das CA/Browser-Forum. Dieses Forum ist ein Zusammenschluss von Browser-Herstellern und Zertifizierungsstellen.

Für interne Anwendungen ist es in den allermeisten Fällen ausreichend, wenn eine interne, nicht öffentliche Zertifizierungsstelle verwendet wird.

Im nächsten Planungsschritt muss festgelegt werden, wie ein Zertifikat beantragt und ausgestellt werden kann und wie die Zertifikate zurückgerufen werden können.



Die Planung der **Certificate Revocation List (CRL)** wird beispielsweise nützlich, wenn Mitarbeiter das Unternehmen verlassen und das Benutzerzertifikat für ungültig erklärt werden soll. Die Planung einer entsprechenden Maßnahme (z. B. einer Gruppenrichtlinie), um Zertifikate unternehmensweit auszurollen, ist ebenfalls wichtig. Das Stammzertifikat der Zertifizierungsstelle muss auf alle beteiligten Systeme als vertrauenswürdiges Zertifikat verteilt werden. Außerdem muss festgelegt werden, wie lange ein Zertifikat gültig ist.

Die Installation einer internen, privaten Zertifizierungsstelle kann unter verschiedenen Betriebssystemen erfolgen. Eine solche Zertifizierungsstelle wird interne Zertifikate erstellen und signieren.

Die Rigudo GmbH möchte die Zertifizierungsstelle unter einem Windows-Server-Betriebssystem installieren. Als erster Punkt muss geklärt werden, ob ein separates System verwendet werden soll oder die Zertifizierungsstelle als zusätzliche Rolle auf den Domain Controller installiert werden kann.

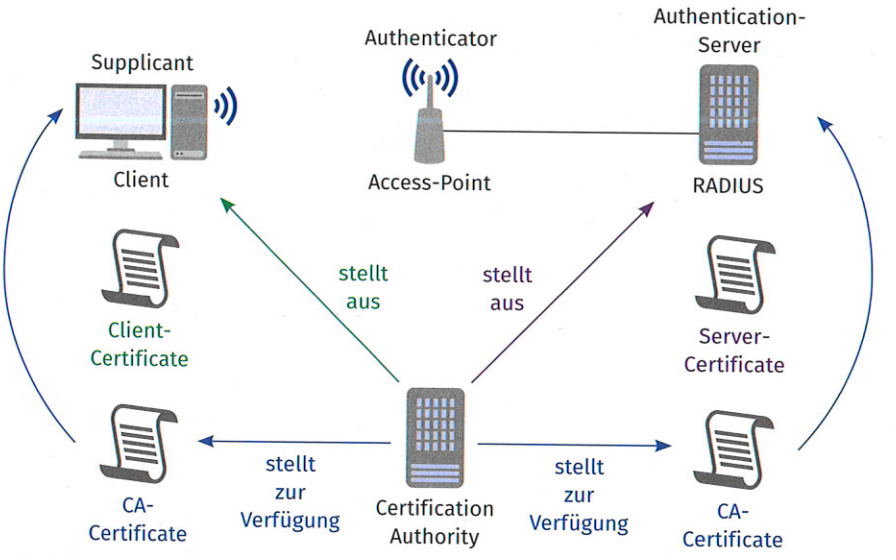
Gerade in kleineren Unternehmen bietet sich die zusätzliche Installation als Rolle auf dem Domain Controller an, da zusätzliche Hardwarekosten gespart werden und keine weiteren Lizenzen anfallen. Die Installation auf separater Hardware hat den Vorteil, dass gegebenenfalls Gruppenrichtlinien einfacher umzusetzen sind. Auch Backups und Updates sind beim dedizierten Einsatz eines Servers einfacher durchzuführen.

Neben der Konfigurationsplanung für einen Server, z. B. die IP-Adresse, muss sich für eine Art der Zertifizierungsstelle (Certification Authority, CA) entschieden werden. Bei einer **Enterprise CA** ist die Zertifizierungsstelle an ein Active Directory angebunden. Das hat den Vorteil, dass die Windows-Gruppenrichtlinien einfach verwendet werden können, um Zertifikate zu verteilen. Eine **Standalone CA** ist unabhängig vom Active-Directory-Dienst.

Außerdem ist zu planen, ob es sich bei der Zertifizierungsstelle um eine **Root CA** oder eine untergeordnete Stelle handelt. Eine Root CA hat keine übergeordnete Zertifizierungsstelle, während eine untergeordneten Zertifizierungsstelle (**Subordinate CA**) von einer übergeordneten Stelle die Erlaubnis hat, Zertifikate auszustellen. Ein untergeordnete Zertifizierungsstelle hat den Vorteil, dass alle Zertifikate für ungültig erklärt werden können, wenn z. B. der private Schlüssel der Zertifizierungsstelle ungewollt bekannt wird.

(3) Signatur-unterstütztes Login planen

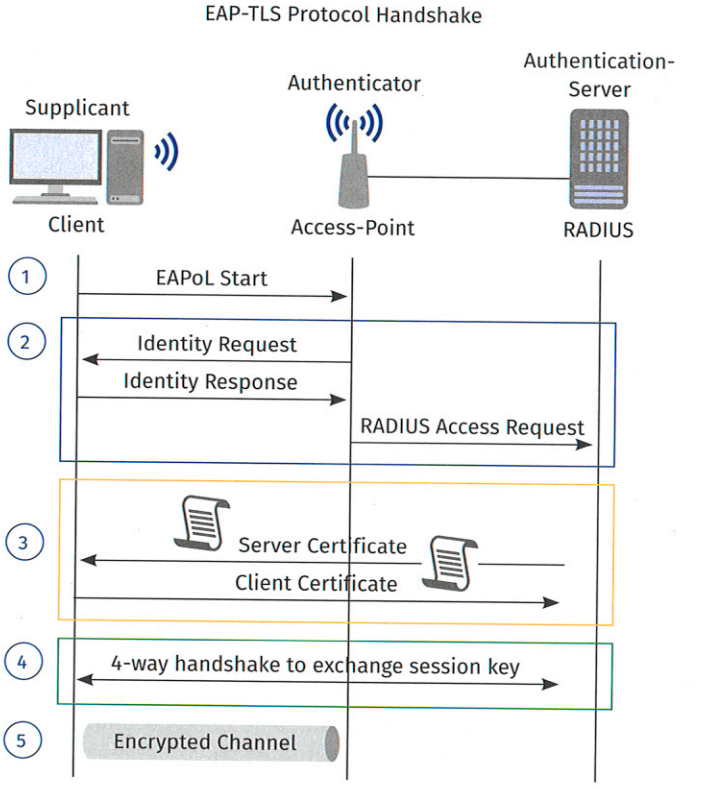
Zertifikatbasierte Authentifizierung (Certificate-based Authentification, CBA) ist eine passwortlose Anmeldung, die gegenüber passwortbasierten Anmeldungen sicherer ist. Schon länger wird die Methode im Zusammenhang mit der Anmeldung in WLAN oder LAN mithilfe von Port-Based Network Access Control (IEEE 802.1X) verwendet. Die Steuersoftware „Elster" oder die Anmeldung bei Cloud-Diensten wie Microsofts Azure sind weitere Beispiele für den Einsatz von zertifikatbasierter Authentifizierung.



Prinzip der zertifikatbasierten Authentifizierung im WLAN

Für Port-Based Network Access Control wird das Extensible Authentication Protocol (EAP) verwendet, das die Authentifizierung in den drei Varianten PAP, CHAP und TLS durchführt. Während bei den beiden ersten Varianten ein Pre-Shared Key verwendet wird, nutzt die TLS-Variante Zertifikate.

EAP-TLS wird aktuell im RFC 9190 beschrieben. Die Authentifizierung erfolgt mithilfe eines asymmetrischen Schlüsselpaars, wobei das Zertifikat den öffentlichen Schlüssel enthält, mit dessen Hilfe die digitale Signatur überprüft werden kann. Durch das Zertifikat wird eine Vertrauenskette aufgebaut, über die dann die rechtmäßige Identität (Authentizität) des Zertifikatsinhabers überprüft werden kann. Über den privaten Schlüssel muss der Zertifikatsinhaber beweisen, dass das Zertifikat ihm gehört.



Protokollablauf einer zertifikatbasierten Authentifizierung

Als Beispiel für eine zertifikatsbasierte Anmeldung in einem WLAN werden die drei Komponenten WLAN-Client (Supplicant), Access-Point (Authenticator) und RADIUS-Server (Authentication-Server) verwendet. In einem Firmenumfeld wird eine eigene CA genutzt, die Zertifikate zur Verfügung stellt. Um Zertifikate der CA zu überprüfen, muss das Zertifikat der CA (CA-Certificate) auf allen nötigen Geräten vorhanden sein.

① Im ersten Schritt verbindet sich der WLAN-Client mit dem Access-Point und sendet mit dem EAPoL-Start die Information, gemäß EAP eine Authentifizierung durchführen zu wollen.

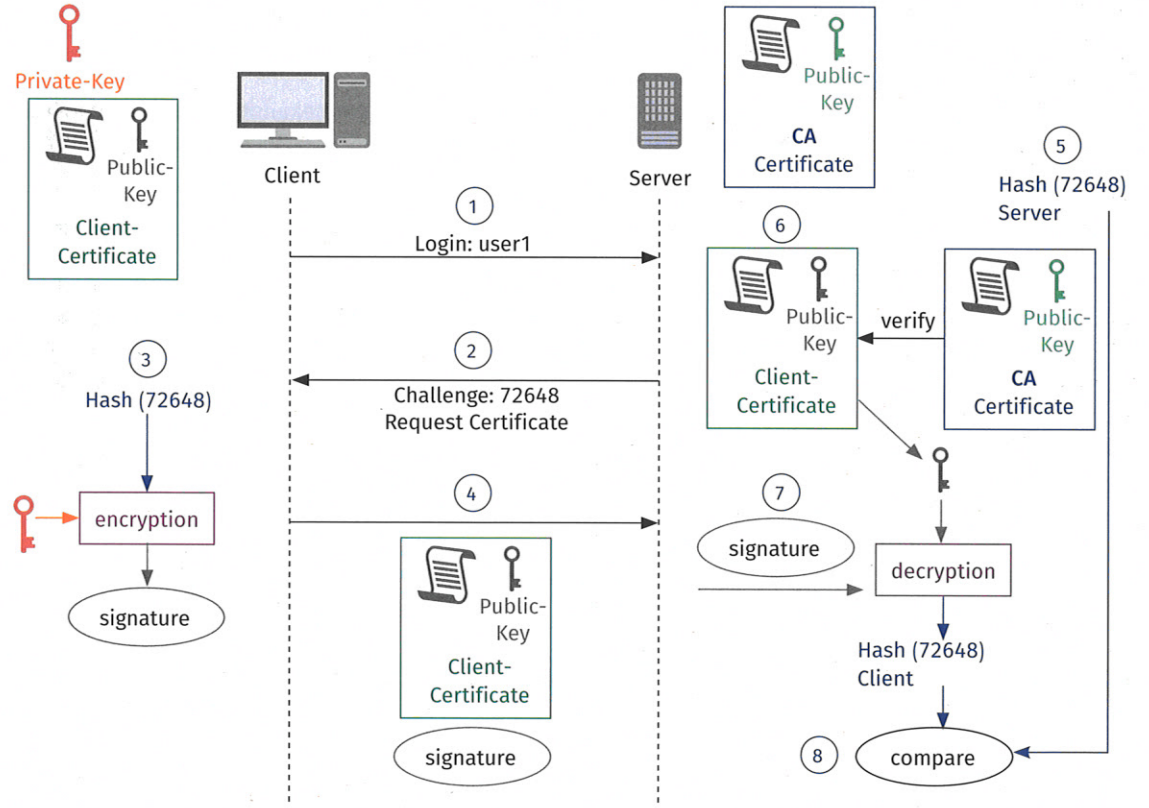
② Im zweiten Schritt ermittelt der Access-Point die Identität des Clients. Nach der Antwort des Clients holt der Access-Point beim RADIUS-Server eine Zugriffsanfrage (Access-Request) ein und der RADIUS startet mit dem Client den eigentlichen Authentifizierungsprozess.

③ Bei dem eigentlichen Authentifizierungsprozess sendet der Server sein Zertifikat an den Client, was dieser mit dem hinterlegten Zertifikat der CA überprüft. Ist das Serverzertifikat überprüft, sendet der Client sein Zertifikat an den Server, was dieser wiederum mit dem hinterlegten CA-Zertifikat überprüft. Nach gegenseitiger Überprüfung der Zertifikate ist die Authentifizierungsphase abgeschlossen.

④ Im vierten Schritt wird mithilfe eines 4-Wege-Handshakes ein Session-Schlüssel erstellt, der für die Transportverschlüsselung verwendet wird.

⑤ Im letzten Schritt wird die verschlüsselte Verbindung aufgebaut und der Client erhält Zugriff auf das über das WLAN angeschlossene Netzwerk.

Mit der Überprüfung eines Zertifikats wird festgestellt, dass die im Zertifikat enthaltenen Daten, z. B. der öffentliche Schlüssel, dem im Zertifikat genannten Inhaber gehören. Voraussetzung für die vertrauensvolle Überprüfung ist, dass ein Vertrauen des Clients gegenüber der Zertifizierungsstelle besteht. Die Überprüfung stellt jedoch noch nicht sicher, dass das Zertifikat auch vom eigentlichen Zertifikatsinhaber gesendet wurde. Ein Zertifikat ist kein geheimes Dokument, was besonders geschützt auf einem Rechner gespeichert ist. Daher wird im Zusammenhang mit Public-Key-Zertifikaten eine sogenannte Challenge-Response durchgeführt. Der Ablauf ist in der folgenden Abbildung dargestellt.



Ablauf einer Challenge-Response zum Login per Zertifikat

Ausgangssituation ist, dass der Client ein Zertifikat mit dem öffentlichen Schlüssel hat. Der hierzu passende private Schlüssel wird auf dem Client gespeichert. Der Server hat von der Zertifizierungsstelle (CA) ein Zertifikat, von der der Client sein Zertifikat ausgestellt bekommen hat.

Der Ablauf in den Schritten 1 bis 8 ist vereinfacht dargestellt, um die eigentliche Authentifizierung zu erklären. So ist beispielsweise die Einigung auf ein bestimmtes Hash-Verfahren und einen Signaturalgorithmus hier ausgespart. Für das Diagramm wird davon ausgegangen, dass Server und Client sich auf ein

gemeinsames Verfahren per Protokoll verständigt haben. Auch weitere Absicherungen sind nicht beschrieben, z. B. gegenüber Man-in-the-Middle-Angriffen oder Mitlesen des Protokollablaufs.

① Der Client sendet eine Login-Anfrage mit dem Benutzernamen „user1" an den Server.
② Der Server sendet dem Client eine Zufallszahl als „Challenge", diese wird auch als „nonce" bezeichnet. In der Antwort sendet er auch die Anfrage für das Client-Zertifikat.
③ Der Client bildet mit der gemeinsam festgelegten Hash-Funktion einen Hash-Wert und verschlüsselt diesen Hash-Wert mit dem privaten Schlüssel. Der verschlüsselte Hash-Wert ist die Signatur der Challenge.
④ Als Antwort sendet der Client die Signatur und das Client-Zertifikat an den Server.
⑤ Der Server bildet ebenfalls von der erzeugten Challenge einen Hash-Wert.
⑥ Das im Schritt 4 empfangene Client-Zertifikat überprüft der Server mithilfe des hinterlegten CA-Zertifikats.
⑦ Aus dem Client-Zertifikat entnimmt der Server den öffentlichen Schlüssel des Clients und entschlüsselt damit die Signatur, die im vierten Schritt vom Client gesendet wurde. Als Ergebnis erhält er den vom Client gebildeten Hash-Wert.
⑧ Der Client-Hash-Wert wird mit dem vom Server errechneten Hash-Wert verglichen. Stimmen beide überein, muss der Client im Besitz des privaten Schlüssels zu dem zugehörigen öffentlichen Schlüssel des Client-Zertifikats sein, dessen Inhaber durch die Zertifizierungsstelle bestätigt wurde.

(4) Multi-Faktor-Authentifizierung planen

Passwortlose Anmeldung mit WebAuthn

Passwortbasierte Anmeldeverfahren haben die Schwäche, dass mit einem bekannten Passwort von jeder erreichbaren Stelle ein Zugriff auf ein System möglich ist. Erwünscht ist dieser Zugriff allerdings nur beim Eigentümer des entsprechenden Benutzerkontos.

Da ein herkömmliches Passwort an keinen Ort gebunden ist, wie es beispielsweise ein physikalischer Schlüssel für eine Tür ist, sind Passwörter ein lohnendes Ziel, um unerlaubten Zugriff auf Benutzerkonten zu erhalten. Seit 2019 existiert der FIDO2-Standard (Fast IDentity Online), der eine passwortlose Anmeldung an Systemen ermöglicht. Analog zu einem physikalischen Schlüssel für eine Tür, basiert das System auf einem Authenticator, der z. B. in einen USB-Stick implementiert ist. Kernkomponenten neben dem Authenticator sind CTAP2 und WebAuthn.

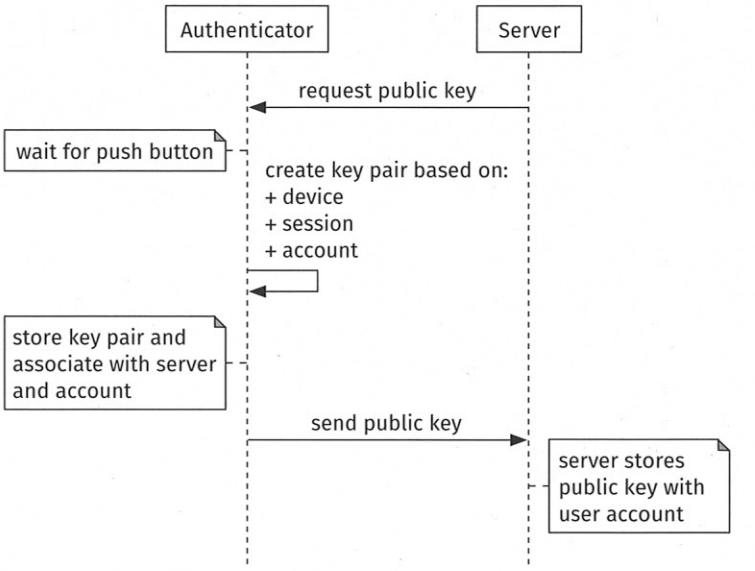


Kernkomponenten des FIDO2-Standards

Kernkomponenten einer passwortlosen Anmeldung	
CTAP2	Client-To-Authenticator-Protocol 2 stellt die Verbindung zwischen dem Authenticator und dem benutzten Client her, z. B. ein Computer, Smartphone oder Tablet.
WebAuthn	Mithilfe von WebAuthn wird die Verbindung hergestellt zwischen dem Client und dem Server, der einen Dienst zur Verfügung stellt und auf dem sich der Benutzer anmelden will.
FIDO-Allianz	Die nicht kommerzielle FIDO-Allianz wurde 2012 von Lenovo, PayPal, Infineon, Nok Nok Labs, Validity Sensors und Agnitio gegründet. Google, NXP und Yubico stießen ein Jahr später hinzu. Ziel der Allianz ist es, offene und lizenzfreie Industriestandards für die Authentifizierung im Internet zu entwickeln.

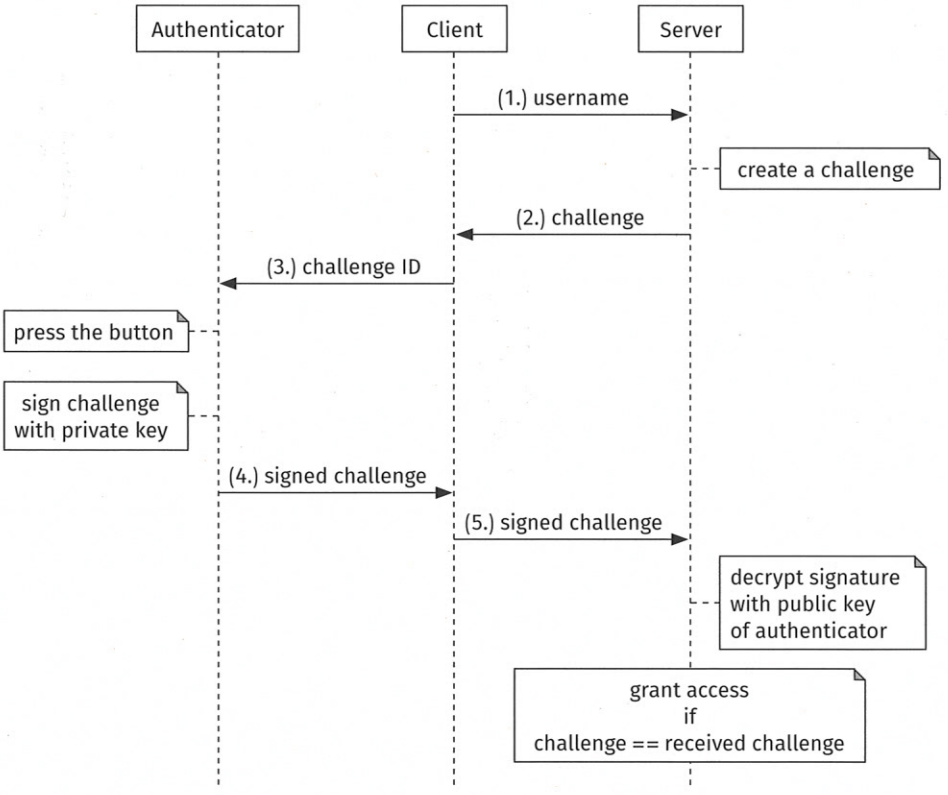
Registrierung eines Gerätes
Im ersten Schritt muss der Authenticator ein Schlüsselpaar für den Dienst erzeugen, gegenüber dem er sich authentifizieren soll. Dies geschieht basierend auf dem Konto bei dem Server. Der öffentliche Schlüssel wird dann zum Server gesendet und dort hinterlegt. Der private Schlüssel wird im Authenticator gespeichert.

Das nebenstehende Sequenzdiagramm beschreibt die Registrierung des Authenticators mit einem Server.



FIDO2-Registrierung eines Gerätes

Anmeldung ohne Passwort
Der Anmeldeprozess ist ein **Challenge-Response-Verfahren** und wird im folgenden Sequenzdiagramm beschrieben.



Anmeldung ohne Passwort

Ein Benutzer möchte sich auf einem Server anmelden und gibt dazu den Kontonamen im Client ein, der daraufhin zum Server gesendet wird. Der Server erstellt eine Challenge, eine zufällige Zahl, die er zum Client sendet. Dieser leitet sie zusammen mit einer Zugangs-ID weiter zum Authenticator.

Der Authenticator verschlüsselt die Challenge mit seinem privaten Schlüssel. Die entstandene Chiffre wird zum Server gesendet. Der Server entschlüsselt die Chiffre mit dem öffentlichen Schlüssel des Authenticators und vergleicht das Ergebnis mit der erzeugten Challenge. Wenn beide gleich sind, ist der Client mit dem Authenticator verbunden, von dem der Server den öffentlichen Schlüssel bekommen hat.

Die Sicherheit des Verfahrens beruht auf dem Konzept, dass der private Schlüssel nie den Authenticator verlässt. Dadurch reduziert sich ein Angriff auf den physischen Zugriff auf den Authenticator.

Zwei-Faktor-Authentifizierung (2FA)
Die Zwei-Faktor-, manchmal auch Mehrfaktor-Authentifizierung beschreibt ein Anmeldeverfahren, bei dem mehrere „Geheimnisse" für die erfolgreiche Authentifizierung eingegeben werden müssen. Dabei unterliegt jeder Faktor einer anderen Technologie. In der Regel ist der erste Faktor das zu einem Benutzerkonto erstellte Passwort. Für den zweiten Faktor können dann u. a. folgende Technologien genutzt werden:

- Pushnachricht oder E-Mail gesendeter Code
- Timed-One-Time-Password (TOTP)
- Hardware-Token

Technologien für die Multi-Faktor-Authentifizierung	
Pushnachricht, E-Mail	Nach der Anmeldung mit Benutzername und Passwort sendet der Authentifizierungsserver per Pushnachricht, E-Mail oder über einen anderen Kanal einen Code, der als zweiter Faktor für die Anmeldung eingegeben werden muss.
Timed-One-Time-Password	Häufig mit einer Authenticator-App verwendet, erfordert die App eine initiale Synchronisation mit dem Authentifizierungsserver. Wenn die App mit dem Server synchronisiert ist, erzeugen Server und App über den synchronisierten Algorithmus für den Benutzernamen zeitlich begrenzt die gleichen Passwörter. Nach der Anmeldung mit dem Passwort erwartet der Authentifizierungsserver die Eingabe des zeitlich begrenzten Codes, den die Authenticator-App erzeugt. Der Server vergleicht diesen mit dem selbst erzeugten Code. In der Regel wechselt der Code jede Minute.
Hardware-Token	Hier kommen verschiedene Technologien zum Einsatz. Der zuvor beschriebene FIDO2-Authenticator ist ein solcher Hardware-Token. Ein weiterer ist der vom Onlinebanking bekannte SmartTAN-Generator. Der Server erzeugt einen Code, der in den Generator eingegeben wird. Im Zusammenhang mit der Bankkarte erzeugt dieser eine Transaktionsnummer, die für die Überweisung eingegeben werden muss.

Für besondere Anforderungen an die Sicherheit können weitere Faktoren hinzugefügt werden, was eine Zwei-Faktor- zu einer Mehrfaktor-Authentifizierung macht.

Kompetenzcheck

1. Beschreiben Sie, auf welche Weise die hybride Verschlüsselung die Vorteile der symmetrischen und der asymmetrischen Verschlüsselung verwendet.

2. Erklären Sie, was man unter AAA (Triple-A) bei einem AAA-System versteht.

3. Mittels CRL lässt sich ein Zertifikat für ungültig erklären. Beschreiben Sie den Zeitpunkt, zu dem die CRL überprüft wird.

4. Erklären Sie, warum man bei der Authentifizierung mit Zertifikat sicher sein kann, dass der Nachweis der Authentizität erbracht ist, wenn beide Hash-Werte beim Vergleich für den Server identisch sind.

5. Sammeln Sie in der Gruppe Beispiele für einen zweiten Faktor bei der Zwei-Faktor-Authentifizierung (2FA).

6. Notieren Sie wesentliche Aspekte aus diesem Abschnitt in Ihrem Projektjournal.

7. Bearbeiten Sie Aufgabe 6 der Lernsituation 3 im Arbeitsbuch.

A6

3.4 Maßnahmen zur Erhöhung der Sicherheit vernetzter Systeme umsetzen

S Sie sollen verschiedene Maßnahmen zur Erhöhung der Sicherheit in vernetzten Systemen unter Beachtung betrieblicher Sicherheitsrichtlinien implementieren.

Im letzten Kapitel wurden Maßnahmen zur Erhöhung der Sicherheit in vernetzten Systemen theoretisch besprochen und einige Besonderheiten beschrieben. In diesem Kapitel soll es nun um die Implementierung und Durchführung verschiedener Maßnahmen gehen. Beschreibungen zu verschiedenen Installationen sollen helfen, verschiedene Programme und Werkzeuge sinnvoll einsetzen zu können.

