

6.3 IT-Security und Betriebssicherheit

Kenntnisse über Gefahren von Viren, Würmern, Trojanern, Spyware, Hackern, Phishing.

Viren:

- Viren sind Schadprogramme, die alle Rechner, Programme und Dateien angreifen und schädigen.
- Man unterscheidet zwischen Computerviren, Programm-viren, Dateiviren und Systemviren.
- Er trägt sich in den Bootbereich (Bootsektor-Virus) ein, oder bettet sich in anderen Dateien ein.
- Verbreitung über Wechselmedien (USB-Sticks, SD-Karten, externe Festplatten).

Würmer:

- Ein Wurm ist ein infizierter Programmcode, der sich über die vorhandene Infrastruktur, über Netzwerkverbindungen oder den Anhang von E-Mails ausbreitet und auf anderen Systemen Schaden anrichtet.

Verbreitung über:

- E-Mail, Adressbuch des Benutzers.
- Netzwerk
- Wechselmedien (USB-Sticks, SD-Karten, externe Festplatten).

Trojaner:

- Ist ein Schadprogramm, eine Malware, das neben seiner eigentlichen Funktion noch weitere, unbekannte Funktionen hat.
- Richtet den Schaden „von innen“ an.
- Dabei werden Datenbestände und Passwörter ausspioniert und über das Internet versendet, ebenso werden auch Systemkonfigurationen verändert oder gelöscht.
- Verbreitet sich über E-Mails und Tauschbörsen.

Spyware:

- Ist der Name aus Spy (Spionieren) und Software.
- Ist eine Software, die das Online-Verhalten (Surfen im Internet) von Webnutzern ausspioniert, und dieses Wissen an andere weitergibt.
- Aktiviert sich meist mit dem Rechnerstart.
- Verändert Einstellungen am Rechner (Startseite, Suchmaschine im Browser)
- Verbreitet sich nicht auf andere Systeme.
- Gewonnene Daten werden kommerziell genutzt.

Hacker:

Unter Hacker versteht man Personen, die sich über öffentliche Netze oder IP-Netze unberechtigten Zugang zu anderen Systemen verschaffen.

- Der unberechtigte Zugang erfolgt in der Regel unter Umgehung der Sicherheitssysteme.
- Er beschäftigt sich mit Sicherheitsmechanismen und deren Schwachstellen, und sucht nach Sicherheitslücken, um sie aufzuzeigen, zu korrigieren oder um sie unerlaubt auszunutzen.

Black Hat Hacker:

- Ein Black-Hat-Hacker ist jemand, der die Sicherheit und Integrität von Computern oder Netzwerken mit böswilligen Absichten oder zum persönlichen Vorteil verletzt.

Black-Hat-Hacker dringen in Computersysteme ein, um diese zum eigenen Vorteil zu nutzen.

- Sie brechen in geschützte Netzwerke ein, um Daten zu löschen, zu bearbeiten oder zu stehlen. Häufig sorgen Black Hat-Hacker auch dafür, dass andere ein Netzwerk nicht mehr regulär nutzen können.

White Hat Hacker:

- Ein White-Hat-Hacker ist ein Computersicherheitsspezialist. White-Hat-Hacker verwenden häufig dieselben Techniken wie Black-Hat-Hacker, um in Computer und Netzwerke einzudringen.
- Der große Unterschied zwischen White-Hat-Hackern und Black-Hat-Hackern liegt in ihren Absichten.
- White-Hat-Hacker hacken von einem ethischen Standpunkt aus. Durch das Eindringen in sichere Computer und Netzwerke versuchen White-Hat-Hacker, Sicherheitslücken zu erkennen.
- Anschließend versuchen sie, Lösungen zur Verbesserung der Sicherheit zu finden. Die Absicht von White-Hat-Hackern ist es, Schwachstellen in der IT-Infrastruktur zu erkennen, bevor Black-Hat-Hacker diese Schwachstellen ausnutzen können.

Grey Hat Hacker:

- Gray-Hat-Hacker gehen ethisch und moralisch gesehen etwas flexibler mit den Regeln um als White-Hat-Hacker.
- Häufig dringen Grey-Hat-Hacker aus Interesse oder Neugier ohne Erlaubnis in Systeme ein. Wenn sie jedoch Sicherheitslücken finden, nutzen sie diese nicht mit böswilligen Absichten aus.
- Manchmal versuchen Grey-Hat-Hacker, eine kleine finanzielle Entschädigung für das Erkennen einer Sicherheitslücke zu erhalten.

Phishing:

- Ist ein Wort aus PASSWORT und FISHING.
- Es ist eine Technik mit denen Betrüger nach Passwörtern angeln.
- Die Angreifer heißen Phisher und versuchen vertrauliche Bankdaten - persönliche Identifikationsnummern (PIN), Transaktionsnummern (TAN) oder Kreditkartennummern - vom Bankkunden über das Internet abzufragen und damit Finanztransaktionen durchzuführen.
- Banken reagiert darauf mit elektronischen Transaktionsnummer (eTAN) und Chip TAN-Verfahren

Fachbegriff Zero-Day-Exploit

Bedeutung und Definition von Zero-Day

Zero-Day-Exploit (Fehler in der Software):

- Ein **Zero-Day-Exploit** ist eine Sicherheitslücke in einer Software, die am selben Tag für einen Angriff ausgenutzt wurde, an dem die Lücke entdeckt wurde.
- Exploit = Ein Exploit (englisch to exploit ‚ausnutzen‘) ist eine systematische Möglichkeit, Schwachstellen auszunutzen, die bei der Entwicklung eines Programms nicht berücksichtigt wurden.

Zero-Day ist ein allgemeiner Begriff und steht für neu entdeckte Sicherheitslücken, über die Hacker Systeme angreifen können. Man spricht von einem Zero-Day-Angriff, wenn Hacker die Schwachstelle ausnutzen können, bevor die Entwickler sie ausmerzen konnten.

- Eine Zero-Day-Schwachstelle ist eine Schwachstelle in der Software, die von Angreifern entdeckt wurde, bevor der Hersteller darauf aufmerksam geworden ist. Da der Hersteller nichts davon weiß, gibt es auch keinen Patch, so dass die Angriffe mit hoher Wahrscheinlichkeit erfolgreich verlaufen.
- Eine Zero-Day-Exploit ist die Methode, die die Hacker zum Angriff auf eine bislang unerkannte Schwachstelle anwenden.
- Ein Zero-Day-Angriff ist die Anwendung eines Zero-Day-Exploits, um Schaden anzurichten oder Daten aus einem geschwächten System zu entwenden.

