IT-Security Management

Modul 182

Titel	IT-Security Management	**Typ**	Kategorie	**Version**	1.2
Thema	Modul 182	**Klasse**	öffentlich	**Freigabe Datum**	05.05.2012
Autor	Janik von Rotz	**Status**	Status		
Ablage/Name	D:\SkyDrive\education\bbzs\4.lehrjahr\sba\Modul184\Modu 184 IT-Security Management.docx				
Schlüsselwörter					
Kommentare					

Dokumentverlauf

Version	Datum	Autor	Beschreibung der Änderung	Status
1.0	28.04.2012	Janik von Rotz	Erstellen Dokument	In Bearbeitung
1.1	05.05.2012	Janik von Rotz	Freigeben	Freigabe
1.2	14.05.2012	Janik von Rotz	Umstruktierung, anpassen Formatvorlagen	Fertiggestellt

Referenzierte Dokumente

Nr.	Dok-ID	Titel des Dokumentes / Bemerkungen	Ablage / Link

Lizenz

Inhaltsverzeichnis

1 Betriebswirtschaftliche Aspekte zur Systemsicherheit

1.1 Auswirkungen von Sicherheitsvorfällen

- **Verlust der Vertraulichkeit von Daten**
  - unerlaubte Kopieroperationen
  - Abhören der Datenübertragung
  - Lücken in der Zugriffssicherheit aufgrund von administrativen Mängeln
  - physischer Zugriff auf Datenträger (Diebstahl von Datenträgern oder Mobilesystemen)
  - Verlust von Vertraulichkeit aufgrund dem Einsatz von Malware (Keylogger, Rootkits)
- **Verlust der Integrität von Daten**
  - aus den gleichen Gründen wie oben
- **Verlust der Verfügbarkeit von Systemen**
  - Unterbrechung der Geschäftsprozesse
  - durch Lahmlegen von wichtigen Systemen
  - Sabotage an Systemen oder Teilsystemen
  - Denial of Service Angriffe gegen exponierte Dienste
- **Verlust der Identität von Benutzern und Host**
  - durch das Ausspionieren von Benutzernamen und Kennwörtern (Social Engineering, Passwort-Cracker)
  - den Diebstahl von privaten Schlüsseln in PKI-Infrastruktureny-> Dritte können unberechtigterweise an Stelle von Personen oder Diensten handeln
- **Verlust der Nichtabstreitbarkeit der Urheberschaft**
  - die Urheberschaft von Dokumenten kann nicht nachvollzogen werden,
  - die Rechtsverbindlichkeit von digitalen Dokumenten kann nicht gewährleistet werden.

Zusammengefasst kann gesagt werden, dass die IT-Security den Auftrag hat die folgenden abstrakten Güter zu schützen:

1. Schutz der Vertraulichkeit von Daten bei Einspeicherung und Übertragung
2. Schutz der Integrität von Daten bei Einspeicherung und Übertragung
3. Schutz der Verfügbarkeit von Systemen und Diensten
4. Schutz vor missbräuchlicher Verwendung der Systeme
5. Schutz der Identitäten von Benutzern und Systemen
6. Schutz der Nichtabstreitbarkeit der Urheberschaft von Daten Prozessen

Die betriebswirtschaftlichen Folgen sind:

- Produktionseinbussen oder Verzögerungen
- Beeinträchtigung des Kundenvertrauens
- Beeinträchtigung des Investorenvertrauens
- Umsatzverluste
- Rufschädigung
- Rechtliche Konsequenzen aufgrund von Haftungsansprüchen von Geschäftspartnern

Die Planung, Implementierung, Überprüfung und Aufrechterhaltung von Sicherheitsmassnahmen verursacht Kosten. Typischerweise betragen diese Kosten nur einen Bruchteil der Kosten, die bei einem Sicherheitsvorfall für die Behebung und Verarbeitung von Schäden aufgewendet werden müssen.

1.2 IT-Sicherheits-Risikomanagement Prozess-Kette

1.2.1 Schritt 1: Identifikation und Bewertung

- Identifizieren der sicherheitsrelevanten IT-Asset Items und Sub-Asset-Items
- Identifizieren der Bedrohungen, denen die Asset-Items ausgesetzt sind
- Festlegen der Sicherheitsrisiken der Sicherheitsrisiken, die sich aus den einzelnen Bedrohungen ergeben
- Liste mit relariver Rangordnung der Sicherheitsrisiken erstellen (Priorisierung der zu ergreifenden Gegenmassnahmen zur Reduzierung von Sicherheitsrisiken
- Identifikations- und Bewertungsprozess auf neue und geänderte System kontinuierlich anwenden (permanente Tätigkeit)

1.2.2 Schritt 2: Entwicklung und Implementierung

- Festlegen von Sicherheitsrichtlinien für die die verschiedenen Sicherheitsmassnahmen und Asset-Items entsprechend ihrer Priorisierung
- Ausarbeitung von Verfahren, die bei Notfällen (Systemausfälle, sicherheitskritische Vorfälle) zur Anwendung kommen müssen
- Austesten der Sicherheitsmassnahmen im Testbetrieb
- Dokumentation der Sicherheitsrichtlinien als praktische Wegleitungen für die Inbetriebnahme und Wartung von Systemen

1.2.3 Schritt 3: Implementierung und Aufrechterhalten der Sicherheitsrichtlinen

- Schulung von IT-Personal und Anwendern
- Anwendung der Sicherheitsrichtlinien bei der Installation und Inbetriebnahme von System
- Anwendung der Sicherheitsrichtlinien bei der Wartung der Systeme

Sicherheitsrichtlinie

Beschreibt, mit welchen Prozessen den verschiedenen Risiken, die auf den verschiedenen Asset-Items festgestellt wurden, begegnet werden soll und wie diese Massnahmen überwacht und weiterentwickelt werden sollen. Zudem werden die Verantwortlichkeiten grundsätzlich geregelt.

1.2.4 Schritt 4: Austesten der Systemsicherheit

Es werden zwei Testarten unterschieden

1.2.4.1 Test aus der Aussensicht -> Penetrationstest

Phase	Bezeichnung	Vorraussetzung	Vorgehen	Tools
1	System aufklären	Tester haben keine Kenntnisse über das System		Social Engineering Netzwerk Scanner (nmap) Paketgenerator (netcat) Vulnerabilty Passwort-Cracker Etc.
2	Security-Audits (Test von innen)	Tester verfügen über eine vollständige Systemdokumentation	Es werden primär Sicherheitsrichtlinien (Prozesse, Vorgehensweisen überprüft)	

Externe Tester überprüfen die IT-Sicherheit mit dem Wissensstand eines externen Angreifers und erstatten detaillierten Bericht.

Die entdeckten Mängel haben Einfluss auf den Sicherheitsprozess (Schritte 1-3) und die eigenlichen Sicherheitsrichtlinien.

1.2.4.1.1 Phasen und Werkzeuge für Penetrationstests

Phase	Bezeichnung/ Zielsetzung	Tools
1	**Anforderungen** Bekanntgabe der zu überprüfenden Adressen und Prozesse	
2	**Footprinting** Informationsbeschaffung (Information-Gathering) mittels Systemtools	• Publikationen der Firma (z.B. Homepage) • Social Engineering • DNS-Einträge zur Firmen-Domäne
3	**Ist-Aufnahme** Mit Scans sollen benutzte IP-Adressen, Betriebssysteme von Hosts und Netzwerkgeräten, Produkte und Versionen von wichtigen Diensten in Erfahrung gebracht werden	• Netzwerkscanner (nmap)
4	**Analyse** Einsatz von Schachstellen-Analysatoren (Vulnerabilty Scanner) Einsatz von Passwort-Cracker gegen Netzwerkgeräte und Serversysteme	• Vulnerability Scanner (Nessus) • Spezielle Vulnerability-Toolsammlungen (BOSS vom BSI)
5	**Report** Berichterstattung über die Ergebnisse des Penetrationstests Massnahmen zur Ausmerzung der erkannten Schwachstellen vorschlagen	

1.2.4.2 Test aus der Innensicht –> Sicherheits-Audit

Externe Tester überprüfen die IT-Sicherheit (Zweckmässigkeit der Sicherheitsprozesse (Schritte 1-3) und die Wirksamkeit der Sicherheitsrichtlinien) unter Mitwirkung der verantwortlichen Administratoren mit dem vollen Systemwissen der Administratoren).

Die entdeckten Mängel haben Einfluss auf den Sicherheitsprozess (Schritte 1-3) und die eigentlichen Sicherheitsrichtlinien.

1.3 Wichtige Sicherheitsbedrohungen – STRIDE

Bedrohungstyp	Beispiele
Spoofing	Fälschen von MAC-Adressen
	Fälschen von IP-Adressen
	Fälschen von FQDNs
	Fälschen von E-Mail-Nachichten
	Replayangriffe mit Authentifizierungspaketen
Tampering	Ändern von Daten bei der Übertragung
	Ändern von Daten in Dateien
Repudiation	Alle Massnahmen, die dazu dienen, die Urheberschaft eines Dokumentes abstreiten zu können.
	Löschen einer kritischen Datei und anschliessendes Verschleiern des Ereignisses
Information disclosure	Offenlegen von Informationen in Fehlermeldungen
	Offenlegen von Programmcode auf Websites
Denial of Services	Überfluten eines Netzwerkes z.B. mit SYN-Flag haltigen TCP-Segmenten oder mit gefälschten ICMP-Paketen
Elevation of Privilege	Ausnutzen von Pufferüberläufen (Buffer Overflow), um root- bzw. Administratoren-Rechte zu erhalten
	Unrechtmässiges Beschaffen von Administratorenrechten

Begriffe im Zusammenhang mit Schwachstellen von Programmen und Angriffe

Vulnerabilty	Schwachstelle einer Software, die das Ausarbeiten eines Angriffs möglich macht (z.B. Buffer overflow, SQL-Injection)
Exploit	Konkretes Angriffsverfahren, das auf einer bestimmten Vulnerability beruht
CERT	Computer Emergency and Response Team
	Organsinsation (meist staatlich), die sich mit der Aufdeckung, Behebung und Dokumentation von Vulnerabilties beschäftigt

1.4 Mehrstufige Verteidigung für das IT-System

IT-Sicherheit muss bekanntlich auf allen IT-Asset-Items und allen darin implementierten OSI-Layern wirksam werden.

Das mehrstufige Konzept erhöht Wahrscheinlichkeit, dass ein Angriff entdeckt wird und vermindert die Wahrscheinlichkeit, dass ein Angriff erfolgreich ausgeführt werden kann.

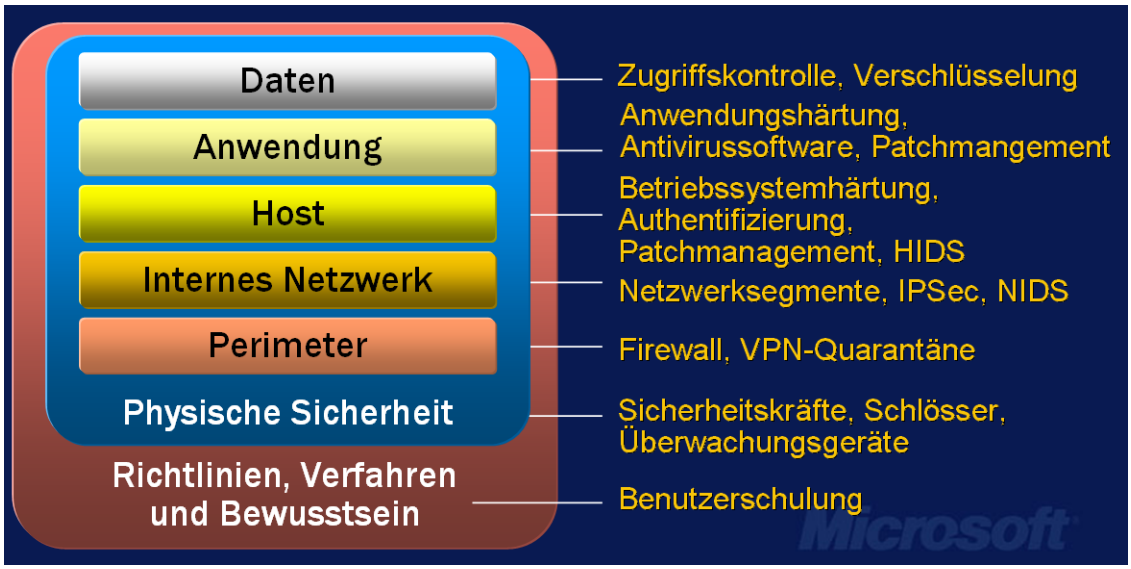


Abbildung 1: Schema Mehrstufige Verteidigung

Mehrstufe Implementierung von Sicherheitsrichtlinien (Quelle: MSFT Webcast „Grundlagen der IT-Sichereheit“)

1.4.1 ISO-OSI Layer 8“ – Der Anwender

Sicherheitsbedrohung erfolgen durch:

- mangelhaftes Sicherheitsbewusstsein (User Awareness), Methoden des „Social Engineerings“ zielen auf die Leichtgläubigkeit und Bedenkenlosigkeit der Benutzer ab (Schulung der Mitarbeiter, Überwachung)
- Regelwidriges Verhalten (z.B. Installation/ Betrieb eines Modems am Netzwerk-Arbeitsplatz)
- Sorglosigkeit im Umgang mit vertraulichen Daten (z.B. Kopien von sensiblen Daten auf Laptop) anlegen
- Opfer von ausgeklügelten Methoden (z.B. Pasword-Phishing)

Gegenmassnahmen:

- Sicherheitsschulungen
- Merkblätter oder Weisungen, die die Benutzer vor Social Engineering schützen sollen. Die Sicherheitsrichtlinien können in Form von Check-Listen, Anweisungen für bestimmte Standardabläufe oder ganze Prozessketten umfassen.
- Verwendung von zentral administrierten Client-Computern (Durchsetzen von Sicherheitsrichtlinien über Gruppenrichtlinien)
- Einsatz von Proxy-Systemen
- Überwachung der Benutzertätigkeit

