5 Sicherheitsmanagement

Da fast alle Systeme innerhalb einer IT-Infrastruktur vernetzt sind, muss dem Thema Sicherheit die nötige Beachtung geschenkt werden. Man kann zu Recht sagen, dass das Netzwerk eines der «Haupteinfallstore» für Angriffe auf die IT-Systeme eines Unternehmens sind. Aus diesem Grund müssen spezielle Massnahmen implementiert werden, damit vonseiten des Netzwerks Angriffe auf die Systeme und Informationen erfolgreich abgewehrt werden können. In diesem Kapitel werden die gängigsten **Sicherheitsmassnahmen** aufgezeigt, die speziell innerhalb des Netzwerks zum Einsatz kommen.

5.1 Ziele und Aufgaben

Das generelle Ziel des FCAPS-Sicherheitsmanagements ist es, innerhalb der Netzwerkinfrastruktur **Sicherheitsrisiken** zu identifizieren und mithilfe geeigneter Massnahmen zu minimieren. Im Folgenden werden die übergeordneten **Schutzziele der IT-Sicherheit** sowie typische Aufgaben eines Netzwerkadministrators beim Management der **Netzwerksicherheit** dargelegt.

5.1.1 Schutzziele der IT-Sicherheit

Die **IT-Sicherheit** umfasst folgende **Schutzziele:**

Schutzziele	Beschreibung
Verfügbarkeit	Der Zugriff auf die Daten und Applikationen des Unternehmens muss innerhalb eines vereinbarten Zeitraums jederzeit gewährleistet sein. Ein Systemausfall muss wirksam verhindert werden.
Integrität	Die Daten des Unternehmens sind korrekt und vertrauenswürdig. Datenänderungen müssen nachvollziehbar sein.
Vertraulichkeit	Die Daten des Unternehmens dürfen nur von berechtigten Personen bzw. Mitarbeitenden eingesehen und bearbeitet werden. Entsprechend müssen der Zugriff auf solche Daten und deren Übertragung sicher sein.
Authentizität	Die Identität der Personen bzw. Mitarbeitenden, die auf die Daten und Applikationen des Unternehmens zugreifen, muss echt sein und wird überprüft.
Verbindlichkeit	Eine Handlung innerhalb des Netzwerks wie z. B. die Einsichtnahme und Bearbeitung von Daten kann eindeutig nachgewiesen werden. Das Abstreiten solcher Handlungen ist nicht möglich.
Zurechenbarkeit	Eine Handlung innerhalb des Netzwerks kann einer bestimmten Person bzw. einem bestimmten Mitarbeiter eindeutig zugeordnet werden.

5.1.2 Aufgaben des Netzwerkadministrators

Bei der **Netzwerksicherheit** geht es darum, die übergeordneten Schutzziele der IT-Sicherheit zu gewährleisten und unerwünschte Sicherheitsrisiken wie z. B. Angriffsmöglichkeiten über das Netzwerk einzuschränken. Folgende **Sicherheitsaufgaben** fallen in den Bereich des Netzwerkadministrators:

- Datenströme filtern
- Systeme und Benutzer authentifizieren
- Gefährdete Netzwerkbereiche abschotten
- Sicherheitsrelevante Aktivitäten erkennen und stoppen

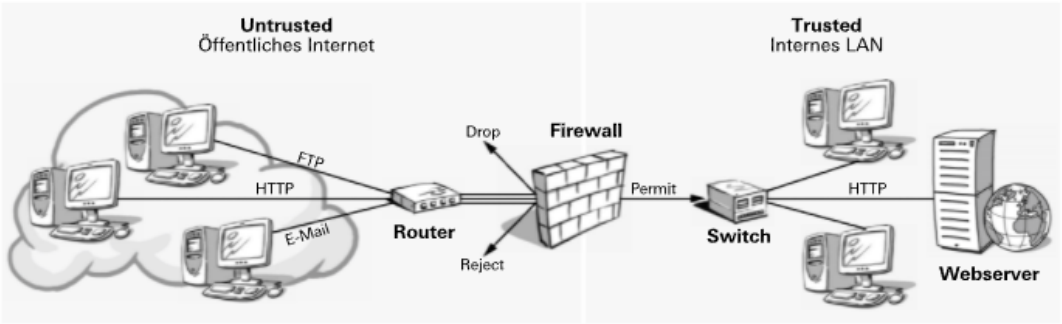
5.2 Massnahmen für die Netzwerksicherheit

Im Folgenden werden typische Massnahmen vorgestellt, die für die Erfüllung dieser Aufgaben infrage kommen. Dabei ist zu beachten, dass ggf. erst die Kombination mehrerer Massnahmen die gewünschte Wirkung erzielt. Je nach Situation bzw. Bedarf reicht es also nicht aus, eine bestimmte Massnahme isoliert umzusetzen.