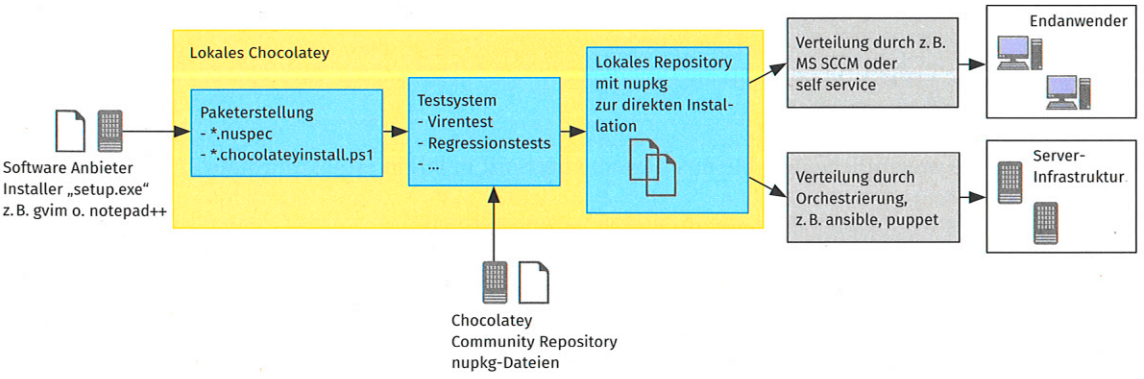
Hinweis: Alle aufgeführten Techniken sollten getestet werden. Dazu können beispielsweise virtuelle Maschinen oder Container verwendet werden. Dies bietet den Vorteil, dass man auf einfache Art und Weise Techniken und Software ausprobieren kann. Falls in Ihrem Betrieb noch kein Testlabor vorhanden ist, ist es sinnvoll, eine Testumgebung anzulegen. In einer solchen Umgebung lassen sich viele Szenarien abbilden, z. B. die Installation eines Load Balancers oder die Verwendung der Paketverteilungsplattform „Chocolatey".

Die in diesem Kapitel verwendeten Programme sollen beispielhaft für eine mittlerweile immense Anzahl an Software stehen. Die hier eingesetzte Software wurde nach Aspekten wie Verfügbarkeit und Marktdurchdringung ausgewählt.

3.4.1 Softwareaktualisierung bei Clients umsetzen

S Sie sollen die Aktualität der Softwareinstallationen auf Clients planen.

Die Lösung „Windows Store for Business" von Microsoft wird voraussichtlich in eine offenere Plattform überführt. Zur sicheren Softwareverteilung kann auch für Windows ein eigenes Repository aufgesetzt werden. Dies soll hier exemplarisch mit der Paketverteilungsplattform „Chocolatey" gezeigt werden (andere mögliche Verteilungsplattformen wären z. B. Google Play Store oder Apple iOS App Store). Es handelt sich um einen quelloffenen Ansatz, der sich leicht in gängige Orchestrierungssysteme (z. B. Ansible) einbinden lässt. Chocolatey gibt es in einer eigenen Business-Version, die lizenzpflichtig und auf große Unternehmen ausgelegt ist. Hier wird zu Testzwecken die sogenannte Community-Version in Form einer vorgefertigten virtuellen Maschine auf einem Linux-Server genutzt.

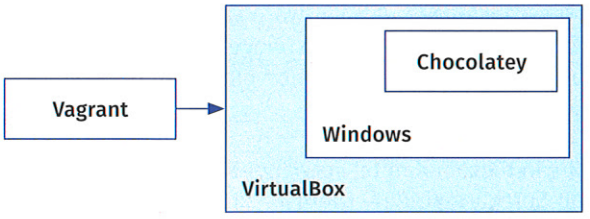


Chocolatey-Systemaufbau mit lokalem Repository

Die Installation lässt sich in folgende Schritte unterteilen:
- Virtualisierungsumgebung in Betrieb nehmen
- Installation des Chocolatey-Servers (CIFS-Freigabe ohne Gallery)
- Repository erstellen
- Paket erstellen (pack) und in Repository einfügen (push)
- Installation des neuen Pakets auf Client

(1) Virtualisierungsumgebung in Betrieb nehmen

Für die Installation der Virtualisierungsumgebung werden folgende Pakete benötigt:
- virtualbox
- virtualbox-guest-additions-iso
- vagrant (inklusive Plugins: winrm, winrm-fs, winrm-elevated),
- Git-Repository „chocolatey-test-environment".



Die einzelnen Installationsschritte werden im Folgenden erklärt.

Neueste Version von VirtualBox installieren

```
wget -q https://www.virtualbox.org/download/oracle_vbox_2016.asc -O- |
sudo apt-key add -
wget -q https://www.virtualbox.org/download/oracle_vbox.asc -O- |
sudo apt-key add -
sudo apt-get install virtualbox virtualbox-guest-additions-iso
sudo apt-get --reinstall install virtualbox-dkms
```

Neueste Version von Vagrant installieren

```
wget -O- https://apt.releases.hashicorp.com/gpg | gpg --dearmor | sudo tee
/usr/share/keyrings/hashicorp-archive-keyring.gpg

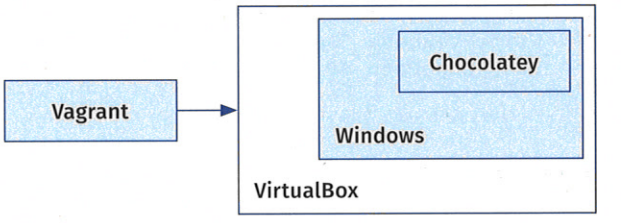
echo „deb [signed-by=/usr/share/keyrings/hashicorp-archive-keyring.gpg]
https://apt.releases.hashicorp.com $(lsb_release -cs) main“ | sudo tee /
etc/apt/sources.list.d/hashicorp.list

sudo apt update && sudo apt install vagrant

vagrant plugin install winrm
vagrant plugin install winrm-fs
vagrant plugin install winrm-elevated
```

(2) Installation des Chocolatey-Servers

Das Chocolatey-Testsystem wird zunächst heruntergeladen. Anschließend wird mit Vagrant die virtuelle Maschine (VM) mit lauffähigem Windows-Betriebssystem gestartet. Der Start kann einige Zeit in Anspruch nehmen, da im Git-Repository lediglich die Softwarekomponenten definiert werden. Vagrant lädt diese während des ersten Starts aus dem Internet herunter.




```
git clone https://github.com/chocolatey-community/chocolatey-test-
environment.git
```

In der Datei „Vagrantfile“ können bei Bedarf der Benutzername und das Passwort für die virtuelle Maschine geändert werden. Im Auslieferungszustand lautet beides „vagrant“ und sollte für eine Produktivumgebung auf jeden Fall geändert werden.

```
vagrant up
```

Um die virtuelle Maschine von einem weiteren Windows-Rechner erreichen zu können, muss die Netzwerkschnittstelle auf „Netzwerkbrücke“ konfiguriert werden. Weiterhin verhindert die Windows-Firewall Verbindungen von außen. Die virtuelle Maschine kann auch per „ssh/scp“ angesprochen werden, allerdings wird ein zusätzlicher Parameter für „ssh-dss“ benötigt, da die vorgegebene VM mit diesem veralteten Verfahren arbeitet:

```
ssh -oHostKeyAlgorithms=+ssh-dss vagrant@192.168.0.48
```

Für ein System in einer Produktivumgebung sollte hier auf RSA-Schlüssel umgestellt werden.

(3) Repository erstellen

In der neuen virtuellen Maschine wird nun mit einem PowerShell-Skript von Chocolatey (https://docs.chocolatey.org/en-us/guides/organizations/set-up-chocolatey-server) ein einfacher IIS-Server als Frontend für das Chocolatey-Repository installiert (siehe Auszug unten). Dieser Server ist in der Lage, die nupkg-Dateien direkt zu verarbeiten und daraus ein einfaches Repository aufzubauen.

„nupkg“ ist das Standarddateiformat von Chocolatey. Es handelt sich dabei um ein im NuSpec-Format komprimiertes ZIP-Archiv mit zusätzlichen Metainformationen.

Die Variable „$sitePath“ bestimmt den Pfad, unter dem der HTTP-Server seine Daten ablegt. Die eigentlichen Pakete werden im Unterordner „c:\tools\chocolatey.server\App_Data\Packages\“ abgelegt.

```
$siteName = 'ChocolateyServer'
$appPoolName = 'ChocolateyServerAppPool'
$sitePath = 'c:\tools\chocolatey.server'

function Add-Acl {
 [CmdletBinding()]
 Param (
   [string]$Path,
   [System.Security.AccessControl.FileSystemAccessRule]$AceObject
 )
 Write-Verbose "Retrieving existing ACL from $Path"
 $objACL = Get-ACL -Path $Path
 $objACL.AddAccessRule($AceObject)
 Write-Verbose "Setting ACL on $Path"
 Set-ACL -Path $Path -AclObject $objACL
}

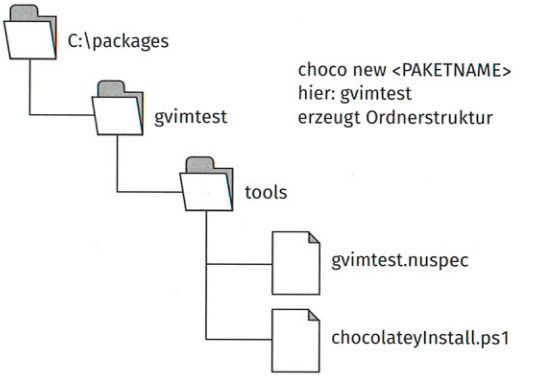
 [...]
```

(4) Paket erstellen (pack) und in Repository einfügen (push)

Sobald der Chocolatey-Server einsatzfähig ist, kann dieser genutzt werden, um die ersten Software-Pakete zu erstellen. Exemplarisch wird hier der Editor „gvim“ verwendet. Dazu wechselt man in den Ordner „C:\packages“ und führt dort den Befehl „choco new <PAKETNAME>“ (z. B. gvimtest) aus. Bei einer SSH-Verbindung muss der Schalter „-oHostKeyAlgorithms=+ssh-dss“ genutzt werden.

```
ssh -oHostKeyAlgorithms=+ssh-dss vagrant@192.168.0.48
cd C:\package
choco new gvimtest
```

Der Befehl „new“ erzeugt einen Unterordner „gvimtest“ und einige Konfigurationsdateien sowie die eigentlichen Installations- und Deinstallationsskripte. Diese sind nach der Erzeugung zunächst mit Standardwerten befüllt und müssen im Anschluss an die zu installierende Software angepasst werden.



Die beiden Dateien „gvimtest.nuspec“ und die Datei „chocolateyInstall.ps1“ befinden sich im Unterordner „tools“. Der minimale Inhalt dieser Dateien sieht wie folgt aus:

```
# gvimtest.nuspec

<?xml version="1.0" encoding="utf-8"?>
<package xmlns="http://schemas.microsoft.com/packaging/2015/06/nuspec.
xsd">
 <metadata>
   <id>gvimtest</id>
   <version>1.0</version>
   <title>gvim (Install)</title>
   <authors>Richard W.</authors>
   <description>gvim Testpaket</description>
 </metadata>
 <files>
   <!-- this section controls what actually gets packaged into the
   Chocolatey package -->
   <file src="tools\**" target="tools" />
 </files>
</package>
```

```
# chocolateyInstall.ps1

$ErrorActionPreference = 'Stop'; # stop on all errors

$packageName = 'gvimtest'
$toolsDir = "$(Split-Path -parent $MyInvocation.MyCommand.Definition)"
$fileLocation = Join-Path $toolsDir 'gvim_9.0.0643_x64.exe'

$packageArgs = @{
   packageName = $packageName
   fileType = 'exe' #only one of these: exe, msi, msu
   file = $fileLocation

   softwareName = 'gvimtest' #part or all of the Display Name as you
 see it in Programs and Features. It should be enough to be unique

   # MSI
   silentArgs = "/S"
   validExitCodes= @(0)

}

Install-ChocolateyPackage @packageArgs
```

Die Variable „$fileLocation“ richtet sich nach der eigentlichen Installationsdatei (hier: „gvim_9.0.0643_x64.exe“). Diese Datei wird vom entsprechenden Anbieter heruntergeladen und ebenfalls im Unterordner „tools“ abgelegt. Die eigentliche Installationsdatei kann z. B. per „wget“ in den Ordner „tools“ heruntergeladen werden.

```
wget https://github.com/vim/vim-win32-installer/releases/download/v9.0.0643/gvim_9.0.0643_
x64.exe
```

Im Anschluss wird mit dem Befehl „choco pack“ das eigentliche Installationspaket für das Chocolatey-Repository generiert. Bei diesem Vorgang wird eine neue Datei mit der Endung „*.nupkg“ erzeugt. Diese Datei ist ein sogenanntes Nu-Archive und enthält alle notwendigen Daten für den Chocolatey-Server. Damit der Server diese Datei anbieten kann, muss sie ihm bekannt gemacht werden. Das geschieht entweder mit dem Befehl „choco push gvimtest.1.0.nupkg --source="<SERVER_ADRESSE>"“ oder durch Kopieren der nupkg-Datei in den Ordner „C:\tools\chocolatey.server\App_Data\Packages\gvimtest.1.0.nupkg“.

(5) Installation des neuen Pakets auf dem Client

Auf dem Client muss zunächst Chocolatey selbst installiert werden. Dies kann in einer PowerShell mit Administratoren-Rechten erfolgen.

```
Set-ExecutionPolicy Bypass -Scope Process -Force;
[System.Net.ServicePointManager]::SecurityProtocol =
[System.Net.ServicePointManager]::SecurityProtocol -bor 3072;
iex ((New-Object System.Net.WebClient).
DownloadString('https://community.chocolatey.org/install.ps1'))
```

Der Chocolatey-Client wird konsequenterweise ebenfalls über ein Nupkg-Paket installiert, daher gibt es keine Installationsdatei. Im Anschluss muss wie bei einem Linux-System das selbst erstellte Repository in die Quellenliste des Clients eingetragen werden. Damit nur das lokale Repository verwendet wird, wird zusätzlich das öffentliche Repository deaktiviert. Würde man diesen Schritt nicht durchführen, so würde auch das öffentliche Repository nach der gewünschten Software durchsucht und das Paket von dort installiert.

```
choco source list
#Ausgabe
 Chocolatey v1.1.0
chocolatey - https://community.chocolatey.org/api/v2/ | Priority 0|Bypass
Proxy - False|Self-Service - False|Admin Only - False.

# öffentliches Repository "chocolatey" deaktiveren
choco source disable --name=chocolatey

# neues Repository unter dem Namen "myChocolateyServer" hinzufügen
choco source add --name="myChocolateyServer"--
source="http://192.168.0.48/chocolatey"
```

Die Installation des erstellten Softwarepakets „gvimtest“ auf dem Client kann mit dem Befehl „choco install gvimtest“ durchgeführt werden.

Sofern das Repository nur wenig Pakete enthält, können mit dem Befehl „choco list“ alle verfügbaren Pakete eines lokalen Repositorys angezeigt werden. Für größere oder öffentliche Repositories sollte der Befehl „choco find <PAKETNAME>“ genutzt werden. Hier kann auch * als Wildcard beliebige Zeichen des Paketnamens ersetzen.

```
choco find gvim*
#Ausgabe
gvimtest 1.0
```

Um das Paket zu installieren, wird der Befehl „choco install <PAKETNAME>“ verwendet. Zur Deinstallation wird der Befehl „choco uninstall <PAKETNAME>“ verwendet. Damit der Deinstallationsvorgang ohne Dialog verläuft, kann im Skript „chocolateyuninstall.ps1“ der entsprechende Silent-Schalter in der Variable „$silentArgs“ gesetzt werden. Dies ist allerdings von der zu installierenden Software abhängig.

Kompetenzcheck ✓

1. Das Softwarepaket „software.exe“ soll in ein Chocolatey-Repository eingepflegt werden. Beschreiben Sie die notwendigen Schritte, die hierzu durchgeführt werden.
2. Notieren Sie wesentliche Aspekte aus diesem Abschnitt in Ihrem Projektjournal.
3. Bearbeiten Sie Aufgabe 1 der Lernsituation 4 im Arbeitsbuch.

A1

3.4.2 Zugriffsmöglichkeit auf vernetzte Systeme im lokalen Netz umsetzen

S **Sie sollen den Zugriff auf vernetzte Systeme im lokalen Netz mit ausgewählten Techniken umsetzen.**

(1) VLAN implementieren

Entsprechend der Planung in Kapitel 3.3.2 sollen nun die Anforderungen der Rigudo GmbH umgesetzt werden. Die Mitarbeiter der jeweiligen Gruppe dürfen nur auf die vorgesehenen Server zugreifen. Die Administratoren dürfen über ein eigenes VLAN 100 auf alle Endgeräte, Server und Netzelemente zugreifen.

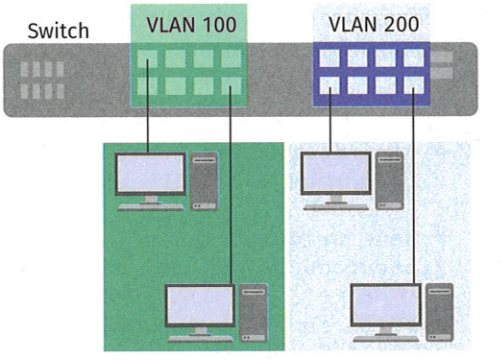
Bei reinen portbasierten VLAN-Zuordnungen kann es leicht zu Fehlern kommen, die Sicherheitsrisiken darstellen.

Im oberen Beispiel der Abbildung können die PCs im grünen Bereich nicht mit den PCs im blauen Bereich kommunizieren, obwohl sie am gleichen Switch angeschlossen sind.

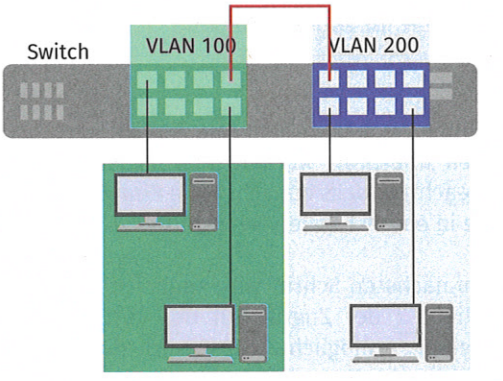
Im unteren Beispiel ist durch die neue Verbindung eine Kommunikation zwischen allen PCs möglich. Hierdurch können unter Umständen Sicherheitslücken entstehen, weil Zugriffe auf eigentlich abgeschottete Systeme möglich sind.

Eine VLAN-Installation sollte daher systematisch und schrittweise erfolgen, damit die Teilschritte besser überprüfbar werden. Darüber hinaus sollten die einzelnen Zugänge gut dokumentiert werden.

Im Folgenden wird die Konfiguration für den GitLab-Server und Clients in der Entwicklung (VLAN 200) sowie der Abteilung Kundenlösungen (VLAN 300) dargestellt.



Getrennte Bereiche



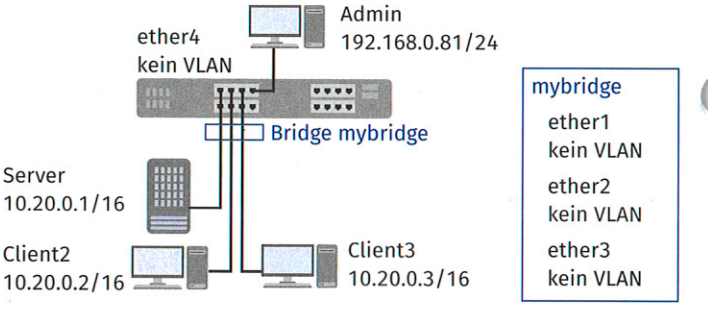
Ungewollte Verbindung durch portbasierte VLANs

Hinweis: Die Umsetzung wird konkret für MikroTik RouterOS exemplarisch durchgeführt. Die Vorgehensweise ist auf Netzgeräten anderer Hersteller in ähnlicher Weise vorzunehmen.

Umsetzung beispielhaft mit MikroTik RouterOS

Geräte mit dem Betriebssystem MikroTik RouterOS haben im Vergleich zu anderen Betriebssystemen, wie z. B. Cisco IOS, eine Besonderheit hinsichtlich der Port-Verwaltung. Da die Geräte sehr viele Funktionen zur Verfügung stellen, werden die Ports nach einem Konfigurations-Reset grundsätzlich voneinander getrennt. Es findet also keine Kommunikation zwischen den Ports statt, wenn diese nicht explizit zu „Bridges" (in der MikroTik-Namensgebung so bezeichnet, es handelt sich hierbei um eine Switch-Funktionalität) zusammengeschaltet werden. Bei vielen Anwendungen ist diese Ausgangslage hilfreich. Es wird demnach zunächst eine neue Bridge „mybridge" angelegt. Weiterhin sollte ein Port zu Konfigurationszwecken genutzt werden, wenn nicht direkt über die serielle Schnittstelle konfiguriert wird. Auf dieser Konfigurationsschnittstelle sollten keine VLANs eingerichtet werden, um die Erreichbarkeit zu gewährleisten. Im Beispiel ist dies Port „ether4".

Zunächst werden die Ports so konfiguriert, dass eine grundsätzliche Erreichbarkeit gewährleistet ist. Bisher sind keine VLANs konfiguriert. Beide Client-Systeme können untereinander kommunizieren und auf den Server zugreifen.
Durch eine VLAN-Konfiguration sollen beide Clients weiterhin auf den Server zugreifen, aber nicht mehr untereinander kommunizieren können.



Netzwerkplan ohne VLAN

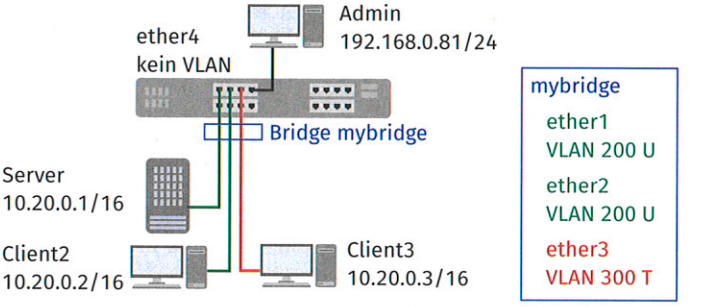
```
# Administrativer Zugang zu Konfiguration
/ip address add address=192.168.0.81/24 interface=ether4

# Neue Bridge anlegen
/interface bridge add name=mybridge

# Ports zu einer Bridge verbinden; MikroTik-spezifisch
/interface bridge port
add bridge=mybridge interface=ether1
add bridge=mybridge interface=ether2
add bridge=mybridge interface=ether3
```

Durch Ping-Tests kann die Erreichbarkeit überprüft werden. Hierbei ist zu beachten, dass zunächst alle Endgeräte in einem lokalen Netz sind.

Im nächsten Schritt wird zunächst nur Client 2 der Zugriff auf den GitLab-Server ermöglicht. Dies wird durch getrennte VLANs für Client 2 und den Server (VLAN-ID 200) sowie Client 3 mit VLAN-ID 300 umgesetzt. Der Server selbst arbeitet in dieser Konstellation noch „untagged".



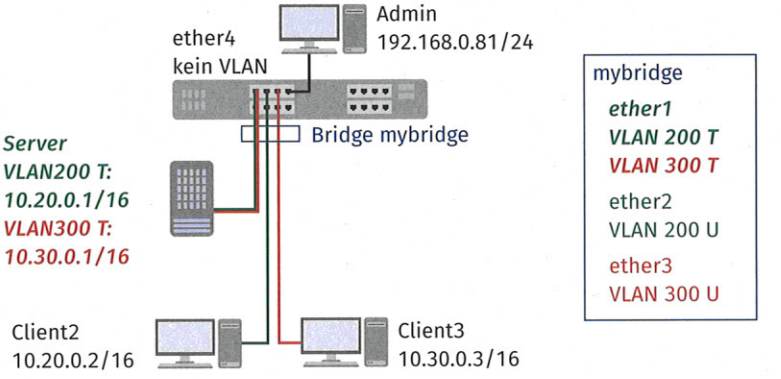
Server mit Client 2 in einem VLAN, Client 3 ist getrennt

```
# Administrativer Zugang zu Konfiguration; Dieser sollte NICHT in VLANs
# konfiguriert werden, da ansonsten die Verbindung u.U. unterbrochen wird.
/ip address add address=192.168.0.81/24 interface=ether4

# Neue Bridge anlegen
/interface bridge add name=mybridge

# Ports einer VLAN-ID zuordnen; MikroTik-spezifisch
/interface bridge port
add bridge=mybridge interface=ether1 pvid=200
add bridge=mybridge interface=ether2 pvid=200
add bridge=mybridge interface=ether3 pvid=300
```

Der Parameter „pvid" wird auf eingehende Rahmen angewendet, wodurch diese entsprechenden VLAN-IDs zugeordnet werden. Durch das Setzen dieses Parameters wird der entsprechende Port automatisch (gekennzeichnet mit D = dynamic) der entsprechenden VLAN-ID zugeordnet. Ein Port darf „untagged" nur genau einem VLAN zugeordnet werden.



Server mit „Tagging" in beiden VLANs verfügbar; Clients jeweils „untagged"

Zunächst wird der Switch um entsprechend „tagged" VLANs erweitert. Die Erweiterung erfolgt über den Befehl „/interface bridge vlan add bridge=<BRIDGENAME> tagged=<ETH-PORT> vlan-ids=<VLAN-ID>". Hier können die zuvor mit „pvid" konfigurierten „untagged" ebenfalls angegeben werden. Dies ist zwar nicht notwendig, verbessert aber die Übersicht. Um beiden Clients den Zugriff zu ermöglichen, wird der Server ebenfalls VLAN-fähig, indem dieser mit „Tagging" konfiguriert wird.

```
#Optional: Ausgabe der verfügbaren Ethernet-Ports und MAC-Adressen
/interface ethernet print

# Administrativer Zugang zu Konfiguration; Dieser sollte NICHT in VLANs
# konfiguriert werden, da ansonsten die Verbindung u.U. unterbrochen wird.
/ip address add address=192.168.0.81/24 interface=ether4

# Neue Bridge anlegen OHNE VLAN-Filtering (für pvid)
/interface bridge add name=mybridge vlan-filtering=no
```

```
# Ports zu einer Bridge verbinden; MikroTik-spezifisch
# Untagged Ports werden mit pvid= in das entsprechende VLAN konfiguriert/
interface bridge port
add bridge=mybridge frame-types=admit-only-vlan-tagged interface=ether1
add bridge=mybridge frame-types=admit-only-untagged-and-priority-tagged
interface=ether2 pvid=200
add bridge=mybridge frame-types=admit-only-untagged-and-priority-tagged
interface=ether3 pvid=300

# Tagged Ports werden explizit im VLAN-Bereich der Bridge-Konfiguration
# eingerichtet
/interface bridge vlan
add bridge=mybridge tagged=ether1 vlan-ids=200
add bridge=mybridge tagged=ether1 vlan-ids=300

# VLAN-Filtering aktivieren (für pvid), damit die VLAN-Konfiguration
# ausgeführt wird.
/interface bridge set mybridge vlan-filtering=yes
```

Die Parameter „frame-types=admit-only-vlan-tagged“ und „frame-types=admit-only-untagged-and-priority-tagged“ sind optional. Diese Parameter schränken die Art der Rahmen ein, die akzeptiert werden. Es werden nur Tagged-Rahmen („admit-only-vlan-tagged“) bzw. nur Untagged-Rahmen („admit-only-untagged-and-priority-tagged“) zugelassen. Wird dieser Parameter nicht verwendet, wird standardmäßig „frame-types=admit-all“ benutzt (wird bei Export nicht angezeigt). Dieser lässt alle VLAN-Typen zu (untagged und tagged).