1.4.2 Ebene der physischen Sicherheit

- **Gefährdung druch:**
  - Beschädigen von Hardware
  - Diebstahl von Datenträgern oder ganzen Systemen

- **Gegenmassnahmen zum Schutz der physischen Sicherheit**
  - Verschliessen von Türen, Installation von Alarmanlagen und Überwachungs-systemen
  - Beschäftigung von Sicherheitspersonal
  - Erzwingen von Zugriffsverfahren
  - Überwachen und Protokollieren des Zugangs/ Zugriffs
  - Beschränken der Zugriffsreche auf Dateieingabe- und Ausgabegeräten
  - Verwenden von anerkannten Sicherheits-Tools für den Remotezugriff zur Erhöhung der Sicherheit

1.4.3 Gefährdungen auf der Perimeter-Ebene

- **Netzwerkperimeter sind Netzwerkübergänge zu**
  - Internet und Internet-Anwendungen
  - Zweigniederlassungen
  - Geschäftspartnern
  - Remotebenutzern
  - Drahtlose Netzwerken

- **Gefährdungen auf Perimeterebene**

Eine Sicherheitslücke im Netzwerkperimeter kann zu Folgendem führen:

  - Angriff auf das Unternhmensnetzwerk
  - Angriff auf Remote-Benutzer
  - Angriff von oder auf Geschäftspartnern
  - Angriff von oder auf Zweigniederlassungen
  - Angriff auf eigene Internetdienste
  - Angriff aus dem Internet

- **Massnahmen zum Schutz der Perimeterebene**

Der Netzwerkperimeterschutz umfasst die folgenden Komponenten:

  - Firewall (Paket- und Anwendungs-Firewall)
  - Sperren von Kommunikationsanschlüssen
  - Port- und IP-Adressübersetzung
  - Virtuelle private Netzwerke (IPSec)
  - Tunnelprotokolle
  - VPN-Quarantäne
  - Sichere Netz-Zugangsverfahren einsetzen (WPA2, IEEE 802.1X mit Client- und Serverzertifikaten)

1.4.4 Ebene des internen Netzwerkes

- Gefährdung durch
  - Nicht autorisierter Zugang auf Systeme
  - Ausspionieren von Paketen im Netzwerk
  - Zugriff auf den gesamten Netzwerk-Datenverkehr
  - Nicht autorisierter Zugriff auf drahtlose Netzwerke
  - Unerwartete Kommunikationsanschlüsse

- **Massnahmen zum Schutz der Ebene des internen Netzwerkes**
  - Implementierung der gegenseitigen Authentifizierung (Kerberos)
  - Segmentierung der Netzwerke (z.B. VLAN)
  - Verschlüsselung der internen Netzwerkkommunikaiton (IPSec)
  - Sperren von Kommunikationsanschlüssen
  - Steuern des Zugriffs auf Netzwerkgeräte (Netzzugangsverfahren: z.B. WPA2, oder IEEE 802.1X z.B. über WPA2)
  - Signieren von Netzwerkpaketen

1.4.5 Hostebne

Spezifische Netzwerkfunktionen

Betriebsystemkonfiguration (Hardening: Härten des TCP/IP-Stacks)

- **Gefährdungen für die Hostebene**
  - Ungesicherte Konfiguration des Betriebssystems
  - Verteilen von Viren, Trojanern, Würmern und Rootkits
  - Nicht überwachter Zugriff
  - Ausnutzen von Schwachstellen des Betriebssystems (z.B. LM-Passwort-Hash, Ausnutzen von unsicher pogrammierten Betriebssystem-Calls für die Durchführung eines Buffer-Overflows)

- **Massnahmen zum Schutz der Hostebene**
  - Generell: Konsequentes Einhalten aller Sicherheitsrichtlinien, die zum Schutz der Host-Systeme definiert worden
  - Schutz der Hosts vor physischem Zugriff
  - Redundante Auslegung von wichtigen Hardware-Komponenten
  - Installation des Betriebssystemes und der Softwaren nur aus sicheren Quellen (Original-Datenträger oder oder Quellen deren Integrität durch Hash-Werte verifiziert werden können)
  - Schutz des Dateisystems auf Laptop-Computern durch Verschlüsselung des Datenträgers
  - Einhalten von Standards bei der Installation (Einsatz des Security Baseline Analyzer (MSBA) und des Microsoft Security Configuration Wizards)
  - Implementieren der gegenseitigen Authentifizierung (Kerberos)
  - Verzicht auf Einspeicherung von LAN-Manager Passwörtern
  - Durchsetzen einer zweckmässigen Passwort-Policy mit Gruppenrichtlinien
  - Reduzieren des Betriebsystems:
    - Entfernen von nicht benötigten Systemteilen,
    - Härten des TCP/IP-Stacks (Schutz gegen DoS-Angriffe)
  - Implementieren der Ressourcen Überwachung
  - Deaktivieren oder Entfernen unnötiger Dienste (-> deaktivieren von unnötigen LISTEN-Ports)
  - Installieren und Verwalten von Antimalware-Software (gegen Viren Würmer und Trojaner)
  - Regelmässiges Einspielen aktueller Sicherheits-Patches für Betriebssysteme, Serverdienste und Anwenderprogramme.
  - Zusammenfassung von Instrastrukturservern in speziellen Organisationseinheiten und Anwendung von dafür sppeziell ausgearbeiteten Gruppenrichtlinien (vergl. Server Sicherheits Handbuch von Microsoft)
  - Einsatz von speziell konfigurierten Host-Firewalls (-> verg. Handbuch Windows Server Security, FW-Konfigurationsdateien für bestimmte Servertypen)

- Konsequente Einhaltung des Prinzips der „niedrigst möglichen Privilegierung“ von Benutzern -> jedem Benutzer nur so viele Rechte und Berechtigungen zuweisen, wie für die Arbeit unbedingt nötig sind.
- Überwachung von wichtigen Infrastrukturservern mit spezieller Managementsoftware
- Bei Micrososoft-Systemen: Zuhilfenahme von geeigneten Security Tools:
  - (Security Update Manager, Windows Server Update Service WSUS, System Management Server 2003 Inventory Tool for Microsoft Updates (SMS-Ergänzung),
  - Microsoft Baseline Security Analyzer (MBSA 2.0), Microsoft Office Visio 2003 Connector for the Microsoft Baseline Security Analyzer;
  - Enterprise Scan Tool;
  - Microsoft Security Assessment Tool
  - Automatic Scan and Update Tools für Windows und Office
- Für Microsoft Systeme: Verwendung der “Best Practice” Anleitungen
- Absichern von speziellen Server-Typen mit geeigneten Hof-Fixes: Z.B. IIS gegen „Directory Traversal“ Techniken, die mit speziell konstruierten Unicode URL funktionieren schützen (Lockdown Tool)

1.4.6 Anwendungsebene

- Anwendungsspezifische Sicherheitsprobleme (z.B. SQL-Injection)
- Gewohnte Funktionalitäten müssen trotzt Sicherheitsoptimierungen wenn immer möglich noch erhalten bleiben.

- **Gefährdungen für die Anwendungseben**
  - Anwendung nicht mehr verfügbar
  - Ausführung von böswilligem Code
  - Übermässige Verwendung einer Anwendung
  - Unerwünschte Verwendung von Anwendungen

- **Massnahmen zum Schutz der Anwendungsebene**
  - Aktivieren nur der eforderlichen Dienste und Funktionen
  - Konfigurieren der Sicherheitseinstellungen der Anwendung
  - Installieren und Aktualisieren von Antiviren-Software
  - Einspielen von Patches für die Anwendungen
  - Ausführen der Anwendung mit dem kleinst möglichen Berechtigungsumfang

1.4.7 Datenebene

- **Gefährdung der Datenebene**
  - Unerlaubtes Anzeigen, Kopieren, Ändern oder Löschen von Informationen
  - Unerlaubtes Abfragen von Verzeichnissen

- **Massnahmen zum Schutz der Datenebene**
  - Verschlüsseln der Dateien mit EFS
  - (EFS ist eine Element der Sicherheitsrichtlinie, Prozesse müssen getestet und geschult werden, Revovery-Möglichkeiten sind nach Schlüsselverlust keine vorhanden)
  - Einschränken des Datenzugriffs mit Zugriffs-Steuerungs-Listen (Access Conrol Lists = ACL) unter Verwendung einer geeignet definierten AD-Sicherheitsgruppen-Infrastruktur)
  - Erstellen von Plänen zur Datensicherung, Vorgehensweise für Wiederherstellung testen und schriftlich festhalten
  - Schützen von Dokumentenund E-Mails-Nachrichten mit Windows Rights Management Services

1.5 Checkliste bei Sicherheitvorfällen

- **Vorgehensweise bei Sicherheitvorfällen**
  - Erkennen, dass ein Angriff stattfindet
  - Identifzieren des Angriffs
  - Melden, dass ein Angriff stattfindet
  - Eindämmen des Angriffs
  - Implementieren von vorbeugenden Massnahmen
  - Dokumentieren des Angriffs

- **Eindämmen der Folgen des Angriffs**
  - Herunterfahren der betroffenen Server
  - Entfernen der betroffenen Computer aus dem Netzwerk
  - Sperren des eingehenden und ausgehenden Netzwerkdatenverkehrs
  - Ergreifen vorbeugender Massnahmen zum Schutz von noch nicht befallenen Computern
  - Sicher der Beweise

1.6 Optimale Methoden für die Sicherheit

- Kontinuierliche Einhaltung der sicherheitsrelevanten Prozesse (Schritte 1-4)
- Mehrstufige Verteidigung
- Sicheres Design (Perimeter-Netzwerke, Segmentierung der internen Netzwerke, sichere Zugansverfahren,…)
- Niedrigste Berechtigung
- Aufrechterhalten der Sicherheitsstufen
- Sicherheitsaspekte müssen für die Benutzer im Vordergrund stehen
- Entwickeln und Testen von Plänen und Verfahren für die Vorgehensweise bei Sicherheitsvorfällen und Betriebsunterbrüchen
- Lernen aus Fehlern

1.7 Sicherheitscheckliste

- Erstellen Sie Dokumente zu Sicherheitsrichtlinien und –verfahren
- Lesen Sie Sicherheitsdokumente (z.B. Microsoft Securiy-Portal, www.heise.de, …)
- Abonnieren Sie E-Mail-Benachrichtigungen mit Sicherhetiswarnungen
- Implementieren Sie eine mehrstufige Verteidigung
- Berücksichtigen Sie für Microsoft-Systeme die „Best Practices“ für die verschiedenen Host-Typen und/ oder deren Systemteile
- Führen Sie regelmässig Sicherungs- und Wiederherstellungsprozeduren durch
- Denken Sie wie ein Hacker/ Cracker
- Testen Sie Ihre Infrastruktur mit geeigneten Testprogrammen auf Sicherheitslücken (z.B. mit Nessus Vulnerability Scanner, nmap, netcat)