Die **Schwachstellen**, die bei einem **Zero-Day-Angriff** gehackt werden, können in einer ganzen Reihe von Systemen auftreten:

- Betriebssysteme
- Webbrowser
- Office-Anwendungen
- Frei zugängliche Komponenten (Open Source)
- Hardware und Firmware
- Internet of Things (IoT)

Daher gibt es auch ein breites Spektrum an potenziellen Opfern:

- Privatpersonen, die ein infiziertes System wie einen Browser oder ein Betriebssystem nutzen.
- Hacker können Sicherheitslücken nutzen, um Geräte anzugreifen und riesige Botnets aufzubauen.
- Personen, die Zugang zu wertvollen Unternehmensdaten
- Hardware-Geräte, Firmware und das Internet der Dinge (IoT)
- Große Unternehmen und Organisationen
- Staatliche Stellen
- Politische Ziele und/oder Bedrohungen der nationalen Sicherheit.

Kenntnisse über Einschränkungsmöglichkeiten bei Benutzerkonten

Wird vom Administrator durchgeführt, bzw. eingestellt für Server - Clients.

Kein(e):

- MS-DOS Eingabeaufforderung
- Registry Editor
- Systemsteuerung
- Startmenü Ausführen
- Startmenü Suchen
- Taskmanager
- Datum/Uhrzeit/ Einstellungen
- Sperrbildschirm (Pause)
- Icon in der Taskleiste (Anzeigen von Hinweisen)
- Laufwerke ausblenden
- Tipps zu nicht erwünschten Starts von Laufwerken
- Installation von Programmen möglich
- Programmzugriff einschränken
- Zugriffsrechte für Dateien und Ordner festlegen
- Jugendschutz/Kindersicherung aktivieren und konfigurieren

Fachbegriff Multifaktor-Authentifizierung

Bei der **MFA** oder auch **Multi-Faktor-Authentifizierung** handelt es sich um eine Verallgemeinerung der **2FA – Zweifaktorauthentifizierung**.

- Mittels voneinander unabhängiger Schlüssel (Faktoren), kannst du Zugang zu einem System erhalten, und dann auch nur, wenn du beide gleichzeitig verwendest.
- Hier dienen mehrere Faktoren der Sicherheit, um eine mögliche Lücke im System auszuschließen.
- Multifaktor Authentisierung zur Sicherheit.

Um Zugang zu einem System zu haben, benötigst du bei der MFA zwei oder mehr Sicherheitsschlüssel. Grundsätzlich gibt es drei Formeln von Schlüsseln, idealerweise sollte aus mindestens zwei verschiedenen Kategorien gewählt werden.

Wissen: Beispiele dafür sind ein Passwort, ein PIN oder eine Sicherheitsfrage ("Wie hieß dein erstes Haustier").

Haben: Beispiele dafür sind dein Smartphone, ein Sicherheitschip, oder ein einfacher realer Schlüssel.


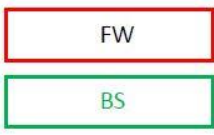
Sein: Dazu zählen etwa dein Fingerabdruck, deine Augen (Iris-Scan) oder eine Gesichtserkennung.

Die größte Sicherheit bringen unterschiedliche Schlüssel, denn falls ein System geknackt werden kann, kann dies nicht auf ein anderes umgelegt werden. Zum Beispiel wären drei Passworte alle aus dem Bereich Wissen. Wenn jemand ein Passwort hackt, ist die Gefahr groß, dass er dies auch bei den anderen schafft. Hingegen ist eine Kombination aus Passwort, authentifiziertem Gerät und Fingerabdruck viel schwerer auszuhebeln.
Mehr Sicherheit

Verwende immer eine MFA, wann immer möglich. Gerade bei Seiten und Anwendungen wie Facebook oder E-Mail-Anbietern, denn über solche können sonst andere Passworte leicht verändert oder ausgelesen werden. Die MFA oder 2FA lässt sich meist in den Einstellungen aktivieren, üblicherweise unter Passwort & Sicherheit. Dort lässt sich auch einrichten, welche Komponenten verwendet werden sollen.

Kenntnis der Sicherheits-Unterschiede zw. Hardware- und Software-Firewall

Auswahlkriterien Firewall System:

„Hardware“ Firewall (Appliance)	„Software“ Firewall
	
vom Betriebssystem des Rechners abgekoppelt	Läuft auf PC oder Server
Effizienter Schutz durch angepasstes Betriebssystem auf Firewall (optimierte Funktion der Dienste)	Eventuell leichter zu warten und aktualisieren als Hardware Firewall
z.B. Cisco, Sonicwall, Fortinet	z.B. lokale Firewall bei Windows, Kaspersky (Forefront TMG)

Die Firewall ist nur so stabil wie das Betriebssystem, auf dem sie läuft. Erlangt Angreifer Systemrechte auf einem Firewall System > Firewall nutzlos

Wichtig: Sicherheit des Betriebssystems, Updateszenario

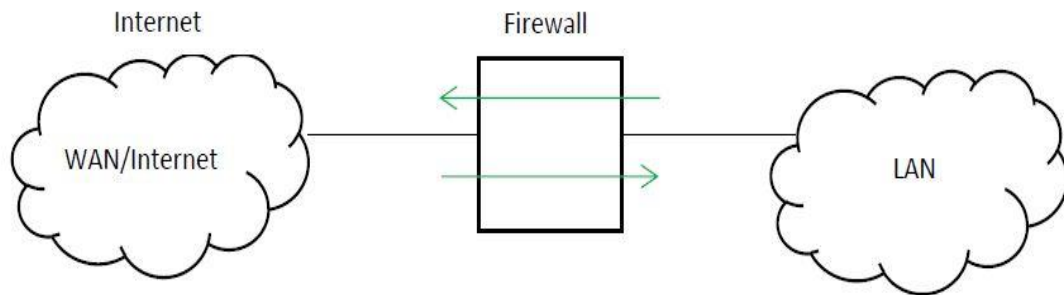
Unterschiede:

- Eine Software-Firewall überwacht den Datenverkehr zwischen Computer und verbundenen Netzwerken.
- Eine Hardware-Firewall überwacht den Datenverkehr zwischen zwei Netzwerken. Dadurch kann sie alle Verbindungen zwischen diesen Netzen überwachen.
- Eine Software-Firewall überwacht die Programme, die lokal auf dem Computer laufen. Die Hardware-Firewall kann nur den Datenverkehr überwachen.
- Über eine Software-Firewall können sich Viren verbreiten oder diese infizieren.
- Bei der Hardware-Firewall nicht. Da diese nicht auf dem zu überwachenden System läuft.
- Eine Software-Firewall überwacht den gesamten Datenverkehr des eigenen Computers.
- Eine Hardware-Firewall überwacht nur die Verbindungen zwischen zwei unterschiedlichen Netzen.
- Eine Software-Firewall verlangsamt den Computer, weil es Ressourcen verbraucht.
- Eine Hardware-Firewall verlangsamt nur den Datenverkehr.

