Schutz- und Sicherheitsfunktionen in Webauftritt integrieren

WSEC

Internet

WSEC

Definition Internet

Weltweites Rechnernetz mit verschiedenen Diensten und Protokollen.

1967 Ausschreibung DARPA für ein Kommunikationssystem:
- PSDN Packet Switch Data Network (x.25) gewann
- TCP/IP Transmission Control Protocol / Internet Protocol erfüllte Vertraulichkeit und Zuverlässigkeit nicht wurde den Universitäten überlassen und von Industrie gesponsert

1989/1990 Tim Berners-Lee entwickelt die Methode für http und damit den öffentlich zugänglichen Dienst des www (früher nur Unix Commands).

Links

http://www.internet-und-sicherheit.de/
http://www.bsi.de/fachthem/sinet/index.htm
http://www.microsoft.com/germany/ms/security/default.mspx
http://www.securityinfo.ch/tipps.html
www.cryptool.de

www.bsi.de Gefährdungskatalog und Baustein 7.5 Webserver 6.1-6.3, 6.7-6.8, 7.2-7.6, 9.2-9.3

Intranet

LAN mit TCP/IP
Netz innerhalb der Firma, geschlossener Benutzerkreis.

Extranet

Teilmenge des Intranet, das einem definierten Benutzerkreis über Internet zur Verfügung steht.

Server in der demilitarisierten Zone

Normale Internet-Dienste

Dienst	Protokoll	Port TCP	Port UDP
www	http	80	---
E-Mail in	pop3 / imap	110 / 143	---
E-Mail out	smtp	25	---
Chat	irc	194	194
Usenet	nntp	119	---
Filetransfer	ftp	21	---
Fernzugriff	telnet	23	---
Namensd.	dns	53	53

Sichere Internet-Dienste

Dienst	Protokoll	Port TCP	Port UDP
www	https	443	---
E-Mail in	pop3s/imaps	995 / 993	---
E-Mail out	smtps	465	---
Chat	ircs	994	---
Usenet	nntps	563	---
Filetransfer	ftps	990	---
Fernzugriff	telnets/ssh	992 / 22	---
www Proxy	http-proxy	8080	---

Internet-Dienste

WSEC

World Wide Web www

Hypertext Transfer Protocol HTTP

- Protokoll der Anwendungsschicht zur Übertragung von Daten im World Wide Web

E-Mail

Simple Mail Transfer Protocol SMTP
Postoffice Protocol Version 3 POP3

- Austausch von elektronischen Nachrichten
- SMTP: Mailversand
- POP3: Mailempfang

Chat

Internet Relay Chat IRC

- Echtzeit-Unterhaltung in virtuellen Chat-Rooms

Usenet

Network News Transport Protocol NNTP

- Diskussionsforen, News-Groups
- lokale Gruppen: nur auf einem Server
- globale Gruppen: automatischer Austausch der Beiträge zwischen allen Servern

Filetransfer

File Transfer Protocol FTP

- Kopieren von Dateien von und zu entfernten Rechnern
- Zugriffsbeschränkung durch Benutzername und Passwort möglich
- oder Benutzername “anonymous” mit E-Mail-Adresse als Passwort (anonymous ftp)
- unverschlüsselte Übertragung von Dateien, inkl. Passwort

Fernzugriff

TELNET

- ältester Dienst des Internets
- Einloggen auf entfernten Rechnern über Kommandozeile
- Übertragung aller Daten inkl. Passwort im Klartext

Domain Name System DNS

Domain Name Service DNS

- Domain Name: Rechner.Subdomains.Top-Level-Domain
- Umsetzung von Hostnamen (Domain) in num. IP-Adressen
- 13 Root-Server, darunter hierarchische Anordnung
- Einträge werden von oben her periodisch erneuert
- IP-Adresse einfach änderbar
- Provider führen zusätzliche eigene Subdomains
- zuständig für Organisation: Internet Corporation for Assigned Names and Numbers ICANN, www.icann.org
- zuständig für Namensvergebung: Network Information Center NIC, www.nic.com
- Dynamic Host Configuration Protocol DHCP, dynamische Zuweisung einer IP-Adresse beim Start, UDP 67

Konfigurationsdateien

Zuunterst in der DNS-Hierarchie, Tabellen auf jedem Rechner, haben die höchste Priorität.