2 Kryptographie

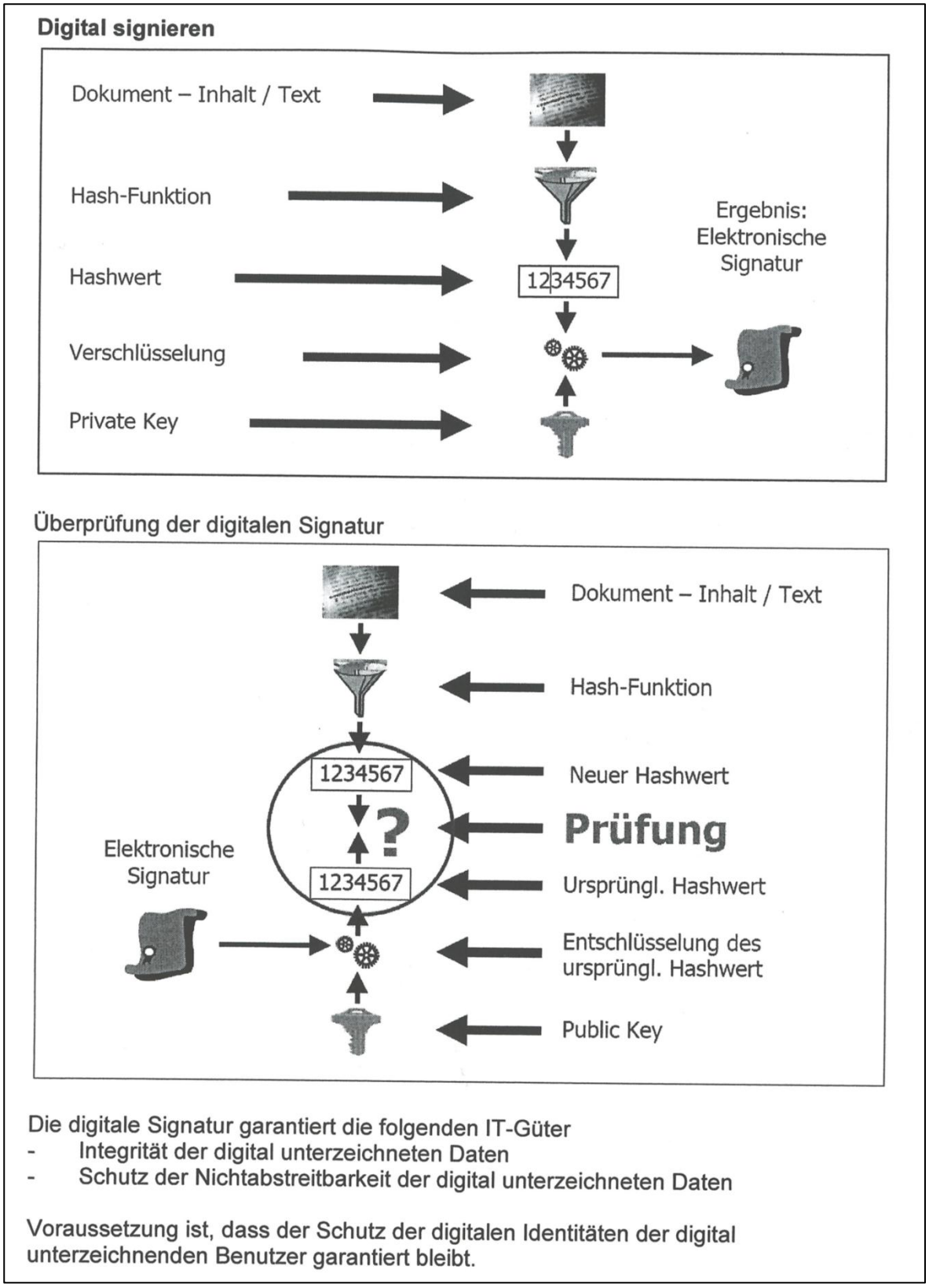


Abbildung 2: Kryptographie kompakt

2.1 Digitale Signatur

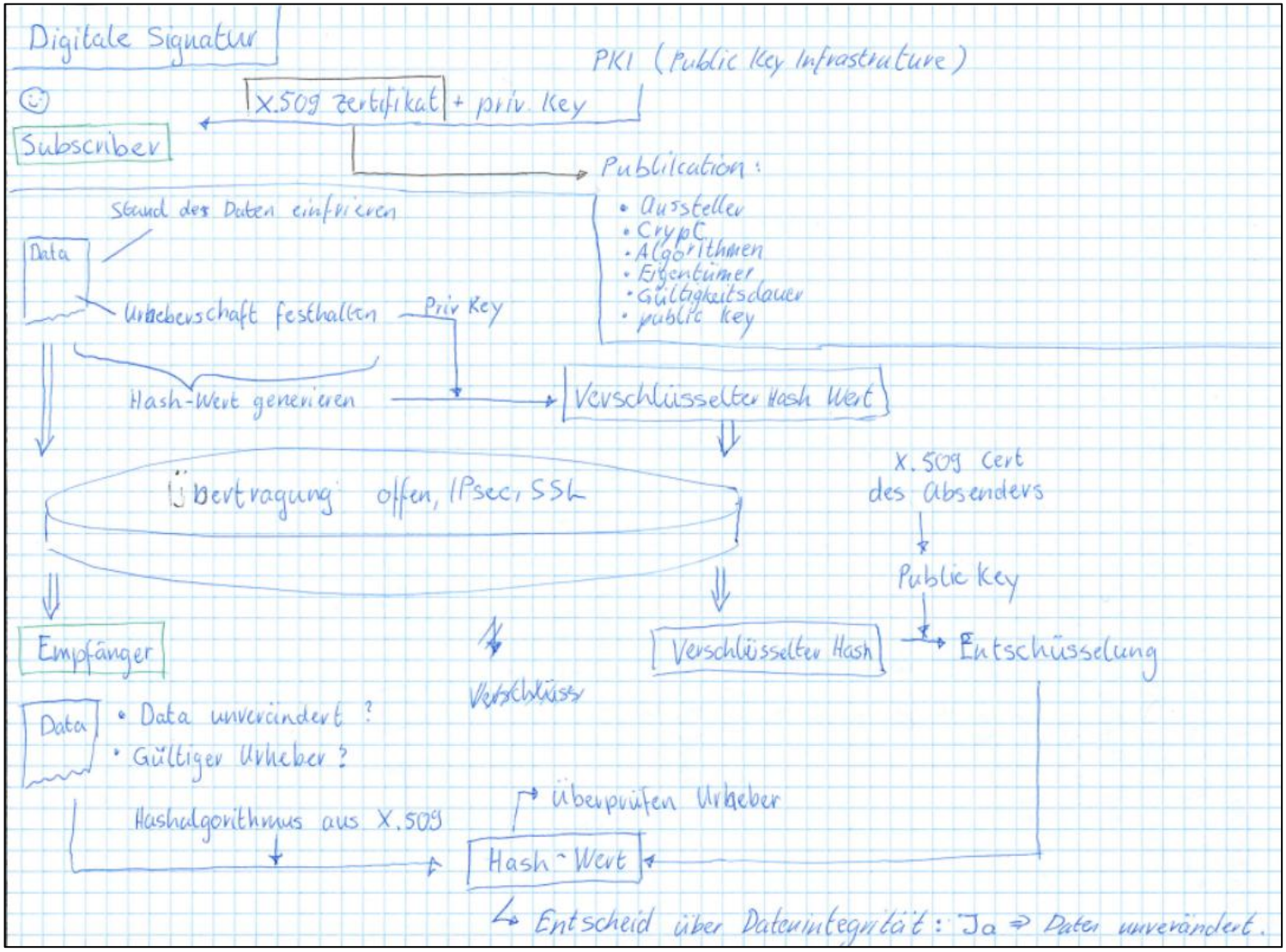


Abbildung 3: Digitale Signatur

2.1.1 Verfahren

Bei der digitalen Signatur (DSig) oder der elektronischen Unterschrift handelt sich um einen asymmetrischen elektronischen Schlüssel, die die Identität des Benutzers sicherstellt. Der Schlüssel wird mit dem privaten Schlüssel des Absenders verschlüsselt und vom Empfänger mit dem öffentlichen Schlüssel gelesen.

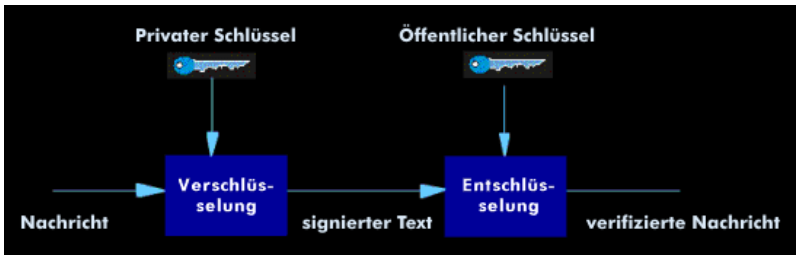


Abbildung 4: Signierung

Die digitale Signatur wird als verschlüsselte Information dem Dokument angehängt. Dieses wird dadurch so gesichert, dass Änderungen am Inhalt sofort erkannt werden. Eine weitere Forderung in Bezug auf die digitale Signatur besagt, dass der Unterzeichner eindeutig erkannt werden muss und identifizierbar ist.

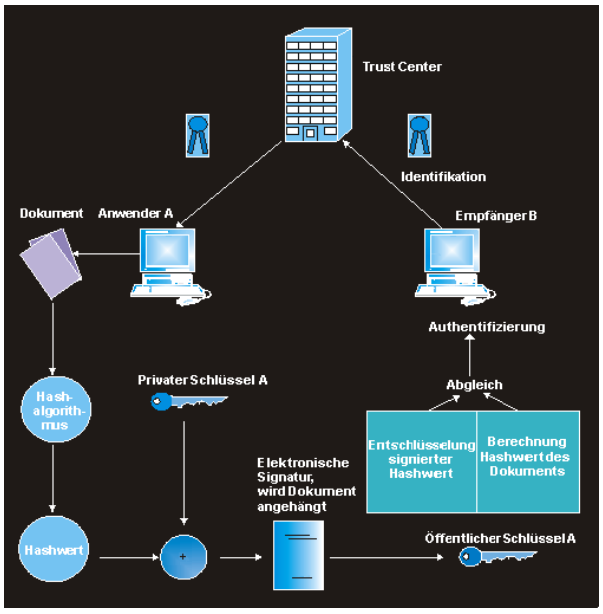


Abbildung 5: Arbeitsweise digitale Signatur

Vom Verfahren her wird für das Dokument der Hashwert ermittelt und mit dem geheimen Schlüssel des Benutzers verschlüsselt. Dieses neue verschlüsselte Dokument wird mit dem Originaldokument übertragen. Der Empfänger berechnet ebenfalls den Hashwert aus dem Originaldokument, entschlüsselt mit dem öffentlichen Schlüssel das verschlüsselte Dokument und vergleicht beide.

Die personenbezogene Zuordnung des öffentlichen Schlüssels übernimmt ein Trustcenter, das ein Zertifikat ausstellt. Der Namen des Zertifikat-Inhabers sowie dessen Zeichnungsberechtigung können im Trustcenter hinterlegt werden. Der geheime Schlüssel kann auf einer Chipkarte gespeichert und durch biometrische Daten, Passwörter u.ä. gesichert sein. Die Trustcenter haften für die Richtigkeit der Zertifikate. Die Mitgliedstaaten können den Einsatz elektronischer Signaturen im öffentlichen Bereich zusätzlichen Anforderungen unterwerfen. Sie gelten in einem Gerichtsverfahren als Beweismittel.

2.2 Public-Key-Verfahren/ Asymmetrische Verschlüsselung

Das Public-Key-Verfaren ist ein asymmetrisches Verschlüsselungsverfahren zur Verschlüsselung und Entschlüsselung von Daten. Das Public-Key-Verfahren kann zur vertraulichen Kommunikation benutzt werden, aber auch für die digitale Signatur.

Bei diesem Verfahren werden zwei verschiedene Schlüssel verwendet: Der Public Key, der öffentlich zugänglich sein kann, und der Private oder Secret Key (SK), der geheim und nur dem Inhaber bekannt ist.

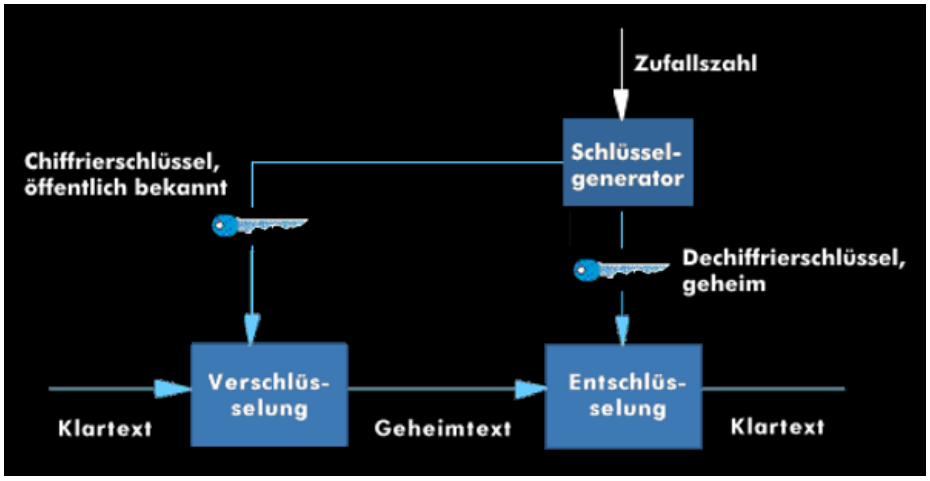


Abbildung 6:Prinzip der Asymmetischen Verschlüsselug

Da die beiden Schlüssel nicht voneinander ableitbar sind, kann ein Schlüssel öffentlich bekannt gegeben werden (Public Key). Die Verschlüsselung des Klartextes erfolgt durch den öffentlichen Schlüssel in Kombination mit einem mathematischen Algorithmus, die Entschlüsselung durch einen geheimen Secret Key.

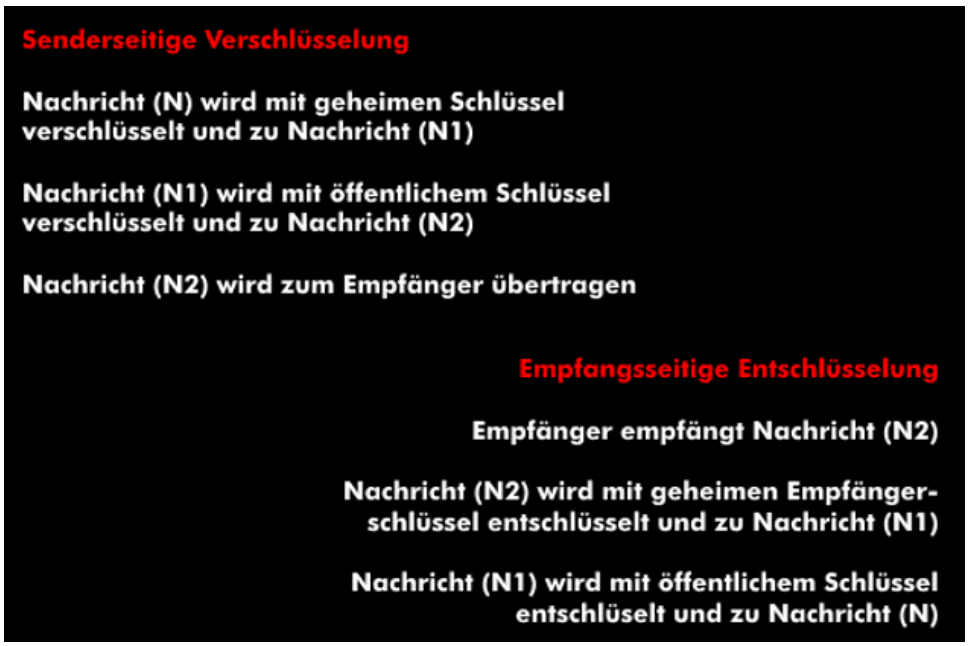


Abbildung 7: Funtionsablauf bei der Asysmmetrischen Verschlüsselung

2.3 Symmetrische Verschlüsselung

Die symmetrische Verschlüsselung kennt nur einen geheimen Schlüssel, der zur Verschlüsselung im Sender und zur Entschlüsselung im Empfänger benutzt wird. Der Sender chiffriert mit diesem Schlüssel die Nachricht, die der Empfänger mit dem gleichen Schlüssel dechiffrieren kann. Nur der Sender und der Empfänger dürfen über den geheimen Schlüssel verfügen, der vor der Kommunikation erzeugt und über einen sicheren Kanal zwischen den Kommunikationspartnern ausgetauscht werden muss. Um einen sicheren Schlüsselaustausch zu gewährleisten, dürfen nur solche Informationen übermittelt werden, aus denen keine Rückschlüsse auf den Schlüssel abgeleitet werden können. Ein solches Protokoll wird vom Diffie-Hellman-Algorithmus unterstützt.