5.2.1 Datenströme filtern

Eine Filterung der Datenströme auf **maliziöse**[1] **Inhalte** geschieht üblicherweise mithilfe einer **Firewall**[2]. Dies ist eine Netzwerkkomponente, die sich zwischen einem sicheren Netzwerk **(trusted Network)** und einem unsicheren Netzwerk **(untrusted Network)** befindet und die zwischen diesen Netzwerken ausgetauschte Datenpakete anhand vorgegebener Regeln bearbeitet.

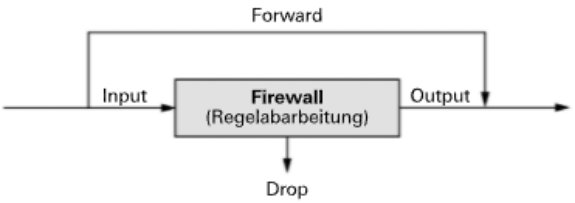
[5-1] Positionierung einer Firewall



Arbeitsprinzip einer Firewall

Eine Firewall kann Datenpakete oder Netzwerkanfragen anhand definierter Regeln filtern und verfügt normalerweise über drei verschiedene **Verarbeitungslinien:** die **Input-Queue,** die **Forward-Queue** und die **Output-Queue.** Die definierten **Firewall-Regeln** bilden eine Art Stapel, der jeweils von oben nach unten abgearbeitet wird. Passt die Anweisung der ersten Regel nicht auf ein Datenpaket bzw. eine Netzwerkanfrage, wird die nächste Regel angewendet. Dieser Prozess wird so lange fortgeführt, bis die letzte Regel abgearbeitet worden ist. Kann keine Regel bzw. keine Anweisung angewendet werden, wird das Paket bzw. die Anfrage verworfen **(dropped)**. Folgende Grafik soll dieses Prinzip veranschaulichen:

[5-2] Verarbeitungslinien einer Firewall



[1] Fremdwort für: boshaft, arglistig, böswillig.

[2] Englisch für: Brandschutzmauer (wörtl.).

Bei der Regeldefinition kommen üblicherweise folgende **Grundoperationen** zum Einsatz:

Operation / Anweisung	Aktion
DROP oder **DENY**	Das Datenpaket bzw. die Netzwerkanfrage wird verworfen, also gesperrt, ohne den Sender des Pakets darüber zu informieren.
REJECT	Das Datenpaket bzw. die Netzwerkanfrage wird zurückgewiesen und der Sender des Pakets darüber informiert.
FORWARD oder **PERMIT**	Das Datenpaket bzw. die Netzwerkanfrage wird erlaubt, d. h., das Paket wird durchgelassen bzw. weitergeleitet.

Zusätzlich zu diesen Operationen bzw. Anweisungen gibt es **erweiterte Möglichkeiten,** die Datenfilterung zu regeln. So könnte ein Angreifer etwa eine **DoS**[1]**-Attacke** starten, um die Webseiten eines Unternehmens durch unzählige Verbindungsanfragen zu blockieren. Dies lässt sich verhindern, indem von einer bestimmten IP-Adresse während einer bestimmten Zeitdauer nur eine begrenzte Anzahl von externen Verbindungen zugelassen wird.

Beispiel für eine Regeldefinition

Ein kleines Dienstleistungsunternehmen möchte, dass Personen von extern via Internet auf den Webserver im LAN zugreifen können. Die IP-Adresse des Webservers lautet `192.168.5.10`. Der Internet-Router der Firma soll für Überwachungszwecke «gepingt» werden können. Die öffentliche IP-Adresse (WAN-Anschluss) des Unternehmens lautet `167.12.9.53`. Alle Benutzer sollen auf das Internet zugreifen können. Der Router mit Firewall verfügt über einen ADSL- und einen Ethernet-Port. Um die gewünschten Datenverbindungen zu ermöglichen, werden auf der Firewall folgende Regeln definiert und aktiviert:

Pos.	Regel	Auswirkung / Beschreibung
1	`DROP Input`	Sperrt alle direkten Verbindungsanfragen aus dem Internet.
2	`DROP Forward`	Erlaubt keine Weiterleitungen.
3	`PERMIT -prot icmp -dest 167.12.9.53 icmp echo-request`	Ping-Aufrufe an den Internet-Router (Destination IP 167.12.9.53) werden beantwortet, jedoch nur Ping-Anfragen an einen anderen Host.
4	`INPUT -p tcp -dport 80;443 -limit 20/minute -limit-max 100`	Es werden höchstens 20 Verbindungsanfragen pro Minute auf die TCP-Ziel-Ports des Webservers (80 und 443) zugelassen. Insgesamt sind maximal 100 Verbindungen (Sessions) erlaubt.
5	`FORWARD -p tcp -d 167.12.9.53 -dport 80;443 -to 192.168.5.10`	Leitet alle TCP-Datenpakete mit der Ziel-IP 167.12.9.53 und den Ziel-Ports 80+443 direkt an die interne LAN-IP 192.168.5.10 (Webserver) weiter.
6	`PERMIT Output`	Direkte Datenverbindungen vom LAN ins Internet sind uneingeschränkt erlaubt. Das bedeutet, dass auch alle Antworten durchgelassen werden, da Firewalls normalerweise nur direkte Verbindungsaufrufe sperren.
7	`DROP ALL`	Alle übrigen (undefinierten) Datenpakete werden verworfen.

Hinweis

▷ Beachten Sie, dass obige Regeln nicht unbedingt die korrekte Schreibweise bzw. Syntax einer Firewall wiedergeben. Ziehen Sie für die Regeldefinition jeweils die spezifischen Vorgaben des Routers bzw. der Firewall zurate.

Je nach **Art der Datenfilterung** lassen sich unterschiedliche **Firewall-Typen** unterscheiden, die nachfolgend näher vorgestellt werden:

[1] Abkürzung für: Denial of Service. Englisch für: Dienstblockade eines überlasteten Systems.

Paketfilter

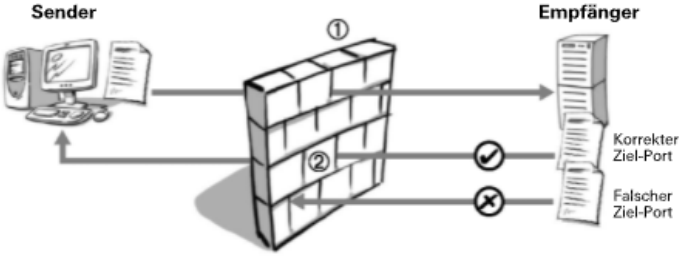
Dieser Firewall-Typ filtert Datenpakete anhand folgender Informationen:

- Layer 2: MAC-Adressen, VLAN-ID, CoS-Typ etc.
- Layer 3: Quell- und Ziel-IP-Adresse, Protokolle TCP, UDP etc.
- Layer 4: Quell- und Ziel-Ports, TCP SYN-Flag, ICMP-Typen etc.

Stateful Packet Inspection (SPI)

Dieser Firewall-Typ filtert Datenpakete anhand einer zustandsorientierten Analyse der Datenverbindung. Dabei wird jedes Datenpaket einer spezifischen **Verbindung (Session)** zugeordnet. Jede Verbindung besitzt immer auch einen bestimmten **Zustand (State).** Ein solcher Zustand ist z. B. der Quell-Port (Source) des Systems, das eine Verbindung initiiert. Entsprechend müssen die Datenpakete, die der Empfänger dem Sender als Antwort zurückschickt, als Ziel-Port (Destination) jeweils die Port-Nummer der Quelle enthalten. Folgende Grafik soll die Prüfung dieser Informationen verdeutlichen:

[5-3] Prinzip einer Stateful Packet Inspection



① Speicherung der Daten in der Statustabelle
② Vergleich der Daten mit der Statustabelle

Application Layer Firewall (ALF)

Dieser Firewall-Typ lässt keine direkte Kommunikation zwischen einem externen Netzwerk (Internet) und einem internen Netzwerk (LAN) zu. Zusätzlich zu den bereits erwähnten Informationen werden hier auch die **Nutzdaten (Paylod)** eines Datenpakets untersucht. Dabei stehen folgende **Ziele** im Vordergrund:

- Unerlaubte Funktionsaufrufe bei Applikationsdaten erkennen und verhindern
- Schädliche Programmcodes bei Applikationsdaten erkennen und verhindern
- Zugriff auf unerwünschte (verbotene) Inhalte aus dem Internet erkennen und verhindern
- In Datenströme eingebettete Schadprogramme (Viren, Trojaner etc.) erkennen
- Datenübertragung durch eine Zwischenspeicherung (Caching) mehrfach abgerufener (identischer) Daten beschleunigen

Entsprechend wird diese Art der Filterung auch **Content Filtering** genannt. Dabei werden auch die Daten der OSI Layer 5 bis 7 analysiert. Folgende Abbildung zeigt beispielhaft die Konfiguration und Aktivierung des URL-Filters (http-Proxy) auf einer Firewall (ZyWALL 35):

[5-4] Content Filter konfigurieren und aktivieren (Beispiel)

Und der folgende Screenshot zeigt beispielhaft die Definition der verbotenen Websites und Ausdrücke sowie möglicher Ausnahmen auf einer Firewall (ZyWALL 35):

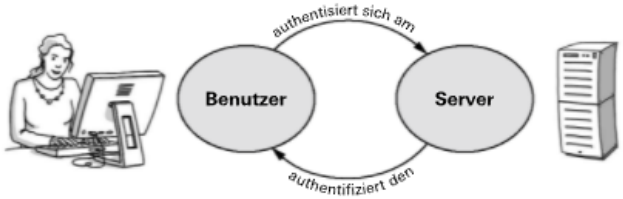
[5-5] Unerwünschte bzw. verbotene Inhalte definieren (Beispiel)

5.2.2 Systeme und Benutzer authentifizieren

Als Netzwerkadministrator möchten Sie nicht nur die übertragenen Datenpakete kontrollieren, sondern auch die Benutzer und Systeme identifizieren, die auf Ihr Netzwerk zugreifen. Für die **Authentifizierung der Benutzer und Systeme** können Sie das speziell dafür entwickelte, standardisierte Protokoll **IEEE 802.1X** sowie einen **RADIUS**[1]**-Server** einsetzen. Damit sind Sie in der Lage, den Zugriff eines Benutzers oder eines Systems an bestimmte Bedingungen zu knüpfen und den Zugriff auf das Netzwerk zu erlauben oder zu verweigern.

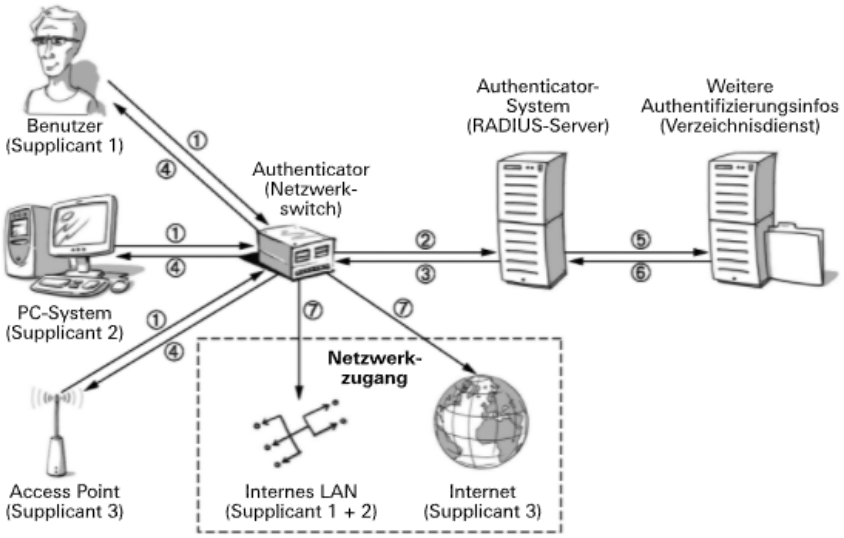
Bei der **Authentifizierung nach IEEE 802.1X** erfolgt die Kontrolle direkt beim Zugang zum Netzwerk auf Layer 2, also noch bevor ein Benutzer oder ein System Zugriff auf eine Ressource innerhalb dieses Netzwerks hat. Dabei wird sichergestellt, dass nur diejenigen Benutzer und Systeme Zugang zum Netzwerk erhalten, die bekannt sind bzw. die Erlaubnis dafür haben. Folgende Grafik soll das zugrunde liegende Prinzip veranschaulichen:

[5-6] Prinzip der Authentifizierung nach 802.1X



Voraussetzung für diese **Authentifizierungsmethode** ist, dass die eingesetzten Netzwerkgeräte «802.1X-kompatibel» sind. Eine Authentifizierungslösung nach diesem Standard beinhaltet folgende Komponenten und Funktionen:

[5-7] IT-Infrastruktur einer Authentifizierungslösung nach 802.1X



[1] Abkürzung für: Remote Authentication Dial-In User Service. Englisch für: Authentifizierungsserver für Fernzugriffe.

Erläuterungen zur obigen Abbildung:

- **Supplicant:** Der Supplicant (Antragssteller) meldet sich beim Authenticator (1) und erbittet den Zugang zum Netzwerk. Der Supplicant kann ein Benutzer, ein System, ein Netzwerkgerät oder eine Applikation sein. Die Antwort, ob ein Zugang erteilt oder abgelehnt wird (4), erhält der Supplicant direkt vom Authenticator.
- **Authenticator:** Der Authenticator (Antragsprüfer) erfüllt die Funktion eines Pförtners oder Türstehers und leitet die Zugangsanfragen (2) an das zentrale Authentication-System weiter. Der Authenticator ist ein Netzwerkgerät (i. d. R. ein Netzwerkswitch oder ein WLAN Access Point), das auf Layer 2 arbeitet.
- **Authentication-System:** Das Authentication-System ist eine zentrale Authentifizierungsstelle (z. B. RADIUS-Server), die die Zugangsanfragen der Supplicanten prüft und den Authenticator anweisen kann (3), den Zugang zum Netzwerk zu erteilen oder zu verweigern.
- **Weitere Authentifizierungsdienste:** Die zentrale Authentifizierungsstelle kann bei Bedarf auf weitere Authentifizierungssysteme zurückgreifen (5 und 6). Dies ist z. B. dann notwendig, wenn die Passwörter der Benutzer zentral in einem Verzeichnisdienst und nicht auf der zentralen Authentifizierungsstelle gespeichert werden.
- **Netzwerkzugang:** Gemäss Anweisung der zentralen Authentifizierungsstelle erteilt der Authenticator den Supplicanten Zugang zu den entsprechenden Netzwerkbereichen (7).

Nachfolgend sehen Sie eine Beispielkonfiguration für die Authentifizierung nach 802.1X via RADIUS-Server:

[5-8] Einstellungen bei einem Authentifizierungsserver (ZyAIR WLAN-AP)