- Hosts
- Networks
- Services
- Protocol

Dateien ohne Endung bzw. mit .sam als Beispiel, können von Hand angepasst werden (wichtig: Umbruch am Ende).
Können aber auch von Trojanern manipuliert werden.

Verschlüsselungs-Protokolle

WSEC

SSH

Secure Shell, Layer 7

Zugriff auf Betriebssystem-Shell eines anderen Rechners mit Public Key-Verschlüsselung.

SSL

Secure Socket Layer, https, Layer 5-7

Erfindung 1994 von Netscape, de facto-Standard für Kommunikations-Verschlüsselung im Webbereich.

Garantiert Vertraulichkeit, Authentizität und Integrität.
Clients kennen standardmässig SSL oder TLS oder beides.

Verwendung:
- E-Banking

TLS

Transport Layer Security, Layer 5-7

Nachfolger von SSL, offizieller Standard.
Gleiche Funktionsweise, aber nicht kompatibel.

Funktionsweise (3way handshake):
- Client: Synchronisationsabfrage
- Server: schickt Public Key des Server Side Certificates
- Client:
  - warnt bei abgelaufenem oder ungültigem Zertifkat, unbekanntem Aussteller oder unpassender Website (kann aber trotzdem verschlüsseln)
  - generiert (evtl. mehrmals) symmetrischen Session Key und sendet ihn mit dem Public Key an den Server
- evtl. Client Side Certificate zur Client-Authentifizierung

IPSec

Internet Protocol Security, von der IPv6-Arbeitsgruppe der IETF (Internet Engineering Task Force) entwickelt.
Verwendung:
- Aufbau sicherer IP-Verbindungen (VPN, WLAN, Telework)

Betriebsmodi:
- Transportmodus: nur Nutzdaten verschlüsselt
- Tunnelmodus: komplettes IP-Paket verschlüsselt

Sicherheitsfunktionen:
- Verschlüsselung auf Layer 3 (mit Header höherer Prot.)
- Authentisierung der Nachricht (Paketintegrität)
- Authentifizierung des Absenders (Paketauthentizität)
- Verwaltung von Schlüsseln

Public Key Infrastructure PKI

Zertifizierungsstellen zertifizieren öffentliche Schlüssel.

Instanzen:
- Registration Authority RA
- Certification Authority CA

Registration Authority

z.B. Banken, Handelskammern

- kontrolliert Zertifikats-Antrag
- nimmt Registration vor
- sendet Zertifikats-Request an CA
- führt Sperrlisten (Certificate Revocation List CRL)
- kann Key-Recovery einleiten

Certification Authority

In der Schweiz Swisscert (früher Swisskey).

- generiert und verwaltet Root-Zertifikat (Zertifikat der CA)
- schützt privaten Schlüssel des Root-Zertifikats
- generiert Zertifikate
- signiert Zertifikate mit ihrem Root-Zertifikat (der Inhaber kann es seinerseits wieder als Root verwenden, ergibt Zertifikats-Hierarchie)
- publiziert Sperrlisten
- hinterlegt privaten Schlüssel für Key-Recovery

Zertifikat

Asymmetrisches Schlüsselpaar.

Verwendung:
- Digitale Signatur
- Verschlüsselung
- Web-Login (kein Username / Passwort mehr)

Schutz vor Diebstahl / Verlust / Vergessen:
- Signatur-Zertifikat: privater Schlüssel beim Antragsteller erstellt
- Verschlüsselungs-Zertifikat: privater Schlüssel bei der CA erstellt und hinterlegt

Qualifiziertes Zertifikat

Merkmale: identifizierter Inhaber, Key einmalig und geschützt

Bestandteile:
- Version (X.509 V3, Standard für die Echtheitsbestätigung von Zertifikaten)
- Seriennummer
- Algorithmus (RSA)
- Aussteller
- Gültigkeit von bis
- Inhaber, kann auch Domain sein
- öffentlicher Schlüssel des Antragstellers
- Signatur des Zertifikats mit dem privaten Schlüssel der Ausgabestelle
- Verwendungszweck
- Zertifikationspfad (Hierarchie der Zertifikate)

Smart Card

Karte im Kreditkartenformat mit Mikroprozessor, für Speicherung Private Key (Alternative: USB-Stick).