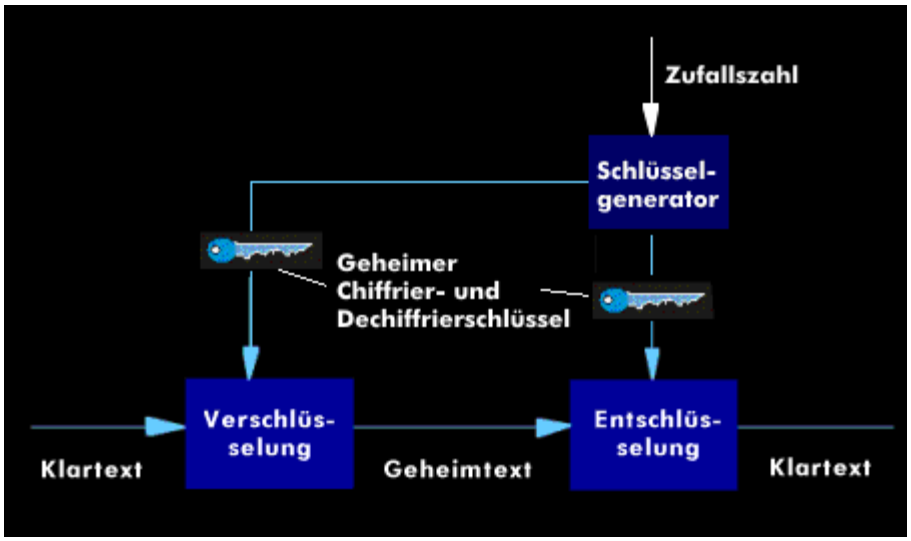


Abbildung 8: Symmetrische Verschlüsselung

Der Vorteil des symmetrischen Verschlüsselungsverfahrens ist das es sehr schnell arbeitet, nachteilig ist, dass Unbefugte, die in den Besitz des Schlüssels kommen, alle Nachrichten dechiffrieren und selber auch verschlüsselte Nachrichten herausgeben können.

3 Packet Firewalls

3.1 Packet Filter Firewalls

3.1.1 Filterbereich

- L3 – IP Protokoll
  Filter auf den folgenden Header-Feldern:
  - IP Destination Address
  - IP Source Address
  - Protocol:
    - 6: TCP
    - 7: UDP
    - 50: ESP
    - 1: ICMP
    - 41: IPv6 over IPv4
    - 4: IP in IP
  - IHL (Internet Header Length)
    Anzahl 4 Byte Blöcke im IPv4 Header:
    - 5: normal
    - >5: Optionsfeld im IPv4 Header ist besetzt => z.B. mit IP-Adressen von Routern zur Festlegung der Übertragungsweges => Potentielle Gefahr!
- L 3,5 ICMP
  Filter auf den folgenden Header Feldern:
  - Typ:
    - 8: Echo Request
    - 0 Echo Reply
    - 3 Dest
  - Code

Beispiel Schema:

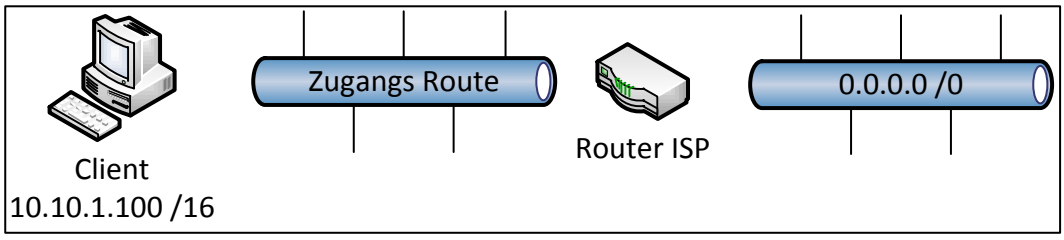


Abbildung 9: Beispiel Schema Paket Firewall

3.1.2 Vorgang:

Ursache	Wirkung			Ergebnis
CL erzeugt	**Wer erzeugt**	**Was wird erzeugt**	**Filterung auf 1 Router ISP**	**Output**
Ping www.oracle.com (ICMP Typ 8 (Echo Request)	www.oracle.com	ICMP Typ0 (Echo Reply)	Weiterleitung	Ping wird ausgeführt für e4606.b.akamaiedge.net [2.20.18.174] mit 32 Bytes Daten: Antwort von 2.20.18.174: Bytes=32 Zeit=22ms TTL=56 Antwort von 2.20.18.174: Bytes=32 Zeit=21ms TTL=56
Ping www.oracle.com -i 56 (TTL gesetzt, dass auf 1. Router ISP TTL=0	1 Router ISP	IMCP Typ11	Aussendung	Ping wird ausgeführt für e4606.b.akamaiedge.net [2.20.18.174] mit 32 Bytes Daten: Antwort von 2.20.18.174: Bytes=32 Zeit=21ms TTL=56 Antwort von 2.20.18.174: Bytes=32 Zeit=21ms TTL=56
Tracert 10.13.1.10	1. Router ISP	ICMP Typ3, code 13	Ja (keine Aussendung)	
Ping www.microsoft.com	www.microsoft.com	ICMP Typ 0	Die ICMP Typ 0 Nachricht wird schon auf www.microsoft.com gefiltert oder kann auf dem Zugangsrouter gefiltert werden.	

3.1.3 Filterbereich

- L4 TCP

  Filterung auf den folgenden Feldern:
  - Destination Port Nr.
  - Source Port Nr. der beteiligten Software Prozesse
  - SYN-Flag aus den Control Bits (z.B. kein TCP-Segment mit gesetztem SYN-Flag in das innere Netz laufen lassen)
- L4 UDP

  Filterung auf folgenden Feldern:
  - Destination Port Nr.
  - Source Port Nr.

3.2 Firewall Topologien

3.2.1 3-Port Firewall

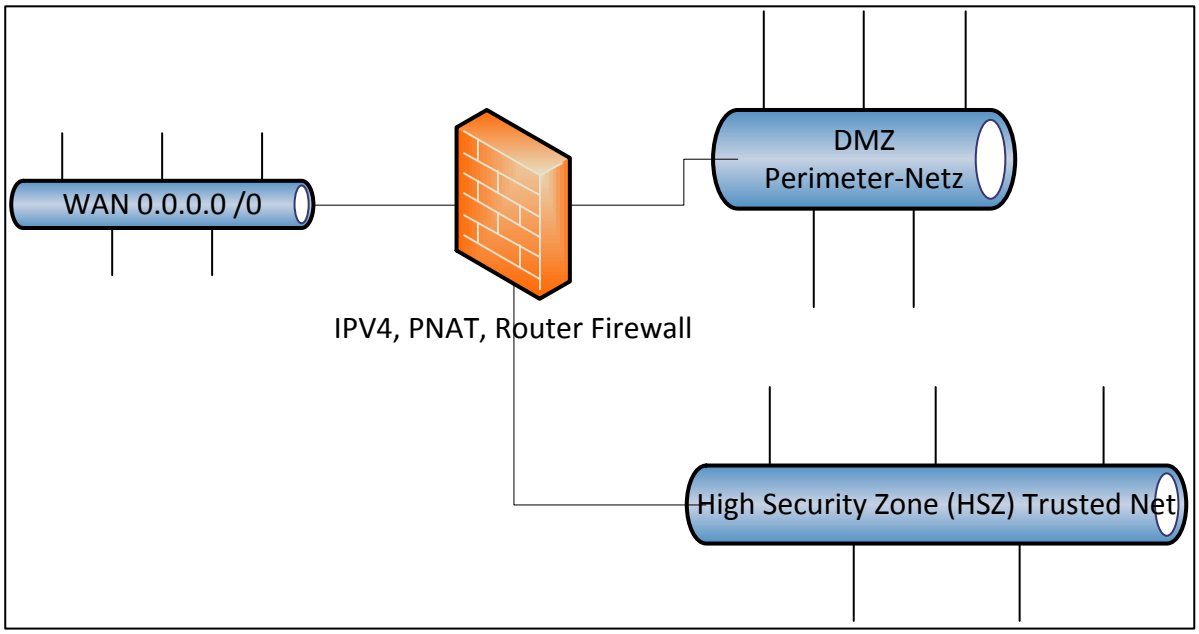


Abbildung 10: 3-Port Firewall

3.3 Screened Subnetz

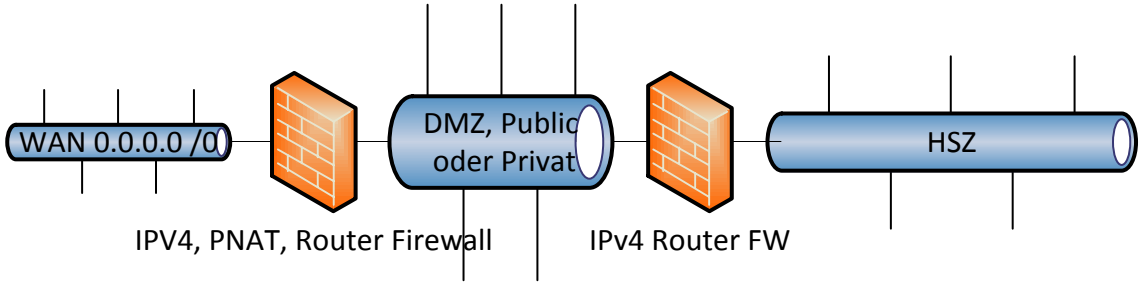


Abbildung 11: Screened Subnet

3.4 Firewall Verfahren

3.4.1 Stateless Firewall (Zustandslose Firewall)

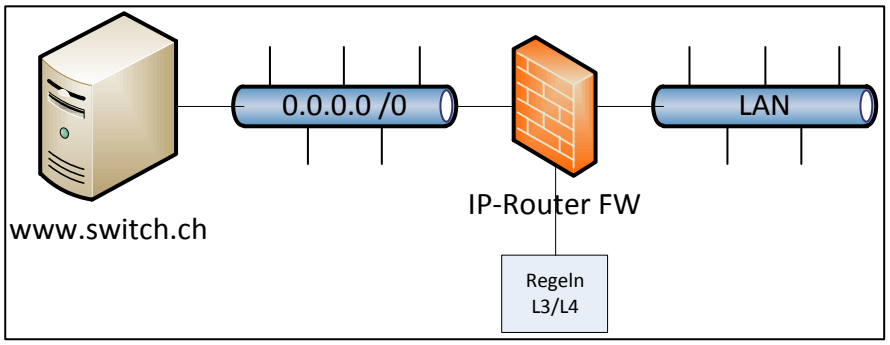


Abbildung 12: Stateless Firewall

3.4.1.1 Regeln

Nr.	Ziel (Net/Host)	Quelle (Net/Host)	Ziel Port	Quell Port	Action
0a	0.0.0.0	LAN	any	any	deny
0b	LAN	0.0.0.0	any	any	deny
1a	LAN	0.0.0.0	80 TCP	>1023 TCP	allow
1b	0.0.0.0	LAN	>1023 TCP	80 TCP	allow

3.4.1.2 Nachteile

- Doppelter Regelsatz
- WAN to LAN Regeln öffnen zu viele Ports

3.4.2 Stateful Firewall

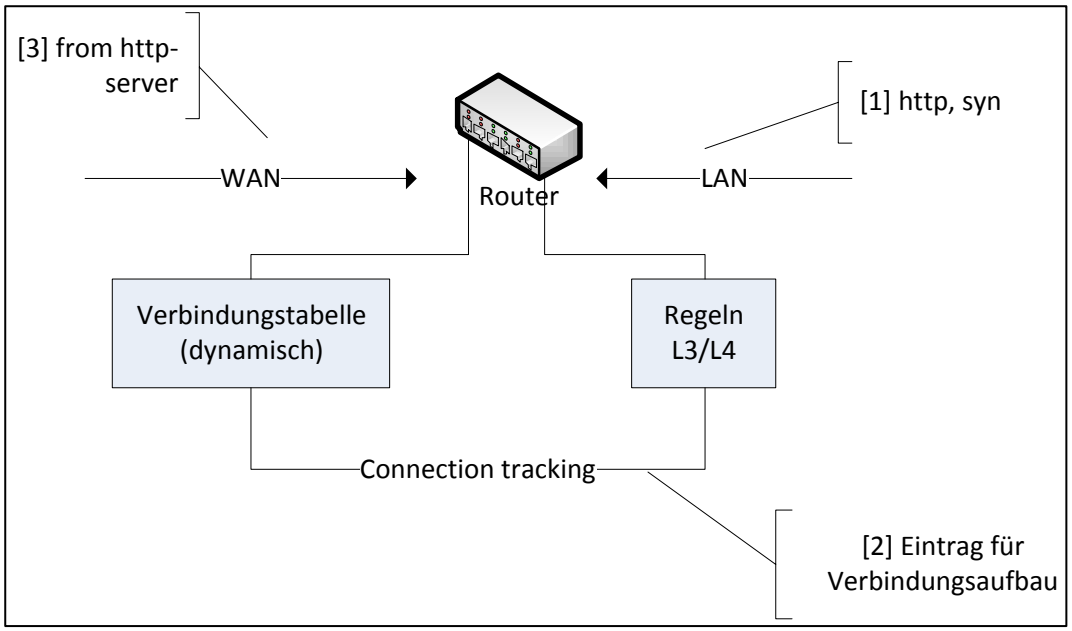


Abbildung 13: Stateful Firewall

[3] Das einlaufende Datagramm wird gemäss in der Connection Tracking Table als zu [1] zugehörige Nachricht erkannt.