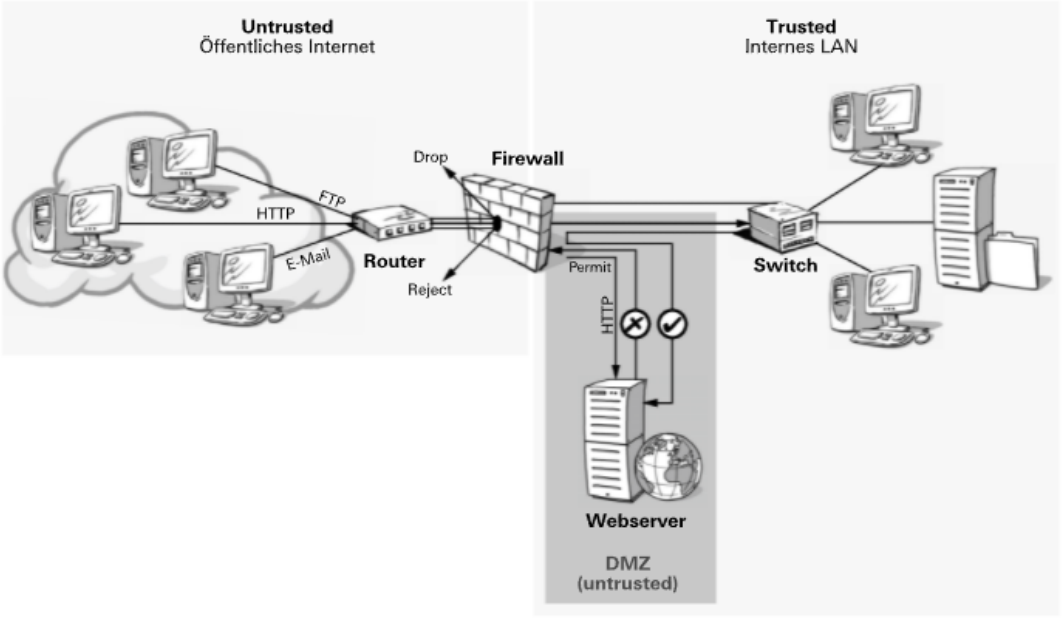
Hinweis

▷ Bei der obigen Server-IP-Adresse handelt es sich um die IP-Adresse des Authentification-Servers, da der Access Point die Funktion des Authenticators übernimmt.

5.2.3 Gefährdete Netzwerkbereiche abschotten

Auch wenn Sie mehrere sinnvolle Massnahmen umsetzen und aufeinander abstimmen, gibt es keine Garantie für absolute Netzwerksicherheit. Aus diesem Grund empfiehlt es sich, besonders gefährdete Systeme von besonders schützenswerten Netzwerkbereichen abzuschotten. Dabei werden vor allem öffentlich zugängliche Systeme wie z. B. Web- oder Mailserver in einer sogenannten **Demilitarisierten Zone (DMZ)** platziert. Ein Angreifer kann auch bei einem erfolgreichen Angriff innerhalb der DMZ nur minimalen Schaden anrichten, weil sich hier keine besonders schützenswerten Systeme befinden und ein direkter Zugriff von einem System in der DMZ (untrusted) auf das LAN (trusted) nicht möglich ist. Folgende Grafik soll diese Trennung verdeutlichen:

[5-9] Prinzip eines abgeschotteten Netzwerkbereichs (internes LAN)

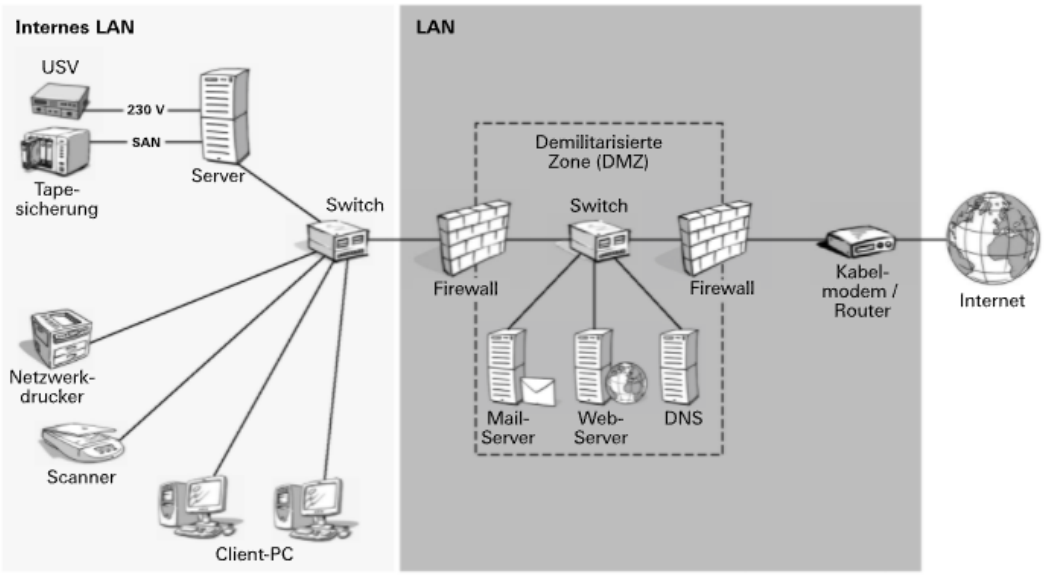


Erläuterungen zur Grafik:

Das obige Netzwerkschema zeigt ein **1-stufiges Firewall-Konzept.** Systeme aus dem internen LAN (trusted) können Anfragen direkt an den Webserver in der DMZ richten. Die Firewall sendet nur Datenpakete ins interne LAN zurück, die auf solche direkte Anfragen antworten. Direkte Anfragen aus der DMZ ins interne LAN dagegen werden von der Firewall abgeblockt. Durch diesen Filtermechanismus ist es für Angreifer besonders schwierig, auf das interne LAN (trusted) zuzugreifen, auch wenn sie ein System innerhalb der DMZ vollständig kontrollieren können.