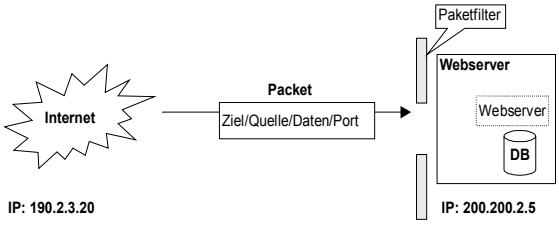
Vorteil: Verlust wird bemerkt

Schutzschichten:
- logisch:
  Kapselung der Methoden signieren und dechiffrieren, Aufruf gibt nur Resultat zurück, nicht den Schlüssel
- mechanisch:
  - Abstrahlschutz (TEMPEST-Standard)
  - tamper-resistent: Selbstzerstörung beim Aufschrauben

Ports

- Jede Applikation auf dem Webserver hat einen Port
- Es gibt 65K Ports, die ersten 1024 sind normiert (z.B. Port 80 = http)
- TCP/IP kennt die normierten Ports
- Browser wandelt URL www.test.ch in www.test.ch:80 um
- Bei einem Verbindungsaufbau muss zwingend der Zielport angegeben werden

Grafik Port



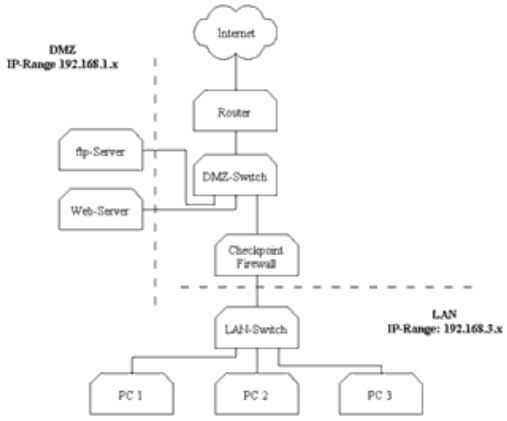
Demilitarisierte Zone DMZ

Geschützter Rechnerverbund zwischen zwei Computernetzwerken, jeweils durch einen Paketfilter gegen das dahinterstehende Netz abgeschirmt.

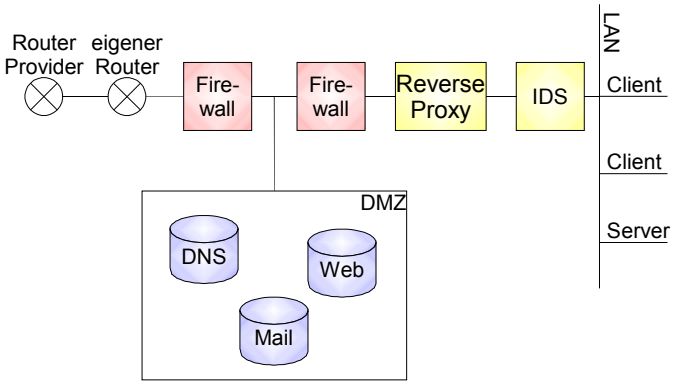
Ziel: möglichst auf sicherer Basis Dienste des Rechnerverbundes sowohl dem einem als auch dem anderem Netz zur Verfügung zu stellen.

Vorteil: im Falle einer Kompromittierung eines Servers in der DMZ bleibt das interne Netzwerk trotzdem noch geschützt.

Grafik DMZ



Sicherheitseinrichtungen



Webauftritt

WSEC

Webserver-Standort

- Hosting:
  Provider unterteilt den Webserver in virtuelle Servers, mehrere Domains unter gleicher IP-Adresse günstig, aber keine Kontrolle über Ports
- Housing:
  dedizierter physischer Webserver beim Provider, eigene IP-Adresse und Firewall, Provider sorgt für Platz, Strom und Internet-Anschluss
- Eigenbetrieb:
  im LAN oder besser in DMZ zwischen zwei Firewalls, eigene IP-Range