3.4.2.1 Erstellung der Connection Tracking Table

tcp	Der Aufbau ist verbindungsorientiert, da TCP zustandsbehaftet
udp, icmp, esp	Zustandlose Protokolle: FW muss Verbindungszustand emulieren: IP Adr Port Nr Sequence Nr Zeitstempel

stateful FW entsprechen dem heutigen Stand der Technik

3.5 Stateful Inspection Firewall

Inspection:

- Beduetet, dass die FW bestimmte Keywords in den Nutzdaten filtern kann.
- Hauptanwendung ist FTP.

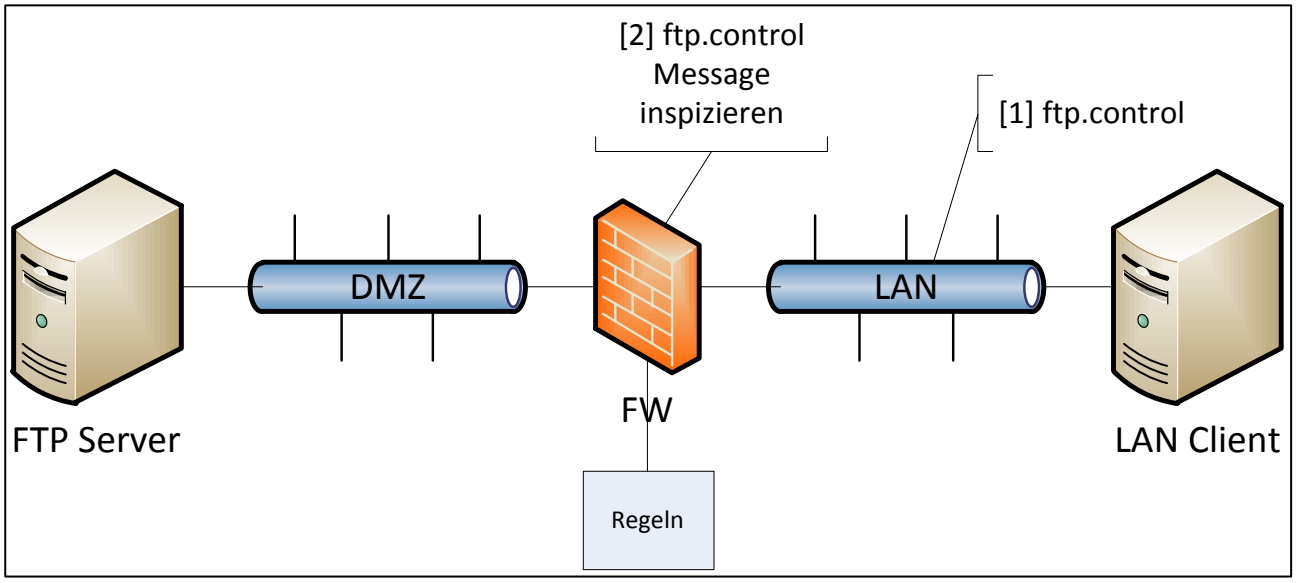


Abbildung 14: Steful Inspection Firewall

Nr	Quell (Net/Host)	Ziel (Net/Host)	Ziel Port	Quell Port	Action
x	LAN	0.0.0.0	21 (ftp.control)	>1023	Allow
keine statische ftp_data Regel vorhanden					

[1] ftp.control: Start der FTP-Session

[2] ftp.control-Message inspizieren:

- Keyword für aktiv/passiv
- Keyword für Port-Nummer des ftp_data channels

>>ftp_data-Verbindung erlauben (Eintrag in connection tracking table)

Je nach dem ob aktives oder passives FTP betrieben wird, lieg die FW-Problematik auf Server- oder Client-Seite

4 Firewall Infrastruktur planen

4.1 Vorgaben

- Öffentliches Netz 83.1.10.0 /28

4.2 Schema

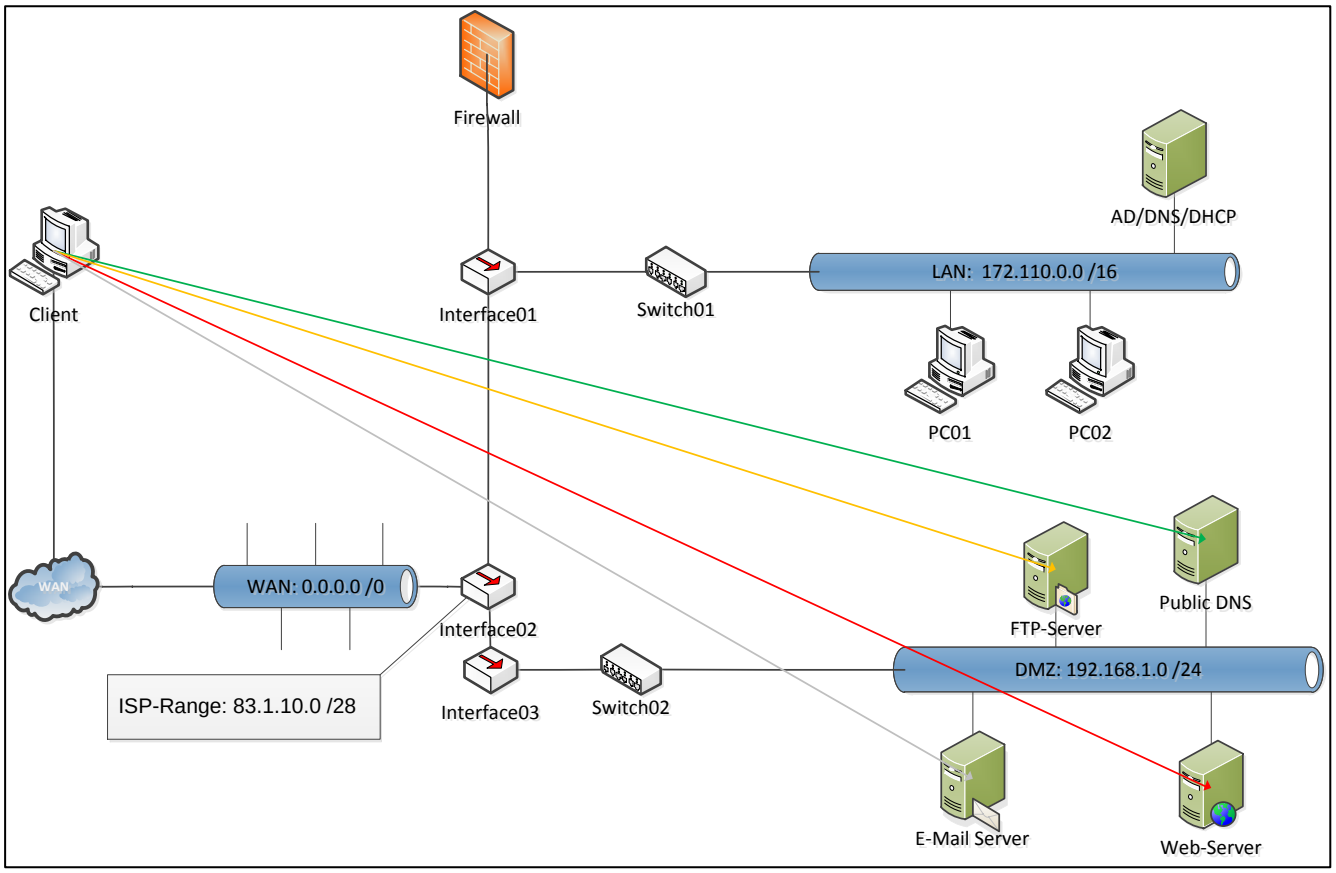


Abbildung 15: Schema Firewall Infrastruktur planen

4.3 Konfigurationen

4.3.1 IP

Device	WAN 0.0.0.0 /0	ISP-Range 83.1.10.0 /28	DMZ 192.168.1.0 /24	LAN 172.110.0.0 /16
Client	x.x.x.x			
Interface02		83.1.10.1		
Interface01				172.110.0.1
Interface03			192.168.1.1	
PC01				DHCP
PC02				DHCP
AD/DNS/DHCP				172.110.0.2
FTP-Server			192.168.1.10	
Public DNS			192.168.1.11	
E-Mail Server			192.168.1.12	
Web-Server			192.168.1.13	

4.3.2 Filtertabelle (für restriktive Firewall

Rule Nr.	Net to Net	SRC-IP-Adr	DST-IP-Adr	IP Proto-col	L4 Proto-col	SRC-Port Nr.	DST Port-Nr	Interface	Action
1	LAN-DMZ	172.168.0.0 /16	192.168.1.11 /24	17	UDP	> 1023	53 (DNS)	IE01 – IE03	Allow
2	LAN-DMZ	172.168.0.0 /16	192.168.1.10 /24	17	TCP	> 1023	21 (FTP)	IE01 – IE03	Allow
3	LAN-DMZ	172.168.0.0 /16	192.168.1.12 /24	17	TCP	> 1023	25 (SMTP)	IE01 – IE03	Allow
4	LAN-DMZ	172.168.0.0 /16	192.168.1.13 /24	17	TCP	> 1023	80 (HTTP)	IE01 – IE03	Allow
…	…	…	…	…	…	…	…	…	…
10	Any	Any	Any	Any	Any	Any	Any	Any	Drop

4.3.3 Port-Forwarding

Beinhaltet folgende Services (WAN to DMZ):

Service	Zielport im einlaufenden TCP/ UDP Segment	Forwarding IP-Adr	Forwarding TCP Port	Forwarding UDP Port
http	80	192.168.1.13	80	
smtp	25	192.168.1.12	25	
dns	53	192.168.1.11		53
ftp	21	192.168.1.10	21	