Für eine noch wirkungsvollere Abschottung kann ein 2-stufiges Firewall-Konzept realisiert werden. Das entsprechende Netzwerkschema sieht wie folgt aus:

[5-10] Prinzip eines 2-stufigen Firewall-Konzepts



Hinweis

▷ Ein 2-stufiges Firewall-Konzept kommt für die meisten KMUs aus Kostengründen nicht infrage.

5.2.4 Sicherheitsrelevante Aktivitäten erkennen und stoppen

Es muss nicht unbedingt sein, dass ein Angreifer von aussen in das Netzwerk eines Unternehmens eindringt. Oft werden Angriffe auch von Mitarbeitenden ausgeführt, die sich bereits im internen LAN, also im trusted Netzwerkbereich, befinden. In solchen Situationen helfen die bisher aufgeführten Massnahmen nicht weiter.

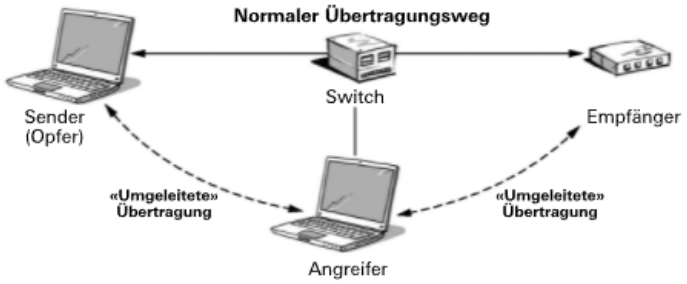
Jede Handlung[1] in einem Netzwerk löst spezifische Aktivitäten aus, die sich in einem bestimmten Muster (Pattern) des Datenstroms niederschlagen. Bei der Suche nach einer maliziösen Handlung geht es darum, Muster innerhalb der Datenströme zu erkennen, die darauf hinweisen. Diese Suche kann von einem sogenannten **Intrusion Prevention System (IPS)** oder **Intrusion Detection System (IDS)** übernommen werden. Ein solches System überwacht den Datenverkehr im Netzwerk und sucht dabei nach spezifischen Mustern. Sobald ein bestimmtes Muster erkannt ist, wird automatisch eine dafür hinterlegte (definierte) Aktion ausgelöst.

[1] Unabhängig davon, ob es eine erlaubte oder unerlaubte, eine interne oder externe Handlung ist.

MITM-Attacke

Bei einer **«Man in the middle»-Attacke** klinkt sich ein Angreifer in die Übertragung zwischen Sender und Empfänger ein. Damit dies gelingt, sendet der Angreifer dem Sender, also dem Opfer, gefälschte **ARP**[1]**-Nachrichten.** In diesen Nachrichten wird dem Opfer mitgeteilt, dass die MAC-Adresse des lokalen Gateways geändert habe. Natürlich handelt es sich bei dieser geänderten MAC-Adresse nicht um die tatsächliche MAC-Adresse des Gateways, sondern um die MAC-Adresse des Angreifers. Da ARP-Nachrichten nicht verifiziert werden, ändert das Opfer «gutgläubig» den entsprechenden Eintrag in seiner lokalen ARP-Tabelle. Das Ändern einer **ARP-Tabelle** mit der Absicht, sich unerlaubt in eine Kommunikation einzuklinken, wird auch «ARP-Poisoning» genannt, also das «Vergiften» der ARP-Tabelle. Ab diesem Zeitpunkt läuft der gesamte Datenverkehr des Opfers über das System des Angreifers. Dieser kann nun den Datenstrom aufzeichnen oder direkt nach bestimmten Informationen analysieren. Das Opfer merkt nichts von diesem Vorgang, da es alle angeforderten Daten erhält trotz der bestehenden «Umleitung». Damit diese Umleitung aufrechterhalten bleibt, muss der Angreifer laufend ARP-Nachrichten an das Opfer senden, um zu verhindern, dass die ARP-Tabelle des Opfers zufällig durch eine korrekte ARP-Nachricht wieder geändert wird. Und genau dieser stetige Versand von ARP-Nachrichten kann von einem IPS erkannt und als Angriff taxiert werden. In diesem Fall könnte z. B. das IPS eine Meldung an den RADIUS-Server schicken mit der Anweisung, den Switchport des Angreifers zu deaktivieren.