Art des Webauftritts

- statische Site: z.B. für Personal Homepage
- dynamische Site: Inhalt, Design, Aufbau variabel, oft mit Datenbank-Anbindung
- Transaktions-Site: z.B. E-Shop, E-Banking
- Portal: z.B. Yahoo, Postfinance, Unternehmens-Intranet

Daten im Webauftritt

- technische Metadaten: Domain, IP-Adresse, Kontaktperson
- Fehlermeldungen: Rückschlüsse auf verwendete Systeme
- Postings, Logs, Verzeichnisse
- Informationen über Firma und Mitarbeiter
- Benutzernamen

Web-Sicherheitskonzept

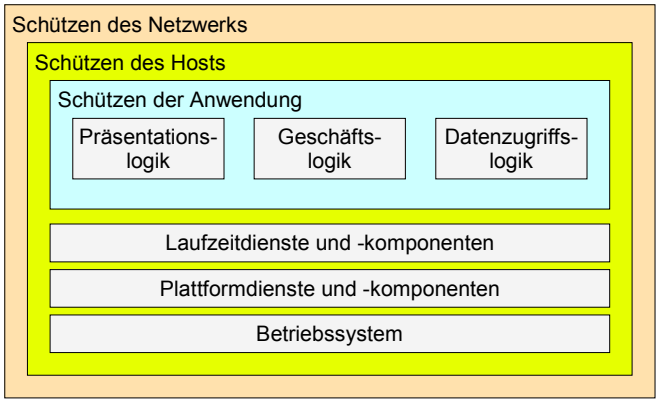
Inventarisierung:

- Daten des Webauftritts
- Daten auf Schnittstellensystemen
- Prozesse: Datenflussdiagramme
- Datenbanken
- Datenfeeds nach aussen
- Administrationszugriffe
- physische Netzzugänge
- vollständiges Netzwerkdiagramm
- Outsourced Services
- Application Development
- Technologien und Architekturen

Ebenen der Websicherheit

WSEC

Ganzheitlicher Sicherheitsansatz



Security Offloading

Prinzip der Auslagerung von Sicherheitsmassnahmen, weg von den Applikationen, zentral an einer Stelle.

Netzwerkkomponenten

- Router:
  - äusserster Ring des Netzwerks
  - leitet Datenpakete zu Ports und Protokollen
- Firewalls:
  - blockiert nicht verwendete Ports und Protokolle
  - stellt anwendungsspezifische Filter bereit
- Switch:
  - trennt Netzwerksegmente

Verlust der Vertraulichkeit

Unbefugter Informationsgewinn durch Zugriff auf vertrauliche Daten.

- Spyware, Spionage: Passwörter, Kreditkarten
- Dialer
- Hacker
- Information Disclosure: unerwünschte Info-Offenlegung
- Passwort knacken
- Frontdoor: versteckter Benutzeraccount, Übernahme eines bestehenden Benutzeraccounts
- root kit: gibt Administratorzugang
- Verletzung des Datenschutzes

Verlust der Integrität

Unbefugte Modifikation, Veränderung, Manipulation von Daten.

- Computerschädlinge: Viren, Würmer, Trojaner, Backdoor
- Aktive Inhalte
- Exploit: Ausnutzung von Systemschwachstellen
- Cracker
- Defacing: Missgestaltung einer Website
- Browser-Hijack: Änderung von Browser-Einstellungen
- Tampering: Datenmanipulation
- SQL Injection: Strichpunkt und eigenen Code eingeben
- Cookie Poisoning: falsche Daten für Server bereitstellen
- Buffer Overflow: Message-Überlänge (braucht Kenntnisse)

Verlust der Verfügbarkeit

Unbefugte Beeinträchtigung der Funktionalität durch Zerstörung von Daten, Hinderung an der Nutzung.

- Spam: Mailflut belastet Internetverbindung und Server, verstopft Postfach
- (Distributed) Denial of Service DoS, DdoS: Überlastung eines Servers durch Blockieren der Ressourcen
  - viele offen gelassene Anfragen beim 3way handshake (SYN, SYN/ACK, ACK)
  - sinnlose Authentisierungsanfragen, braucht nicht viel Bandbreite

Verlust der Authentizität

Vortäuschung einer falschen Identität.