5 Aktive FTP und FW-Regeln

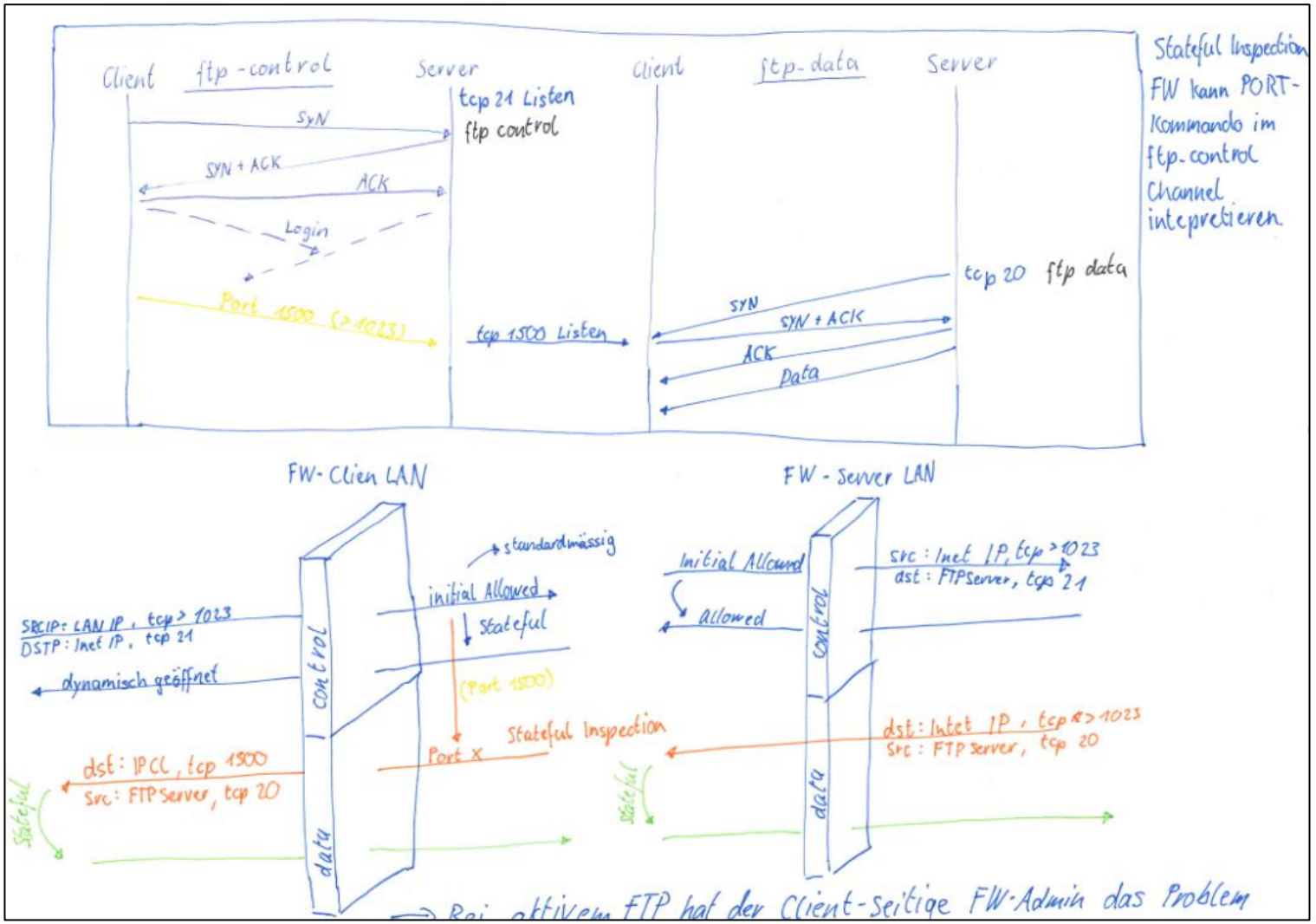


Abbildung 16: Aktives FTP

6 Passives FTP und FW Regeln

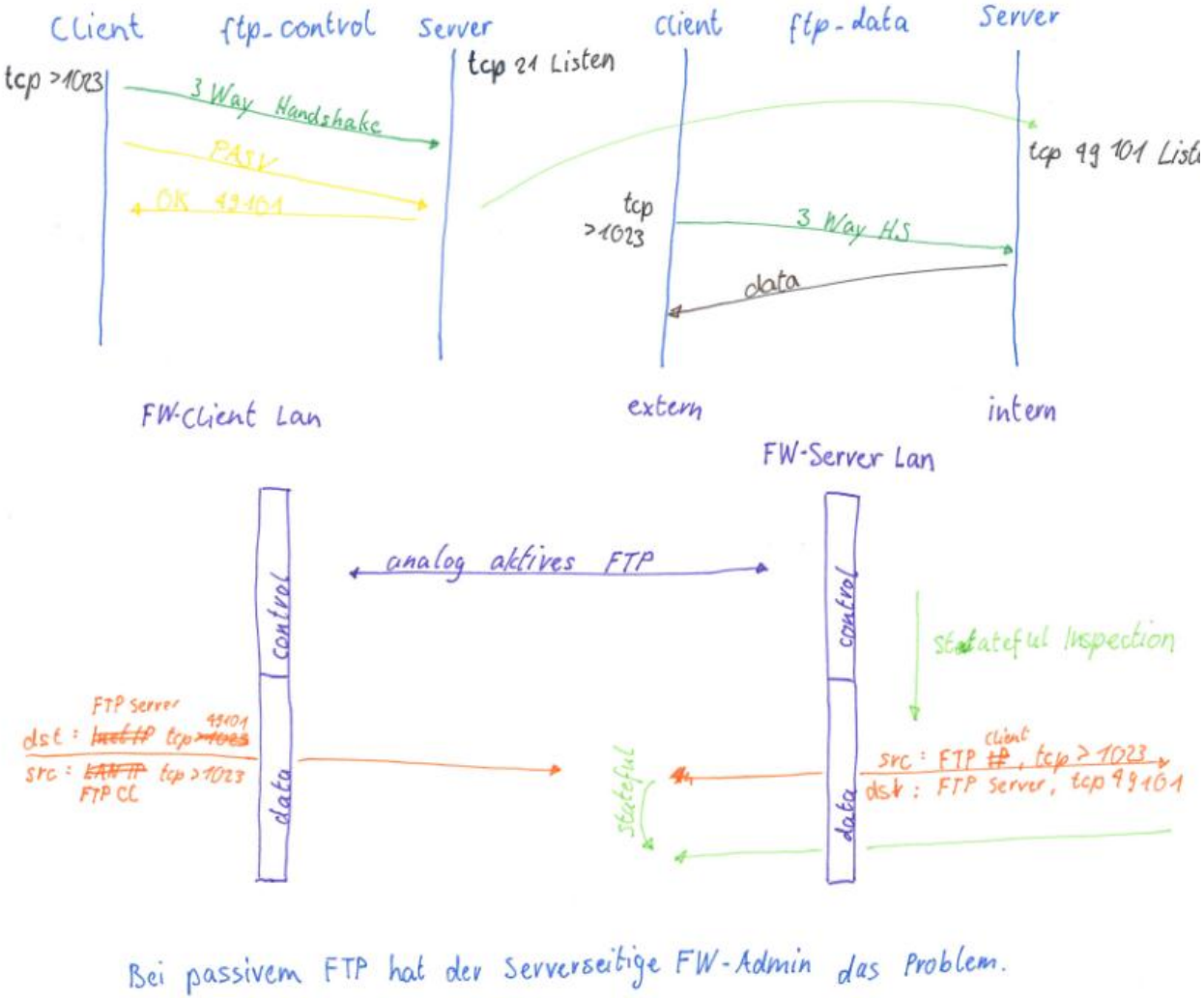


Abbildung 17: Passives FTP

7 IDS (Intusion Detection System)

7.1 Fragen und Antworten

7.1.1 Zweck der Intrusion Detection Systems?

Welchen Zweck verfolgen die IDS?

Ein Intrusion Detection System (IDS) bzw. Angrifferkennungssystem ist ein System zur Erkennung von Angriffen, die gegen ein Computersystem oder Computernetz gerichtet sind.

7.1.2 Typen von Intrusion Detection Systems

IDS werden in zwei unterschiedlichen Architekturen angeboten, die sich hinsichtlich des Bereiches, für den ein IDS zuständig ist, unterscheiden. Wie heissen die beiden Architekturtypen?

- Host-Basierte IDS
- Netzwerk-Basierte IDS
-

7.1.3 Host-basierte IDS

Fassen Sie den Aufgabenbereich und die Funktionen der Host-basierten IDS kurz zusammen und notieren Sie je einen Vor- und einen Nachteil dieser Systemarchitektur!

HIDS werden aus Hosts installiert. Sie ergänzen das Betriebssystem in der Erkennung von Angriffen. Dazu werden Log-Dateien des Betriebssystems ausgewertet.

Vorteile:

- Sehr spezifische Aussagen über den Angriff.
- Kann ein System umfassend überwachen.

Nachteile:

- Kann durch einen DoS-Angriff ausgehebelt werden.
- Wenn das System außer Gefecht gesetzt wurde, ist auch das IDS lahmgelegt.

7.1.4 Netzwerk-basierte IDS

Fassen Sie den Aufgabenbereich und die Funktionen der Netzwerk-basierten IDS kurz zusammen und notieren Sie je einen Vor- und einen Nachteil dieser Systemarchitektur!

Vorteile:

- Ein Sensor kann ein ganzes Netz überwachen.
- Durch Ausschalten eines Zielsystems ist die Funktion des Sensors nicht gefährdet.

Nachteile:

- Keine lückenlose Überwachung bei Überlastung der Bandbreite des IDS.

- Keine lückenlose Überwachung in geswitchten Netzwerken (nur durch Mirror-Port auf einem Switch).

7.1.5 Funktionsweise von IDS

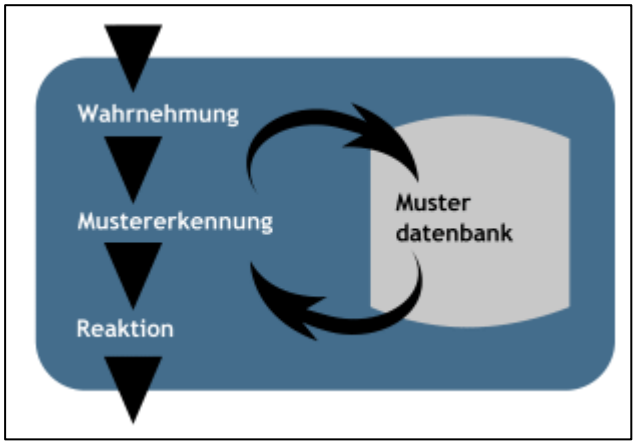
Der Bau eines IDS ist eine äusserst komplexe Herausforderung für die Netzwerktechniker und Software-Entwickler. Oft weichen die tatsächlichen Leistungen eines IDS stark von jenen, die in den Prospekten versprochen werden, ab.

Ein grosses Problem beim Betrieb von IDS sind die "Falschmeldungen". Die Falschmeldungen können unterschiedlicher Natur sein und werden in der Fachsprache wie folgt bezeichnet:

Bezeichnung	Bedeutung
falsch positiv / false positive	Ein IP-Datagramm wird fälschlicherweise vom IDS als positiv getestet. (im IP-Datagramm wurde ein bestimmtes Angriffsmuster festgestellt). Vereinfacht gesagt: „Falscher Alarm“
falsch negativ / false negative	Ein Angriffsmuster in einem IP-Datagramm wird fälschlicherweise nicht erkannt. Vereinfacht gesagt: „Fälschlicherweise wurde kein Alarm ausgegeben“.

7.1.6 Funktionsweise der IDS

Obwohl die IDS überaus komplexe Aufgaben erfüllen müssen, lässt sich dennoch ein recht übersichtliches Funktionsprinzip der IDS beschreiben. Zeichnen und beschriften Sie ein Diagramm, aus dem hervorgeht, wie ein IDS grundsätzlich funktioniert, bzw. funktionieren sollte!



Der komplette Prozess unterteilt sich dabei in drei Schritte:

7. Die Wahrnehmung eines IDS wird durch Sensoren ermöglicht, die Logdaten (HIDS) oder Daten des Netzwerkverkehrs (NIDS) sammeln.
8. Während der Mustererkennung überprüft und verarbeitet das Intrusion Detection System die gesammelten Daten und vergleicht sie mit Signaturen aus der Musterdatenbank.

   Treffen Ereignisse auf eines der Muster zu, so wird ein „Intrusion Alert“ (Einbruchs-Alarm) ausgelöst.

7.1.7 IDS Software

Ein theoretisches Funktionsprinzip hat natürlich keinen grossen Wert, wenn es keine Softwaren gibt, die das Prinzip auch wirklich implementiert haben. Suchen Sie Softwareprodukte, die sich als HIDS oder NIDS eigenen. Erstellen Sie eine Tabelle, die etwa die folgenden Attribute aufweist:
Hersteller, Produktbezeichnung, Einsatz als HIDS oder NIDS, dediziertes Gerät oder reine Software-Lösung,Produkt ist kommerziell oder open Source, versprochene Leistungen (Stichworte).

IDS Systeme werden von verschiedenen Herstellern von Netzwerkgeräten angeboten.

Ein wichtiges, reines Software IDS-Produkt ist „Snort“. Snort ist eine OSS.

- **Snort** ist ein freies Netzwerk-IDS für Unix/Linux-, Mac OS X- und Windows-Systeme. Snort kann mittels diverser Module zur Auswertung der Daten (bsp. ACID) oder Module zur Intrusion Prevention (bsp. SnortSAM) aufgewertet werden.
- **Samhain** ist ein Host-basierendes System, das auf vielen Plattformen läuft. Viele Linux-Distributionen enthalten bereits vorgefertigte Pakete dieser Software. Durch kryptographische Signaturen können Verfälschungen an Konfigurations-Dateien und der Kommunikation über Netzwerk aufgedeckt werden.
- **Prelude** als hybrides IDS, welches diverse andere Programmpakete (Snort, Samhain u. a.) integriert, steht ebenso für die Plattformen Linux, BSD, Solaris und OSX zur Verfügung (auch für unterschiedliche Architekturen wie x86, PowerPC, SPARC usw.).
- **Projekt Hogwash**. Dieses IDS arbeitet auf Layer 2 und bindet sich somit mit keiner IP-Adresse an angeschlossene Netzwerke. Es wird dadurch schwerer angreifbar und ermöglicht es, ohne aufwendige Konfiguration der beidseitig angeschlossenen Systeme eingesetzt zu werden.
- **Xray IDS** ist ein auf Windows ausgelegtes Host-IDS. Es ist das erste System, das speziell für Windows entwickelt wurde.

7.1.8 Abgrenzung gegenüber Honeypots

Was ist ein Honeypot?

- Ein Honeypot ist ein Computer im Netzwerk, der Hacker verleiten soll genau diesen anzugreifen.
- Auf diesem Computer befinden sich weder wichtige Daten noch Dienste, die regulär genutzt werden.
- Er dient lediglich dazu, die Angriffe auf einen isolierten Teil des Netzwerkes zu lenken, indem bewusst Sicherheitslöcher geöffnet bleiben.

7.1.9 In welcher Beziehung stehen IDS zu Honeypots?

Der Honeypot ist damit ein weiterer Bestandteil des IDS. Das Konzept des Honeypots hat allerdings einen entscheidenden Nachteil: Er kann als Einsprungpunkt für den Hacker dienen, von dem aus weitere Angriffe auf das Netzwerk gestartet werden.

Ein IDS soll dem Angreifer verborgen bleiben. Es soll von den Angreifern unerkannt, deren Angriffe registrieren, protokollieren und möglichst aus klassifizieren können. Zudem sollen die zuständigen Administratoren über die Angriffe orientiert werden,

Ein Honeypot soll sich dem Hacker als mögliches Angriffziel präsentieren. Die Betreiber der Honeypots sollen dadurch die Möglichkeit erhalten die Angriffsmuster studieren zu können, um noch bessere Abwehrsysteme (Firewalls, IDS) konstruieren zu können.

7.1.10 Einsatz-Szenarien für NIDS

Notieren Sie, für welche Systemumgebungen der Einsatz von NIDS speziell empfehlenswert ist!

Das wichtigste Einsatzgebiet von NIDS sind die Perimeter-Netzwerke (Übergangsnetzwerke, DMZ). Hier sind Angriffe aus dem Internet besonders häufig zu registrieren.

7.1.11 Einsatz-Szenarien für HIDS

Notieren Sie, für welche Host-Typen der Einsatz von HIDS besonders empfehlenswert ist!

Serversysteme, die typischerweise häufig Angriffen ausgesetzt sind: Alle Arten von Internetdienst-Server (http, https, smtp, pop3, imap, ftp, dns)

8 ISAKMP

IP	UDP srcP: 500 dstP:500	IKEv1V4 Mai

A) Proposal
   a. Proposal Daten
      i. HASH-Algor
      ii. ESP Krypot
   b. Länge des DH-Vorschlüssel
   c. Auth-Verfahren Tunnel End Point
      i. PSK
      ii. Kerberos
      iii. Zertifikate X.509
B) Proposal-Entscheid (Vorschlag)
C) DH Key Erstellen →
D) DH Key Erst. ←
E) X.509 Zert. signiert →
F) X.509 Zert. signiert ←

IP src IP: TEP A dst: TEP B Protocol: 50	ESP Header	Encrypted Data IP: Cl ←→ Cl Mai

Begriff	**Bezeichnung**
TEP	Tunnel-End-Point
Cl	Client
PSK	Preshared Key
DH	Diffie Hellmann
Zert.	Zertifikat
ESP	Encapsulating Security Payload

9 Beispiel IT-Security Management Laptop-Computer

9.1 Einleitung

9.2 Zweck des Dokumentes

In diesem Dokument beinhaltet IT-Asset, Bedrohungsanalyse und Sicherheitsrichtlinien für Laptop-Computer der Firma Versicherung AG.