Funktion einer Hardware-Firewall

Aufgabe:

- Ist ein System oder eine Gruppe von Systemen die die Kommunikation zu und von einem Netzwerk anhand von Regeln (Policies) erlaubt oder verbietet.
- Ohne Regeln nutzlos.
- Ist zwischen dem lokalen Netzwerk und dem Internet platziert.
- Strategien
- Alles ist gesperrt. Erwünschte Vorgänge müssen erlaubt werden. Aufwendig zu konfigurieren.
- Alles ist erlaubt. Unerwünschte Vorgänge müssen gesperrt werden
- Standardmäßig ist alles erlaubt.



Definition Policy (Richtlinie):

Ist eine Zusammenfassung von mehreren Sicherheitsregeln.

Firewall System:

Führt Sicherheitsrichtlinien aus!

Sicherheitsrichtlinien:

Ist eine Abfolge von Sicherheitsregeln

5W-Regel:

WER darf WIE von WORAUS und WANN auf WORAUF zugreifen?

Wer ist betroffen?

Wie ist er betroffen?

Woraus greift er zu?

Wann macht er das?

Worauf greift er zu?

Standardrichtlinie/Default Policy:

- Diese Sicherheitsrichtlinie regelt die Handhabung von Paketen, für die es keine 5W-Regel gibt.
(z.B. wenn UDP Protokoll nicht in der Access Control List Regel nicht erwähnt wurde.)

2 Möglichkeiten:

- Default Deny (standardmäßig alles verbieten)
- Default Permit (standardmäßig alles erlauben)

Vorteile:

Vom Betriebssystem eines Rechners abgekoppelt

Speziell angepasstes Betriebssystem für Firewall Anwendungen

Beispiel: Cisco, SonicWall, Fortinet

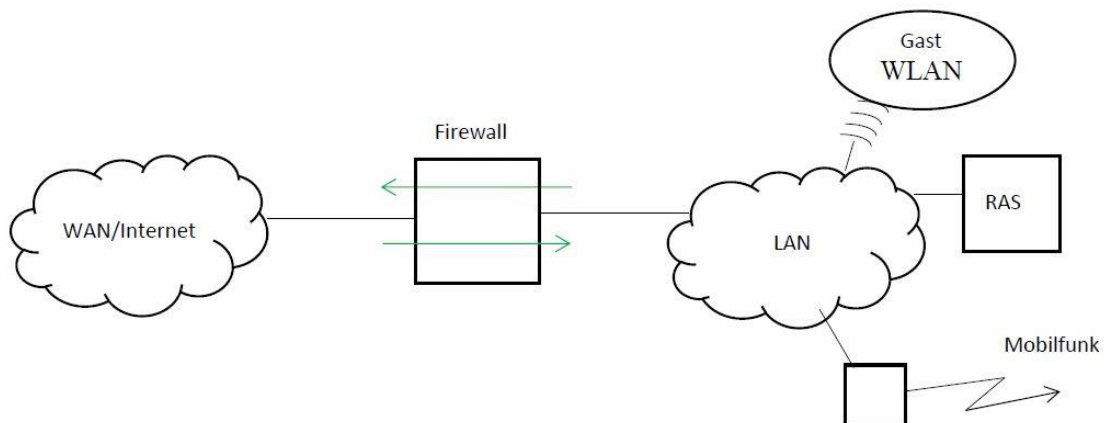
Grundlegende Forderung an Firewall-Konzept:

- Der gesamte Datenverkehr, in und aus dem geschützten Netzwerk, muss durch die Firewall gehen.

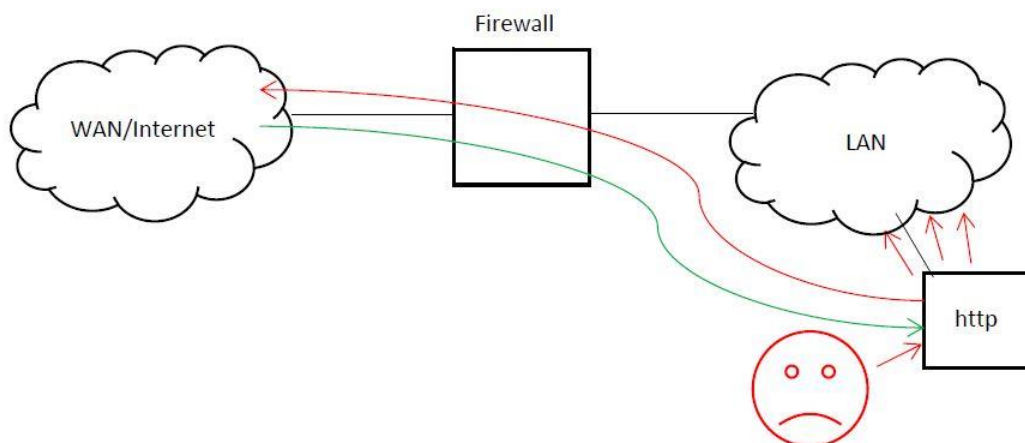
Netzwerk-Probleme durch öffentlich zugängliche Serverdienste:

- Ein öffentlicher Server bildet einen Angriffspunkt für Hacker, und kann in der Folge für weitere Angriffe auf das Netzwerk verwendet werden.

Einfaches Firewall Konzept:



Angriff Firewall:



Kenntnisse über notwendige Einstellungen bei Virenschanner

- Scan Häufigkeit
- Gescannte Verzeichnisse
- Updatefunktion der Virendefinition
- Quarantäne
- Computerschutz: Echtzeit-Dateischutz, Host Intrusion Prevention System (HIPS) (erkennt und verhindert unerwünschte Anwendungen).
- Internet-Schutz: E-Mail-Schutz, Phishing-Schutz, Web-Schutz (Erkennung und Sperrung von Webseiten mit bösartigen Inhalten).