Tagged VLAN auf Linux-Server einrichten

Unter Linux wird die VLAN-Ethernet-Erweiterung (802.1Q) über ein Kernel-Modul angeboten. Dieses muss zunächst mit dem Befehl „modprobe 8021q“ geladen werden. Mit „lsmod | grep 8021q“ kann überprüft werden, ob das Modul aktiv ist. In der Ausgabe werden die entsprechenden Prozess-IDs angezeigt.

```
lsmod | grep 8021q
# Ausgabe:
8021q     33208    0
garp      14384    1    8021q
mrp       18542    1    8021q
```

Um ein Tagged-VLAN zu nutzen, wird eine eigene Schnittstelle eingerichtet. Die Befehle zeigen die entsprechende Vorgehensweise.

```
# Hier wird auf der physischen Schnittstelle enp0s3 das virtuelle
# Interface mit dem Namen „enp0s3.200“ mit der VLAN-ID 200 angelegt.
# Virtuelles Interface mit VLAN-ID 200 anlegen
sudo ip link add link enp0s3 name enp0s3.200 type vlan id 200

# neue Schnittstelle aktivieren
sudo ip link set enp0s3.200 up

# neuer Schnittstelle eine IP-Adresse zuweisen
sudo ip address add 10.20.0.1/16 dev enp0s3.200
```

Der Parameter „name“ der neu anzulegenden Schnittstelle kann frei gewählt werden. Lediglich die VLAN-ID muss dem tatsächlichen VLAN entsprechen. Man könnte demnach statt „enp0s3.200“ auch „clown1“ verwenden. Bei einem System mit vielen VLAN-Schnittstellen ist eine leicht nachvollziehbare Bezeichnung sinnvoll (z. B. voip.70 für das VLAN-70, welches für Voice-over-IP genutzt wird). Für das zweite VLAN 300 ist der Vorgang mit den entsprechenden Werten zu wiederholen.

Mit dem Befehl „ip address“ (oder als Kurzform „ip a“) kann die Konfiguration überprüft werden.

```
# Ausgabe ip a
[...]
4: enp0s3.300@enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
noqueue state UP group default qlen 1000
   link/ether 08:00:27:5c:80:e3 brd ff:ff:ff:ff:ff:ff
   inet 10.30.0.1/16 brd 10.30.255.255 scope global enp0s3.300
      valid_lft forever preferred_lft forever
   inet6 fe80::a00:27ff:fe5c:80e3/64 scope link
      valid_lft forever preferred_lft forever
5: enp0s3.200@enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
noqueue state UP group default qlen 1000
   link/ether 08:00:27:5c:80:e3 brd ff:ff:ff:ff:ff:ff
   inet 10.20.0.1/16 brd 10.20.255.255 scope global enp0s3.200
      valid_lft forever preferred_lft forever
   inet6 fe80::a00:27ff:fe5c:80e3/64 scope link
      valid_lft forever preferred_lft forever
[...]
```

Um die Anwendung zu überprüfen, kann „tcpdump“ oder Wireshark eingesetzt werden. Mit „tcpdump --micro -n -i enp0s3 -e“ werden alle ankommenden Rahmen im Terminal angezeigt. Die Überprüfung kann auf dem Server durchgeführt werden, da diesem die Tagging-Informationen übergeben werden. Die beiden Clients erhalten ihre Rahmen ohne VLAN-Tag.

Client 1 und Client 2 senden Pings auf den Server, dort wird der Datenverkehr mit „tcpdump“ mitgeschnitten.

```
root@vlan-server:~# tcpdump --micro -n -i enp0s3 -e
# Ausgabe
[...]

16:01:14.594972 08:00:27:69:10:bb > 08:00:27:5c:80:e3,
ethertype 802.1Q (0x8100), length 102: vlan 200, p 0,
ethertype IPv4 (0x0800), 10.20.0.2 > 10.20.0.1:
ICMP echo request, id 24, seq 732, length 64

16:01:14.594999 08:00:27:5c:80:e3 > 08:00:27:69:10:bb,
ethertype 802.1Q (0x8100), length 102: vlan 200, p 0,
ethertype IPv4 (0x0800), 10.20.0.1 > 10.20.0.2:
ICMP echo reply, id 24, seq 732, length 64

16:01:14.957089 08:00:27:da:3f:a1 > 08:00:27:5c:80:e3,
ethertype 802.1Q (0x8100), length 102: vlan 300, p 0,
```

```
ethertype IPv4 (0x0800), 10.30.0.3 > 10.30.0.1:
ICMP echo request, id 19, seq 12, length 64

16:01:14.957115 08:00:27:5c:80:e3 > 08:00:27:da:3f:a1,
ethertype 802.1Q (0x8100), length 102: vlan 300, p 0,
ethertype IPv4 (0x0800), 10.30.0.1 > 10.30.0.3:
ICMP echo reply, id 19, seq 12, length 64

4 packets captured
4 packets received by filter
0 packets dropped by kernel
```

Konfiguration dauerhaft anwenden

Um die Konfiguration dauerhaft auch nach einem Neustart des Servers zu speichern, müssen Änderungen in den Konfigurationsdateien vorgenommen werden. Die IP-Adressen und VLAN-IDs werden mittels „netplan" konfiguriert. Das Kernel-Modul „8021q" wird in der Datei „/etc/modules" durch Hinzufügen von „8021q" in einer eigenen Zeile dauerhaft aktiviert.

```
# VLAN und IP-Adresse in netplan Konfiguration /etc/netplan
network:
  version: 2
  ethernets:
    enp0s3:
      addresses:
        - 192.168.0.88/24 # falls benötigt
      routes:
        - to: 0.0.0.0
          via: 192.168.0.1

  vlans: # Einrückung muss unter "ethernets" stehen
    enp0s3.200:
      id: 200
      link: enp0s3
      addresses: ["10.20.0.1/16"]

    enp0s3.300:
      id: 300
      link: enp0s3
      addresses: ["10.30.0.1/16"]
```

Hinweis zu Cisco-Geräten: Bei Cisco-Geräten ist es üblich, dass zunächst der Trunk-Mode für Tagged-VLANs eingerichtet wird. Dabei werden zunächst alle VLAN-IDs freigeschaltet. Hierdurch können alle Anwendungen miteinander kommunizieren. Es werden aber auch beliebige Zugriffe möglich, die unter Umständen nicht gewünscht sind. Daher sollten im zweiten Schritt alle nicht explizit benötigten VLAN-IDs deaktiviert werden.

Hinweis zu Windows-PCs: Wie in Kapitel 3.3.2 bereits beschrieben, hat Windows keine einheitliche Schnittstelle für die Einrichtung von Tagged-VLANs. Es wird hier auf die Herstellerdokumentation der Netzwerkkarten verwiesen.

(2) Firewall implementieren

Die Rigudo GmbH möchte eine demilitarisierte Zone (DMZ) einsetzen. Die Firewall zwischen der DMZ und dem Internet wurde als Paketfilter-Firewall mit Stateful Packet Inspection eingeplant. Die Wahl fiel auf die Software „nftables". Innerhalb der DMZ wird ein Webserver betrieben, der aus dem externen Netzwerk erreichbar sein soll. Eine Verbindung von außen soll nur zum Webserver möglich sein. Weitere Verbindungen ins Internet müssen im internen Netzwerk oder der DMZ initiiert werden. Für den Übergang zwischen der DMZ und dem internen Netzwerk soll eine andere Firewall eingesetzt werden. Die Rigudo GmbH hat sich hier für das Produkt „OPNsense" entschieden.



Firewall-System mit DMZ

Die **Software „nftables"** ist eine auf dem Softwarepaket „Netfilter" basierende Firewall. Genau wie „iptables" arbeitet nftables unter Linux und kann, falls es noch nicht installiert ist, über das Standard-Repository installiert werden. Im Gegensatz zu iptables sind bei der Firewall „nftables" alle Funktionen unter einem Befehl vereint. Nftables kann beispielsweise mit IPv4 und IPv6 arbeiten. Ein weiterer Vorteil ist, dass bei nftables die Regeln bei einem Systemneustart erhalten bleiben.

Nftables arbeitet wie auch iptables mit Tabellen und Regelwerken (sogenannte Chains), verwendet jedoch im Gegensatz iptables keine festgelegten Tabellen. Zunächst wird eine Tabelle angelegt (vgl. Zeile 1 unten). Diese Tabelle gilt für das Protokoll „IPv4" und trägt den Namen „Firewall". Statt dem Parameter „ip" könnte auch z. B. „inet" angegeben werden. Dann gilt die Tabelle für IPv4 und IPv6. In der Tabelle können Regelwerke und Regeln angelegt werden.

Mit dem Befehl „nft list ruleset" in der zweiten Zeile kann die Konfiguration angezeigt werden. Der Befehl in der dritten Zeile fügt der eben angelegten Tabelle ein Regelwerk mit dem Namen „input" hinzu. Dieses Regelwerk ist vom Typ „filter". Das ermöglicht es, Pakete nach bestimmten Regeln zu erlauben oder zu verbieten.

Ein anderer Regelwerk-Typ ist z. B. „nat" für die Veränderung von IP-Paketen durch die Network Address Translation. Die Angabe „hook input" beschreibt, an welcher Stelle des Weges das Regelwerk eingesetzt wird. Der Wert „input" veranlasst, dass das Regelwerk bei allen eingehenden Paketen angewendet wird, die für das System adressiert sind. Das Regelwerk könnte auch vor oder nach einem Routing (Prerouting, Postrouting) zur Anwendung kommen oder nur bei ausgehendem Verkehr (Output) eingesetzt werden.

```
1 sudo nft add table ip firewall
2 sudo nft list ruleset
3 sudo nft 'add chain ip firewall input { type filter hook input priority
filter; policy drop;};'
4 sudo nft add rule ip firewall input tcp dport 443 accept
```

Der Parameter „priority" wird verwendet, wenn es mehrere Regelwerke für eine „hook" gibt. Dann kann angegeben werden, welches Regelwerk zuerst zum Einsatz kommt. Mit „policy" wird festgelegt, was mit Paketen passiert, auf die keine Regel zutrifft. Es beschreibt die „default policy". Mit dem Befehl in der vierten Zeile wird eine Regel im Regelwerk „firewall" angelegt. Diese Regel erlaubt eingehenden Verkehr auf Port 443 (HTTPS).

```
maximuster@firewall1:~$ sudo nft list rulest
table ip firewall {
}
```

Leeres Regelwerk vor Konfiguration

```
maximuster@firewall1:~$ sudo nft list rulest
table ip firewall {
        chain input {
                type filter hook input priority filter; policy drop;
                tcp dport 443 accept
                ct state { established, related, new } tcp dport 22 log prefix "SSH" accept
        }
}
```

Regelwerk nach Ausführung der Konfiguration

Die Regeln auf diese Weise einzugeben, kann mit hohem Aufwand verbunden sein. Außerdem ist eine ständige Kontrolle nötig, ob die Regeln richtig ins Regelwerk geschrieben wurden. Einfacher ist es, eine Datei mit den Regeln zu erstellen und diese in die Firewall zu importieren.

Für das Beispiel von oben würde eine entsprechende Datei wie folgt aussehen:

```
table ip firewall {
    chain input {
        type filter hook input
        priority filter
      policy drop
        tcp dport 443 accept
    }
}
```

Mit dem Befehl „nft -f Dateiname“ kann die Datei geladen werden.

Die Firewall „nftables“ kann als **Stateful Packet Inspection (SPI)** eingerichtet werden. Dazu kann das sogenannte Connection Tracking aktiviert werden.

```
ct state { established } accept
```

Dadurch werden Pakete, die zu aufgebauten erlaubten Verbindungen gehören, ebenfalls erlaubt. Nftables erlaubt es, neue Verbindungen mit dem Zustand „related“ aufzubauen, wenn diese zu einer bereits erlaubten Verbindung gehören. Ein Beispiel für die Anwendung ist das File Transfer Protocol (FTP). Dies baut zunächst eine Steuerverbindung auf. Durch diese Steuerverbindung kann jetzt eine Verbindung zum Datenaustausch aufgebaut werden.

Mit der Regel „icmp type echo-reply accept“ kann das eigene System andere Systeme „anpingen“. Der „Ping“ besteht aus Anfrage und Antwort. Die Antwort „icmp type 0 echo-reply“ kommt an den Rechner zurück und wird durch diese Regel erlaubt. Die Anfragen anderer Systeme („icmp type 8 echo-request“) werden, wie jeder andere Verkehr, der nicht explizit erlaubt ist, verworfen.

Es ist sinnvoll, die Aktivität der Firewall zu protokollieren. Mit der Software „nftables“ kann ein einfaches Protokollieren aktiviert werden. Es genügt, in einer Regel mit dem Parameter „log“ die Protokollierung für alle Pakete, auf die diese Regel zutrifft, zu aktivieren. Im angeführten Beispiel wird HTTP-Verkehr protokolliert. Im Kernel-Log wird der Meldung die Nachricht „HTTP-Verbindung:“ vorangestellt.

```
tcp dport 80 log prefix "HTTP-Verbindung: " accept
```

Im Journal kann nun nach dieser Meldung gesucht werden, um die verworfenen Pakete näher zu untersuchen.

```
maximuster@firewall1:~$ sudo journalctl |grep HTTP-Verbindung
maximuster user-VirtualBox kernel: HTTP-Verbindung: IN=enp0s3 OUT=
MAC=08:00:27:08:e2:16:08:00:27:0e:15:76:08:00
SRC=172.16.0.103
DST=172.16.0.101
LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=23085 DF PROTO=TCP SPT 47372 DPT=80
WINDOW=64240 RES=0x00 SYN URGP=0
```

Protokollierung der Firewall mit selbst definiertem Präfix

Die Regeln können bei nftables persistent angelegt werden. Dazu müssen sie in die Datei „/etc/nftables.conf" geschrieben werden. Mit der Software „uncomplicated firewall (ufw)" können die Regeln für nftables – je nach aktueller Konfiguration auch iptables – einfach angelegt werden. Nach dem Starten der „ufw" sind alle ausgehenden Verbindungen erlaubt und alle ankommenden Verbindungen verboten. Mit dem Befehl „sudo ufw ssh allow" werden beispielsweise SSH-Verbindungen zugelassen. Dazu wird im nftables-Regelwerk eine entsprechende Regel ergänzt.

```
chain ufw-user-input {
    meta l4proto tcp tcp dport 22 counter packets 0 bytes 0 accept
}
```

Eine andere Art der Herangehensweise verfolgt die Firewall „OPNsense". Diese bietet eine umfangreiche GUI zur Konfiguration der Firewall an. OPNsense basiert auf dem Betriebssystem „FreeBSD" und ist eine Open-Source-Paketfilter-Firewall, die eine große Anzahl zusätzlicher Funktionen anbietet, die teilweise durch Module bereitstehen. OPNsense kann beispielsweise als VPN-Gateway dienen oder ein IDS/IPS bereitstellen.

Die Software kann als ISO-Image-Datei heruntergeladen werden. Dieses Image kann direkt als Betriebssystem auf der Hardware oder in einer virtuellen Maschine installiert werden. Sinnvollerweise stehen der Software zwei Netzwerkschnittstellen zur Verfügung. Die Schnittstellen sind jeweils mit dem internen LAN und der DMZ verbunden.

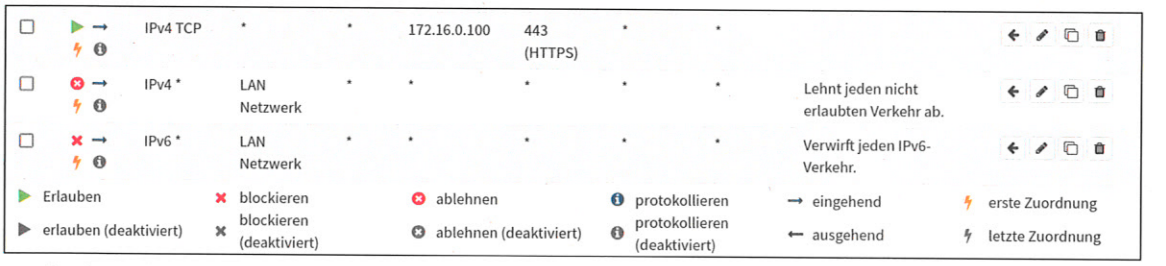
Die Installation von OPNsense ist menügeführt. Nach der Anmeldung mit den Standardzugangsdaten (installer/opnsense) können die Tastatursprache, das Installationsziel und das zu installierende Dateisystem gewählt werden. Für den produktiven Einsatz muss das Root-Passwort während der Installation geändert werden. Nach dem Festlegen der IP-Adressen für die Schnittstellen kann vom lokalen Netzwerk auf das Web-Interface der Firewall zugriffen werden. Im Web-Interface kann mithilfe eines Konfigurationsassistenten die Netzwerkkonfiguration, z. B. die Adresse des NTP-Zeitservers, vervollständigt werden. Für die Verwendung von OPNsense als interne Firewall muss bei der Konfiguration „Block RFC1918 Private Networks" deaktiviert werden, denn die DMZ verwendet einen privaten IP-Adressbereich.

Aus dem internen Netzwerk sollen zunächst nur HTTPS-Verbindungen zum Proxy in der DMZ und ICMP-Verbindungen in die DMZ zugelassen werden. Alle anderen Verbindungen soll die Firewall blocken. Für ein produktives Netzwerk muss meist noch weiterer Verkehr, z. B. für den E-Mail-Versand und -Empfang, zugelassen werden.

Im abgebildeten Regelwerk „LAN" sind drei Regeln hinterlegt. Die erste Regel erlaubt HTTPS-Verkehr (Zielport TCP/443) vom internen Netzwerk zur IP-Adresse 172.16.0.100. Unter dieser IP-Adresse ist der

HTTPS-Proxy erreichbar. Die zweite Regel lehnt jeglichen anderen IPv4-Verkehr ab. Die dritte Regel verbietet jeglichen IPv6-Verkehr, da im internen Netzwerk kein IPv6 verwendet wird.

Wird Verkehr abgelehnt, bekommt der Sender eine Information, dass der Verkehr abgelehnt wurde. Bei einer TCP-Verbindung wird ein TCP-Segment mit gesetztem RST-Flag (Reset-Flag) zurückgesendet. Bei UDP-Verkehr wird eine ICMP-Fehlermeldung erzeugt. Wenn Pakete durch eine Regel verworfen werden, erfolgt keine Art von Meldung.



Regelwerk „LAN“

Wie in Kapitel 3.3.2, Abschnitt (2) über die Planung der Firewall beschrieben wurde, ist die Reihenfolge der Regeln im Regelwerk wichtig. Wenn in diesem Beispiel die zweite Regel („verbiete jeglichen IPv4-Verkehr“) vor der ersten Regel stehen würde, könnte die HTTPS-Regel nie angewendet werden. HTTPS-Verkehr nutzt das Internet Protocol (IP), somit wird die erste Verbotsregel unmittelbar ausgeführt.

Beim Anlegen der Regeln müssen einige Parameter beachtet werden. Die Tabelle zeigt einen Auszug aus den möglichen Optionen.

Ausgewählte Parameter der OPNsense-Firewall	
Parameter	**Bedeutung**
Schnell	Wird diese Option nicht gesetzt, wird diese Regel nicht automatisch auf den passenden Verkehr angewendet, sondern es wird im Regelwerk nach weiteren passenden Regeln gesucht. Die letzte passende Regel wird dann verwendet.
Schnittstelle	Mit dieser Option wird die Schnittstelle festgelegt, auf der die zu prüfenden Pakete ankommen.
Richtung	Hier kann zwischen den Werten „in“ und „out“ gewählt werden. Die Wahl von „in“ bedeutet, dass der Verkehr in Richtung Firewall gesendet wird, während bei „out“ der Verkehr die Firewall verlässt.
Quelle/Ziel Quell-Port-/ Ziel-Portbereich	Hier können die IP-Adressen und Ports von Quelle und Ziel festgelegt werden. Dabei sind IP-Netze oder einzelne IP-Adressen als Angabe möglich. Genauso können einzelnen Ports angegeben werden (z. B. 443 für HTTPS) oder auch ganze Port-Bereiche.
Protokoll	Wenn diese Option aktiviert wird, wird jede Regelanwendung protokolliert. Das Protokoll kann in der Web-Oberfläche der Firewall eingesehen werden.
Kategorie	Zur besseren Übersicht lassen sich Regeln gruppieren. Diese Gruppierung spielt aber bei der Regelüberprüfung keine Rolle.

Den zu einer Anfrage aus dem internen Netzwerk gehörenden Antwortverkehr lässt die Firewall ohne weitere Regel zu.

Wird bei einer Regel der Schalter „Protokoll“ aktiviert, protokolliert die Firewall alle Anwendungen der Regel. Der Administrator kann die Regelanwendung aufbereitet betrachten. So lassen sich z. B. geblockte Datenverbindungen einfach nachvollziehen.

Schnittstelle	Zeit	Quelle	Ziel	Protokoll	Etikett
wan	2022-10-20T22:36:57	192.168.100.100:45900	172.16.0.100:80	tcp	let out anything from firewall host itself
lan	2022-10-20T22:36:57	192.168.100.100:45900	172.16.0.100:80	tcp	

Erlaubt HTTP-Verbindung vom internen Netzwerk in die DMZ

Nachfolgend wird eine Regel erstellt, die es erlaubt, aus dem internen Netzwerk Systeme innerhalb der DMZ mittels Ping-Befehl auf die Erreichbarkeit zu überprüfen. Systeme aus der DMZ sollen keine internen Systeme mittels Ping-Befehl erreichen können. Als Protokoll kommt das ICMP zum Einsatz. Um nur einen Ping aus dem internen Netzwerk in die DMZ zu lassen, wird nur der ICMP-Typ „Echo-Request" zugelassen. Das Quell-IP-Netzwerk ist das „LAN Netzwerk" (192.168.100.0/24). Das Ziel-IP-Netzwerk ist das „WAN Netzwerk" (172.16.0.0/16). Ports werden nicht benötigt, da ICMP kein OSI-Schicht-4-Transportprotokoll wie UDP oder TCP verwendet. Es ist nötig, dass die Regel vor diejenige Regel verschoben wird, die IPv4-Verkehr grundsätzlich verbietet.

	IPv4	LAN	*	WAN	*	*	*
	ICMP	Netzwerk		Netzwerk			

Entsprechend konfigurierte Regel

(3) Proxy implementieren

Die Umsetzung des Proxy-Servers für die Rigudo GmbH soll wie geplant realisiert werden. Zunächst werden die Grundparameter des Systems betrachtet. Im Anschluss werden die Protokollierung und die Möglichkeit zur Filterung behandelt. Der eingesetzte Proxy „Squid" wird standardmäßig in der Datei „/etc/squid/squid.conf" konfiguriert. Die Standarddatei enthält viele auskommentierte Parameter. Die folgende Tabelle zeigt die wichtigsten Parameter und deren Bedeutung.

Wesentliche Parameter des Squid-Proxy	
Parameter	**Bedeutung**
http_port	Angabe der IP-Adresse und des Ports, über den der Proxy erreichbar ist
cache_mem	Größe des Cache-Zwischenspeichers; wird in MiB angegeben (abweichend von der Syntax „MB")
cache_dir	Gibt das Dateisystem, den Pfad des Cache-Ordners, die Größe des Cache-Ordners sowie die Anzahl der Ordner auf erster und zweiter Ordnerebene an; es können mehrere Cache-Speicher angegeben werden, um diese auf verschiedene Partitionen zu verteilen
access_log	Aktiviert die Zugriffsprotokolldatenerfassung und den Speicherort der Datei „access.log"

```
# Beispielkonfiguration
http_port 10.30.0.1:3128
cache_mem 16 MB
cache_dir ufs /usr/local/squid/var/logs/cache.log 100 16 256
access_log /usr/local/squid/var/logs/access.log
cache_log /usr/local/squid/var/logs/cache.log

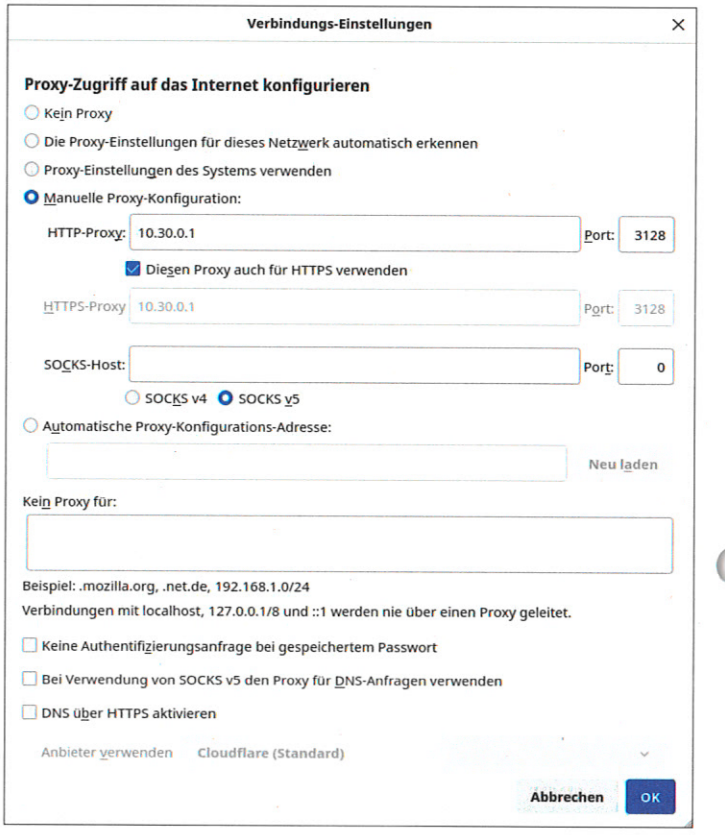
# Zugriffe mit protokollieren
access_log /var/log/squid3/access.log squid

# Einfache Access-Regeln
# Alle anderen Quellen aus dem angegebenen Netz dürfen alles
acl localnet src 10.30.0.0/24
http_access allow localnet
```

Neben dieser einfachen Zugriffsprotokolldatenerfassung kann der Proxy auch zur Kontrolle von Zugriffen konfiguriert werden. Hierzu werden sogenannte Access-Control-List-Regeln (ACL-Regeln) verwendet.

Der Aufbau einer ACL-Regel besteht im Normalfall aus zwei Zeilen. Zunächst wird definiert, wodurch die Regel ausgelöst wird. Im Beispiel muss die Anfrage aus dem Netz 10.30.0.0/24 stammen. In der zweiten Zeile wird dann die Aktion definiert. Im Beispiel wird der HTTP-Zugriff gewährt. Als Referenz zwischen den beiden Zeilen wird der Name der ACL („localnet“) verwendet. Dieser ist frei wählbar.

Zu Testzwecken kann der Proxy manuell gestartet werden. Dies wird über den Befehl „sudo squid -d 2“ vorgenommen. Es werden wesentliche Informationen direkt im Terminal ausgegeben. Um die Zugriffe auf den Proxy zu überprüfen, kann der Befehl „tail -f /var/log/squid/access.log“ verwendet werden.



Firefox Proxy-Konfigurationsdialog

Die Abfrage des aktuellen Status bzw. Start/Stop/Restart des Squid-Daemon kann mit den folgenden Befehlen erfolgen:

```
sudo systemctl status squid.service
sudo systemctl start squid.servic
sudo systemctl stop squid.service
sudo systemctl restart squid.service
```

Der Client muss so konfiguriert werden, dass er den Proxy nutzt. Die Proxy-Konfiguration kann systemweit hinterlegt werden, ist aber anwendungsabhängig und damit keine betriebssystemeigene Funktion. In Firefox geschieht dies z. B. im Untermenü „Netzwerk“ durch das Aktivieren der Proxy-Optionen.

Zu Testzwecken eignen sich die Programme „curl“ und „wget“, da diese keinen eigenen Cache-Zwischenspeicher verwalten. Firefox, wie auch fast alle anderen Browser, puffert eigenständig bereits abgerufene Inhalte lokal. Bei Tests des Proxy-Cache-Verhaltens kann dies störend sein.

```
# Einmaliger Aufruf von wget mit Proxy
wget -e use_proxy=yes -e http_proxy=10.30.0.1:3128 http://irgendwo.net

# Feste Konfiguration des Proxy in /etc/wgetrc
use_proxy=on
http_proxy=http://10.30.0.1:3128/
https_proxy=http://10.30.0.1:3128/
```

Um die zwischengespeicherten Daten im Proxy einfacher finden zu können, kann die Anzahl der Unterordner im Cache-Ordner reduziert werden. Die erste Zahl des Parameters bestimmt die Größe in MiB. Dann folgt die Anzahl der Unterordner auf der 1. und 2. Ebene.

```
cache_dir ufs /var/spool/squid 2000 16 256

2000: Cache-Größe in MiB, bis zu der der Cache anwachsen darf
16: Anzahl der level1-Ebene im Cache-Ordner
256: Anzahl der level2-Ebene
```

Damit werden insgesamt 16 · 256 = 4 096 Unterordner angelegt. Zu Testzwecken kann dies reduziert werden und der Cache in einen speziellen Testordner verlegt werden. Der administrative Benutzer „proxy" muss Besitzer und Gruppe für diesen Testordner sein. Die erste Anfrage geht direkt an den Server. Die zweite Anfrage geht schon über den Proxy. Das kann per „tcpdump" auf dem Server überprüft werden. Die entsprechende log-Datei befindet sich im „cache_dir" (Standardverzeichnis: „/var/spool/squid").