9.2.1.1 Referenzierte Dokumente

[1] Generelle Richtlinien zum IT-Security Management der Versichrung AG

9.3 Allgemeiner Rahmen

Die Firma Versicherung AG bietet Consulting und Lösungen für Versicherungen von Firmenkunden an. Die Versichrung AG ist in der ganzen Schweiz tätig und unterhält Niederlassungen in Zürich, Luzern, Bern und Lausanne.

Die Versicherung AG beschäftigt 30 Mitarbeiterinnen und Mitarbeiter im Aussendienst. Diese Mitarbeiter beraten Firmenkunden umfasend vor Ort und benötigen daher Online-Zugriff auf zentral gespeicherte Daten.

9.4 Einsatz der Laptop-Computer

Der Laptop-Computer ist das wichtigste Arbeitsmittel für den Aussendienst. Damit haben die Mitarbeiter Zugriff auf

- - zentral gespeicherte Daten
- - lokal gespeicherte Daten
- - firmenspezifische Anwendungen für die Beratung und die Offertierung

Im Innendienst-Einsatz sind die Laptops mit dem Firmennetzwerkk über Ethernet verbunden.

Im Aussendienst-Einsatz erfolgt die Verbindung über das eingebaute WWLAN-Modul / 3G-Modul. Die Datenübertragung wird mit IPSec verschlüsselt.

Im Aussendienst-Einsatz wird das lokal gespeicherte Benutzerprofil verwendet

9.5 Beschreibung der Latptop-Hardware

- DualCore Prozessoren, die Harware Virtualisierung erfmöglichen
- 4 GB RAM
- 1000 GB Harddisk
- DVD Laufwerk
- Ethernet-, WLAN-, und WWLAN-Schnittstelle
- 6 USB Ports

9.6 Einbezug der generellen IT-Security Richtlinien

Gemäss [1] sind die folgenden generellen Sicherheitsrichtlinien explizit in die Sicherheitsrichtlinien für Laptop-Computer zu integrieren:

- BIOS muss durch Kennwort geschützt sein
- Hardware Virtualisierungstechnologie muss deaktiviert sein
- Benutzerkonten müssen durch Kennwortrichtlinien (auch für lokalte Konten) geschützt sein
- Für den Zugriff auf Ressourcen muss das Prinzip „Nur so viel Zugriffsberechtigung erteilen, wie für die Arbeit erforderlich ist“
- Daten müssen bei Einspeicherung und Übertragung ausreichend geschützt sein
- Das Betriebssystem und die Anwendungen müssen durch regelmässiges Updaten auf dem neusten Stand gehalten werden
- Die Konnektivität muss durch angepasste Filterregeln mit Host-Firewall geschützt sein

9.7 IT-Asset, Bedrohungs-Analyse

Komponenten-/ Item-Nr	Komponenten- / Item-Bezeichnung	Bedrohung Nr.	Bedrohungsanalyse	Verweis auf Sicherheitsrichtlinie
1	**Hardware Laptop-Computer**			
1.1	BIOS	1.1.1	Neuinstallation des Computers mit Boot-Medium	1.2 BIOS-Boot-Diable
		1.1.2	Ändern der Bios-Settings	1.1 BIOS-Schutz
		1.1.3	Installation einer VM auf dem Host-Computer	1.3 BIOS-Settings-Virtualisation
1.2	Festplatte	1.2.1	Festplatte nach Entsorgung auslesen	1.4 Festplatte-Verschlüsseln
		1.2.2	Festplatte wird nicht korrekt entsorgt	1.5 Festplatten-Entsorgung
		1.2.3	Daten auf formatierter Festplatte sind nach aufwändigem Recovery wieder verwendbar.	1.6 Festplatten-Formatierung
		1.2.4	Auf der Festplatte schleust sich einer tojanische VM ein.	1.3 BIOS-Settings-Virtualisation
2	**Lokalgespeicherte Geschäftsdaten**	2.1.1	Geschäftsdaten geraten unverschlüsselt in falsche Hände.	2.1 Vertrauliche Geschäftsdaten
3	**lokal gespeicherte firmenspezifische Anwendungen**	3.1.1	Eine Firmenanwendung ist ohne Benutzer und Passwort zugänglich.	3.1 Zugang Firmenanwendung
4	**Internetverbindung über WWLAN**	4.1.1	Vertrauliche Daten werden über ein unsichers Netz versendet	4.1 Senden vertrauliche Daten
		4.1.2	Firmendaten werden unverschlüsselt an die Firma gesendet.	4.2 Verschlüsselte Datenübertragung Firma

5	**lokales Administratoren-Konto**			
5.1	Benutzername	5.1.1	Der Benutzername des Administrators wurde nicht geändert und ist somit die erste Auswahl bei einer Brute-Force Attacke.	5.1 Adminstrator Benutzername
5.2	Passwort	5.1.2	Das Passwort wird gecrackt.	5.2 Sicheres Admin Passwort
6	**lokales Benutzerkonto und Benutzer**			
	Private Daten	6.1.1	Der Benutzer speichert persönliche Daten auf einem ungeschützten Ordner.	7.2 Lokale Berechtigungen
	Passwort		Das Passwort wird gecrackt.	6.1 Sichers Benutzer Passwort
7	**Windows OS**			
7.1	Windows OS Security	7.1.1	Für das Windows existiert ein Exploit mithilfe dessen sich der Laptop kompromittieren lässt.	7.3 Windows Updates
		7.1.2	Das OS ist mit Malware jeglicher Art infiziert.	7.5 Antivirus
8	**Lokale Firewall**	8.1.1	Die Firewall wurde schlecht konfiguriert und es sind viele ungenutzte Ports offen.	8.1 Allgemeine FW-Regeln
		8.1.2	Der User schaltet die Firewall aus.	8.2 Ausschalten lokale FW
9	**Anwender**			
9.1	Daten	9.1.1	Der Benutzer arbeitet mit vertraulichen Daten in der Öffentlichkeit.	9.1 Korrekte Bedienung
		9.1.1	Benutzer schreibt Passwort auf Notizzettel	9.1 Korrekte Bedienung
9.2	Computerverwendung	9.2.1	Computer ist ungesperrt einer Drittperson zugänglich	7.4 Computer-Sperre
		9.2.2	Computer wird einer Drittperson ausgeliehen	9.1 Korrekte Bedienung

9.8 Sicherheitsrichtlinien

9.8.1 Sicherheitsrichtlinien für Hardware Laptop-Computer

Nr	Sicherheitsrichtlinie	
1.1	BIOS-Schutz	BIOS muss durch Kennwort geschützt sein
1.2	BIOS-Boot-Disable	Es darf nicht von Medien wie anderen Festplatten, USB-Sticks oder CDs gebootet werden.
1.3	BIOS-Settings-Virtualisation	Hardware Virturalisierungstechnologie muss deaktiviert sein
1.4	Festplatte-Verschlüsseln	Festplatte muss mit Bit-Locker (http://windows.microsoft.com/de-CH/windows7/products/features/bitlocker) verschlüsselt werden.
1.5	Festplatten-Entsorgung	Festplatte wird, sofern diese nicht wiederverwendet wird zertrümmert.
1.6	Festplatten-Formatierung	Die Festplatte, sofern wiederverwendet, wird mit einem zertifizierten Wipe-Tool vor der Neuverwendung gelöscht.

9.8.2 Sicherheitsrichtlinien für Lokal gespeicherte Geschäftsdaten

Nr	Sicherheitsrichtlinie	
2.1	Vertrauliche Geschäftsdaten	Vertrauliche Geschäftsdaten werden mit dem Tool AxCrypt (http://www.axantum.com/axcrypt/) verschlüsselt.

9.8.3 Sicherheitsrichtlinien für lokal gespeicherte firmenspezifische Anwendungen

Nr	Sicherheitsrichtlinie	
3.1	Zugang Firmenanwendung	Jede Firmenanwendung, die auf einem Laptop installiert wird, darf nur mit einem Benutzer und Passwort zugänglich sein.

9.8.4 Sicherheitsrichtlinien für Internetverbindung über WWLAN

Nr	Sicherheitsrichtlinie	
4.1	Senden vertrauliche Daten	Daten müssen bei Einspeicherung und Übertragung ausreichend geschützt sein
4.2	Verschlüsselte Datenübertragung Firma	Die Datenübertragung zur Firma findet auf verschlüsseltem Weg über einen Site to End IPsec Tunnel statt.

9.8.5 Sicherheitsrichtlinien für lokales Administratoren-Konto

Nr	Sicherheitsrichtlinie	
5.1	Adminstrator Benutzername	Der Administrator Benutzername darf nicht „Administrator“ laufen, da dieser zu bekannt für Brute-Force attacken ist.
5.2	Sicheres Admin Passwort	Das Admin Passwort besteht aus mind. 16 Alphanummerischen- und 4 Sonder-zeichen

9.8.6 Sicherheitsrichtlinien für lokales Benutzerkonto und Benutzer

Nr	Sicherheitsrichtlinie	
6.1	Sicheres Benutzer Passwort	Das Passwort des Benutzers besteht aus mindestens 8 alphanummerischen Zeichen.

9.8.7 Sicherheitsrichtlinien für Windows OS

Nr	Sicherheitsrichtlinie	
7.1	Benutzer Kennwortschutz	Benutzerkonten müssen durch Kennwortrichtlinien (auch für lokalte Konten) geschützt sein
7.2	Lokale Berechtigungen	Für den Zugriff auf Ressourcen muss das Prinzip „Nur so viel Zugriffsberechting erteilen, wie für die Arbeit erforderlch ist“
7.3	Windows Updates	Das Betriebssystem und die Anwendungen müssen durch regelmässiges Updaten auf dem neusten Stand gehalten werden
7.4	Computer-Sperre	Der Computer wird bei nichtverwendung nach 1. Minute gesperrt.
7.5	Antivirus	Jeder Laptop enthält eine Antiviren Software der Avira Antivirus Premium Edition.

9.8.8 Sicherheitsrichtlinien für lokale Firewall

Nr	Sicherheitsrichtlinie	
8.1	Allgemeine FW-Regeln	Die Konnektivität muss duch angepasste Filterregeln mit Host-Firewall geschützt sein
8.2	Ausschalten lokale FW	Der lokale FW-Service darf nicht durch den User ausgeschaltet werden können.

9.8.9 Sicherheitsrichtlinien für Anwender

Nr	Sicherheitsrichtlinie	
9.1	Korrekte Bedienung	Anwender vorgängig für die Verwendung des Computers geschult und sensibilisiert.

10 Zusammenfassung

10.1 Die abstrakten IT-Güter

	IT-Gut	Geeignete Technologie/ Massnahme	Das IT-Gut kann bedroht werden durch …
DATEN	Vertraulichkeit der Daten (Unberechtigte können die Daten nicht sinnbezogen lesen)	Verschlüsselte Datenübertragung in authentifizierten, verschlüsselten Tunnel (IPSec)	Netztraffic capturen, z.B. auf Routern im Internet Man in the middle Angriffe
		Datenträgerverschlüsselung für mobile Datenträger (z.B. USB-Drives und Laptops)	Diebstahl iund Verlust von Datenträger
		Zugriffssteuerung (Sicherheits-Gruppen und DACLs)	Unzweckmässig festgelegte Zugriffslisten, Identitätsklau
	Integrität der Daten (Daten können nicht verändert werden ohne dass dies vom Eigentümer bemerkt wird. Der Eigentümer ist imstande das Original wieder herzustellen.)	VPN (z.B. IPSec) Hashbildung auf Dateien (z.B. bei digital signierten Emails	Man in the Middle Angriffe
		Redundante Datenträgersysteme (RAID)	Verlust von eingespeicherten Daten und Backupdaten
		Backup- und Einlagerungskonzept Regelmässige Restore-Tests	Verlust der Restore-Möglichkeit entstanden durch Inkompatibilitäten (HW, SW)

	IT-Gut	Geeignete Technologie/ Massnahme	Das IT-Gut kann bedroht werden durch …
SYSTEME	Verfügbarkeit der Systeme (Unberechtigte sollen nicht in der Lage sein, die Verfügbarkeit der Systeme massgeblich zu stören) Unterbrüche durch technische Ausfälle, Naturereignisse	OS Hardening gegen SYN-Flood Angriffe Netz-IDS zur Auswertung von Angriffen (= DoS-Angriff) Redundante Auslegung von wichtigen Systemeinheiten, Servervirtualisierung (z.B. für schnellere Wiederherstellung von wichtigen Systemen) Passwortrichtlinien um Identitätsklauf mit zerstörerischer Absicht, zu verhindern Einsatz von Anti-Malware Software OS und Anwendungen regelmässig updaten	(D)DoS-Angriffe: SYN-Flood Angriffe gegen TCP Ports im LISTEN Zustand Technische Ausfälle von Systemteilen Naturereignisse Identitätsklau von administrativen Konten Ausnutzen von Schwachstellen bei OS oder Anwendungssoftwaren
	Missbräuchliche Verwendung der Systeme (Unberechtigte sollen nicht in der Lage sein, Systemressourcen für ihre Zwecke zu nutzen)	Host IDS und Netz IDS einsetzen und dereln Fehlermeldungen auswerten Logs von Zugangsprotokollen auswerten Server-Dienste sachgemäss konfigurieren (Ereignisprotokoll Einsatz von Anti-Malware Software Betriebssystem und Anwendungen regelmässig updaten	Missbräuchliche Verwendung von Systemen (auch Netzwerk-Ressourcen oder Netzwerzugängen) augrund von ungenügend geschützten Zugängen Missbräuchliche Verwendung von Serverdiensten (z.B. Email-Weiterleitung für Spamer) aufgrund von unsachgemäss konfigurierten Server- anwendungen (z.B. SMTP-Relaying) oder nach erfolgtem Identitätsklau für Serverzugänge Einsatz von Malware, um Systeme für (D)DoS-Angriffe ohne Wissen des Betreibers zu nutzen

	IT-Gut	Geeignete Technologie/ Massnahme	Das IT-Gut kann bedroht werden durch …
BENUTZER	Digitale Integrität der Benutzer (Niemand soll sich in IT-Systemen als andere Person ausgeben können oder an Stelle einer anderen Person handeln können)	Passwortrichtlinien um den Aufwand von Brute Force Angriffen zu erhöhen (der aufwand steigt exponential, nicht nur linear mit der Länge des Passwortes Verwendung von sicheren Authentifizierungsverfahren (Kerberos, iEEE 802.1X, CHAP bei PPP, X.509 Zertifikate für IPSec, SSL-Tunnel über das Web -> https für authentifizierte Umgebungen) Zweikomponenten-Authentifizierung: „Etwas haben und etwas wissen“ (Smartcard mit private Key, PIN-Code für den Zugriff)	Identitätsklau, um so unerlaubt Zugriff auf Systeme und Ressourcen zu erhalten
	Nichtabstreitbarkeit der Urheberschaft (Die Urheberschaft eines Dokumentes steht zweifelsfrei und dauerhaft fest)	Digitale Signatur von Dokumenten zum Nachweis der Urheberschaft und zum Nachweis der Integrität des Dokumentes („wissen was man unterschrieben hat“ -> keine nachträgliche Änderungen ohne Wissen des Subscribers möglich!)	Verfassen anonymen Dokumenten

10.2 Technologien und IT-Güter

Kreuzen Sie an, welche IT-Güter bei nachstehend beschriebenen Situationen geschützt sind!