Kenntnisse über Möglichkeiten Client-PCs vor Missbrauch zu schützen

- Virenschutzprogramm, zur Prüfung auf Schadprogramme.
- Personal Firewall, zur Kontrolle von ein- und ausgehenden Verbindungen.
- Gerätekontrolle, um die Verwendung von Geräten an externe Schnittstelle wie USB zu verhindern.
- Ausführungskontrolle, damit nur erlaubte Programme gestartet werden können.

- Benutzerrechte einschränken.
- Regelmäßige Updates und ständige Kontrolle aller Komponenten.
- Protokollierung relevanter Ereignisse und regelmäßige Auswertung der Protokolldaten.

Kenntnisse über sichere Planung von Backups

Datensicherung bezeichnet das Kopieren von Daten in der Absicht, diese im Fall eines Datenverlustes zurückkopieren zu können.

- Die auf dem Speichermedium gesicherten Daten werden als Sicherungskopie (Backup), bezeichnet.
- Die Wiederherstellung der Originaldaten aus einer Sicherungskopie bezeichnet man als Datenwiederherstellung, Datenrücksicherung (Restore).
- Wann wird gesichert?
- Welche Daten werden gesichert?
- Welche Sicherungsmethode soll verwendet werden?
- Auf welche Medien wird gesichert?
- Wo und wie lange lagern die Sicherungsmedien?
- Welche Daten müssen gesichert werden?
- Welche Software braucht man für die Datensicherung?
- Welche Hardware braucht man für die Datensicherung?
- Welche Sicherungsmethode sollte eingesetzt werden?
- Wie oft soll die Datensicherung durchgeführt werden?
- Wann soll die Datensicherung durchgeführt werden?
- Wo kann man die Datensicherungen aufbewahren?
- Wie kann man die Datensicherungen auf Fehler überprüfen?
- Aufbewahrungsfrist der Daten.
- Verschlüsselung der Daten.
- Wiederherstellungs-Prozedur.

Kenntnisse über verschiedene Backup-Prinzipien

Komplett/Vollsicherung:

- Alles wird gesichert/kopiert.
- Dauert sehr lange.
- Sicherungssoftware notwendig.
- Keine zusätzliche Software notwendig, wenn z.B. über Explorer gesichert wird.

Differenzielle Sicherung:

- Alle Dateien, die seit der Komplettsicherung verändert wurden, werden neu gespeichert.
- Es werden die Daten des zu sichernden Laufwerks mit dem Sicherungsdatenträger verglichen.
- Das Sicherungsprogramm untersucht, ob neue Dateien und Ordner hinzugekommen sind, und ob Dateien oder Ordner verschoben oder gelöscht wurden.
- Gegenüber einer Vollsicherung spart man Speicherplatz und Zeit.
- Bei der Wiederherstellung nimmt man die Komplettsicherung + die letzte Differenzielle Sicherung.
- Sicherungssoftware notwendig.

Inkrementelle Sicherung:

- Es wird eine Komplettsicherung gemacht.
- Dann bei der nächsten Sicherung eine Inkrementelle Sicherung.
- Es werden dabei immer nur die Daten gespeichert, die seit der letzten inkrementellen Sicherung geändert wurden oder neu hinzugekommen sind. Es wird immer auf der letzten inkrementellen Sicherung aufgebaut.
- Kette von Sicherungen die aufeinander aufbauen.
- Sicherung kann auf mehreren Datenträgern erfolgen.
- Bei der Wiederherstellung nimmt man die Komplettsicherung + alle inkrementellen Sicherungen.
- Hat den Nachteil, dass bei einer Wiederherstellung die Daten aus mehreren Teilen wieder zusammengesucht werden müssen.
- Sicherungssoftware wird dazu benötigt.

Speicherabbildsicherung:

- Dabei wird von der kompletten Festplatte ein Abbild (Image) erstellt.
- Wird verwendet, wenn der gesamte Datenträger inkl. Programme und System gesichert werden soll.

Kenntnisse über Backup-Medien und deren richtiger Lagerung

Backup-Medien:

- Optische Medien: CD, DVD, Blu-ray
- USB-Sticks, externe Festplatten, Magnetbänder (DAT, DLT, SLR, LTO), NAS-Geräte, SAN, RDX-Wechselfestplatte (über SATA und RDX-Laufwerk)
- Cloud, FTP Server

Richtige Lagerung:

- CD, DVDs, Blu-ray, bei Raumtemperatur, Dunkel, Trocken lagern, damit sich die empfindliche Reflexionsschicht nicht vorzeitig zersetzt.
- Direkte Sonneneinstrahlung vermeiden.
- Auf Beschriftungen oder Aufkleber verzichten
- CD, DVDs, Blu-ray... Sind empfindlich gegen UV-Strahlung und mechanische Beschädigungen. Deswegen sollten sie zum Schutz in Jewel Cases gegeben werden.
- Keine No-Name Produkte kaufen.
- Vor Stürze, Kratzer, Verschmutzungen schützen.
- Jährliche Funktionsprüfung durchführen. Neue Sicherungskopien anlegen.
- Blu-ray haben eine deutlich höhere Lebensdauer.

Fachbegriff DMZ

DMZ (Demilitarisierte Zone > Niemansland, Perimeternetzwerk):

Bedeutung:

- Von außen zugreifbarem Servern, werden in einen vorgelagerten Bereich (zwischen Interner und Externer Firewall) zwischen Intranet und Internet verlagert.

Aufgabe:

- Firewall erlaubt den eingehenden Datenverkehr nur wenn das Ziel ein Serverdienst im DMZ ist.
- Interne Firewall blockiert denn Zugriff vom Internet auf das Intranet. Ermöglicht Zugriff von Computer aus dem Intranet auf das firmeneigene WWW oder FTP Server.