Content-Filterung

Der Squid-Proxy ermöglicht die Filterung der HTTP-Anfragen. Hierzu muss zunächst mit „request_header_access" gefiltert werden, sodass im Anschluss ein neuer Wert eingefügt werden kann („request_header_replace").

Beispiel für Header-Rewriting: UserAgent oder Via Info entfernen bzw. ersetzen

```
# Filterung
request_header_access User-Agent deny all
request_header_access Via deny all

# Ersetzen
request_header_replace User-Agent mywget/9.99.9
request_header_replace User-Agent mySQUID/9.9.9
```

Achtung: Das Ersetzen von Header-Informationen kann zu Fehlern führen, da die HTTP-Server häufig Daten in Abhängigkeit dieser Informationen ausliefern.

Kompetenzcheck

1. Geben Sie bezogen auf VLAN an, was an den Aussagen falsch ist:
   a) Ein Hybrid-Port kann nur genau einem Tagged-VLAN zugewiesen werden.
   c) Eine Ethernet-Schnittstelle auf einem Linux-System kann ohne zusätzliches Kernel-Modul als Tagged-Port arbeiten.
   b) Jede Windows-Ethernet-Schnittstelle kann mit 802.1Q betrieben werden.

2. Eine nftables-Firewall soll alle eingehenden Pakete auf die IP-Adresse 10.0.0.10 mit TCP-Port 2007 verwerfen. Geben Sie die entsprechende Regel im nftables-Format an.

3. Ein Squid-Proxy soll auf der IP-Adresse 10.0.0.10 und dem Port 2007 betrieben werden. Geben Sie den notwendigen Konfigurationsparameter an.

4. Notieren Sie wesentliche Aspekte aus diesem Abschnitt in Ihrem Projektjournal.

5. Bearbeiten Sie Aufgabe 2 der Lernsituation 4 im Arbeitsbuch.

A2

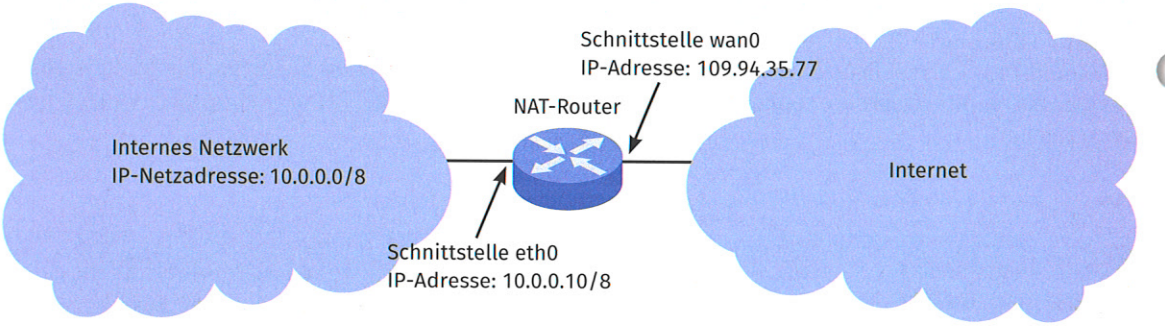
3.4.3 Zugriffsmöglichkeit auf vernetzte Systeme am Internet-Anschluss umsetzen

S **Sie sollen den sicheren Zugriff auf vernetzte Systeme am Internet-Anschluss mit ausgewählten Techniken umsetzen.**

(1) Einsatz der Network Address Translation (NAT) implementieren

Bei den meisten NAT-Systemen ist die NAT-Technik nicht der Hauptbestandteil des Funktionsumfangs, sondern nur ein Teil eines Gesamtpakets. Oftmals ist die NAT-Technik integrativer Bestandteil einer Routing-Software oder einer Firewall.

Eine einfache Möglichkeit, die NAT-Technik anzuwenden, bietet die Software „nftables" (siehe Kapitel 3.4.2). Sie wird verwendet, um IP-Pakete zu klassifizieren, zu filtern und zu manipulieren, z. B. um eine Firewall-Funktionalität zu erhalten oder die NAT-Technik anzuwenden. Beispielhaft wird NAT im folgenden abgebildeten Netzwerk implementiert.



Aufbau einer NAT-basierten Internetanbindung

Das interne Netzwerk arbeitet mit privaten IP-Adressen aus dem IP-Bereich 10.0.0.0/8. Diese Adressen werden im öffentlichen Netzwerk nicht weitergeleitet. Am Übergang zwischen dem internen und dem öffentlichen Netzwerk findet ein NAT-Vorgang statt. Die internen Adressen werden durch die öffentliche IP-Adresse des NAT-Routers ersetzt.

Mit dem Befehl „nft" kann die Software „nftables" konfiguriert werden.

In diesem Beispiel wird entweder die Technik **„Source-NAT" (SNAT)** oder die Technik **„Masquerade"** benötigt. Bei Masquerade wird die interne Adresse automatisch in die verfügbare IP-Adresse übersetzt. Wenn die WAN-Schnittstelle durch den Internet Service Provider (ISP) eine dynamische IP-Adresse bezieht, ist die Masquerade-Technik die präferierte Wahl, da die internen Adressen immer mit der wechselnden zugewiesenen öffentlichen IP-Adresse ersetzt werden. Bei SNAT kann nicht auf eine wechselnde IP-Adresse reagiert werden. Die internen IP-Adressen (als Quelle) werden durch feststehende öffentliche IP-Adressen ersetzt. Verwendet ein Unternehmen feste externe IP-Adressen, ist SNAT die präferierte Wahl, da es schneller arbeitet als Masquerade.

Im folgenden Beispiel kommt die Technik „Masquerade" zum Einsatz. Zunächst wird eine Tabelle mit dem Namen „nat" angelegt. Tabellen können beispielsweise Regelwerke enthalten (Zeile 1). Anschließend wird innerhalb der Tabelle ein Regelwerk (Chain) angelegt (Zeile 2). Das Regelwerk gilt für den Datenverkehr nach dem Routingprozess (Postrouting) des NAT-Routers. Die Angabe „type nat hook x" gibt an, wann es eine Übereinstimmung mit dem Regelwerk gibt. Die Priority gibt an, an welcher Stelle im Regelwerk die

Standard-Regel steht. Das Zeichen „\" wird als Escape-Zeichen verwendet, damit das nachfolgende „;" richtig interpretiert wird. Alternativ können die Regeln auch im interaktiven Modus angegeben werden (Befehl „nft -i"), dann ist kein Escape-Zeichen nötig. Mit dem nächsten Befehl (Zeile 3) wird das Regelwerk an eine Schnittstelle gebunden (im Beispiel „eth0") und die Maskierung der Pakete festgelegt.

```
1 sudo nft add table nat
2 sudo nft add chain nat POST { type nat hook postrouting priority 100 \;}
3 nft add rule nat POST oifname "eth0" masquerade
```

Zur Überprüfung sendet ein Client aus dem internen Netzwerk einen „Ping" an ein System im externen Netzwerk. Wenn die Nachrichten auf dem NAT-Router sowohl auf der internen als auch auf der externen Schnittstelle mitgeschnitten werden, kann man den NAT-Vorgang nachverfolgen.

No	Source	Destination	Protocol	Info
1	10.0.0.100	109.94.35.78	ICMP	Echo (ping) request
2	109.94.35.77	109.94.35.78	ICMP	Echo (ping) request
3	109.94.35.78	109.94.35.77	ICMP	Echo (ping) reply
4	109.94.35.78	10.0.0.100	ICMP	Echo (ping) reply
5	10.0.0.100	109.94.35.78	ICMP	Echo (ping) request

Wireshark-Mitschnitt einer Ping-Anfrage über NAT

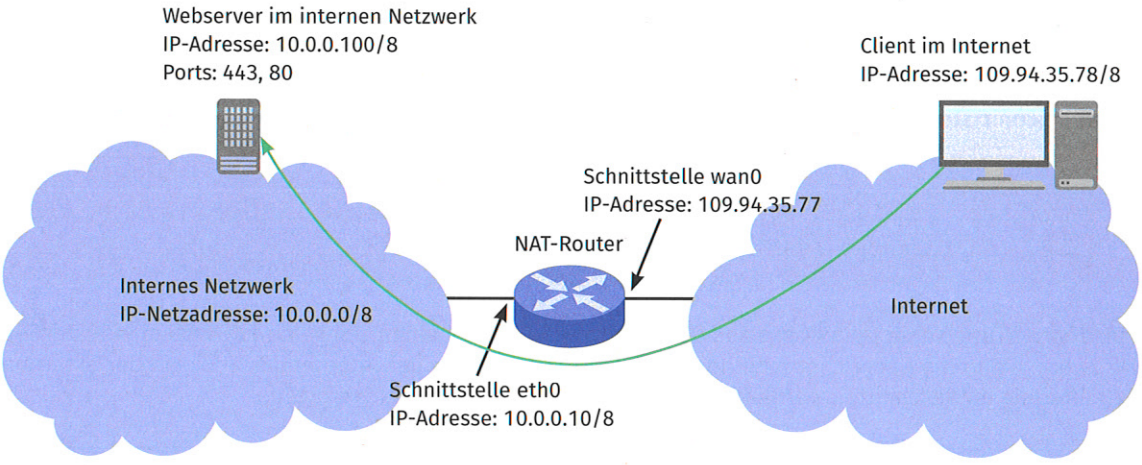
Die vier Nachrichten im abgebildeten Mitschnitt zeigen die beiden Nachrichten eines Pings. Die Anfrage „Echo Request" und die darauffolgende Antwort „Echo Reply" sind jeweils zweimal abgebildet. Die erste Echo-Request-Nachricht wurde vor dem NAT-Vorgang auf der internen Schnittstelle mitgeschnitten. Die Quell-IP-Adresse ist aus dem internen Netzwerk (10.0.0.100). Die zweite Nachricht wurde nach dem NAT-Vorgang an der externen Schnittstelle aufgenommen. Die Quell-IP-Adresse ist nun durch die externe Adresse des NAT-Routers (109.94.35.77) ersetzt.

Die NAT-Regeln lassen sich bei nftables auch statisch konfigurieren, damit sie bei einem Neustart geladen werden. Dazu wird die Konfiguration in einer Konfigurationsdatei („/etc/nftables.conf") vorgenommen. Für das gezeigte Beispiel wird die Konfiguration wie folgt erweitert:

```
1 table nat {
2  chain postrouting
3       type nat hook postrouting priority 100; policy accept;
4       log prefix "nft.NAT";
5       ip saddr 10.0.0.0/8 oifname eth0 masquerade;
6  }
7 }
```

In dieser Konfiguration ist zusätzlich die Protokollierung (Logging) aktiviert. In das Syslog („/var/log/syslog") des Betriebssystems werden beim NAT-Vorgang Einträge mit dem Präfix „nft.NAT" erzeugt.

Das Szenario kann nun noch erweitert werden. Im internen Netzwerk soll ein Webserver aus dem externen Netzwerk erreichbar sein. Auf dem NAT-Router muss dazu eine Port-Weiterleitung (Destination NAT) konfiguriert werden.



NAT mit Port-Weiterleitung auf internen Server

Für die externe Schnittstelle des Routers muss eine Regel definiert werden, die den eingehenden Datenverkehr auf den TCP-Ports 80 (HTTP) und 443 (HTTPS) an die IP-Adresse des internen Webservers (10.0.0.100) weiterleitet. Die Regel muss vor dem Routing-Prozess abgearbeitet werden, dazu wird in der Tabelle „nat" (Zeile 1) von nftables ein weiteres Regelwerk angelegt: die sogenannte Prerouting-Chain (Zeile 3). Innerhalb dieses Regelwerks wird eine Regel (Zeile 5) definiert, die jeglichen eingehenden Datenverkehr auf der externen Schnittstelle („eth1"), der die Zielports („dport" für „destination port") 80 oder 443 verwendet, an die IP-Adresse 10.0.0.100 weiterleitet.

```
1 table nat {
2   ...
3   chain prerouting {
4       type nat hook prerouting priority 100; policy accept;
5       ip saddr 0.0.0.0/0 iifname "eth1" tcp dport {80, 443} dnat to
        10.0.0.100;
6   }
7 }
```

No	Source	Destination	Protocol	Info
1	109.94.35.78	109.94.35.77	TCP	60928 -> 80 [SYN] Seq=0
2	109.94.35.78	100.0.0.100	TCP	60928 -> 80 [SYN] Seq=0

Erfolgreiche Port-Weiterleitung auf internen Webserver

Der Wireshark-Mitschnitt zeigt eine erfolgreiche Port-Weiterleitung. Die Nachricht kommt beim Router an (Zeile 1), dabei ist die Zieladresse die öffentliche Adresse des NAT-Routers (109.94.35.77) und der Ziel-Port 80. In der zweiten Zeile sieht man die identische Nachricht nach dem NAT-Vorgang. Die Ziel-IP-Adresse ist durch die Adresse des internen Webservers (10.0.0.100) ersetzt.

(2) Load Balancing als Sicherheitsaspekt implementieren

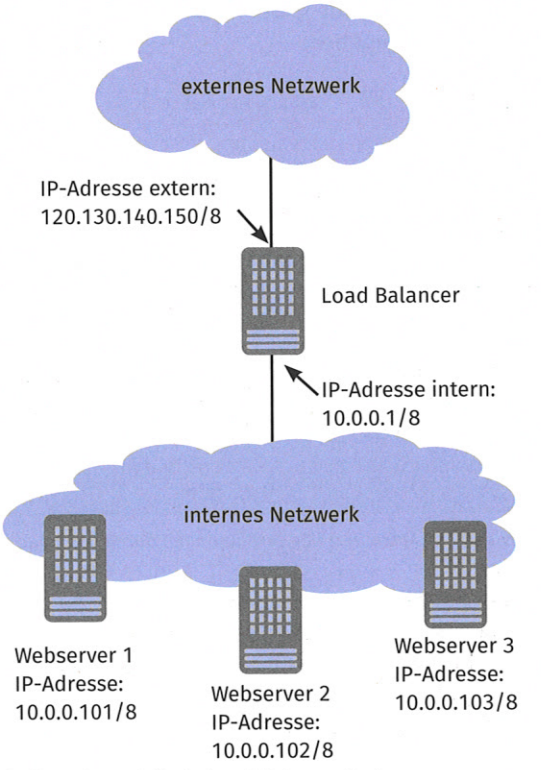
Als einführendes Beispiel wird ein einfaches Szenario betrachtet. Ein Load Balancer wartet auf eingehende Verbindungen, hier auf eingehende HTTP-Verbindungen. Der Load Balancer verteilt die ankommenden Verbindungsanfragen an die drei Webserver. Im internen Netzwerk, in dem die Webserver platziert sind, werden private IPv4-Adressen aus dem Netzwerk 10.0.0.0/8 verwendet.

Die Software „HAProxy“ ist eine frei verfügbare Open-Source-Software. Mit dieser Software kann ein Load Balancer unter Linux realisiert werden. Die Software kann über die Standard-Repositories der meisten Linux-Distributionen heruntergeladen werden.

Die Konfiguration findet über die Datei „/etc/haproxy/haproxy.cfg“ statt. Diese Datei ist sektionsweise aufgebaut.

Für einen einfachen Load Balancer, wie er im Beispielnetzwerk verwendet wird, müssen nur die Sektionen **„frontend“** und **„backend“** zur Standardkonfiguration hinzugefügt werden.

Die Sektion „frontend“ beinhaltet Anweisungen, wie mit dem aus dem externen Netzwerk ankommenden Datenverkehr verfahren werden soll.



Aufbau eines einfache Load Balancer-Systems

```
1 frontend http_front
2     bind *:80
3     default_backend http_back
```

In der ersten Zeile wird ein Bereich „frontend“ mit dem Namen „http_front“ definiert. Dieser Name ist frei wählbar. In der zweiten Zeile wird der Port 80 in den Zustand „listen“ gesetzt. Der Load Balancer wartet auf diesem Port auf eingehende Verbindungen. Der Port wird durch „*“ an alle zur Verfügung stehenden IP-Adressen. In der dritten Zeile wird festgelegt, welche Backend-Sektion verwendet werden soll.

Die Sektion „backend“ beinhaltet Anweisungen, an welche Server der Load Balancer die Verbindungsanfragen weiterleiten soll.

```
1 backend http_back
2     server webserver_1 10.0.0.101:80
3     server webserver_2 10.0.0.102:80
4     server webserver_3 10.0.0.103:80
```

In der ersten Zeile wird eine Backend-Sektion mit dem Namen „http_back“ definiert. Auf diese Sektion wird in der oberen Frontend-Sektion verwiesen. In den Zeilen 2 bis 4 sind die jeweiligen Server definiert, an die die Verbindunganfragen weitergeleitet werden. Dazu wird nach dem Schlüsselwort „server“ ein frei wählbarer Name des Servers angegeben, gefolgt von dessen IP-Adresse und Portnummer, auf dem der Dienst auf der IP-Adresse auf eingehende Verbindungen wartet. Die Kombination aus IP-Adresse und Port (<IP-ADDRESS>:<PORT>) wird Socket genannt.

Um eine Konfiguration zu testen, kann der Befehl „sudo haproxy -f haproxcy.cfg -c“ verwendet werden. Der Befehl kontrolliert die Konfigurationsdatei und zeigt Fehler in der Konfiguration als Alert-Meldung an.

Der nachfolgende Screenshot zeigt einen erkannten Fehler. Statt „bind“ wurde in der Konfiguration „xbind“ angegeben.

```
[ALERT]    (1599) : parsing [haproxy.cfg:37] : unknown keyword 'xbind' in 'frontend' section; did you mean 'bind' maybe ?
[ALERT]    (1599) : Error(s) found in configuration file : haproxy.cfg
[ALERT]    (1599) : Fatal errors found in configuration.
```

Ausschnitt der Konfigurationsprüfung der Datei „haproxy.cfg“

Genau wie ein Proxy baut der Load Balancer zwei Verbindungen auf: die eine mit dem externen, anfragenden System, die andere mit dem internen Server.

No	Source	Destination	Protocol	Length	Info
1	1.2.3.5	1.2.3.4	HTTP	494	GET / HTTP/1.1
2	10.0.0.1	10.0.0.102	HTTP	470	GET / HTTP/1.1
3	10.0.0.102	10.0.0.1	HTTP	294	HTTP/1.1 200 OK (text/html)
4	1.2.3.4	1.2.3.5	HTTP	294	HTTP/1.1 200 OK (text/html)

Wireshark-Mitschnitt der Verbindungen durch den Load Balancer

Im abgebildeten Mitschnitt werden diese beiden Verbindungen dargestellt. In der ersten Zeile ist ein eingehender HTTP-Request abgebildet. Die Quell-IP-Adresse, also die IP-Adresse des Clients, lautet 1.2.3.5. Die Adresse des Ziels, also des Load Balancers, lautet 1.2.3.4. In der zweiten Zeile ist die identische HTTP-Anfrage abgebildet. Der Load Balancer hat aber beide Adressen entsprechend der zweiten Verbindung zwischen Load Balancer und Webserver im internen Netzwerk umgeschrieben. In den Nachrichten 3 und 4 kann man die Umsetzung der IP-Adressen in die andere Richtung verfolgen.

In Kapitel 3.3.3, Abschnitt (2) über die Planung des Einsatzes eines Load Balancers wurde beschrieben, dass eine TLS-Termination am Load Balancer sinnvoll ist. Dazu wird eine Datei benötigt, die das Zertifikat und den privaten Schlüssel des Zertifikats beinhaltet. Nur so kann der Load Balancer eine verschlüsselte Verbindung mit dem externen Client aufbauen.

Die Konfiguration kann nun erweitert werden.

```
1 frontend http_front
2       bind *:80
3       bind *:443 ssl crt /etc/certs/serverkey.key
4       default_backend http_back
```

In der dritten Zeile wird der Port 443 auf allen IP-Adressen freigegeben. Der Load Balancer wartet hier auf eingehende SSL-Verbindungen (oder TLS-Verbindungen). Einem anfragenden Client wird vom Load Balancer das Zertifikat ausgeliefert.

Die Backend-Sektion bleibt unverändert, da die Kommunikation zwischen Load Balancer und Webservern im internen Netzwerk unverschlüsselt abläuft.

(3) VPN als sichere Netzwerkverbindung implementieren

Die Umsetzung des VPN-Tunnels zwischen den beiden Standorten der Rigudo GmbH soll über IPsec realisiert werden. Es gibt einige IPsec-Umsetzungen am Markt, die sich in der Art der Konfiguration unterscheiden. Die wesentlichen Parameter sind aufgrund des Standards identisch und werden meist auch wie im Standard bezeichnet.

Aktuelle IPsec-Umsetzungen für Linux sind strongSwan, Libreswan und Openswan. Sie sind Open-Source-Projekte und lösen die ältere Umsetzung „ipsec-tools“ ab, die 2014 wegen Sicherheitsproblemen einge-

stellt wurde. Die drei Projekte basieren auf FreeS/WAN (Free Secure Wide Area Networking). Der Schwan im Logo der Pakete steht demnach für S/WAN, also „sicheres öffentliches Netz". Der Aufbau eines VPN-Tunnels wird im Folgenden exemplarisch mit strongSwan realisiert.

strongSwan

Die Software strongSwan selbst hat eine längere Entwicklungsgeschichte durchlaufen. Die ältere, strokebasierte Konfiguration über ipsec.conf wird zwar häufig in Anleitungen erwähnt, ist allerdings veraltet. Im Folgenden wird auf die aktuelle Konfiguration über „swantctl" eingegangen (siehe https://docs.strongswan.org/docs/5.9/config/config.html).

Das strongSwan-Paket wird mit dem folgenden Befehl installiert:

```
sudo apt install strongSwan strongswan-pki libcharon-extra-plugins
```

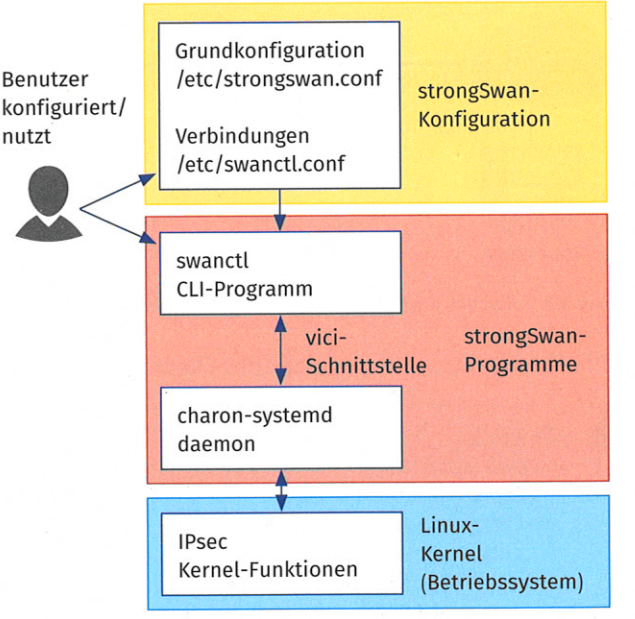
Die Konfiguration von strongSwan erfolgt im Wesentlichen in den zwei Dateien „strongswan.conf" (Grundkonfiguration der strongSwan-Module) und „swanctl.conf" (enthält die Konfiguration der Verbindungen). Beide Dateien werden standardmäßig unter „/etc/strongswan.conf" bzw. „/etc/strongswan.d/swanctl.conf" abgelegt.

In der Datei „strongswan.conf" werden die Grundkonfigurationen festgehalten. Wenn beispielsweise für alle Verbindungen ein bestimmter Parameter immer gesetzt werden soll, so kann dies hier hinterlegt werden und muss nicht bei jeder Verbindung explizit angegeben werden. Hierdurch werden Fehlkonfigurationen minimiert.

```
# strongswan.conf - strongSwan
# configuration file
#
# Refer to the strongswan.
# conf(5) manpage for details
#
# Configuration changes should
# be made in the included
# files

charon {
    load_modular = yes
    plugins {
        include strongswan.d/
charon/*.conf
    }
    start-scripts {
        load-all = /usr/sbin/
swanctl --load-all
    }
}

include strongswan.d/*.conf
```



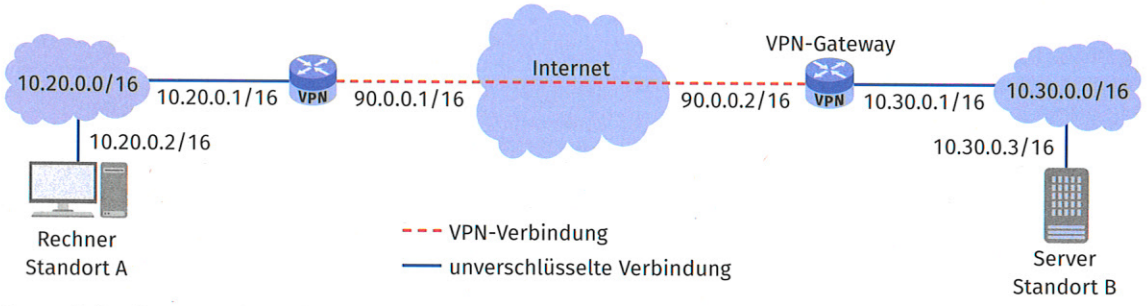
Systemaufbau und Schnittstellen von strongSwan

Zur Steuerung von strongSwan wird das Programm „swanctl" genutzt. Dieses gibt per vici-Schnittstelle (vici = Versatile IKE Control Interface) die Kommandos an den Daemon „charon" weiter, der seinerseits die eigentlichen IPsec-Kernel-Funktionen konfiguriert bzw. aufruft (Charon ist in der griechischen Mythologie der Fährmann auf dem Fluss Styx zwischen Menschenwelt und Totenreich).
Mit dem Befehl „swanctl --list-conns" werden alle bereits konfigurierten Verbindungen ausgegeben. Die folgende Tabelle enthält die wesentlichen Befehle für „swanctl".

Wesentliche Kommandozeilenparameter von „swanctl“	
Parameter	Bedeutung
--help oder -h	zeigt die möglichen Parameter an
--reload-settings oder -r	lädt die Grundkonfiguration aus „strongswan.conf“ erneut
--load-all oder -q	lädt Zugangsdaten, Zertifizierungsstellen, Pools und Verbindungen
--list-conns oder -L	zeigt alle konfigurierten Verbindungen an
--list-sas oder -l	zeigt alle aktuell aktiven IKE-SAs an
--initiate oder -i	startet eine Verbindung
--terminate oder -t	beendet eine Child- oder IKE-Verbindung
--child oder -c bzw. --child-id oder -C	gibt die entsprechende Child-Verbindung per Name oder ID (nur bei „terminate“) an
--ike oder -i bzw. --ike-id oder -I	gibt die entsprechende IKE-Verbindung per Name oder ID (nur bei „terminate“) an

Site-to-Site-Tunnel

Der Site-to-Site-Tunnel wird zur Verbindung zwischen den beiden Standorten (z. B. zwei LAN-Bereiche) über ein öffentliches Netz genutzt. Zunächst müssen die Clients in den lokalen IP-Netzen konfiguriert werden. Die Clients, die das VPN nutzen sollen, müssen das VPN-Gateway als Standardroute eingetragen haben. Die folgende Abbildung zeigt den zugrunde liegenden Netzwerkplan.