[5-11] Schematischer Ablauf einer «Man in the middle»-Attacke (MITM)



Grundkonfiguration einer IPS / IDS

In KMUs wird ein IPS bzw. IDS i. d. R. direkt in den Datenstrom zwischen dem Internet und den internen Netzwerkbereichen wie DMZ und internes LAN geschaltet. So besteht die Möglichkeit, den gesamten ein- und ausgehenden Datenstrom bei Bedarf auf unerlaubte Netzaktivitäten hin zu analysieren. Dabei ist aber zu beachten, dass diese Analysen eine gewisse **Latenz** verursachen. Je mehr Analysefunktionen aktiviert werden, desto grösser wird auch die dadurch verursachte Verzögerung bei der Datenübertragung. Aus diesem Grund sollten Sie sich gut überlegen, welche Analysen wirklich unbedingt vorgenommen werden müssen. Ist es beispielsweise sinnvoll, dass das IPS bzw. IDS nach Viren und Spammails sucht, wenn alle Clients und Server mit einem Virenscanner ausgerüstet worden sind und beim Mailserver ein wirkungsvoller Spamfilter installiert wurde? Nachfolgend sehen Sie ein Beispiel für die Definition und Aktivierung der zu überwachenden Objekte in einem IPS.

[1] Abkürzung für: Address Resolution Protocol. Weist einer IP-Adresse die MAC-Adresse der Netzwerkschnittstelle zu.

[5-12] Einstellungen bei einem IPS (Cisco SA520W)

Überwachte Netzwerkbereiche

Bei diesem IPS wird der Datenverkehr vom Internet (WAN) zur DMZ und zum LAN analysiert.

Updates der Angriffsmuster

Damit die IPS immer über die neuesten Angriffsmuster (Patterns) verfügt, muss die interne Muster-DB regelmässig aktualisiert werden. Dieser Vorgang ist vergleichbar mit der Aktualisierung der Viren-Muster bei einem Antivirenscanner. Dieser Updateservice ist i. d. R. kostenpflichtig.

Automatisieren der Musterupdates

Am besten aktiviert man die automatische Aktualisierung der Muster-DB, damit dies nicht vergessen geht. Nur mit aktuellen Mustern lassen sich aktuelle, bekannte Angriffe erkennen und abwehren.

Das oben abgebildete IPS erlaubt folgende Analysemöglichkeiten:

- **IPS Policy:** Welche Angriffskategorien sollen überwacht werden?
- **Protocol Inspection:** Welche Netzwerkprotokolle sollen zusätzlich auf maliziöse oder ungewöhnliche Inhalte wie z. B. eingebetteter, «protokollfremder» Code / Befehle untersucht werden? Zum Beispiel könnten dies SQL-Befehle innerhalb von HTTP-Daten sein, sogenannte «SQL Injections».
- **IM and P2P Blocking:** Welche unerlaubten Netzwerkfunktionen wie z. B. Peer-to-Peer-Aktivitäten (P2P) mittels bestimmter Filesharing-SW oder der Nachrichtenversand (Instant Messaging, IM) über bestimmte Nachrichtendienste sollen blockiert werden?

Die Thematik **Netzwerksicherheit** ist ein Teilbereich innerhalb der IT-Sicherheit. Die Schutzziele der Netzwerksicherheit decken sich mehrheitlich mit denen der IT-Sicherheit. Doch bei der Netzwerksicherheit liegt der Fokus hauptsächlich auf der Erkennung und Verhinderung der Übertragung von maliziösen Daten über das Netzwerk. Dazu sind folgende Aktivitäten nötig:

- **Analysieren und Filtern der Datenströme** auf maliziöse Inhalte
- **Authentifizierung von Systemen / Benutzern** beim Netzzugang
- **Abschottung gefährdeter Netzwerkbereiche** für bestimmte Systeme und Funktionen
- **Erkennen und Stoppen** von unerlaubten Netzaktivitäten

Mit den folgenden technischen Massnahmen werden die oben aufgeführten Aktivitäten durchgeführt:

- **Firewalls** für das Filtern und Analysieren der Datenströme
- **Einsatz von 802.1X** zur Authentifizierung beim Netzzugang
- **Realisieren einer DMZ** zur Trennung von «trusted» und «untrusted» Netzwerkbereichen
- **Einsatz eines Intrusion Prevention System IPS** zum Aufspüren und Unterbinden von unerlaubten Netzaktivitäten