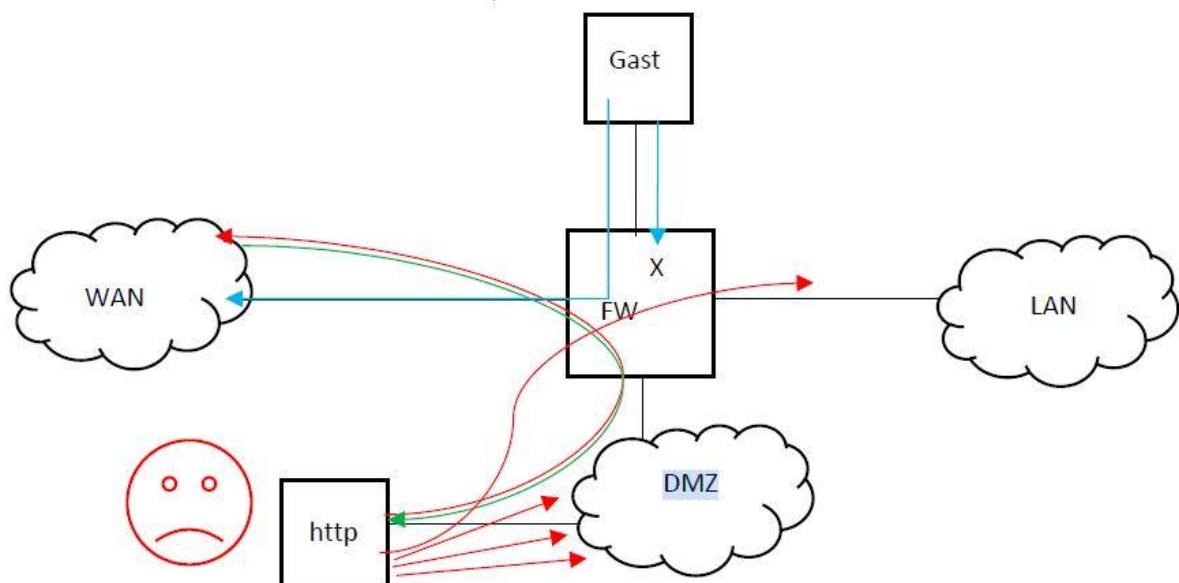
- Internetnutzung wird an der Externen Firewall unterbunden (nur für Server der DMZ erlaubt)
- Übernimmt ein Hacker die Externe Firewall oder einen Server aus der DMZ, blockiert die interne Firewall. Der Hacker hat nur Zugriff auf die DMZ.

Realisierung:

Durch Zweistufige Firewall mit DMZ



Firewall mit frei konfigurierten Interfaces



- Realisierbar durch Firewall Appliance oder Firewall Rechner mit mehreren Interfaces
> spezielle Konfiguration von unterschiedlichen DMZ möglich.

Fachbegriff Stateful Packet Inspection

Schutzmechanismen:

Zugriffsschutz - OSI Layer 1 – 4

Inhaltsschutz - OSI Layer 5 – 7

Paketfilter-Firewall:

Arbeitsweise:

- Arbeitet statisch

- Vorgegebene Zulassen/Verbieten Regeln (aus Access Control List) geben vor welche Art von Datenverkehr überprüft wird.
- Regeln werden nacheinander abgearbeitet.
- Trifft die Regel bei einem Paket zu, wird das Regelwerk verlassen.

Aufbau einer Access Control List:

Name der ACL

Aktion

Protokoll

Quelle (Netz, Host)

Ziel (Netz, Host)

Arten der Configuration:

- Sperren von jedem nicht genutzten (gewollten) Verkehr,
- oder nur definierten (gewollten) Verkehr erlauben.

Automatische System-Regel:

- Damit es immer einen Match gibt, lautet die letzte Regel standardmäßig immer deny ip any oder deny ip any any (bei einer erweiterten ACL)
- (Alle Pakete, egal von welcher IP Adresse, werden verworfen)

Durch eine Paketfilter-Firewall (Access Control List) überprüfte Informationen:

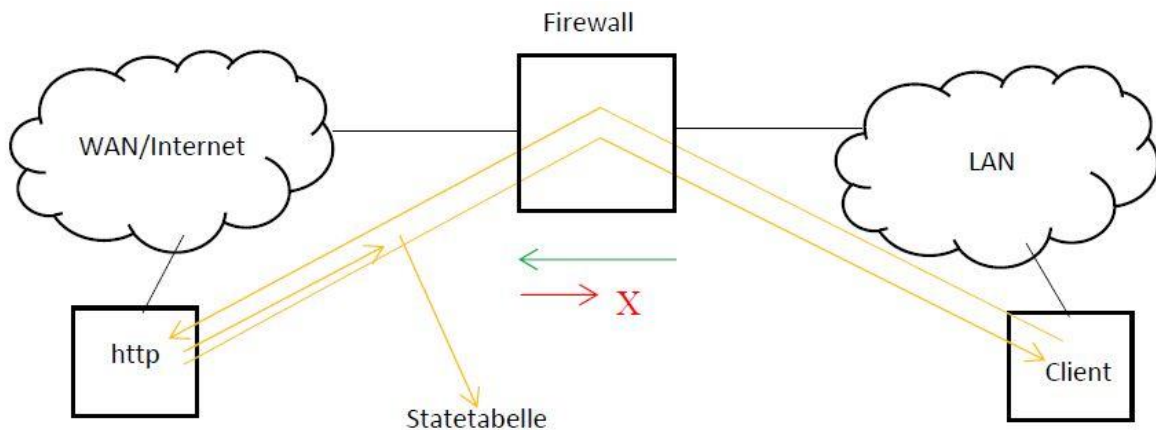
- Quell- und Zieladresse (Layer 3)
- Protokolle und Portnummer (Layer 4) (TCP, UDP, ICMP)

Dynamische Filtermethode Stateful Inspection, Regel- und State-Tabelle:

- Arbeitet dynamisch
- Zieht Merkmale und individuellen Kontext für die Weiterleitung des Pakets in Betracht.
- Nutzt zusätzlich zur Regeltabelle eine State-Tabelle, in der alle Zustände der ein- und ausgehenden Verbindungen eingetragen sind.
- Ports grundsätzlich geschlossen. Bei Anfrage von innen heraus, wird der Port für den genutzten Zeitraum geöffnet.

Dynamische Filtermethode Stateful Inspection, Regel- und State-Tabelle:

- Arbeitet dynamisch
- Zieht Merkmale und individuellen Kontext für die Weiterleitung des Pakets in Betracht.
- Nutzt zusätzlich zur Regeltabelle eine State-Tabelle, in der alle Zustände der ein- und ausgehenden Verbindungen eingetragen sind.
- Ports grundsätzlich geschlossen. Bei Anfrage von innen heraus, wird der Port für den genutzten Zeitraum geöffnet.



Paket erlaubt, wenn...

- durch Regel festgelegt (REGELTABELLE - statisch)
- es eine gültige Anforderung gibt (STATETABELLE - dynamisch)

Durch eine Stateful Inspection-Firewall überprüfte Informationen:

(Es werden die gleichen Informationen wie bei der Regeltabelle überprüft)

- Quell- und Zieladresse
- Protokolle und Portnummer
(Zusätzlich Protokoll Informationen im Detail (z.B. bei TCP))
- Flags
- Sequenznummer, ACKs

Funktionsweise eines Port-Scanners

Portscanner:

Portscanner ist eine Software mit der überprüft werden kann welche Dienste ein System mit TCP und UDP über das Internetprotokoll anbietet.