Netzwerkplan des verwendeten Site-to-Site-Tunnels

Die Konfiguration für „netplan“ des Clients im LAN-A sieht wie folgt aus:

```
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3: # Schnittstelle in LAN-A
      addresses:
        - 10.20.0.2/16
      dhcp4: no
      routes:
        - to: 0.0.0.0/0 # Standardroute zu VPN-Gateway
          via: 10.20.0.1
```

Die Konfiguration für „netplan“ des VPN-Gateways am LAN-A sieht wie folgt aus:

```
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3: # Schnittstelle in LAN-A; Bezeichnung im System kann abweichen
      addresses:
        - 10.20.0.1/16
      dhcp4: no
    enp0s8: # Schnittstelle zum Internet (in Richtung zweites VPN-Gateway)
      addresses:
        - 90.0.0.1/16
      dhcp4: no
```

Die Konfigurationen für die Clients in LAN-B und das entsprechende VPN-Gateway sind mit den entsprechenden Werten bei **addresses** und **via** identisch aufgebaut. Auf beiden VPN-Gateways muss gegebenenfalls das Routing („ip-forward“) aktiviert werden.

Die Konfiguration wird mit den Befehlen „sudo netplan generate“ und „sudo netplan apply“ aktiviert. Die Verbindung sollte vor der VPN-Konfiguration auf Erreichbarkeit (ping) in beide Richtungen geprüft werden.

PKI-Erstellung

Zur Authentifizierung der VPN-Gateways werden Zertifikate eingesetzt. Diese können entweder durch öffentliche Zertifizierungsstellen erworben oder lokal selbst erstellt werden. Die selbst erstellten Zertifikate können allerdings nicht ohne Aufwand im öffentlichen Bereich eingesetzt werden, da die ausstellende Zertifizierungsstelle eine Vertrauensstellung im öffentlichen Bereich besitzt.

Für die selbst erstellten Zertifikate wird zunächst der Schlüssel („ca-Key.pem“) der Zertifizierungsstellen erstellt. Die Schlüsseldatei „ca-Key.pem“ sollte nicht auf einem System mit Internetzugang gespeichert werden. Würde ein Angreifer diese Datei erbeuten, so wäre die gesamte PKI kompromittiert und müsste neu installiert und konfiguriert werden.

```
pki --gen --type ed25519 --outform pem > ca-Key.pem
```

Im nächsten Schritt stellt sich die Zertifizierungsstelle ein eigenes Zertifikat „ca-cert.pem“ aus. Das Zertifikat kann mit dem Befehl „pki --print“ ausgegeben werden.

```
pki --self --ca --lifetime 3650 --in ca-Key.pem --type rsa ↵
           --dn "C=DE, O=rigudo, CN=Rigudo Root CA" ↵
           --outform pem > ca-cert.pem ↵
pki --print --in ca-cert.pem
# Mögliche Ausgabe:
  subject:  "C=DE, O=rigudo, CN=Rigudo Root CA"
  issuer:   "C=DE, O=rigudo, CN=Rigudo Root CA"
  validity:  not before Sep 11 14:31:16 2022, ok
             not after  Jun 07 14:31:16 2025, ok (expires in 999 days)
  serial:    52:94:8f:25:f6:b9:7f:0e
  flags:     CA CRLSign self-signed
  subjkeyId: 9f:cf:fb:f9:db:cc:7b:81:f5:b3:73:31:e9:02:ff:a9:ba:1f:fd:a4
  pubkey:    RSA 2048 bits
  keyid:     80:30:74:97:d6:72:79:1f:b6:54:2d:71:3f:de:22:e9:3f:7b:84:47
  subjkey:   9f:cf:fb:f9:db:cc:7b:81:f5:b3:73:31:e9:02:ff:a9:ba:1f:fd:a4
```

Die Option „lifetime“ gibt die Gültigkeit des Zertifikates in Tagen (hier: 3650 Tage) an. Der Parameter „dn“ gibt den Namen innerhalb des Verzeichnisdienstes (z. B. Active Directory oder LDAP) an. Der CA-Schlüssel und das CA-Zertifikat werden genutzt, um für jede beteiligte Maschine einen eigenen Schlüssel und ein eigenes Zertifikat zu erstellen.

```
pki --gen > serverX-key.der
pki --issue --in serverX-key.der --type priv --cacert ca-cert.pem ↵
    --cakey ca-key.pem --dn "C=DE O=rigudo CN=serverX" ↵
    --san 90.0.0.X
> serverX-cert.der
```

Für die Endpunkte werden eigene Zertifikate benötigt. Zur Generierung der Zertifikate wird folgender Befehl genutzt:

```
pki --gen --type rsa --outform pem > clientA.pem
pki --gen --type rsa --outform pem > clientB.pem
```

Die so erstellten Zertifikate müssen den beiden VPN-Gateways bekanntgegeben werden. Im Ordner „/etc/swanctl/“ werden standardmäßig die entsprechenden Unterordner angelegt. Die Zertifikate der Endpunkte (VPN-Gateway und Clients) werden in „/etc/swanctl/x509“ abgelegt. Um die Echtheit der Zertifikate überprüfen zu können, muss das Zertifikat der ausstellenden Stelle (CA) im Ordner „/etc/swanctl/x509ca“ abgelegt werden. Die Schlüssel von Server A und B („serverX-key.der“) werden jeweils auf dem Server selbst abgelegt.

Konfiguration der Site-to-Site-Verbindung

In der Datei „swanctl.conf“ werden die einzelnen Verbindungen konfiguriert. Hier werden die Parameter für die initiale IKE-Verbindung sowie für die eigentliche Nutzdatenverbindung („child“) festgelegt. Die Klammerung spiegelt die Abhängigkeit der Verbindungen wider. Die äußere Klammer umfasst die initiale IKE-Verbindung, die zunächst existieren muss, um hierüber gesichert die Parameter der Nutzdatenverbindung austauschen zu können.

```
connections {
   gw-gw {
      local_addrs = 90.0.0.1 # öffentliche IP der eigenen Seite
      remote_addrs = 90.0.0.2 # öffentliche IP der Gegenstelle

      local {
         auth = pubkey
         certs = servera-cert.der

         # Die ID ist freiwählbar; hier wurde die IP-Adresse verwendet
         id = 90.0.0.1
      }
      remote {
         auth = pubkey
         certs = serverb-cert.der
         id = 90.0.0.2
      }
     children {
        net-net {
           # local_ts: privates Netz auf der eigenen Seite
           local_ts = 10.20.0.0/16
           # remote_ts: privates Netz auf der Gegenstelle
           remote_ts = 10.30.0.0/16
```

```
            # Start-/Stop-Skript zur Konfiguration der Firewall-Regeln
            updown = /etc/swanctl/vpn-up.sh
            esp_proposals = aes128gcm128-x25519 # Verschlüsselungsverfahren
        }
    }
    version = 2
    mobike = no
    proposals = aes128-sha256-x25519
  }
}
```

Parameter der IKE-Verbindung		
Parameter	**Bedeutung**	**Beispiel**
<conn>	Verbindungsname; hier Gateway zu Gateway	gw-gw
local-addrs	IP-Adresse des konfigurierten Endpunktes für die IKE-Verbindung	local_addrs = 90.0.0.1
remote_ addrs	IP-Adresse des entfernten Endpunktes (Gateway oder einzelner PC, z. B. im Homeoffice) für die IKE-Verbindung	remote_addrs = 90.0.0.2
local	Konfiguration der lokalen Authentifikationsparameter; enthält eine frei wählbare ID und den Authentifikationsmechanismus	local { auth = pubkey certs = servera-cert.der id = 90.0.0.1 }
remote	Konfiguration der entfernten Authentifikationsparameter; enthält eine frei wählbare ID und den Authentifikationsmechanismus	remote { auth = pubkey certs = serverb-cert.der id = 90.0.0.2 }
children	Konfiguration der Nutzdatenverbindung; enthält Netzadresse des Netzwerks hinter dem VPN-Gateway und Verschlüsselungsverfahren	children { remote_ts = 10.30.0.0/16 … esp_proposals = aes128gcm128-x25519 }

Wenn der Transport-Mode verwendet werden soll, so wird dies mit dem Parameter „mode = transport“ in der äußeren Klammer angegeben. Wenn nichts angegeben wird, wird die Verbindung standardmäßig im Tunnel-Mode konfiguriert. Mit dem Parameter „version“ wird das sichere IKEv2 ausgewählt.

Neben diesen grundlegenden Konfigurationen wird die Firewall über die neue Verbindung mit dem Parameter „updown“ (up: Start, down: Abbau) informiert, damit die IPsec-Pakete der Gegenstelle weitergeleitet werden. Der Aufruf dieser Firewall-Regeln erfolgt über ein Skript, welches im Parameter „updown“ angegeben wird.

Ein möglicher Inhalt dieses Skript könnte wie folgt aussehen:

```
# vpn-up.sh Start/Stop Script für IPsec-Verbindung
# Hinweis: Hier ist nur der START-Teil gezeigt

ip route add 10.30.0.0/16 via 90.0.0.2
iptables -A INPUT -i enp0s8 -p esp -j ACCEPT
iptables -A FORWARD -s 10.30.0.0/16 -d 10.20.0.0/16 --proto esp -j ACCEPT
iptables -A FORWARD -s 10.20.0.0/16 -d 10.30.0.0/16 --proto esp -j ACCEPT
iptables -A OUTPUT -o enp0s8 -p esp -j ACCEPT
```

Alternativ kann hier auch nftables verwendet werden. Die Parameter „rekeying“ und „reauthentication“ (im Beispiel nicht genutzt) legen fest, nach welchem Zeitraum die Schlüssel neu generiert werden müssen bzw. nach welchem Zeitraum die Verbindung erneut authentifiziert werden muss.

Die Konfiguration kann mit dem Befehl „swanctl --load-all“ geladen werden.

```
swanctl --load-all

# Ausgabe:

loaded certificate from '/etc/swanctl/x509/servera-cert.der'
loaded certificate from '/etc/swanctl/x509/clientb-cert.der'
loaded certificate from '/etc/swanctl/x509/clienta-cert.der'
loaded certificate from '/etc/swanctl/x509/serverb-cert.der'
loaded certificate from '/etc/swanctl/x509ca/ca-cert.pem'
loaded RSA key from '/etc/swanctl/private/servera-key.der'
no authorities found, 0 unloaded
no pools found, 0 unloaded
loaded connection 'gw-gw'
successfully loaded 1 connections, 0 unloaded
```

Die konfigurierten Verbindungen können über den Befehl „swanctl --list-conns“ angezeigt werden.

```
swanctl --list-conns

# Ausgabe:

gw-gw: IKEv2, no reauthentication, rekeying every 14400s
  local: 90.0.0.1
  remote: 90.0.0.2
  local public key authentication:
    id: 90.0.0.1
    certs: C=DE 0=rigudo CN=servera
  remote public key authentication:
    id: 90.0.0.2
    certs: C=DE 0=rigudo CN=serverb
  net-net: TUNNEL, rekeying every 3600s
    local: 10.20.0.0/16
    remote: 10.30.0.0/16
```

Zu Testzwecken kann die IPsec-Verbindung mit dem Befehl „swanctl --initiate --child net-net“ gestartet werden. Der Ablauf entspricht dem in Kapitel 3.3.3, Abschnitt (3) beschriebenen VPN-Verbindungsaufbau mit IKEv2.

```
swanctl --initiate --child net-net

# Ausgabe:

[IKE] initiating IKE_SA gw-gw[12] to 90.0.0.2
[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_
IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
```

```
[NET] sending packet: from 90.0.0.1[500] to 90.0.0.2[500] (240 bytes)
[NET] received packet: from 90.0.0.2[500] to 90.0.0.1[500] (273 bytes)
[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP)
CERTREQ N(FRAG_SUP) N(HASH_ALG) N(CHDLESS_SUP) N(MULT_AUTH) ]
[CFG] selected proposal: IKE:AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_
SHA2_256/CURVE_25519
[IKE] received cert request for "C=DE, O=rigudo, CN=Rigudo Root CA"
[IKE] sending cert request for "C=DE, O=rigudo, CN=Rigudo Root CA"
[IKE] authentication of '90.0.0.1' (myself) with RSA_EMSA_PKCS1_SHA2_256
successful
[IKE] sending end entity cert "C=DE 0=rigudo CN=servera"
[IKE] establishing CHILD_SA net-net{35}
[ENC] generating IKE_AUTH request 1 [ IDi CERT N(INIT_CONTACT) CERTREQ IDr
AUTH SA TSi TSr N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
[ENC] splitting IKE message (1568 bytes) into 2 fragments
[ENC] generating IKE_AUTH request 1 [ EF(1/2) ]
[ENC] generating IKE_AUTH request 1 [ EF(2/2) ]
[NET] sending packet: from 90.0.0.1[500] to 90.0.0.2[500] (1252 bytes)
[NET] sending packet: from 90.0.0.1[500] to 90.0.0.2[500] (388 bytes)
[NET] received packet: from 90.0.0.2[500] to 90.0.0.1[500] (1252 bytes)
[ENC] parsed IKE_AUTH response 1 [ EF(1/2) ]
[ENC] received fragment #1 of 2, waiting for complete IKE message
[NET] received packet: from 90.0.0.2[500] to 90.0.0.1[500] (324 bytes)
[ENC] parsed IKE_AUTH response 1 [ EF(2/2) ]
[ENC] received fragment #2 of 2, reassembled fragmented IKE message
(1488 bytes)
[ENC] parsed IKE_AUTH response 1 [ IDr CERT AUTH SA TSi TSr ]
[IKE] received end entity cert "C=DE 0=rigudo CN=serverb"
[CFG] using trusted ca certificate "C=DE, O=rigudo, CN=Rigudo Root CA"
[CFG] checking certificate status of "C=DE 0=rigudo CN=serverb"
[CFG] certificate status is not available
[CFG] reached self-signed root ca with a path length of 0
[CFG] using trusted certificate "C=DE 0=rigudo CN=serverb"
[IKE] authentication of '90.0.0.2' with RSA_EMSA_PKCS1_SHA2_256 successful
[IKE] IKE_SA gw-gw[12] established between 90.0.0.1[90.0.0.1]...90.0.0.2
[90.0.0.2]
[IKE] scheduling rekeying in 14240s
[IKE] maximum IKE_SA lifetime 15680s
[CFG] selected proposal: ESP:AES_GCM_16_128/NO_EXT_SEQ
[IKE] CHILD_SA net-net{35} established with SPIs c46dee1f_i cbf49406_o and
TS 10.20.0.0/16 === 10.30.0.0/16
initiate completed successfully
```

Die eckigen Klammern geben den Bereich an. In der ersten [CFG]-Zeile wird das ausgewählte Proposal für die IKE-Verbindung angezeigt. Im Anschluss findet die Authentifizierung der Gegenstellen mittels Zertifikaten statt. In der letzten Zeile werden die verwendeten SPIs „c46dee1f_i“ und „cbf49406_o“ angezeigt.

! Der Security Parameter Index (SPI) dient als Referenz auf die Sicherheitsparameter und wird im IPsec-Header übertragen.

Mit dem Anhang „_i“ bzw. „_o“ wird angegeben, in welche Richtung (Input bzw. Output) der jeweilige SPI genutzt wird. Eine bestehende IPsec-Verbindung kann mit dem Befehl „swanctl --terminate --child net-net“ abgebaut werden. Soll nur die IKE-Verbindung abgebaut werden, so wird der Befehl „swanctl --terminate --ike gw-gw“ verwendet.

Kompetenzcheck

1. Diskutieren Sie in der Gruppe, ob der Einsatz der NAT-Technik bei IPv6 sinnvoll ist.
2. Erläutern Sie, warum es sinnvoll sein kann, eine HTTPS-Verbindung beim Load Balancer enden zu lassen und die Daten nicht bis zum bedienenden Webserver zu verschlüsseln.
3. Sie sollen die Konfiguration für die Site-to-Site-VPN-Verbindung ergänzen. Erstellen Sie die „netplan"-Konfiguration für den Client und das VPN-Gateway in LAN-B für das vorgestellte Beispiel.
4. Notieren Sie wesentliche Aspekte aus diesem Abschnitt in Ihrem Projektjournal.
5. Bearbeiten Sie Aufgabe 3 der Lernsituation 4 im Arbeitsbuch.

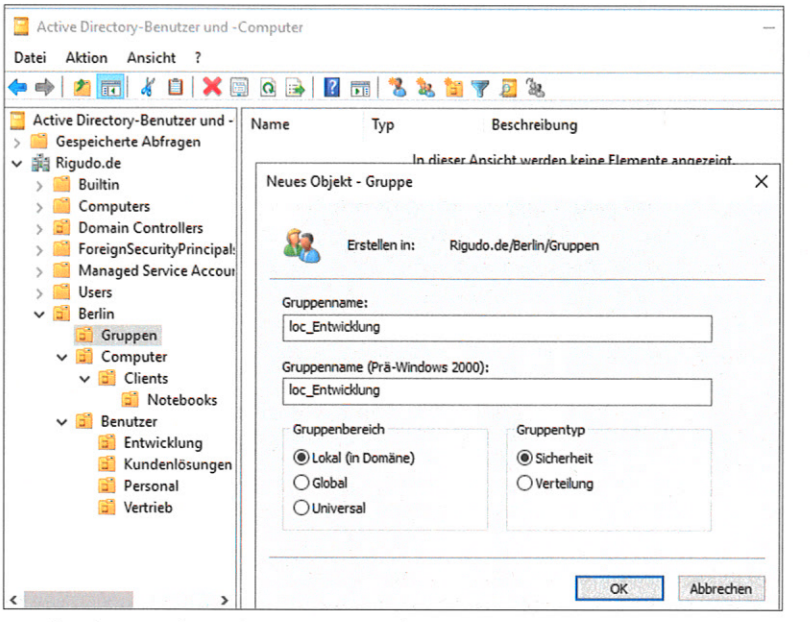
A3

3.4.4 Sicherheitsgruppen und Gruppenrichtlinien umsetzen

S **Sie sollen mithilfe von Sicherheitsgruppen Role Based Access Control umsetzen und mithilfe von Gruppenrichtlinien Netzwerkfreigaben in die Arbeitsumgebung von Benutzern einbinden.**

(1) Sicherheitsgruppen implementieren

Die Abteilungen Vertrieb, Personal, Kundenlösungen und Entwicklung sollen ihre Daten auf zentralen Servern abspeichern (siehe auch Kapitel 3.3.5). In diesem Kapitel soll die Speicherung über Netzwerkfreigaben in der Windows-Domäne betrachtet werden und wie damit Role Based Access Control (RBAC) umgesetzt wird. Die Umsetzung soll nach dem AGDLP-Schema erfolgen. Es werden folgende Schritte durchlaufen (siehe auch Kapitel 1.3.1):



Erstellen der Domain Local Group „loc_Entwicklung"

1. Domain Local Group erstellen
2. NTFS-Berechtigungen mithilfe der Domain Local Group setzen
3. Freigabe einrichten
4. Globale Group erstellen und der Domain Local Group zuordnen
5. Benutzer aus den Abteilungen der Global Group zuordnen

1. Domain Local Group erstellen

Mit dem Hochstufen eines Windows-Servers zu einem Domain Controller erfolgt die ganze Benutzerverwaltung unter dem Tool „Active Directory-Benutzer und -Computer". Dort findet eine Gruppierung mithilfe von Containern und Organizational Units (OU) statt. Im Gegensatz zu OUs sind Container nicht löschbar. Unter dem Bereich „Benutzer" sind alle Benutzer und Sicherheitsgruppen aufgenommen. OUs haben im Ordnersymbol ein kleines Piktogramm, wohingegen Container nur mit einem Ordnersymbol

dargestellt werden. OUs lassen sich beliebig erstellen und anordnen und bilden die Grundlage, um die Struktur von Organisationen abzubilden.

Für die Rigudo GmbH wird für den Standort Berlin eine OU erstellt, unter der jede weitere Organisation von Computern und Nutzern des Standorts vorgenommen wird. Für Sicherheitsgruppen wird eine OU-Gruppe erstellt und darin für jede Netzwerkfreigabe eine Domain Local Group. Es ist sinnvoll, eine bestimmte Nomenklatur der Bezeichnung zu verwenden, was zur Übersichtlichkeit und zur Vermeidung von Fehlern beiträgt. Hier wurde das Präfix „loc_" für Domain Local Groups gewählt.

2. NTFS-Berechtigungen mithilfe der Domain Local Group setzen

NTFS-Berechtigungen können über den Dateiexplorer im Kontextmenü „Eigenschaften → Sicherheit" angezeigt und verändert werden. Es sind vier Gruppen voreingestellt:

- ERSTELLER-BESITZER
- SYSTEM
- Administratoren
- Benutzer

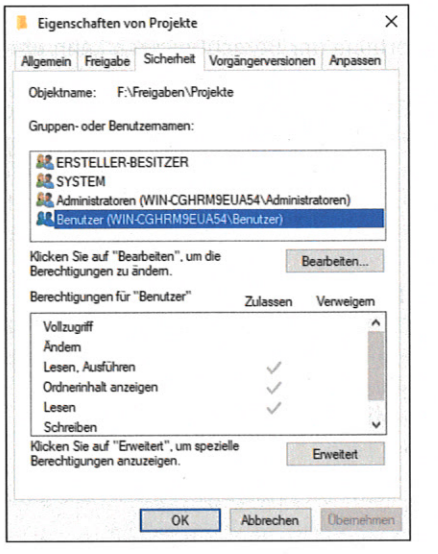
Die mit Großbuchstaben geschriebenen Gruppen sind sogenannte spezielle Identitätsgruppen (special identity groups).

Beispiel: Die Gruppe ERSTELLER-BESITZER beinhaltet den Benutzer, der den Ordner oder die Datei erstellt hat.

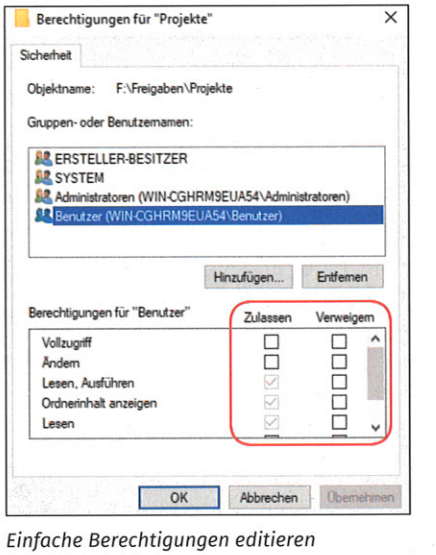
Schaut man in die Berechtigungen für die Gruppe „Benutzer", sieht man die sogenannten **einfachen Berechtigungen**:

- Vollzugriff
- Ändern
- Lesen, Ausführen
- Ordnerinhalte anzeigen
- Lesen
- Schreiben

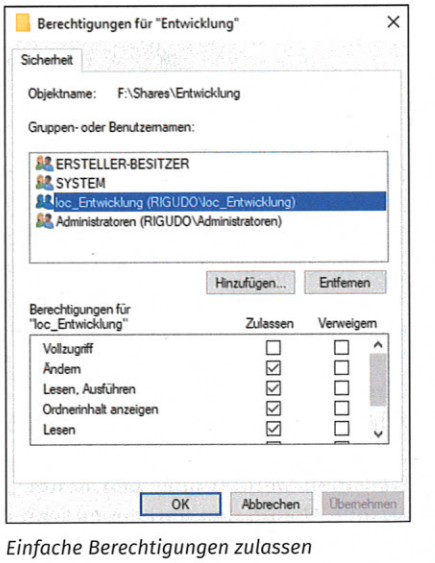
Mit der Auswahl „Bearbeiten" wird die Darstellung etwas anschaulicher. Zu sehen sind die zwei Spalten „Zulassen" und „Verweigern", die eine Eigenheit der NTFS-Berechtigungen beschreiben, die aber auch in einem Linux-Dateisystem eingeschaltet werden können. Zu sehen ist, dass die Haken beim „Lesen, Ausführen", „Ordnerinhalte anzeigen" und „Lesen" ausgegraut sind. Diese Haken können nicht entfernt werden, da die Berechtigungen vom übergeordneten Ordner geerbt wurden. Diese Berechtigungen können nur dort geändert werden. Es ist aber möglich, weitere Berechtigungen zu erteilen: Ist z. B. die Zulassenbox für „Ändern" nicht ausgegraut, kann dort ein Haken gesetzt werden. Dadurch wird die Berechtigung aktiviert und erscheint im Unterordner dann ausgegraut als vererbte Berechtigung. Für die Einschränkung von Berechtigungen steht die „Verweigern"-Spalte zur Verfügung. Wird hier der Haken bei „Lesen, Ausführen" gesetzt, wird die Berechtigung überschrieben. Damit wird für untergeordnete Ordner die Berechtigung vererbt übernommen, eine weitere Änderung ist nicht möglich.



Einfache Berechtigungen anzeigen



Einfache Berechtigungen editieren



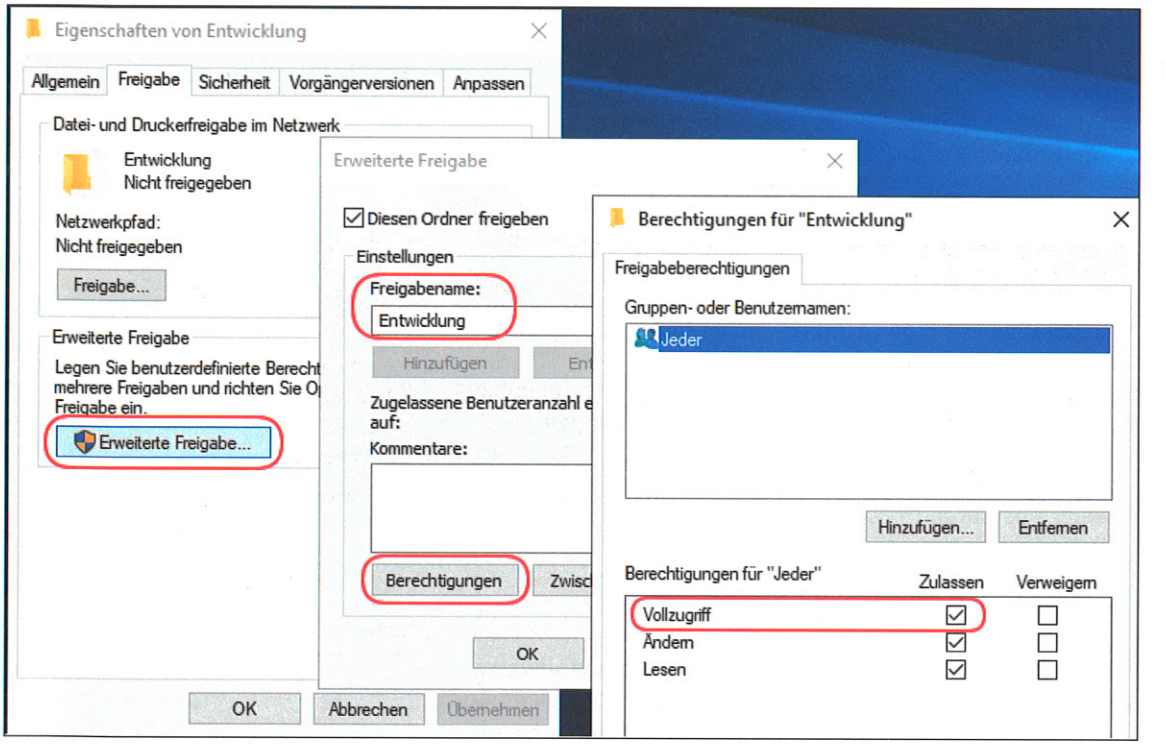
Einfache Berechtigungen zulassen

Weitere Änderungen sind an dieser Stelle nur noch durch Aufhebung der Vererbung möglich. Die Vererbung der Berechtigungen kann über „Erweiterte Einstellungen“ aufgehoben werden.