1	Active Directory Inter-Standort Verbindung Als IP-in-IP Protokoll wird IPSec eingesetzt.	Welche Daten -> Daten bei der Übertragung ☒ Vertraulichkeit der Daten -> welche Daten? ☒ Integrität der Daten Welche Systeme -> IPSec Tunnel-Endpunkt ☒ Verfügbarkeit der Systeme -> welche Systeme? ☒ Keine Missbräuchlich Verwendung der Systeme ☐ Digitale Integrität der Benutzer -> welche Benutzer? ☐ Nichabstreitbarkeit der Urheberschaft
2	WLAN-Zugang über WPA2-PSK	Welche Daten -> bei Übertragung! ☒ Vertraulichkeit der Daten ☒ Integrität der Daten -> welche Systeme -> WLAN AP, WLAN Bandbreite ☒ Verfügbarkeit der Systeme ☒ Keine Missbräuchlich Verwendung der Systeme ☐ Digitale Integrität der Benutzer -> welche Benutzer? ☐ Nichabstreitbarkeit der Urheberschaft
3	WLAN-Zugang über IEEE 802.1X	Welche Daten -> Daten bei der Übertragung ☒ Vertraulichkeit der Daten -> welche Daten? ☒ Integrität der Daten Welche Systme -> WLAN AP, WLAN Bandbreite ☒ Verfügbarkeit der Systeme -> welche Systeme? ☒ Keine Missbräuchlich Verwendung der Systeme Welche Identität? -> Persönliche Identität zur Auth am AD und IEEE 802.+X Portfreischaltung ☒ Digitale Integrität der Benutzer -> welche Benutzer? ☐ Nichabstreitbarkeit der Urheberschaft

4	Bezahlen einer Rechnung nach einem Einkauf im Internet mit PayPAL	Welche Daten -> Daten bei der Übertragung -> Daten bei der Einspeicherung ☒ Vertraulichkeit der Daten -> welche Daten? ☒ Integrität der Daten Welche Systeme -> Auth Server ☒ Verfügbarkeit der Systeme .. -> welche Systeme? ☒ Keine Missbräuchlich Verwendung der Systeme Welche Identität -> Identität des PayPal-Konteninhabers ☒ Digitale Integrität der Benutzer -> welche Benutzer? ☒Nichabstreitbarkeit der Urheberschaft
5	DNS-Abfrage eines Clients auf dem Nameserver <ns1.bluewin.ch>	Welche Daten -> Daten bei der Übertragung -> RR auf einem klassischen DNS-Server ☐ Vertraulichkeit der Daten -> welche Daten? ☐ Integrität der Daten Welches System -> DNS-Server ☐ Verfügbarkeit der Systeme -> welche Systeme? ☐ Keine Missbräuchlich Verwendung der Systeme ☐ Digitale Integrität der Benutzer -> welche Benutzer? ☐ Nichabstreitbarkeit der Urheberschaft
6	Benutzeranmeldung auf einem Acitve Directory integrierten Client mit dem Active Directory Benutzerkonto	☐ Vertraulichkeit der Daten -> welche Daten? ☐ Integrität der Daten ☐ Verfügbarkeit der Systeme -> welche Systeme? ☐ Keine Missbräuchlich Verwendung der Systeme ☐ Digitale Integrität der Benutzer -> welche Benutzer? ☐ Nichabstreitbarkeit der Urheberschaft

7	Email mit PGP-Technologie versenden	Welche Daten -> Daten bei der Übertragung -> Daten bei der Einspeicherung ☒ Vertraulichkeit der Daten -> welche Daten? ☒ Integrität der Daten Welche Systeme -> KDC auf DC ☒ Verfügbarkeit der Systeme -> welche Systeme? ☒ Keine Missbräuchlich Verwendung der Systeme Welche Identität -> Identität des AD-Benutzers ☒ Digitale Integrität der Benutzer -> welche Benutzer? ☐ Nichabstreitbarkeit der Urheberschaft

10.3 Erweiterte Firewall Regeln für einen DNS-Serverver

Die Firma RADON AG unterhält an ihrem Haupsitz in Luzern eine DMZ mit dem IP-Adressbereich <84.1.1.16/ 29>. Die öffentlichen Zonen werden wie folgt gehostet:

Server	**autorisierend in der Rolle …**
Host <84.1.1.20> mit BIND 9.3	Als Master aurorisierend für die Zonen <radon..ch> <16/29.1.1.84.in-addr.arpa>
Host <212.9'.198.185> mit BIND 9.3	Als Master aurorisierend für die Zonen <radon..ch> <16/29.1.1.84.in-addr.arpa>

DMZ und WAN sind durch einen Router mit mit stateful und FTP-stateful Inspection Firewall-Funktionalität getrennt.

Erstellen Sie die Firewall-Regeln für

- die DNS-Queries von Clients aus dem Internet
- die DNS-Queries von Resolvern aus der HSZ bzw. aus der DMZ
- Studieren Sie neu noch, welche Regeln (Richtung und L4 Protokoll) erforderlich sind, damit der Zonentransfer zwischen Master und Slave funktioniert!

Nr.	**Richtung In/ out**	**L3 Protocol**	**Quelle**		**Ziel**		**SF j/ n**	**Aktion**	**Beschreibung (L7 Protokoll)**
			Host-IP-Adr./ Netz-IP.-Adr	**L4 Protokoll Port Nr**	**Host-IP-Adr./ Netz-IP.-Adr**	**L4 Protokoll Port Nr**			
1	HSZ->DMZ	IP	HSZ_NETIPAdr/24	> 1023	84.1.120	udp 53	J	Allow	HSZ_DNSQueries
2	DMZ-WAN	IP	84.1.1.20	> 1023	ANY	udp 53	J	Allow	DMZ_DNS_ServerQue
3	WAN-DMZ	IP	ANY	> 1023	84.1.1.20	udp 53	J	Allow	WAN_to-DMZ_DNSQ
4	WAN-DMZ	IP	212.9.198.185	> 1023	84.1.1.20	tcp 53	J	Allow	DNS_Slave-A/IXFR
5	DMZ_WAN	IP	84.1.1.20	> 1023	212.9.198.185	Tcp 53	J	Allow	toSlaVeNOTIFY

Notieren Sie, was bei Windows Server System zum Schutz gegen (D)DoS-Angriffe zu tun wäre. Erwähnen Sie, die Nummer der KB und welche Konfigurations-Items angefasst werden müssten!

ls –d <Zone>

Der DNS-Server <84.1.1.20> in der DMZ untersteht Ihnen zur Administration. Sie haben einen Zugang über SSH eingerichtet (TCP LISTEN Port 22). Dadurch muss dem Schutz der Verfügbarkeit des Systems besondere Aufmerksamkeit geschenkt werden. Beschreiben Sie kurz, welche Möglichkeiten Sie haben um ein Linux System gegen (D)DoS-Angriffe zu schützen!

Es geht um „Hardening des TCP/IP-Stacks des OS gegen SYN-Flood Angriffe“

Unter Linux gibt es einen Mechanismus, der unter der Bezeichung Syncookies bekannt ist. Die Einstellung liegt im /proc-System:

proc/sys/net/ipv4/tcp_syncookies

Nähere Details entnimmt man einem HowTo.

Grundsätzlich gibt es keinen wirchlich effizienten Schutz gegen SYN-Flood Angriffe, da es sich um ein systemimmanentes Problem handelt: LISTEN-Ports sind nun halt einfach dazu gedacht, TCP-Verbindungsanfragen entgegenzunhmen.

Dermassen gehärtete Systeme, ob Linux oder Windows, verbrauchen einen Teil der CPU- und RAM-Ressourcen für die SYN-Flood Schutzfunktion.

Notieren Sie, was bei Windows Server System zum Schutz gegen (D)DoS-Angriffe zu tun wäre. Erwähnen Sie, die Nummer der KB und welche Konfigurations-Items angefasst werden müssten!

Microsoft hat eine KB unter dem Titel „How To: Harden the TCP/IP Stack?“ herausgegeben.

Es müssen verschiedene Kernel-Funktionen über das Setzen von Registry-Keys aktiviert werden.

SynAttackProtect TcpMaxPortsExhausted TcpMaxHalfOpenRetried cpMaxConnectResponseRetransmissions

TcpMaxHalfOpen TcpMaxDataRetransmissions EnablePMTUDiscovery KeepAliveTime

NoNameReleaseOnDemand

10.4 IIS mit Datenbank basierter Webapplikation in der DMZ

In der DMZ läuft ein IIS auf einem Windows Server 2003. Darauf wird eine Datenbank basierte Webshopapplikation betrieben. Im Rahmen der IT-Sicherheitsmanagement Prozesskette führen Sie in der nachstehenden Tabelle für das Asset-Item „IIS“ die folgenden Schritte aus:

- Erfassen der Sub-Items
- Identifizieren der hauptsächlichen Bedrohungen
- Bewertung des Risikos (Wahrscheinlichkeit des Eintretens x Schadensausmass)
- Liste möglicher Massnahmen

1	**IIS mit Datenbank basierter Webapplikation**				
Sub Item	**Bezeichnung/ Beschreibung**	**Bedrohung**	**Risikobewertung**		
			Wahrscheinlichkeit	Schadensausmass	
1.1	Serverhardware	Technisch bedingte Systemausfälle	7	5	47
1.2	Betriebsssystem Windows 2003 Server R2	(D)DoS-Angriffe gegen den TCP/IP-Stack Ausnutzen von Vulnerbiltites mit konkreten Expoits Übernahme von admin-Rechte und Berechtigungen durch Hacker	7	7	49
1.3	Administratives Konto, digitale Identität des Administrators	Identitätsklau durch Passwort-Hacking	5	9	45
1.4	IIS	Exploits auf Vulnerabilities des IIS	4	7	28
1.5	ASP .NET-Framework	Exploits auf Vulnerabilties des ASP.NET Frameworks	4	7	28
1.6	ASP.NET-Webanwendung	Ausnutzen von von Sicherheitsmängeln in der Web-Anwendung (z.B. SQL-Injection, Cross-Site Scripting)	6	7	42
1.7	Benutzer und Geschäftsdaten (Bestellungen, Lieferungen, offene Rechnungen,…) der Webanwendung	Verlust von wichtigen Datenteilen durch Inkonsistenz der Anwendungssoftware Diebstahl der Daten durch Extraction aus dem RDBMS Verlust von Backup-Daten aus organisatorischen oder technischen Gründen	7	10	70

10.5 Ausarbeitung von Sicherheitsrichtlinien

Sie arbeiten nun für den IIS Sicherheitsrichtlinien aus. Formulieren Sie Sicherheitsrichtlinien für den IIS, den den Schutz der Vertraulichkeit und Integrität der Daten bei Einspeicherung und Transport garantieren sollen!

DATA.S01	Restriktives Datenzugriffskonzept für den Zugriff auf die RDBMS gespeicherten Benuthzer und Geschäftsdaten planen, anwenden und testen.
DATA.S02	Petetrationstest und Security-Audit für die RDBMS-Einspeicherung durchführen
DATA.S03	Sicherheitstests für die Webapplikation entwickeln und durchführen lassen
HW.S01	Redundante Auslegung wichtiger Systemteile (RAID, USV, Internetkonnektivität) -> Virtualisierung der Server für http un das RDBMS
OS.S01	Installtion der OS nur aus sicheren Quellen und in speziell gesicherten Umgebungen (Firewall)
OS.S02	Anwendung des Microsof Security Base Line Analyzers, Anwendung von spziellen Gruppenrichtlinien und Host-Firewall Regeln gemäss Microsoft Windos Server Security Handbuch
OS.S03	OS TCP/IP-Stack gegen SYN-Flood Angriffe härten
OS.S04	Regelmässiges Einspielen von Betriebssystem-Updates
OS.S05	Installation von Anti-Malware Software
IIS.S01	Applikation regelmässig updaten
IIS.S02	Microsoft- und CERT-Publikationen zur aktuell verwendten Version des IIS verfolgen und Empfehlungen umsetzen

11 Abbildungsverzeichnis

12 Kontakt

Name	Janik von Rotz
E-Mail	contact@janikvonrotz.ch
Website	http://www.janikvonrotz.ch