Funktionsweise:

- Der Portscanner nutzt den Drei-Wege-Handshake.
- Er sendet ein TCP-SYN-Paket.
- Wenn der Port offen ist, dann bekommt der Portscanner ein TCP-SYN/ACK-Paket zurück.
- Es wird kein vollständiger Verbindungsaufbau durchgeführt.
- Der Portscanner beschränkt sich nur auf einen Verbindungsversuch.

Wird verwendet für:

- Erkennung von Sicherheitslücken und Schwachstellen in einem Netzwerk
- Erkennung welche Anwendungen aktive und erreichbar sind (Erreichbarkeit wird über den Zustand der Ports bestimmt)
- Inventur von Computern und der angebotenen Dienste
- Prüfen der Einhaltung von Richtlinien
- Verfügbarkeitstests
- Fehlersuche im Netzwerk

Ports:

- Ports bilden die Schnittstelle zu den Services und Anwendungen, die auf einem Computer laufen.
- Sie bilden den Übergang von der paketorientierten Übertragung zum Datenstrom, der von und zu den Anwendungen fließt.

- Anhand der Portnummer weiß ein System an welche Anwendung ein Datenpaket übertragen werden muss.

Kenntnisse über Sicherheitstechnologie TLS

TLS (Transport Layer Security):

TLS ist ein Protokoll zur Authentifizierung und Verschlüsselung von Internet-Verbindungen.

Hauptaufgaben:

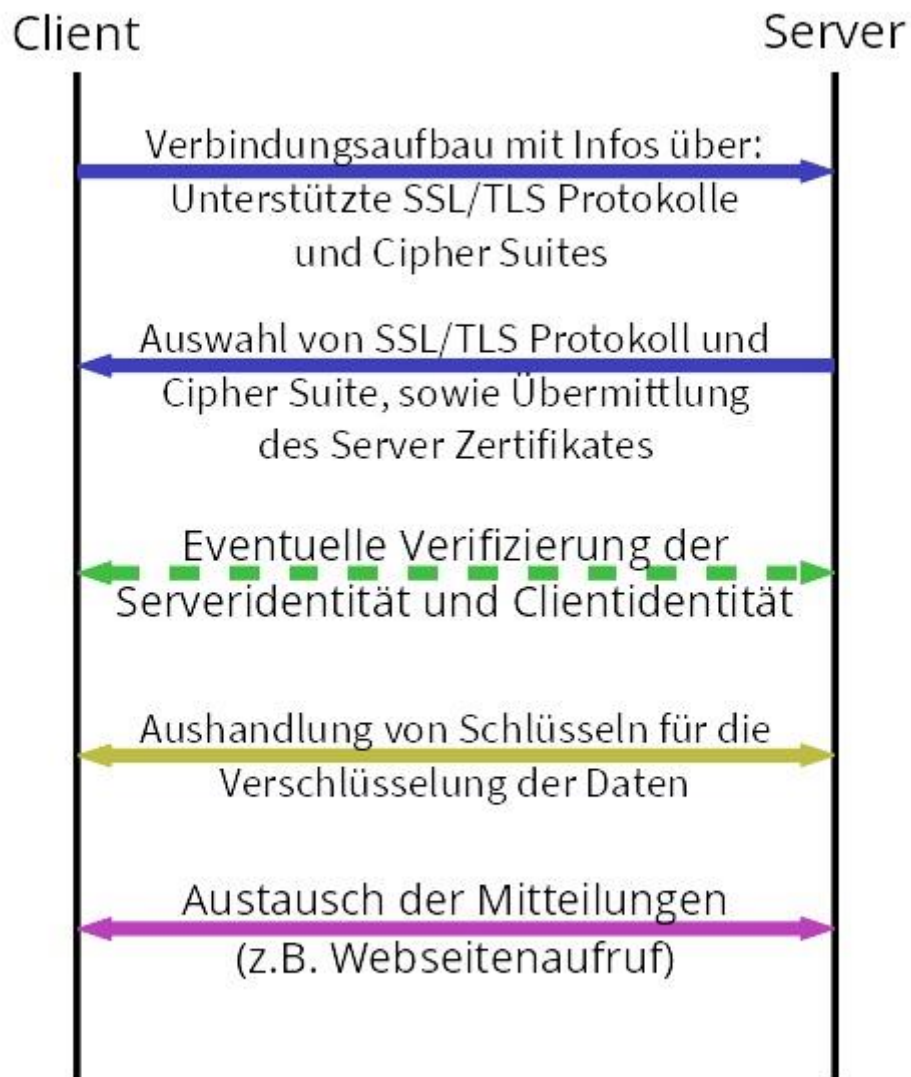
- Authentifikation der Kommunikationspartner
- Ende zu Ende Datenübertragung
- Sicherstellung der Integrität der transportierten Daten (Die Daten müssen nachweislich vollständig und unverändert sein)

Einsatzgebiete:

- HTTPS, SMTP, IMAP, POP3, FTP

Verbindungsaufbau:

- Der Client baut eine Verbindung zum Server auf und teilt ihm die Verschlüsselungsverfahren, die er unterstützt, mit. (**REQUEST**)
- Der Server wählt ein Verfahren aus und schickt dem Client sein Zertifikat mit dem öffentlichen Schlüssel des Servers. (**Authentifizierung**)
- Der Client überprüft das Zertifikat auf Vertrauenswürdigkeit und Übereinstimmung, in dem er es an die Zertifizierungsstelle (CA) schickt.
- Optional kann sich auch der Client mit einem **Zertifikat** gegenüber dem Server authentifizieren.



- Dann schickt der Client dem Server eine mit dem öffentlichen Schlüssel des Servers verschlüsselte geheime Zufallszahl oder...
- Die beiden berechnen mit dem Diffie-Hellman-Schlüsselaustausch ein gemeinsames Geheimnis.
- (Zur Berechnung nutzen beide Parteien dazu ihren eigenen Privaten Schlüssel und den Öffentlichen Schlüssel des anderen)
- Aus diesem Geheimnis wird dann ein kryptografischer Schlüssel abgeleitet. Dieser wird dann für die Verschlüsselung aller Nachrichten der Verbindung verwendet.
- Es wird symmetrisch verschlüsselt.
- Anschließend generiert der Client den Sitzungsschlüssel für ein symmetrisches Verschlüsselungsverfahren. Dieser Schlüssel wird nun mit dem öffentlichen Schlüssel des Servers verschlüsselt und zum Server übertragen. Nur dieser kann ihn mit dem privaten Schlüssel wieder entschlüsseln.
- Optional kann nun eine Clientidentifizierung erfolgen, die ähnlich der Serveridentifikation abläuft. Der Client muss jedoch über ein gültiges Zertifikat verfügen.