Für die Einrichtung eines Gruppenordners werden folgende Schritte durchgeführt:
- Aufheben der vererbten Berechtigungen
- Löschen der Berechtigungen für die Gruppe Benutzer
- Erstellen einer Gruppe, die Berechtigungen erhält
- Zuordnung der Gruppe zum Ordner und Berechtigungen auf „Ändern“ setzen

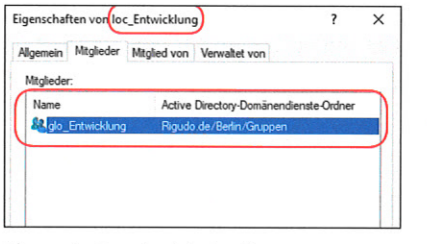
3. Freigabe einrichten

Damit der eingerichtete Ordner als Netzwerkfreigabe auf Clients eingebunden werden kann, muss er als Freigabe konfiguriert werden. Freigaben erfolgen über Zuweisung von Berechtigungen:
- Vollzugriff
- Ändern
- Lesen



Freigabe einrichten

Die NTFS-Berechtigungen und die Freigabe-Berechtigungen werden nacheinander geprüft. Ein Benutzer, der über ein Netzwerk zugreift, muss zuerst die entsprechenden Freigabe-Berechtigungen haben. Hat er beispielsweise lesenden Zugriff, muss auch mindestens der lesende Zugriff per NTFS-Berechtigung vorhanden sein. Höhere NTFS-Berechtigungen ergeben jedoch keine höheren Berechtigungen für den Zugriff. Daher ist es sinnvoll, die Freigabe-Berechtigung immer auf Vollzugriff zu setzen und dann die gewünschten Berechtigungen per NTFS zu vergeben. Dadurch sind die Berechtigungen sowohl beim Netzwerkzugriff als auch beim lokalen Zugriff gleich.

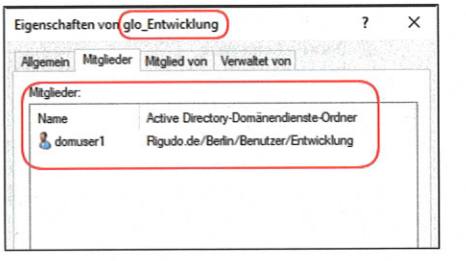


Eigenschaften der lokalen Gruppe

Freigaben werden über den Reiter „Freigaben“ über das Kontextmenü „Eigenschaften eines Ordners“ erstellt. Neben den Berechtigungen kann ein abweichender Freigabename gewählt werden, der für alle Freigaben auf dem Server eindeutig sein muss.

4. Global Group erstellen und der Domain Local Group zuordnen
Auf gleiche Weise, wie die Domain Local Groups zuvor eingerichtet wurden, werden jetzt die Global Groups erstellt. Hier wird für die Nomenklatur das Präfix „glo_" verwendet. Anschließend wird die Zuordnung der globalen zur lokalen Gruppe vorgenommen. Die Schachtelung der Gruppen ergibt sich aus der Reichweite (Scope) der unterschiedlichen Gruppen. Global Groups können über mehrere Domains verwendet werden, wenn diese eine Vertrauensstellung zueinander haben. Dahingegen können Domain Local Groups nur in einer Domain verwendet werden.

5. Benutzer aus den Abteilungen der Global Group zuordnen
Im letzten Schritt der AGDLP-Konfiguration werden die eigentlichen Benutzer angelegt und der Global Group zugewiesen. Damit ist die Konfiguration abgeschlossen. Um neuen Benutzern aus der jeweiligen Abteilung Zugriff auf die Freigabe zu geben, müssen diese nur der entsprechenden globalen Gruppe zugewiesen werden. Benutzer, die in eine andere Abteilung wechseln, werden zwischen den jeweiligen Gruppen verschoben.

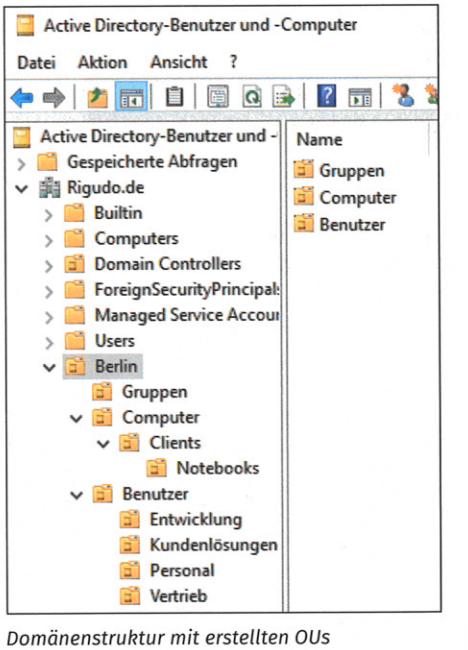


Eigenschaften der globalen Gruppe

(2) Gruppenrichtlinien implementieren

Wie zuvor beschrieben, wird die abzubildende Organisationsstruktur mit OUs erstellt. Für den Standort Berlin ist eine OU und darunter die bereits besprochene Gruppen-OU zu unterteilen. Somit stehen eine OU für Benutzer und eine für Computer zur Verfügung. Diese Unterteilung dient dazu, Gruppenrichtlinien anzuwenden.

Wie in Kapitel 1.3.1 dargelegt, werden Gruppenrichtlinien in ihrer Wirkung in Computerrichtlinien und Benutzerrichtlinien unterschieden. Exemplarisch wird hier die Einbindung der Netzlaufwerke für die jeweiligen Benutzer gezeigt. Als zweites Beispiel soll die Umsetzung der vom BSI empfohlenen Härtungsmaßnahmen für Windows-Clients besprochen werden.

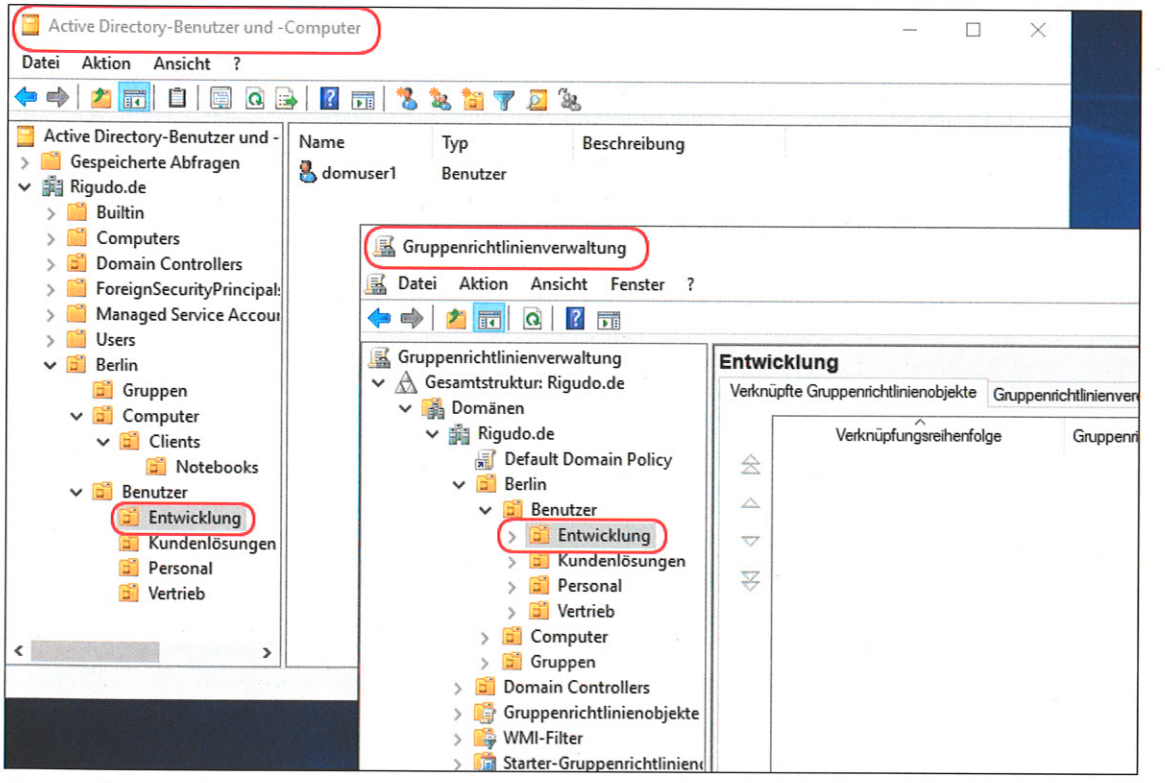


Domänenstruktur mit erstellten OUs

Im vorherigen Abschnitt wurde die Einrichtung der Netzwerkfreigabe für die Abteilungen Personal, Vertrieb und Entwicklung dargestellt. Für einen Benutzer der Abteilung soll automatisch die Netzwerkfreigabe auf einem Windows-Client eingebunden werden. Dabei soll die Bindung unabhängig vom Computer sein, auf dem er sich anmeldet. Dieser Hinweis deutet auf eine Benutzerregel hin, die entsprechend an eine OU mit Benutzern gekoppelt wird. Alle Benutzer der Entwicklung werden also in die OU „Berlin/Benutzer/Entwicklung" verschoben.

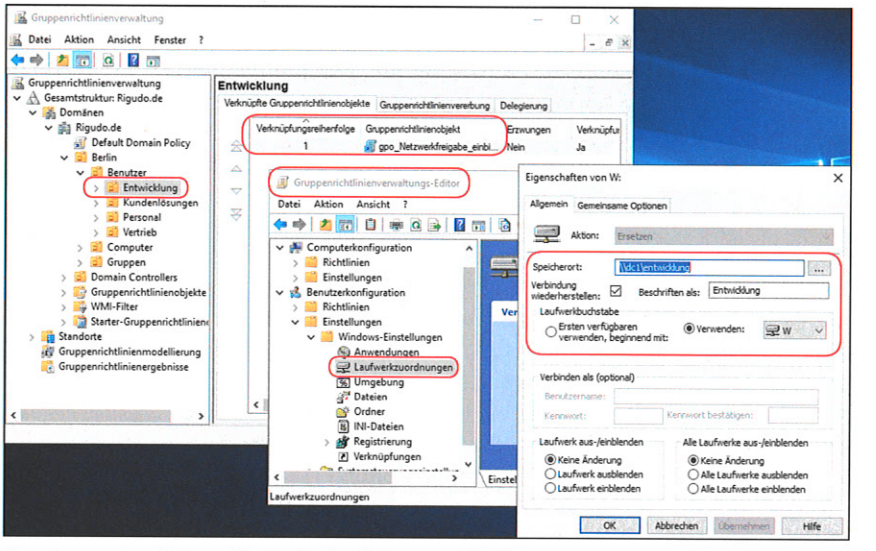
Im Bereich **„Active Directory-Benutzer und -Computer"** wird die OU-Struktur erstellt und die Benutzer bzw. Computer werden in die jeweilige OU sortiert. Innerhalb des **„Gruppenrichtlinienverwaltung"** wird die so erzeugte OU-Struktur automatisch abgebildet und es können Gruppenrichtlinien zugeordnet werden.

Für die OU „Entwicklung" wird ein Group Policy Object (GPO) erstellt. In diesem GPO können alle Gruppenrichtlinien editiert werden, die für die entsprechende OU angewendet werden sollen. Grundsätzlich könnten im erstellten GPO alle nötigen Einstellungen für die OU vorgenommen werden. Es empfiehlt sich aber, die Einstellungen zu gruppieren und für jede Gruppe ein eigenes GPO zu erstellen. Hier wird die erstellte Freigabe als Laufwerksbuchstabe „W:" auf dem Client eingebunden. Zu beachten ist, dass die Informationen aus Sicht des Clients zu betrachten sind. Daher ist die Quelle der Freigabe in der sogenannten **Uniform Naming Convention (UNC)** in der Form „\\dc1\Entwicklung" anzugeben.



Zusammenhang zwischen AD-Struktur und Gruppenrichtlinienverwaltung der OU „Entwicklung“

In der OU-Struktur sind unter „Computer“ etwa die OU „Clients“ und darunter Notebooks in extra OUs gruppiert. Für Notebooks sind beispielsweise gesonderte Absicherungen oder eine Anbindung über VPN an das Firmennetzwerk zu konfigurieren. Das kann über spezielle Gruppenrichtlinien erfolgen, die für die Desktops nicht nötig sind. Werden aber beide Systeme mit Windows betrieben, können Gruppenrichtlinien, die sowohl für Desktops als auch für Notebooks sinnvoll sind, auf die OU „Clients“ angewendet werden.



Zuordnung einer Netzwerkfreigabe durch Gruppenrichtlinie

Ein Beispiel für solche Gruppenrichtlinien sind die Einstellungen, die das Bundesamt für Sicherheit in der Informationstechnik (BSI) für die Härtung von Windows-Clients empfiehlt (vgl. APP.2.2 für AD und SiSyPHuS für Windows-Clients).

Kompetenzcheck

1. Beschreiben Sie ein Szenario, bei dem es sinnvoll ist, dass die stationären Rechner in einer OU und die Notebooks in einer untergeordneten OU organisiert werden.
2. Recherchieren Sie den Begriff „administrative Freigabe“ und beschreiben Sie diesen in eigenen Worten.
3. Notieren Sie wesentliche Aspekte aus diesem Abschnitt in Ihrem Projektjournal.
4. Bearbeiten Sie die Aufgabe 4 der Lernsituation 4 im Arbeitsbuch.

A4

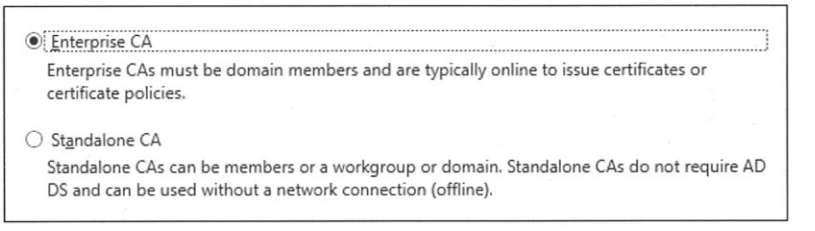
3.4.5 Zertifikatsmanagement implementieren

In Kapitel 3.3.6, Abschnitt (2) zur Planung einer Zertifizierungsstelle (Certificate Authority, CA) wurde beschrieben, dass die Rigudo GmbH eine CA auf Basis eines Windows-Servers plant. Als Grundlage werden dazu ein Windows-Server, in diesem Beispiel Windows Server 2019, und die Sicherheitsupdates installiert.

Für die Installation einer Zertifizierungsstelle muss im „Server Manager“ die Serverrolle „Active Directory Certificate Services“ installiert werden. Als „Role Service“ wird zunächst „Certificate Authority“ ausgewählt.

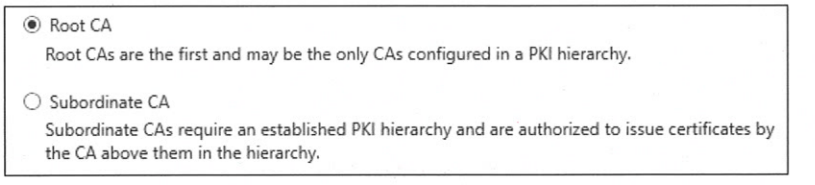
Nach der Installation der CA-Rolle muss die Zertifizierungsstelle konfiguriert werden. Hier muss der Benutzer angegeben werden, unter dessen Privilegien der Dienst konfiguriert wird. Für eine vom Active Directory (AD) unabhängige Zertifizierungsstelle reichen die Rechte des lokalen Administrators aus. Wenn die CA in das AD integriert sein soll, wird ein Account eines AD-Administrators benötigt.

Bei der Wahl des Typs der Zertifizierungsstelle hat sich die Rigudo GmbH für „Enterprise CA“ entschieden. Dieser Typ wird hier ausgewählt.



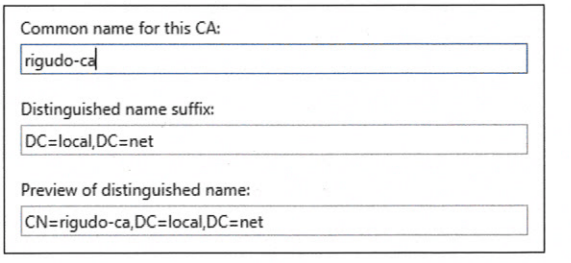
Festlegung des Typs der Zertifizierungsstelle

Anschließend kann zwischen Root CA und untergeordneter Zertifizierungsstelle gewählt werden. Während der Planung für die interne Zertifizierungsstelle hat sich die Rigudo GmbH für eine Root-CA entschieden.



Verfeinerung der CA Auswahl

Im nächsten Schritt kann ein vorhandener privater Schlüssel angegeben oder ein neuer privater Schlüssel angelegt werden. Die Rigudo GmbH verwendet noch keine Zertifikate und legt einen neuen Schlüssel an. Dazu müssen zuerst Verschlüsselungsparameter festgelegt werden. Dabei ist es sinnvoll, eine ausreichend große Schlüssellänge zu wählen (für RSA z. B. mind. 2048 Bit). Anschließend wird der Name der Zertifizierungsstelle „rigudo-ca“ festgelegt. Der Name ist in allen signierten Zertifikaten der CA enthalten.

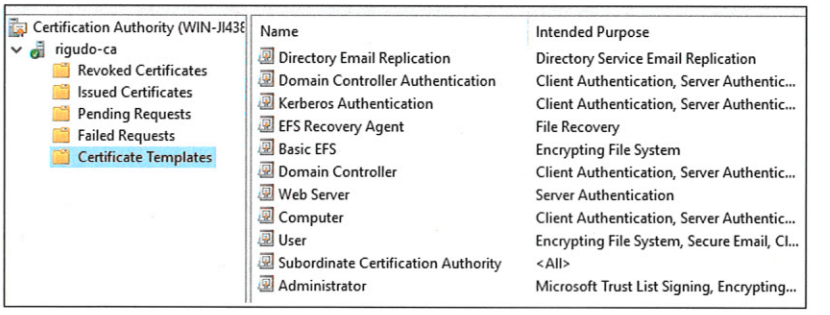


Festlegung des Namens der CA

Im Anschluss wird der Gültigkeitszeitraum des Stammzertifikats festgelegt. Dieser Zeitraum sollte größer als der Gültigkeitszeitraum der ausgestellten Zertifikate sein. Mit einer langen Gültigkeitsdauer ist es nicht nötig, Zertifikate zu verlängern. Wird ein langer Zeitraum gewählt, muss mit funktionierenden Certificate Revocation Lists gearbeitet werden, damit Zertifikate widerrufen werden können.

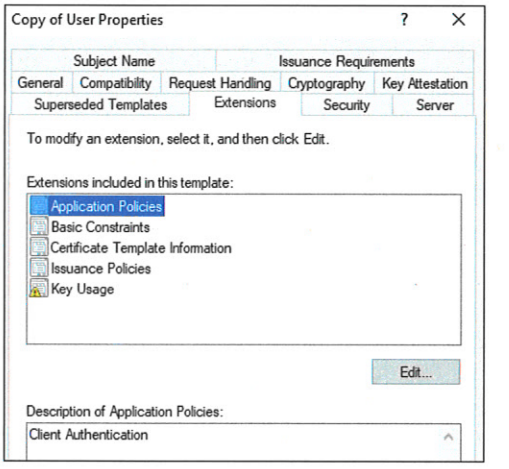
Nach Angabe der Verzeichnisse für die Zertifikatsdatenbank ist der Dienst grundlegend startbereit.

Unter der Windows CA ist es nötig, die „Vorlagen für Zertifikate" (Certificate Templates) anzupassen. Diese Vorlagen beschreiben, welche Geräte welches Zertifikat anfordern dürfen und für welche Geräte es auch automatisch erstellt wird. Die Vorlagen unterscheiden sich beispielsweise in den Vorgabewerten, z. B. Gültigkeitsdauer. Die Anpassungen werden über die „Certificate Templates Console" durchgeführt. Hier können auch neue Vorlagen, z. B. für spezielle Serverarten, angelegt werden.



Vorlagen für Zertifikate

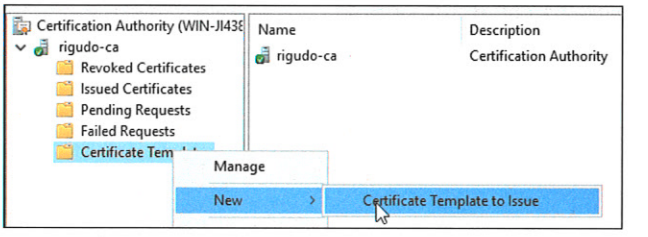
Es kann sinnvoll sein, die Vorlagen durch eine geänderte Kopie anzulegen. Bei einer internen Zertifizierungsstelle ist es gegebenenfalls nicht erwünscht, dass ein Benutzer E-Mails signieren oder die Festplatte verschlüsseln kann, ohne dass ein „Key Recovery" beim Client konfiguriert ist. In der Vorlage „User" dieser Zertifikatsmöglichkeiten kann eine Kopie des Zertifikats „User" angelegt werden. In dieser Kopie werden unter den „Extentions" der Application Policies die Punkte „Encrypting File System" und „Secure Email" gelöscht.



Kopie der Vorlage „User Properties"

Nach dem Kopieren oder Anlegen einer Vorlage muss diese der Zertifizierungsstelle zugewiesen werden, damit sie verteilt und verwendet werden kann.

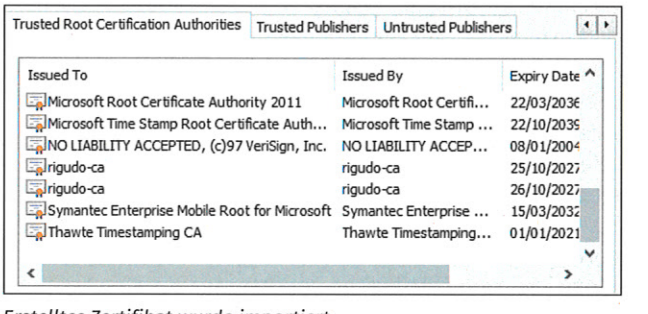
Nachdem die Vorlagen angepasst sind, werden diese auf den jeweiligen Systemen, wenn gewünscht, automatisch angewendet.



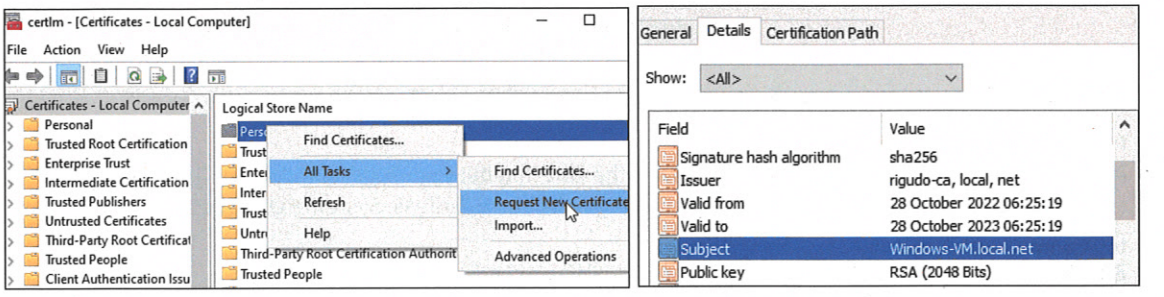
Erstellen eines neuen Zertifikats

Das Stammzertifikat wird beispielsweise an alle Geräte verteilt, damit andere Zertifikate der lokalen CA validiert werden können.

Der Benutzer kann auch Zertifikate selbst anfordern. Diese Verfahrensweise muss, in Abhängigkeit des Zertifikats, beim Server in der jeweiligen Vorlage konfiguriert sein. Auf den Request erfolgt das Ausrollen des Zertifikats.



Erstelltes Zertifikat wurde importiert



Kompetenzcheck

1. Beschreiben Sie die Funktion eines Templates bei der Zertifizierungsstelle.
2. Besprechen Sie zu zweit, welche Vorteile die Verwendung einer untergeordneten CA bietet, wenn die übergeordnete CA eine öffentliche CA ist.
3. Erläutern Sie, warum es sinnvoll sein kann, wenn ein Unternehmen sowohl eine interne Zertifizierungsstelle als auch eine interne untergeordnete CA verwendet.
4. Notieren Sie wesentliche Aspekte aus diesem Abschnitt in Ihrem Projektjournal.
5. Bearbeiten Sie die Aufgaben 4 und 5 der Lernsituation 4 im Arbeitsbuch.

A4
A5

3.5 Wirksamkeit der umgesetzten Maßnahmen überprüfen

S **Sie sollen die Sicherheit des vernetzten Systems prüfen und das erreichte Sicherheitsniveau in Bezug auf Kundenanforderungen, eingesetzte Maßnahmen und Wirtschaftlichkeit bewerten.**

Nach der Planung verschiedener Maßnahmen wurden einige davon im letzten Kapitel exemplarisch umgesetzt. In diesem Kapitel wird beschrieben, wie sich die Auswirkungen von Maßnahmen überprüfen lassen. Dazu wird beispielsweise gezeigt, wie ein Netzwerk auf Schwachstellen überprüft wird und mit welchen Möglichkeiten das Berichtswesen dazu realisiert werden kann.

3.5.1 Maßnahmen auf Wirksamkeit prüfen

S **Sie sollen die umgesetzten Maßnahmen auf Wirksamkeit prüfen.**

Die getroffenen Maßnahmen zur Erhöhung der Sicherheit in der Rigudo GmbH sind auf ihre Wirksamkeit zu prüfen. Hierzu sind unterschiedliche Ebenen zu betrachten, die im Folgenden vorgestellt werden.

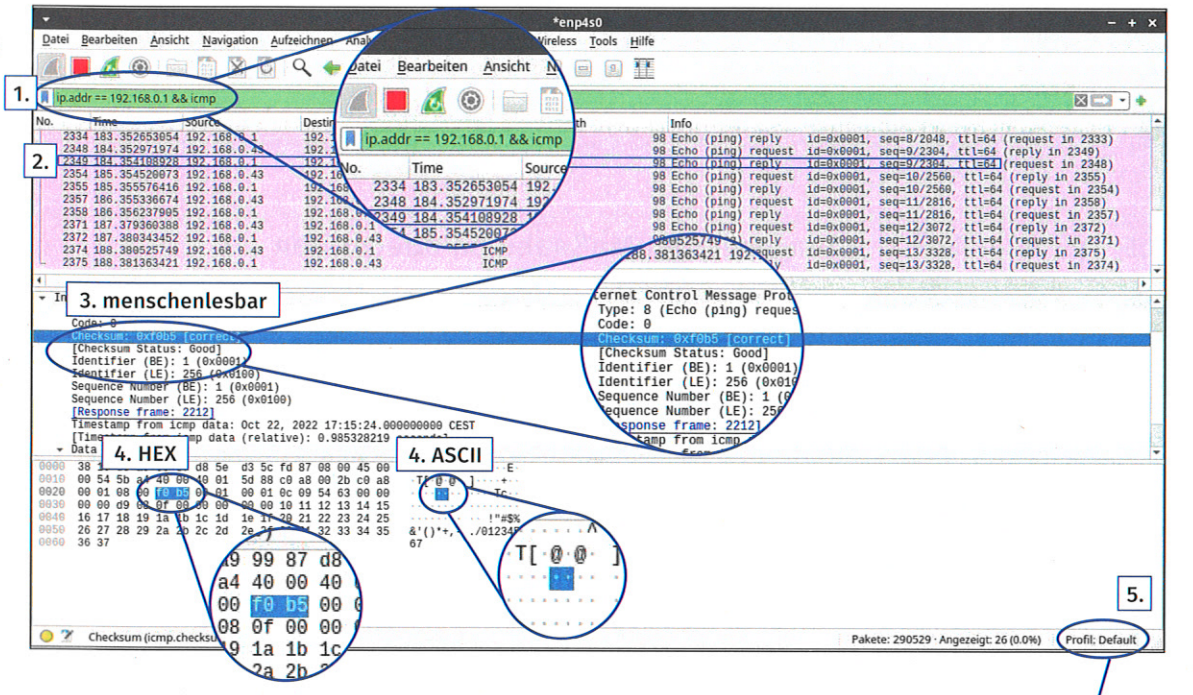
(1) Analysewerkzeuge

Einen wesentlichen Baustein zur Sicherung von Netzen liefert der aktuelle Blick auf die transportierten Daten und geöffneten Schnittstellen (Anwendungs-Ports). Mit folgenden Tools kann eine Analyse des Datenverkehrs durchgeführt werden.