Fachbegriff CA in Zusammenhang mit Zertifikaten

CA (Certification Authority - Zertifizierungsstelle):

- Ist eine Organisation die digitalen Zertifikate herausgibt und prüft.
- Das Zertifikat dient dazu einen bestimmten öffentlichen Schlüssel einer Person oder Organisation zuzuordnen. Das wird von der Zertifizierungsstelle mit der eigenen Unterschrift beglaubigt.
- Sie ist verantwortlich für die Bereitstellung, Zuweisung und Integrität (Daten müssen vollständig und unverändert sein) der von ihnen ausgegebenen Zertifikaten.

Fachbegriffe Private Key und Public Key

Werden bei Asymmetrischer Verschlüsselungsverfahren eingesetzt.

Asymmetrische Verfahren:

Jede der kommunizierenden Parteien besitzt ein Schlüsselpaar, bestehend aus

- einem geheimen Teil (Privater Schlüssel)
- einem nicht geheimen Teil (Öffentlicher Schlüssel)

Öffentlicher Schlüssel:

Ein öffentlicher Schlüssel ermöglicht jedem:

- Daten für den Inhaber des privaten Schlüssels zu verschlüsseln
- dessen digitale Signaturen zu prüfen
- ihn zu authentifizieren

Privater Schlüssel:

Ein privater Schlüssel ermöglicht es dem Inhaber:

- Verschlüsselte Daten zu entschlüsseln
- Digitale Signaturen zu erzeugen
- sich zu authentifizieren

Öffentlicher und privater Schlüssel:

- Ein öffentlicher Schlüssel ist jedem frei zugänglich.
- Ein privater Schlüssel wird vom Inhaber geheim gehalten.
- Beide Schlüssel stehen in einer bestimmten mathematischen Beziehung zueinander.

Prinzip:

- Verschlüsselung mit öffentlichem Schlüssel > Entschlüsselung mit privatem Schlüssel
- Verschlüsselung mit privatem Schlüssel > Entschlüsselung mit öffentlichem Schlüssel

Erzeugung des Schlüsselpaares:

- Aus einer großen Zufallszahl wird das Schlüsselpaar durch eine Funktion generiert.

Ver- und Entschlüsselung:

- Unverschlüsselter Text wird durch Anwendung des öffentlichen Schlüssels verschlüsselt.
- Verschlüsselter Text wird dann vom Inhaber des privaten Schlüssels wieder entschlüsselt.

Signatur:

- Es wird ein Hashwert aus der zu verschickenden Nachricht erstellt, und mit dem privaten Schlüssel verschlüsselt.

- Der Empfänger prüft die Signatur in dem er den Hashwert entschlüsselt und mit dem Hashwert der Nachricht vergleicht.

Public Key Verfahren und symmetrische Verschlüsselung:

- Durch Kombinieren eines privaten und öffentlichen Schlüssels kann ein gemeinsames Geheimnis errechnet werden.

RSA (Rivest Shamir Adleman) Verfahren:

- 1977 entwickelt, Sicheres Verfahren
- **Vorteil:** Verschlüsseln und Signieren in beide Richtungen.

Hybride Verfahren:

- Asymmetrische Verfahren sind 1000-mal langsamer als Symmetrische Verfahren.

Daher...

- Aufbau einer verschlüsselten Verbindung erfolgt über ein asymmetrisches Verfahren.
- Session Keys werden ausgetauscht mit denen dann symmetrisch verschlüsselt wird.

Sicherstellen von Datenvertraulichkeit bei gemeinsamen Netzlaufwerken

Vertraulichkeit /Zugriffsschutz

- Nur berechtigte Personen sollen Daten oder Nachrichten lesen dürfen, oder Informationen über den Inhalt erlangen.

Sicherstellung durch:

- Benutzerauthentifizierung
- VLAN
- Verschlüsselung
- Zugangskontrolle

Erarbeiten von Berechtigungskonzepten im Active Directory

In einem Berechtigungskonzept wird beschrieben, welche Zugriffsregeln für die einzelnen Benutzer oder Benutzergruppen auf die Daten gelten.

Anforderungen:

- Benutzer bekommen neue Aufgaben und Rollen, wechseln die Abteilung
- Es gibt Vertretungen bei Krankheit und Urlaub
- Neue Nutzer kommen in das Unternehmen, andere verlassen die Firma
- Neue Geräte, Anwendungen und Daten kommen hinzu oder werden entfernt
- Cloud-Dienste, Benutzer bringen ihr private Geräte in das Unternehmen mit (BYOD)

Vorgehensweise:

- Alle Benutzer, Geräte und Anwendungen erfassen
- Berechtigungen Benutzern, Geräten und Anwendungen zuweisen
- Rollenkonzept nutzen: Rollen definieren und den Benutzern, Geräten und Anwendungen zuweisen
- Berechtigungskonzept regelmäßig prüfen

Festlegen von Gruppenrichtlinien (GPOs)

Die **Gruppenrichtlinien in Active Directory** ermöglichen eine zentrale Verwaltung der Konfigurationseinstellungen von Windows. Die Gruppenrichtlinien dienen vor allem für in die

Domäne eingebundene Client-Geräte, da sie eine detailliertere Kontrolle ermöglichen als andere Lösungen.

Die Einstellungen von Gruppenrichtlinien werden in Gruppenrichtlinienobjekten (GPOs) konfiguriert. Sie können GPOs mit Domänen, Standorten und Organisationseinheiten verknüpfen. Um eine noch bessere Kontrolle zu erzielen, können Gruppenrichtlinienobjekte auf der Grundlage der Ergebnisse von WMI-Filtern (Windows Management Instrumentation) angewendet werden. WMI-Filter sollten jedoch sparsam verwendet werden, da sie die Richtlinienverarbeitung deutlich verlangsamen können.

Die Gruppenrichtlinien-Verwaltungskonsolle (GPMC) ist ein integriertes Tool für die Verwaltung von Windows, mit dem Administratoren Gruppenrichtlinien in einer Active Directory-Gesamtstruktur verwalten und Daten für die Fehlerbehebung in Gruppenrichtlinien abrufen können. Die Gruppenrichtlinien-Verwaltungskonsolle können Sie über das Menü „Tools“ im Microsoft Windows Server-Manager aufrufen. Da es nicht empfehlenswert ist, für routinemäßige Verwaltungsaufgaben die Domänencontroller zu verwenden, sollten Sie die Remoteserver-Verwaltungstools (RSAT) für Ihre Windows-Version installieren.

Richtlinien führen nicht zu einer Ansammlung zahlreicher Einträge in der Registrierung: Wird eine Einstellung eines Gruppenrichtlinienobjekts geändert oder liegt das Gruppenrichtlinienobjekt außerhalb des Bereichs, wird die Richtlinieneinstellung gelöscht und stattdessen der ursprüngliche Wert verwendet. Richtlinieneinstellungen heben stets die Konfigurationseinstellungen einer Anwendung auf und sind ausgeblendet, damit Benutzer sie nicht ändern können.

Einstellungen hinterlassen standardmäßig eine Vielzahl von Einträgen in der Registrierung. Dieses Verhalten kann jedoch für jede Einstellung konfiguriert werden. Einstellungen setzen die Konfigurationseinstellungen einer Anwendung außer Kraft, ermöglichen den Benutzern jedoch eine Änderung der Konfigurationselemente. Viele der konfigurierbaren Elemente in den Gruppenrichtlinieneinstellungen wurden bislang häufig mit einem Anmeldeskript konfiguriert, beispielsweise die Laufwerkszuordnungen und die Druckerkonfiguration.

Erzwingen von Passwortrichtlinien

Ein Passwort sollte aus mindestens zehn Zeichen bestehen. Innerhalb des Passworts sollte mindestens ein Sonderzeichen enthalten sein. Es sollten sowohl Groß- als auch Kleinbuchstaben sowie Ziffern in Verwendung sein (4 aus 4 Kriterien-Regel). Ein Passwort darf bei der Eingabe nicht am Bildschirm angezeigt werden.

z.B: Windows Active Directory:

Diese Richtlinie erzwingt bei Aktivierung folgende Regeln für neue, von Benutzern erstellte Passwörter:

- Das Passwort muss mindestens 6 Zeichen lang sein.
- Soll aus den 4 Kategorien Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen bestehen.

Kenntnisse über User Account Control (UAC)

UAC (User Account Control – Benutzerkontensteuerung):

- Mit der Benutzerkontensteuerung kann verhindert werden, das potenzielle schädliche Programme Änderungen am Computer vornehmen können.
- Für eine Administrative Aufgabe ist eine zusätzliche Bestätigung erforderlich.

- Hat den Vorteil das administrative Aufgaben ausgeführt werden, ohne dass eine neue Anmeldung mit einem administrativen Account notwendig wird.

Arbeitsweise:

- Administrative Benutzer bekommen 2 Security-Token zugewiesen.
- Standardmäßig wird mit dem Token gearbeitet, das sie als Standardbenutzer identifiziert.
- Sollen nun administrative Aufgaben (Softwareinstallation, Änderungen) durchgeführt werden, erscheint ein Dialogfenster zum Bestätigen.
- Durch die Bestätigung wird auf den anderen Token gewechselt, der ihm volle administrative Berechtigungen gibt.

UAC-Abfrage - Es gibt 4 Stufen:

(In der Systemsteuerung zu finden)

Stufe 1 (Schieberegler ganz oben):

- Immer Benachrichtigen

Stufe 2:

- Nur benachrichtigen, wenn Änderungen an meinem Computer vom Programm vorgenommen werden (Standardeinstellung)

Stufe 3:

- Nur benachrichtigen, wenn Änderungen an meinem Computer vom Programm vorgenommen werden (Desktop nicht abblenden)

Stufe 4 (Schieberegler ganz unten):

- Nie Benachrichtigungen

Die UAC kann Problem verursachen:

- Man will ein Softwareproblem beheben, ein Programm besser ausführen können, oder zwei Programme sollen besser untereinander interagieren.
- Es können bei Anwendungen Zeitüberschreitungsmeldungen auftreten, weil die UAC das Ausführen blockiert.

Zur schnellen Sicherheits-Einschätzung wird eine farbige Fensterleiste verwendet:

- blaugrüne Fensterleiste: Es handelt sich um ein signiertes Programm von Microsoft
- graue Fensterleiste: Es handelt sich um ein signiertes Programm von einem Drittanbieter
- gelbe Fensterleiste: Es handelt sich um ein unsigniertes Programm

Kenntnisse über Möglichkeiten Client-PCs vor Missbrauch zu schützen

Schutz durch:

- Zutrittskontrolle zu Räumen
- Zugangskontrolle (Benutzerlogin verwenden)
- Zugriffskontrolle (Benutzer Berechtigungen einschränken)
- PC sperren, wenn er verlassen wird
- Schnittstellen am PC sperren (USB deaktivieren)
- Softwareinstallationen verbieten
- Ausführungskontrolle (damit nur erlaubte Programme gestartet werden können)
- Kontrolle wer welche Daten verarbeitet hat
- Virens Scanner, Personal Firewall (Software)
- Regelmäßige Kontrolle der Komponenten

Kenntnisse über Methoden der sicheren Löschung von Daten

- Wenn Daten gelöscht werden, werden sie nur aus dem Index gelöscht. Sie können aber trotzdem durch spezielle Programme wiederhergestellt werden.
- Erst wenn der Bereich, wo die Daten gespeichert waren, überschrieben wird, sind sie endgültig gelöscht.

Sicheres Löschen:

- Löschen und Mehrfaches Überschreiben der Daten. Durch Einsatz von Programmen. (Eraser, CCleaner, Hersteller Tools von Corsair, Intel, Samsung, SanDisk)
- Verwendung von komplexer Verschlüsselung
- Optische Datenträger können mit einem Brenner „überbrannt“ werden (nur wieder-beschreibbare Datenträger)
- Datenträger entmagnetisieren
- Physische Zerstörung des Speichermediums (bohren, zerbrechen, zerschneiden, zerkratzen)

Inhalte von Unternehmensrichtlinien für Datenträgerentsorgung

- Zwecks Datenschutzes müssen Datenträger so vernichtet werden, dass keine Daten wiederhergestellt werden können.
- Datenträger vor der Entsorgung unbrauchbar machen, und entmagnetisieren.
- Einen Festplatten Datenvernichter benutzen (Shreddern)
- Oder wenn kein Vernichter im Unternehmen steht, Datenträger nicht einfach zum Altstoffsammelzentrum bringen, sondern zu einer Firma, die das professionell macht.