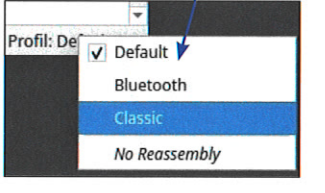
Tools zur Datenverkehrsanalyse
Wireshark Universelles Netzwerkanalysetool, für alle gängigen Betriebssysteme verfügbar
tshark Arbeitet wie Wireshark, allerdings ohne grafische Oberfläche; die mitgeschnittenen Daten werden standardmäßig direkt im Terminalfenster ausgegeben; für Headless-Systeme geeignet
tcpdump Ähnlich wie tshark; Terminal-Anwendung, für Headless-Systeme geeignet
Nmap Port-Analyser zur Untersuchung offener Ports
Postman Zur Überprüfung speziell von Webanwendungen, z. B. REST-Schnittstellen

Wireshark

Der Port-Analyser Nmap wird in Abschnitt (4) genauer beschrieben. Mit dem universellen Netzwerkanalysetool Wireshark können sowohl live als auch offline Untersuchungen vorgenommen werden. Die Standardansicht von Wireshark ist in fünf Bereiche eingeteilt (siehe unten).



1. In Bereich 1 werden die Filter definiert. Es ist möglich, mehrere Filter logisch mit UND, ODER bzw. NICHT zu verknüpfen.
2. Im Bereich 2 werden die mitgeschnittenen Pakete zeilenweise dargestellt. Der Infobereich kann durch Aktivieren des Schalters „Bearbeiten – Einstellungen – Name Resolution – Resolve transport names – ENABLE“ mit den jeweiligen Anwendungsinformationen aussagefähiger gestaltet werden.
3. Im Bereich 3 wird das im Bereich 2 ausgewählte Paket detailliert dargestellt. Jede Zeile kann aufgeklappt werden, um sich weitere Informationen anzeigen zu lassen. Die Darstellung der Zeilen entspricht dem ISO-OSI-Modell in umgekehrter Reihenfolge (höchste Schicht befindet sich unten).
4. Im Bereich 4 wird der Paketinhalt als Rohdaten in Hexadezimal byteweise und ASCII-decodiert angezeigt. Werden Buchstaben oder Texte im Paket transportiert, sind sie somit lesbar. Eine Auswahl eines Feldes oder einer Zeile im Bereich 3 wird entsprechend im Bereich 4 markiert.



5. Im Bereich 5 können Profile für unterschiedliche Umgebungen angelegt werden. Diese enthalten alle vorgenommenen Einstellungen.

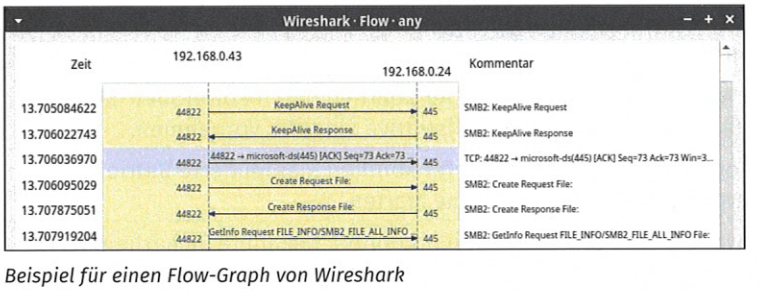
Der Einsatz von Wireshark in großen Netzen wird erst durch Filterung sinnvoll. Die aufgezeichnete Datenmenge kann durch entsprechende Capture-Filter deutlich reduziert werden. Durch den Capture-Filter werden nur bestimmte Daten aufgezeichnet. Bei Live-Mitschnitten kann durch Display-Filter die Ansicht auf die Daten dynamisch angepasst werden, ohne dass Pakete verworfen werden.

Wireshark-Filterbeispiele	
Filter	**Beschreibung**
ip.addr eq 192.168.0.1 and icmp oder alternativ: ip.addr == 192.168.0.1 && icmp	Pakete, die die IP-Adresse 192.168.0.1 und ein ICMP-Paket (z. B. Ping) enthalten (für ODER: or bzw. ||)
ip.dst eq 192.168.0.1	Pakete, die die IP-Adresse 192.168.0.1 als Zieladresse enthalten
tcp.dstport==443	Pakete, die den Ziel-TCP-Port 443 (HTTPS) enthalten
tls	Pakete, die eine mit TLS verschlüsselte Verbindung enthalten
sip.To contains "0691234"	Pakete, die im SIP-Feld „To“ den String „0691234“ enthalten

Durch Rechtsklick in die Filterzeile kann der Anzeigefilterausdruck-Dialog geöffnet werden. Hier können alle verfügbaren Protokolle inklusive der darin enthaltenen filterbaren Protokollelemente ausgewählt werden. Weiterhin können hier auch Relationen („ist gleich“, „und“ usw.) sowie die entsprechenden Werte eingegeben und von dort direkt in die Filterzeile übernommen werden.

Um einen schnellen Überblick über alle Verbindungen zu erhalten, ist es möglich, im Menü „Statistiken – Verbindungen“ den Nachrichtenfluss der untersten vier OSI-Schichten aufzulisten. Ebenfalls finden sich hier die Anzeige der Protokollhierarchie und der I/O-Graph im Bereich „Statistik“. Die Protokollhierarchie gibt die Anzahl von Paketen auf den unterschiedlichen Protokollebenen an. Hier können Unregelmäßigkeiten bzw. ungewöhnliche Protokolle identifiziert werden. Der I/O-Graph zeigt die Anzahl von Paketen über die Zeit an, sodass die Auslastung der Netzwerkkomponenten beobachtet werden kann.

Der Flow-Graph kann bei Verbindungsproblemen helfen. Hier wird die Abfolge der Nachrichten zwischen verschiedenen Endpunkten grafisch dargestellt.

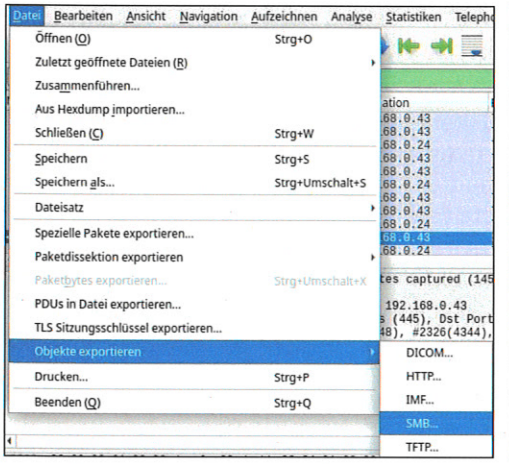


Beispiel für einen Flow-Graph von Wireshark

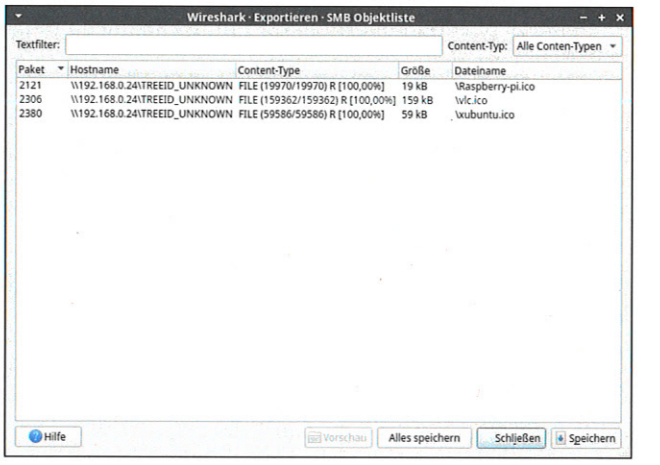
Durch Rechtsklick auf ein beliebiges Protokollfeld im mittleren Bereich kann dieses als Spalte oder Filter für die Ansicht im Bereich 2 hinzugefügt werden. Dadurch wird die Sortierung nach bestimmten Kategorien, z. B. bestimmten IP-Adressen oder TCP-Ports, ermöglicht.

Im aufgezeichneten Datenverkehr zeigt Wireshark zusammengehörende Pakete als sogenannte Objekte an, die direkt aus dem Datenverkehr gespeichert werden können.

Hinweis: Wireshark darf insbesondere im betrieblichen Umfeld nur nach Rücksprache eingesetzt werden, da das Programm hinsichtlich des Datenschutzes problematisch ist.



Export eines SMB-Objekts in Wireshark



Drei Dateien könnten exportiert werden

(2) Einzelne Geräte testen

Unter dem Schlagwort „Device Security Check" werden Maßnahmen zusammengefasst, die die Einhaltung der Sicherheit auf einem Einzelplatzrechner überprüfen. Diese sollten turnusmäßig und idealerweise softwareunterstützt (z. B. per Skript) durchgeführt werden. Die Ergebnisse dieser Tests können dann zu weiteren Maßnahmen führen.

> **!** Eine gute Übersicht über die zu testenden Aspekte liefert das Projekt „SiSyPHuS Win10" (Studie zu Systemintegrität, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10) des BSI, vgl. www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/SiSyPHuS_Win10/SiSyPHuS_node.html [01.01.2023].

Die folgenden Bereiche sollten dabei abgedeckt werden:

Bereiche eines Einzelplatzrechnertests		
Bereich	**Erklärung**	**Mögliche Auswirkung**
Trusted Platform Module (TPM)	Überprüfung, ob die notwendigen KBAs eingespielt sind und das System ordnungsgemäß funktioniert	Angreifer könnten an private Schlüssel gelangen.
PowerShell	Überprüfung der Ausführungsrechte für PowerShell-Skript	Angreifer könnten durch PowerShell-Skripte administrative Eingriffe vornehmen.
Secure Boot-Konfiguration	Aktualität der Boot-Signaturen im UEFI-Bereich überprüfen	Angreifer könnten manipulierte Betriebssysteme starten.
Software	Anwendungssoftware sollte auf aktuelle Versionen geprüft werden	Angreifer könnten bekannte Sicherheitslücken von Anwendungssoftware ausnutzen.
Sicherheitssoftware	Aktualität der Antivirensoftware bzw. sonstiger Sicherheitssoftware	Angreifer könnten Schadsoftware über E-Mails oder Webseiten einschleusen.
Microsoft-Telemetriekomponente	Überprüfung des Erhebungsumfangs	Die Menge der übertragenen Informationen kann zu unerwünschtem Abfluss von Informationen auf ausländische Server führen. Es können bis zu 400 Event-Provider aktiv sein, die Datenmenge steigt entsprechend. Mit Betriebssystemaktualisierungen können diese Einstellungen durch Microsoft geändert werden.

(3) Identity und Access Management (IAM)

Unternehmen müssen in heutiger Zeit eine große Menge vielfältiger Identitäten überprüfen können. Diese Identitäten können z. B. Angestellte, Kunden oder Geschäftspartner sein. Jede dieser Identitätsgruppen hat andere Anforderungen an das Unternehmen und daraus resultierende Berechtigungen bei der Zusammenarbeit mit dem Unternehmen.

Die einfachste Art der digitalen Identitätsprüfung ist die Verwendung von Benutzername und Passwort. Diese Identitätsüberprüfung ist meist an einen bestimmten Dienst gebunden. Idealerweise ist die Überprüfung von Identitäten benutzerbezogen. Das bedeutet, ein Benutzer kann den Identitätsnachweis bei vielen unterschiedlichen Diensten unterschiedlicher Hersteller verwenden (Single-Sign-On).

Durch ein Identity and Access Management (IAM) lässt sich verhindern, dass ein Benutzer viele Identitäten für verschiedene Konten pflegen muss. Es erleichtert es den beteiligten Diensten festzulegen, welche Berechtigungen ein Benutzer für welche Ressourcen zugewiesen bekommt. Ein IAM dient dazu, die Erteilung von Berechtigungen aufgrund von vorher festgelegten Sicherheitsrichtlinien zu gewährleisten. Ein umfassend automatisiertes IAM sollte möglichst nicht zu komplex sein, damit alle Berechtigungen nachvollziehbar bleiben.

Identity Governance and Administration (IGA) ist eine Unterkategorie eines IAM. Damit wird ein IAM um die Einhaltung von gesetzlichen Vorschriften erweitert. Das ist nötig, um beispielsweise beim Security-Audit nachzuweisen, dass alle Richtlinien eingehalten werden.

(4) Penetrationstest

In den vorausgehenden Kapiteln wurden verschiedene Maßnahmen beschrieben, um Angriffe auf Netzwerke und Server abzuwehren. Nachdem die Netzwerkinfrastruktur abgesichert ist, ist es sinnvoll, diese Absicherung zu testen. Dadurch kann die Wirksamkeit der angewendeten Maßnahmen sichergestellt werden.

Bei einem Penetrationstest wird die IT-Infrastruktur auf Schwachstellen untersucht. Dazu wird das Vorgehen eines Angreifers simuliert. Ein Angreifer sucht Schwachstellen, z. B. Zero-Day-Exploits oder andere Sicherheitslücken. Diese Schwachstellen verwendet er, um in ein System einzudringen und dort weitere Berechtigungen zu erlangen und letztendlich Daten des Unternehmens unberechtigt zu manipulieren oder herunterzuladen. Der Angriff muss nicht von außerhalb des Netzwerks – also dem Internet – kommen, sondern kann auch aus dem internen Netzwerk gestartet werden.

Zero-Day-Exploit

Ein Zero-Day-Exploit (0-Day-Exploit) ist das Ausnutzen einer Schwachstelle in einem IT-System, die ein Angreifer entdeckt hat, bevor der Hersteller Kenntnis von der Schwachstelle hat. Damit existiert noch kein Sicherheitspatch für diese Schwachstelle. Das Exploit kann verwendet werden, ohne dass es explizite Gegenmaßnahmen gibt.

Ein Penetrationstest, insbesondere im betrieblichen Umfeld, darf nur nach Absprache durchgeführt werden. Die Untersuchung der IT-Infrastruktur darf niemals destruktiv sein.

Destruktiver Test

Bei einem destruktiven Test wird ein verletzbares System absichtlich beschädigt. Dabei lernt der Tester die Schwachstellen kennen und kann ermitteln, was passiert, wenn diese Schwachstellen ausgenutzt werden. Bei einem produktiven System wird normalerweise kein destruktiver Test durchgeführt, da die Infrastruktur nicht durch das Testen gefährdet werden darf, um die Verfügbarkeit und Funktionalität zu gewährleisten.

Vor einem Test muss dessen Umfang abgestimmt werden. Dabei wird festgelegt, welche IT-Systeme, z. B. Server oder Koppelelemente, untersucht werden sollen. Der Aufwand für einen ausführlichen Penetrationstest der kompletten IT-Infrastruktur ist sehr hoch. Deshalb kann es sinnvoll sein, die zu untersuchenden Systeme einzuschränken.



Für das Ausnutzen einer Schwachstelle über ein Netzwerk muss ein System aus dem Netzwerk erreichbar sein. Im Normalfall bietet ein System Dienste über eine IP-Adresse und einen oder mehrere TCP- oder UDP-Ports an. Bei einem Penetrationstest werden zunächst das Netzwerk und dessen Systeme untersucht, um Informationen über die zu scannenden Systeme zu gewinnen. Zum Untersuchen des Netzwerks kommt oftmals ein Netzwerkscanner, z. B. Nmap, zum Einsatz. Wenn die Informationen über das Netzwerk gesammelt und Schwachstellen identifiziert wurden, kann auf die gefundene Schwachstelle gegebenenfalls ein Exploit angewendet werden, um bestimmte Rechte auf dem System zu erlangen.

Exploit

Ein Exploit ist eine Vorgehensweise oder ein Programm, um eine Schwachstelle eines Systems auszunutzen. Das Ziel des Exploits ist es, administrative Rechte zu erlangen.

Nach dem Test folgen eine ausführliche Berichterstattung und die Abgabe einer Dokumentation über den Penetrationstest. Die Abgabe muss zunächst keine Vorschläge für Gegenmaßnahmen enthalten. Ähnlich wie bei der Umsetzung des BSI-Grundschutzes kann für Systeme mit Schwachstellen eine Risikoanalyse erstellt werden. In dieser werden dann die Maßnahmen aufgeführt und es lässt sich abschätzen, wie sich das Risiko durch die Maßnahme reduziert. Durch die Implementierung der Maßnahmen kann die Sicherheit der einzelnen Systeme erhöht werden.

Es ist sinnvoll, die Durchführung eines Penetrationstests als regelmäßige Maßnahme zur Erhöhung der Sicherheit einzuführen. Nur durch einen kontinuierlichen Sicherheitsprozess kann ein bestimmtes Sicherheitsniveau aufrechterhalten werden.

Nmap

Nmap ist ein bekannter Portscanner und steht als Open-Source-Software für verschiedene Betriebssysteme zur Verfügung. Mit Nmap kann die Erreichbarkeit eines Systems untersucht und es können die geöffneten Ports eines Systems über das Netzwerk ermittelt werden. Zusätzlich zu den geöffneten Ports können beispielsweise der Dienstname und die Versionsnummer des Dienstes ausgegeben werden, der auf einen bestimmten Port gebunden ist. Das ist für einen Penetrationstest sinnvoll, da die meisten Schwachstellen nur für bestimmte Programmversionen gelten.

Mit Nmap kann ein einzelner Host oder ein IP-Subnetz gescannt werden. Die folgende Abbildung zeigt zunächst einen einfachen Scan ohne die Angabe von Optionen.

Mit dem Befehl „nmap 192.168.178.23“ können geöffnete Ports des Systems mit der IP-Adresse 192.168.178.23 festgestellt werden. Im Beispiel ist auf diesem System ein Webserver auf Port 80 (HTTP) und Port 443 (HTTPS) gebunden. Außerdem ist Port 53 für DNS-Anfragen geöffnet.

```
Nmap scan report for fritz.repeater (192.168.178.23)
Host is up (0.00053s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
```

Ausgabe des Befehls „nmap 192.168.178.23“

Mit dem Parameter „-sV“ (Version detection) wird zusätzlich die Version der Dienste ermittelt. Zusammen mit der Version wird auch der Programm-

name angezeigt. Nmap kann diese Information darstellen, da viele Dienste beim Verbindungsaufbau ein sogenanntes Banner senden. Dieses Banner kann Informationen über den jeweiligen Dienst enthalten. Das Banner kann auch manuell ausgelesen (z. B. mit netcat bzw. nc) werden wie in der folgenden Abbildung zu sehen ist.

```
johannes@linux-arbeit:~$ nc 192.168.178.29 22
SSH-2.0-OpenSSH 7.4
```

Verbindungsaufbau mittels Befehl „nc" („netcat")

Die nächste Abbildung zeigt den Ausschnitt einer Ausgabe des Befehls „nmap -sV 192.168.178.29". Auf Port 22 wartet beispielsweise ein SSH-Dienst auf eingehende Verbindungen. Es wird die Software „OpenSSH" in der Version 7.4 verwendet.

```
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.4 (protocol 2.0)
80/tcp   open  http        nginx
111/tcp  open  rpcbind     2.4 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
```

Ausgabe des Befehls „nmap -sV 192.168.178.29"

Eine umfassende Ausgabe stellt Nmap mit dem Parameter „-A" bereit. Hier werden beispielsweise zusätzliche Angaben zum Betriebssystem des Ziels angezeigt. Die folgende Abbildung zeigt einen Auszug der Ausgabe für den Befehl „nmap -A 192.168.178.29".

```
MAC Address: 00:11:32:1E:32:32 (Synology Incorporated)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.19 - 2.6.36
Network Distance: 1 hop
Service Info: Host: DISKSTATION; OS: Linux; CPE: cpe:/o:linux:linux_kernel:2.6.32.12
```

Auszug der Ausgabe für „nmap -A 192.168.178.29"

Nach dem Untersuchen der Zielsysteme und dem Sammeln der Informationen können Schwachstellen ermittelt werden, die in den jeweiligen Diensten und Versionen aufgedeckt wurden. Ein möglicher Anlaufpunkt dafür sind beispielsweise Webseiten für IT-Sicherheit, auf denen nach Exploits für bestimmte Dienste gesucht werden kann, z. B. „www.packetstormsecurity.com". Mit der Software „Metasploit" kann ebenfalls einfach nach Schwachstellen für Dienste gesucht werden. Mit dieser Software ist es zusätzlich möglich, die Schwachstelle entsprechend auszunutzen.



Werkzeuge und Exploits von Metasploit, um den Webserver „Apache" anzugreifen

Der Screenshot zeigt einen Ausschnitt zur Verfügung stehender Exploits für den beliebten Webserver „Apache". Um ein Exploit auszuführen, bedarf es nur der Angabe weniger Parameter, z. B. der IP-Adresse des Hosts. Manche Exploits bieten nach der Ausführung direkt den Zugang zu einer Root-Shell.

Eine weitere Möglichkeit, ein Netzwerk nach Schwachstellen abzusuchen, ist ein Schwachstellen-Scanner.

Das Cybersicherheitsunternehmen Tenable bietet beispielsweise mit dem Programm „Nessus" einen solchen Schwachstellen-Scanner an. Die Software ist nur unter kommerzieller Lizenz verfügbar. Der Vorteil ist eine „schnelle" Auflistung aller (Nessus bekannten) Schwachstellen im Netzwerk.

Die Abbildung zeigt einen Ausschnitt der Überprüfung eines lokalen Netzwerks. Es lassen sich Hostsysteme des Netzwerks und die auf diesen gefundenen Schwachstellen anzeigen. Außerdem können über die einzelnen Schwachstellen genauere Informationen bezogen werden.

Host	Vulnerabilities ▼
192.168.178.59	
192.168.178.29	
192.168.178.54	
192.168.178.37	
192.168.178.1	1 1

Übersicht der Schwachstellen; Copyright Agent Tenable, Inc., Columbia

Sev	Score ▼	Name	Family	Count
CRITICAL	10.0 *	NFS Exported Share Information Disclosure	RPC	1
HIGH	8.8	Samba 4.0.x < 4.13.17 / 4.14.x < 4.14.12 / 4.15.x < 4.15.5 Multiple Vulnerabilities	Misc.	2
MEDIUM	6.5	IP Forwarding Enabled	Firewalls	2
MEDIUM	5.3	SMB Signing not required	Misc.	2

Details zu einzelnen Schwachstellen; Copyright Agent Tenable, Inc., Columbia

Bei vielen gefundenen Schwachstellen gibt der Netzwerk-Scanner Hinweise zu den zu ergreifenden Maßnahmen. Eine detaillierte Auseinandersetzung mit den Schwachstellen und ein regelmäßig erneuerter Scan sind nötig, um die Sicherheit der IT-Infrastruktur zu gewährleisten.

Kompetenzcheck

1. Geben Sie die Wireshark-Filterregel für die IP-Adresse des Senders „10.0.0.1", der einen Ziel-Port 443 anspricht, an.
2. Erläutern Sie, worin sich der „lokale Administrator" und der „Domain-Administrator" unterscheiden.
3. Erstellen Sie mit einem Partner eine Liste mit Vorteilen, die durch den Einsatz eines IAM entstehen.
4. Überlegen Sie, warum der Netzwerk-Scan des Netzwerks A „120.128.0.0/14" länger dauert als der Scan des Netzwerks B „120.128.0.0/23". Annahme: Für das Prüfen einer einzelnen IP-Adresse wird eine Sekunde benötigt. Geben Sie die Zeiten der Scans an.
5. Notieren Sie wesentliche Aspekte aus diesem Abschnitt in Ihrem Projektjournal.
6. Bearbeiten Sie Aufgabe 1 der Lernsituation 5 im Arbeitsbuch.

A1

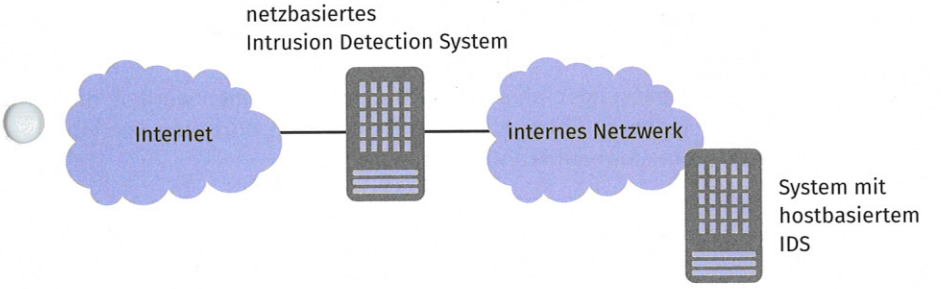
3.5.2 Überwachungssysteme zur Angriffserkennung

S **Sie sollen Überwachungssysteme für vernetzte IT-Systeme einsetzen können.**

(1) Intrusion Detection System (ISD)

Ein Intrusion Detection System (IDS) erkennt Einbruchversuche, d.h. Angriffe auf ein System oder ein Netzwerk. Wird ein Angriff erkannt, informiert das IDS die zuständige Person über den Angriff. Diese Alarmierung kann beispielsweise via E-Mail erfolgen. Das IDS führt keine Maßnahmen zur Verhinderung des Angriffs durch. Die Gegenmaßnahmen müssen durch die zuständige Person eingeleitet werden.

Damit ein Angriff vom IDS erkannt werden kann, muss der Netzwerkverkehr mitgeschnitten werden. Dazu ist es nötig, Sensoren in bestimmten Punkten im Netzwerk zu betreiben.



Beispiel für netz- und hostbasierte IDS

IDS lassen sich in hostbasierte und netzbasierte Systeme unterteilen. Bei einem hostbasierten IDS ist der Sensor auf dem zu überwachenden Hostsystem installiert. Der ein- und ausgehende Verkehr wird analysiert und zusätzlich werden die log-Dateien untersucht. Bei einem netzbasierten IDS wird der Sensor idealerweise an einem Netzübergang, also einem Gateway, installiert.

In großen Netzen kann es sinnvoll sein, an mehreren Punkten den Netzwerkverkehr zu analysieren. Je nach Datenrate des Netzwerkes müssen sehr viele Pakete geprüft werden. Deshalb ist es nötig, dass dem eingesetzten IDS ausreichend Ressourcen zur Verfügung stehen.

Bei der Analyse der Datenpakete wird zunächst überprüft, ob eine Regel auf das Datenpaket zutrifft. Wenn eine Regel erfüllt ist, wird auch der Inhalt des Pakets auf Angriffsmuster überprüft.

(2) Intrusion Prevention System (IPS)

Während ein Intrusion Detection System bei einem Angriff den Administrator über den Angriff informiert, kann ein Intrusion Prevention System (IPS) einen Angriff verhindern. Dazu kann das IPS automatisiert Regeln für die angeschlossene Firewall erstellen. Diese Regeln unterbinden den Angriff, indem die entsprechenden Pakete von der Firewall verworfen werden.

Eine bekannte IPS-Software ist die Open-Source-Software „Snort". In der kostenlosen Community-Version enthält die Software über knapp 4000 Regeln, um Angriffe zu erkennen. Snort verfügt wie alle IPS über eine Komponente, die den Netzwerkverkehr mitschneidet und an das System weitergibt. Der mitgeschnittene Verkehr wird nun aufbereitet und auf Angriffsmuster untersucht. Wird ein Angriff erkannt, erzeugt Snort einen Alarm oder kann eine Firewall-Regel erstellen, um den Angriff zu unterbinden.

Eine Regel besteht bei Snort aus zwei Teilen. Im sogenannten Header der Regel wird zum einen beschrieben, auf welches Protokoll, welche IP-Adressen und welche Ports (Ziel- und Quelladressen) sie angewendet wird. Zum anderen wird festgelegt, was passieren soll, wenn die Regel zutrifft. Der zweite Teil, die sogenannte „Rule Option", beschreibt, wann ein Paket als Angriff gewertet wird.

Beispiel für eine Regel bei Snort:

```
alert tcp $HOME_NET 31785 -> $EXTERNAL_NET any ( msg:"MALWARE-BACKDOOR
HackAttack 1.20 Connect"; flow:established,to_client; content:"host";
metadata:ruleset community; classtype:misc-activity; sid:141; rev:10; )
```

Die Regel erzeugt eine Alarmmeldung, wenn es sich um TCP-Verkehr aus dem eigenen Netzwerk mit dem Quell-Port 31785 handelt, der an das externe Netzwerk gesendet werden soll. Die Alarmmeldung enthält den Hinweis, dass eine Malware entdeckt wurde. Snort analysiert, ob die TCP-Verbindung aufgebaut ist und ob es sich um eine Antwort auf eine Anfrage aus dem externen Netzwerk handelt. Außerdem muss das Wort „host" im Paket vorkommen. Abschließend werden noch Parameter aufgeführt, die die Regel einem Regelwerk zuschreiben und diese eindeutig identifizieren.
Ein weiteres Beispiel für ein IPS ist die Software „Fail2ban". Die Software ist frei verfügbar und kann aus dem Standard-Repository einer Linux-Distribution installiert werden. Ein Einsatzgebiet ist z. B. das Absichern des SSH-Zugangs eines Servers.

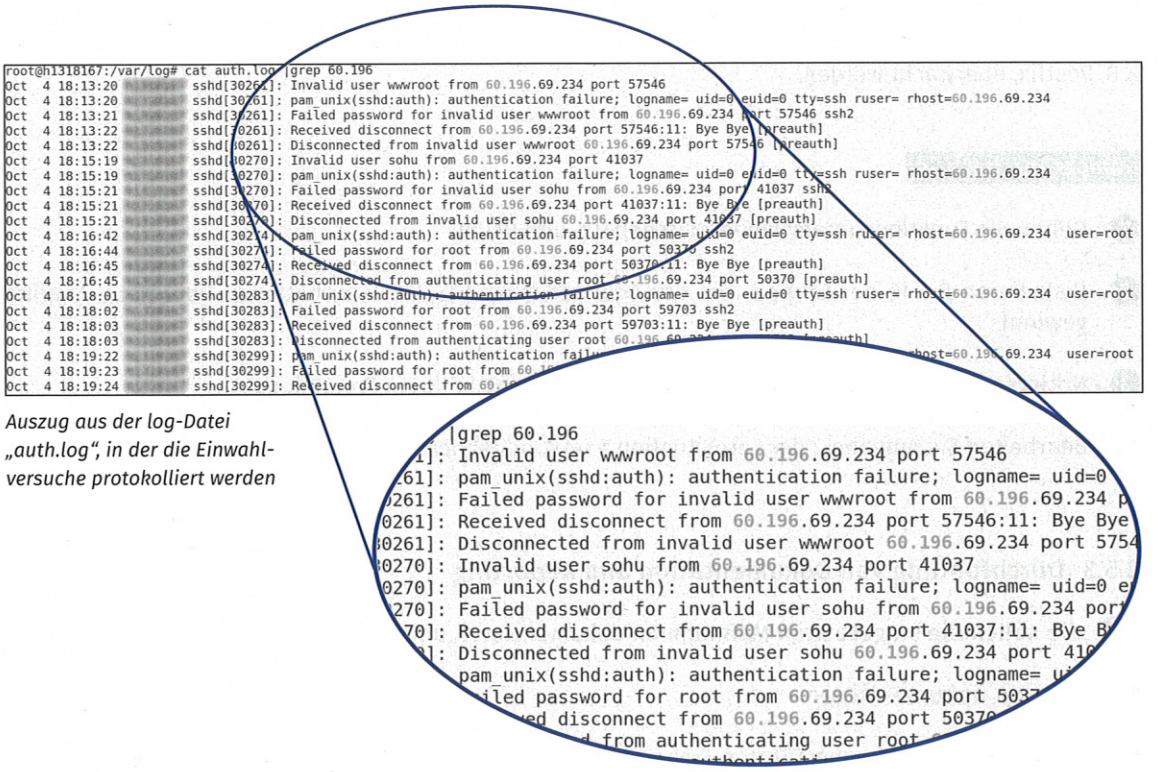
In der Datei „/etc/fail2ban/jail.local" können Anpassungen an den Diensten vorgenommen werden, die die Software „Fail2ban" überwachen soll. Für jeden zu überwachenden Dienst kann dort eine Sektion angelegt werden. Für den SSH-Dienst existiert eine Standardkonfiguration.

```
1 [ssh]
2 filter = ssh
3 action = iptables[name=ssh, port=ssh]
4 logpath = /var/log/auth.log
5 maxretry = 3
6 enabled = true
7 port = ssh
```

In Zeile 2 wird der Name des zu überwachenden Daemons angegeben. Zeile 3 verweist auf die Aktion. Diese wird in einer separaten Datei festgelegt. In der vierten Zeile wird die zu überwachende log-Datei angegeben. In Zeile 5 wird angegeben, dass die Aktion nach drei fehlgeschlagenen Anmeldeversuchen durchgeführt wird. Zeile 7 gibt den zu überwachenden Port an. Hier SSH auf dem Well-Known-Port 22.

Zur Überwachung des SSH-Dienstes wird somit nach einer bestimmten Anzahl von misslungenen Anmeldeversuchen die IP-Adresse, über die die Anmeldeversuche gestartet wurden, für eine bestimmte Zeitdauer gesperrt. Dazu ist es nötig, dass die Software eine Schnittstelle zur Firewall hat. Wird eine IP-Adresse als schädlich identifiziert, weil es beispielsweise fünf erfolglose Anmeldeversuche mit dieser IP-Adresse (im folgenden Beispiel 60.196.69.234) gab, wird in der Firewall „iptables" eine entsprechende Regel automatisch angelegt. Diese Regel sperrt die jeweilige IP-Adresse.

Von der IP-Adresse 60.196.69.234 wurde versucht, sich mit verschiedenen Benutzernamen, z. B. www root, sohu und root, am SSH-Dienst anzumelden. Die Software „Fail2ban" analysiert verschiedene log-Dateien, um einen Angriff zu erkennen. Dazu gehört auch die Datei „auth.log". Dadurch kann die Software auf die fehlgeschlagenen Login-Versuche reagieren und in der Firewall eine entsprechende Regel erstellen. Dazu wird durch Fail2ban ein Befehl ausgeführt, bei dem verschiedene Variablen durch feste Werte ersetzt werden. Der Befehl „actionban = iptables -I f2b-<name> 1 -s <ip> -j <blocktype>" ergibt im Beispiel „iptables -I f2b-ssh 1 -s 60.196.69.234 -j REJECT".



```
root@h1318167:/var/log# cat auth.log |grep 60.196
Oct  4 18:13:20 [redacted] sshd[30261]: Invalid user wwwroot from 60.196.69.234 port 57546
Oct  4 18:13:20 [redacted] sshd[30261]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=60.196.69.234
Oct  4 18:13:21 [redacted] sshd[30261]: Failed password for invalid user wwwroot from 60.196.69.234 port 57546 ssh2
Oct  4 18:13:22 [redacted] sshd[30261]: Received disconnect from 60.196.69.234 port 57546:11: Bye Bye [preauth]
Oct  4 18:13:22 [redacted] sshd[30261]: Disconnected from invalid user wwwroot 60.196.69.234 port 57546 [preauth]
Oct  4 18:15:19 [redacted] sshd[30270]: Invalid user sohu from 60.196.69.234 port 41037
Oct  4 18:15:19 [redacted] sshd[30270]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=60.196.69.234
Oct  4 18:15:21 [redacted] sshd[30270]: Failed password for invalid user sohu from 60.196.69.234 port 41037 ssh2
Oct  4 18:15:21 [redacted] sshd[30270]: Received disconnect from 60.196.69.234 port 41037:11: Bye Bye [preauth]
Oct  4 18:15:21 [redacted] sshd[30270]: Disconnected from invalid user sohu 60.196.69.234 port 41037 [preauth]
Oct  4 18:16:42 [redacted] sshd[30274]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=60.196.69.234  user=root
Oct  4 18:16:44 [redacted] sshd[30274]: Failed password for root from 60.196.69.234 port 50370 ssh2
Oct  4 18:16:45 [redacted] sshd[30274]: Received disconnect from 60.196.69.234 port 50370:11: Bye Bye [preauth]
Oct  4 18:16:45 [redacted] sshd[30274]: Disconnected from authenticating user root 60.196.69.234 port 50370 [preauth]
Oct  4 18:18:01 [redacted] sshd[30283]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=60.196.69.234  user=root
Oct  4 18:18:02 [redacted] sshd[30283]: Failed password for root from 60.196.69.234 port 59703 ssh2
Oct  4 18:18:03 [redacted] sshd[30283]: Received disconnect from 60.196.69.234 port 59703:11: Bye Bye [preauth]
Oct  4 18:18:03 [redacted] sshd[30283]: Disconnected from authenticating user root 60.196.69.234 port 59703 [preauth]
Oct  4 18:19:22 [redacted] sshd[30299]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=60.196.69.234  user=root
Oct  4 18:19:23 [redacted] sshd[30299]: Failed password for root from 60.196.69.234 port 59999 ssh2
Oct  4 18:19:24 [redacted] sshd[30299]: Received disconnect from 60.196.69.234 port 59999:11: Bye Bye [preauth]
```

Auszug aus der log-Datei „auth.log", in der die Einwahlversuche protokolliert werden

Die folgende Abbildung zeigt die entsprechenden Regeln der Firewall.

```
admin@server # iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
f2b-ssh    tcp  --  anywhere             anywhere            tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain f2b-ssh (1 references)
target     prot opt source               destination
REJECT     all  --  61.177.173.61        anywhere            reject-with icmp-port-unreachable
REJECT     all  --  68.183.87.50         anywhere            reject-with icmp-port-unreachable
REJECT     all  --  103.185.185.65       anywhere            reject-with icmp-port-unreachable
REJECT     all  --  193.227.16.23        anywhere            reject-with icmp-port-unreachable
REJECT     all  --  61.177.173.10        anywhere            reject-with icmp-port-unreachable
REJECT     all  --  60.196.69.234        anywhere            reject-with icmp-port-unreachable
RETURN     all  --  anywhere             anywhere
```

Automatisch erzeugte Firewall-Regeln, um von Fail2ban erkannte IP-Adressen zu sperren

Im Regelwerk für den eingehenden Datenverkehr (INPUT-Chain) gibt es nur eine Regel. Diese trifft auf jeglichen Verkehr zu, der als Zielport (Destination-Port oder dport) den Port 22, also SSH, hat. Die Regel verweist auf das Regelwerk „f2b-ssh". In diesem Regelwerk sind die Regeln zum Blockieren bestimmter IP-Adressen hinterlegt. Zum Beispiel verbietet die vorletzte Regel ankommenden Datenverkehr der Quell-IP-Adresse 60.196.69.234. Somit kann der SSH-Dienst nicht mehr erreicht werden. Der Client bekommt die Antwort „port unreachable".

Neben der Absicherung des SSH-Dienstes kann die Software „Fail2ban" auch die Anmeldung an verschiedenen Webservern wie Apache oder Lighttpd überwachen. Außerdem können verschiedene Mail-Server, z. B. Postfix, überwacht werden.

Kompetenzcheck

1. Geben Sie Funktionsunterschiede zwischen IDS und IPS an.
2. Diskutieren Sie in der Gruppe, wie der Anbieter eines IDS/IPS Informationen über neue Angriffe gewinnt.
3. Notieren Sie wesentliche Aspekte aus diesem Abschnitt in Ihrem Projektjournal.
4. Bearbeiten Sie Aufgabe 2 der Lernsituation 5 im Arbeitsbuch.

A2

3.5.3 Durchführung von Dokumentation und Reporting

S Sie sollen die umgesetzten Maßnahmen dokumentieren und in Reports zusammenfassen.

(1) Analysen dokumentieren

Die Auswertung eines durchgeführten Sicherheitsaudits, z. B. eines Penetrationstests, muss dokumentiert sein. In einer solchen Dokumentation müssen verschiedene Punkte besprochen werden. Neben der Angabe des Zeitraums der Datenerfassung muss auch der Grund der Analyse angegeben werden. Der Umfang des Penetrationstests ist ebenfalls zu dokumentieren, also welche Systeme untersucht wurden und welche nicht. Anschließend sollte erklärt werden, welche Techniken und Werkzeuge zur Informationsgewinnung und Ausnutzung der gefundenen Schwachstellen zum Einsatz gekommen sind.

Die Angabe und Erläuterung der gefundenen Schwachstellen sind der zentrale Teil eines Reports. Bei jeder Schwachstelle muss eine genaue Beschreibung angegeben werden. Außerdem sollte erläutert werden, wie die Schwachstelle ausgenutzt werden kann. Die Schwachstelle muss zudem kategorisiert werden. Die Kategorie ist von den Daten abhängig, die durch die Schwachstelle betroffen sind. Eine Möglichkeit ist es, die Gefahren – ähnlich wie bei der Schutzbedarfsfeststellung – in Kategorien einzuteilen. Die Tabelle „Information Security Risk Rating Scale" des PTES (Penetration Testing Execution Standard) beispielsweise unterteilt gefundene Schwachstellen in fünf Risikobereiche. Das BSI schlägt in einem Leitfaden vor, Schwachstellen nach vier Kategorien zu bewerten (vgl. BSI: Praxis-Leitfaden: IT-Sicherheits-Penetrationstest, 2016).

Die Analyse des Penetrationstest schließt mit einer Zusammenfassung ab. In dieser Zusammenfassung können Ratschläge für die Weiterführung des Sicherheitsprozesses gegeben werden, z. B. in Form von Handlungsanweisungen zur Beseitigung der gefundenen Schwachstellen. Auch ein Fahrplan für den Sicherheitsprozess, in dem beschrieben wird, welche Tätigkeiten in welchem zeitlichen Rahmen durchgeführt werden sollten, kann in der Zusammenfassung beschrieben werden.

Bei der Bearbeitung der in der Dokumentation gefundenen Probleme und Schwachstellen sollte mit den Problemen der höchsten Dringlichkeitsstufe („extreme" oder „hoch") begonnen werden. Damit werden unternehmenskritische Schwachstellen zuerst geschlossen.

(2) Compliance-Reports

Neben dem in diesem Kapitel vorgestellten BSI-Sicherheitskonzept gibt es weitere Security-Systeme. Hierzu zählen ISO 27001, NIST 800-53 und SOC 2-Reports. Es handelt sich bei allen drei Systemen um Standardlösungen zur Ermittlung des Sicherheitsstands eines Unternehmens. Dabei werden meist von externen Dienstleistern Audits durchgeführt, um die aktuellen Sicherheitsstandards eines Unternehmens zu prüfen. Um diese Überprüfungen durchführen zu können, muss das Unternehmen entsprechende Reports über die eigenen Maßnahmen und Vorgehensweisen vorhalten.

Weiterhin unterliegen alle Unternehmen, die personenbezogene Daten regelmäßig verarbeiten, gemäß Artikel 30 der DSGVO einer Dokumentationspflicht.

Zusätzlich zu diesen Standards kommen in Bereichen, die staatlicher Aufsicht unterliegen, z. B. Banken, Versicherungen, weitere Dokumentationspflichten gegenüber den entsprechenden Aufsichtsbehörden hinzu. Diese sind ebenfalls in Compliance-Reports abzulegen.

(3) Härtungsmaßnahmen aus Informationen ableiten

Härtung von IT-Systemen

Unter Härtung eines Systems versteht man die Reduktion der verwendeten Software und Schnittstellen auf das Minimum des für den Betrieb notwendigen Maßes. Ziel der Härtung ist es, die Angriffsfläche so gering wie möglich zu halten.

Eine aktuell installierte Software kann eine zum Installationszeitpunkt unbekannte Sicherheitslücke enthalten, die erst zu einem viel späteren Zeitpunkt aufgedeckt wird. Ein solches System ist ab Bekanntwerden der Sicherheitslücke („Zero-Day-Exploit") potenziell gefährdet. Mit steigender Anzahl der installierten Software steigt auch die Gefahr einer solchen Sicherheitslücke. Durch Härtung der Systeme werden die potenziellen Angriffsmöglichkeiten reduziert.

Durch gezielte Reduktion des Systems auf das für den Betrieb absolute Minimum an notwendiger Software wird damit automatisch auch das Risiko für eine Sicherheitslücke reduziert. Darüber hinaus werden insbesondere bei Windows-Betriebssystemen alle nicht zwingend benötigten Dienste deaktiviert, sofern diese nicht deinstalliert werden können. Der BSI hat entsprechende Empfehlungen in der Studie „SiSyPHuS Win10" zusammengefasst.

Für Linux-Systeme gibt es für die wichtigsten Distributionen eigene Sicherheitsempfehlungen, die unter dem Begriff „Hardening" im Internet verfügbar sind. Zu den wichtigsten Maßnahmen gehören hier das Absichern der notwendigen Dienste (z. B. Webserver oder BIND), das Entfernen von nicht benötigten Programmiersprachen (insbesondere Interpreter) und das Reduzieren des Kernels auf ein Minimum an Modulen. Hier kann es sinnvoll sein, den Kernel speziell für den Einsatzzweck mit den notwendigen Modulen zu kompilieren. Der Prozess ist verhältnismäßig einfach durchzuführen und setzt keine Programmierkenntnisse voraus. Die notwendige Konfiguration wird über Assistenten durchgeführt.

Eine weitere Möglichkeit ist die Installation von sogenannten Harden-Paketen auf Debian-Systemen. Harden-Pakete sind Metapakete, die absichtlich Paketkonflikte hervorrufen, um beim Installationsversuch von unsicheren Paketen darauf aufmerksam zu machen. Beispielsweise führt ein Installationsversuch der unsicheren Software „telnetd" zu einer Fehlermeldung, wenn das Sicherheitspaket „harden-servers" zuvor installiert wurde.

Die Bemühungen der Härtung setzen immer aktuelle Softwarestände voraus. Ein funktionierendes Update-System ist daher Grundvoraussetzung.

Kompetenzcheck

1. Erstellen Sie eine Grafik, die die Struktur eines Reports abbildet.
2. Nennen Sie mindestens drei Gründe, warum es notwendig ist, Compliance-Reports zu erstellen.
3. Beschreiben Sie mögliche Härtungsmaßnahmen für Windows 10 und Linux-Systeme.
4. Notieren Sie wesentliche Aspekte aus diesem Abschnitt in Ihrem Projektjournal.
5. Bearbeiten Sie Aufgabe 3 der Lernsituation 5 im Arbeitsbuch.

A3

3.6 Sicherheit im Unternehmen und deren Umsetzung betrachten

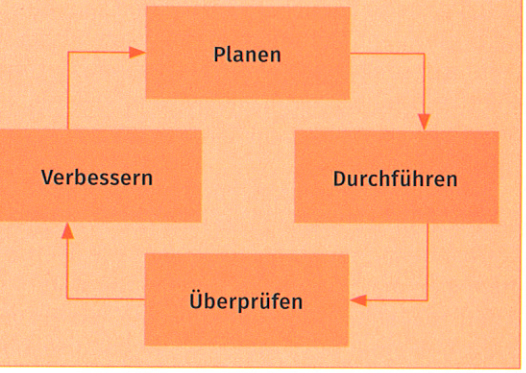
S **Sie sollen den Arbeitsprozess hinsichtlich möglicher Optimierungen reflektieren und das Ergebnis in Bezug auf den Begriff der relativen Sicherheit des vernetzten Systems diskutieren.**

In diesem Kapitel wird der Sicherheitsprozess reflektiert und es soll ein Überblick über eine wichtige Entwicklung im Bereich der Unternehmenssicherheit gegeben werden: das Umdenken in Unternehmen, dass die (IT-)Sicherheit auch in der Führungsetage verankert sein muss.

(1) Sicherheitsprozess reflektieren

In diesem Kapitel 3 wurden zunächst der Sicherheitsprozess wiederholt und einzelne Gefährdungen vertieft. Anschließend standen die Planung und das Implementieren ausgewählter Maßnahmen im Fokus. Im nächsten Schritt wurden verschiedene Möglichkeiten zur Überprüfung der Wirksamkeit solcher Maßnahmen vorgestellt. Der Sicherheitsprozess ist allerdings nach der Implementierung und Überprüfung der Maßnahmen nicht abgeschlossen, sondern bleibt ein fortlaufender Prozess. Das BSI spricht hier vom PDCA-Zyklus.

! Im Modell des **PDCA-Zyklus** des BSI werden Maßnahmen zunächst geplant (PLAN), dann werden die Maßnahmen umgesetzt, d. h. durchgeführt (DO), anschließend wird die Wirksamkeit der Maßnahmen überprüft (CHECK) und auf Grundlage der Überprüfung wird eine Verbesserung angestrebt (ACT). Diese Maßnahmen für die Konfiguration müssen wiederum geplant (PLAN) werden usw.



Die Sicherheit der IT-Infrastruktur muss kontinuierlich verbessert werden. Die regelmäßige Überprüfung der Sicherheitsprozesse ist dabei zentral. Dies wird beispielsweise durch Sicherheitsaudits, Sicherheitsübungen und Angriffssimulationen gewährleistet. Für eine Überprüfung der IT-Sicherheit ist es sinnvoll, Kennzahlen zu definieren und festzulegen, wie diese Kennzahlen zu interpretieren sind. Durch die Festlegung sinnvoller Kennzahlen können Ziele für die Sicherheitsstrategie eines Unternehmens definiert und die Wirksamkeit von Maßnahmen überprüft werden.

Wichtig ist es, alle Schritte der Planung, Durchführung, Überprüfung und Verbesserung zu dokumentieren. Eine solche Dokumentation kann dann beispielsweise für eine Zertifizierung nach ISO 27001 (Norm für das Informationssicherheitsmanagement) verwendet werden. Auch die ISO 27001 basiert auf einem kontinuierlichen Sicherheitsprozess mittels PDCA-Zyklus. Eine solche Zertifizierung zeigt Kunden und

Partnern, dass die IT-Sicherheit im Unternehmen ein wichtiges Unternehmensziel ist und das Unternehmen einer IT-Strategie mit festgelegten Zielen folgt. Eine Zertifizierung verschafft dem Prozess der IT-Sicherheit Transparenz. Es wird dadurch klarer, welche Schritte schon im Unternehmen etabliert sind und welche noch nötig sind, um den IT-Sicherheitsprozess zu ritualisieren.

Ohne wiederkehrende Überlegungen und verbesserte Maßnahmen findet keine Anpassung an die sich ständig ändernde Bedrohungslage statt. Bei allen getätigten Maßnahmen und Sicherheitsvorkehrungen muss immer bedacht werden, dass kein System sicher ist. Mit genügend Aufwand können Angreifer, z. B. durch Social Engineering, Zugang zu fast jedem System bekommen und Schaden anrichten.

Eine wichtige nicht technische Maßnahme ist die Schulung von Mitarbeitern. Nur durch eine stetige Schulung kann die Sensibilisierung der Mitarbeiter erreicht werden und es kann auf IT-Sicherheitsprobleme aufmerksam gemacht werden.

(2) Ausblick: Sicherheit denken

Für die Umsetzung einer effektiven und effizienten Sicherheitsstruktur innerhalb des Unternehmens ist die Verankerung des Themas IT-Sicherheit in der Organisationsstruktur von großer Bedeutung. Als Leitfaden sollte die Frage nach dem „Warum" im Vordergrund stehen. Die Hauptgründe für die Umsetzung von Sicherheitsstrukturen sind zum einen die Einhaltung von Verträgen bzw. Gesetzesvorgaben (Compliance) und zum anderen die Reduktion von Risiken für die Erreichung der geschäftlichen Ziele. Eine Standardlösung für die Verankerung der Sicherheitsbeauftragten in der Unternehmensorganisation gibt es daher nicht.

In großen Unternehmen, z. B. Banken oder Versicherungen, bei denen oft umfangreiche gesetzliche Vorgaben beachtet werden müssen, ist eine zentrale und relativ nah an der Geschäftsführung angesiedelte Sicherheitsabteilung mit zusätzlichen Sicherheitsbeauftragten in den verschiedenen Abteilungen sinnvoll. In kleinen und mittleren Unternehmen (KMU) wäre ein solcher Überbau zu umfangreich und kaum finanzierbar. Hier sind eher an den Produktions- bzw. Wertschöpfungspunkten angesiedelte Sicherheitsbeauftragte sinnvoll.

Um Sicherheit dauerhaft im Unternehmen herzustellen, bedarf es der kontinuierlichen Überprüfung der Risiken wie auch der gegen diese Risiken umgesetzten Maßnahmen. Daher ist es unabdingbar, dies in das tägliche Geschäft fest zu integrieren. Sicherheitsaudits, die nur nach bestimmten Zeiträumen durchgeführt werden, sind zwar sinnvoll, um den akuten Handlungsbedarf zu identifizieren. Die Umsetzung der aus solchen Audits ermittelten Maßnahmen wird allerdings durch den punktuellen Charakter außerhalb des Tagesgeschäfts wesentlich erschwert.

Kompetenzcheck

1. Im Verlauf des Lernfeldes wurden Sie aufgefordert, Notizen in Ihrem Projektjournal anzulegen. Nehmen Sie diese Notizen zur Hand. Bilden Sie Gruppen und stellen Sie sich gegenseitig die erstellten Notizen vor. Nutzen Sie hierzu die folgenden Leitfragen.
   a) Welche Informationen haben Sie sich notiert? Wurden die Notizen regelmäßig erstellt?
   b) Haben Sie ausformulierte Sätze notiert oder nur Stichpunkte? Wie aussagekräftig sind Ihre Notizen?
   c) Können Sie die Notizen inhaltlich noch zuordnen? Was müsste geändert werden?
   d) Können Sie aus Ihren Notizen positive bzw. negative Erfahrungen ablesen?
   e) Können Sie die Vorgehensweise nachvollziehen und daraus Rückschlüsse für zukünftige Aufgabenstellungen und Projekte ziehen?
   f) Notieren Sie sich Punkte, die Sie bei einer nächsten Aufgabe anders umsetzen werden (positive oder negative Aspekte).

2. Bearbeiten Sie Aufgabe 1 der Lernsituation 6 im Arbeitsbuch.

A1

4 Betrieb und Sicherheit vernetzter Systeme gewährleisten (Lernfeld 11d)



Enterprise Zone Industrial Zone Area Zone Cell Zone Process
Schutzbedarf Systemstatus Dashboard Purdue-Modell Cyberkriminelle
Cyberangriff Überwachung Monitoring Gefahrenquellen IEC 62443
Blacklist Whitelist ICS Industrial Control System Operational Technology

Darüber werden wir sprechen, uns kompetent und aktiv beteiligen, genauer im Arbeitsbuch folgende Lernsituationen/Lernarrangements bearbeiten:

Lernsituation 1: Wir kennen den Schutzbedarf von Operational-Technology-(OT-)Netzwerken und setzen Strategien der Ausfallsicherheit um.

Lernsituation 2: Wir sichern gemeinsam mit den Mitarbeitern der Produktion und der Automatisierungstechnik industrielle Maschinen und Anlagen nach international gültigen Standards ab.

Lernsituation 3: Wir überwachen den Systemstatus von cyber-physischen Systemen und vernetzten Maschinen und Anlagen.

In diesem Lernfeld der Fachrichtung „Digitale Vernetzung" werden der Betrieb und die Sicherheit von vernetzten industriellen Produktionssystemen in den Blick genommen. Dabei wird nicht nur die Vernetzung im industriellen Umfeld betrachtet, vielmehr werden auch die Inhalte aus Kapitel 3 integriert.

Die Technologien in der Fertigungsindustrie entwickeln sich kontinuierlich und in schnellem Tempo weiter, nicht zuletzt durch die ständige Weiterentwicklung der Vernetzung von Produktionsmaschinen und Fertigungsprozessen. Durch den Fokus auf die Digitalisierung entstehen kontinuierlich auch komplett