- Missbrauch des PCs als Sprungbrett (hopping station) oder Spamschleuder
- Spoofing
- Man-in-the-Middle-Angriff: Sitzungsübernahme
- Phishing: Password fishing, Links auf gefälschte Webseiten in Emails zur Erlangung von Zugangsdaten
- Cross-site Scripting XSS: Seite im eigenen Frame anzeigen
- Zugriff auf Authentisierungsserver

Verlust der Verbindlichkeit

Abstreitung der (rechtlichen) Bindung eines Geschäfts.

- Repudiation: Abstreiten getätigter Aktionen oder Transaktionen

Verlust der Vertraulichkeit

WSEC

Hacker

Dringen in fremde Computersysteme ein, ohne Schaden anzurichten.

Hacker-Methoden

- Footprinting: Profil der Internet-, Remote- und Intranet-/ Extranet-Zugänge des potenziellen Opfers zusammenstellen
- Scanning: Ausspionieren offener Ressourcen
- Sniffing: Analyse des Netzwerkverkehrs
  - Abhören der Leitung (im Netz, z.B. mit Trojaner)
  - Abhören elektromagnetischer Abstrahlung mit Antenne und Empfänger
- Trashing: Computerabfall als Informationsquelle
- Social Engineering

Social Engineering

Soziale Manipulation, psychologische Tricks zur Erlangung von Informationen.

- Computer based SE:
  z.B. Popups für Gewinnspiele
- Human based SE:
  z.B. Telefonat, als Mitarbeiter anderer Abteilung ausgeben
- Reverse SE:
  nach Problemverursachung Hilfestellung leisten

Passwort knacken

- Brute force:
  Passwörter durchprobieren, braucht lange
- Dictionary Attack:
  beliebigen Frame auf Hashwert des Passworts abhören, Hashwerte aus Wörterbuch bilden und vergleichen

Cracker

Dringen in fremde Computersysteme ein, um Schaden anzurichten.

Vorgehen externer Angriff:

- Informationen sammeln
- Angriff planen, Alternativen und Notfallplan vorsehen
- Angriff durchführen: Informationen beschaffen, System beschädigen usw.
- evtl. Backdoor einbauen: Benutzeraccount aktivieren, Trojaner
- Spuren verwischen: falsche Fährten legen, Logfile manipulieren
- Abgang

Computerschädlinge

WSEC

Viren

nicht selbständige Programmroutinen, die sich selbst reproduzieren

- File-Viren:
  hängen sich an eine Programmdatei und werden bei dessen Start ausgeführt
- Boot-Viren:
  stehen im Boot-Sektor von Datenträgern und werden beim Starten des Rechners aktiv
- Makro-Viren:
  befinden sich in Office-Dokumenten in Makroprogrammiersprachen, z.B. VBA, und werden beim Start der entsprechenden Programme ausgeführt

Würmer

legen neue Dateien an
Verbreitung per Massenmail oder Tauschbörsen

Trojaner

verborgene schädliche Funktion zusätzlich zur bekannten Nutzfunktion
Verbreitung nicht aus eigener Kraft, sondern per Download oder Spam

Backdoor

richten in der Internetverbindung eine Hintertüre ein

Spoofing

Vortäuschung einer anderen Identität.

IP-Spoofing (URL-Spoofing):
- Absenderadresse ändern: keine Antwort möglich, z.B. für Bombe, DoS
- Zieladresse ändern: DNS-Server manipulieren

ARP-Poisoning:
- MAC-Adresse ändern: falsches Mapping im ARP-Cache

Schutzmassnahmen

WSEC

Schutz der Vertraulichkeit

- Zugriffsschutz
- Firewall
- IDS und IRS
- VPN
- Browsereinstellungen auf höchster Sicherheitsstufe
- restriktive Serverkonfiguration
- sichere E-Mail-Einstellungen
- Kryptographie, Verschlüsselung: PGP, IPSec, SSL
- TEMPEST: Standard für elektromagnetische Abschirmung, Abstrahlschutz im Gehäuse
- Risikobewusstsein fördern
- Honeypot / Honeynet: produktionsähnliches System als Falle zur Analyse von Angreifer-Verhalten
- Penetration Test

Schutz der Integrität

- Virenschutzprogramm
- Aktivierung Makro-Virenschutz von Anwendungen
- Plausibilitätskontrolle, logische Prüfung
- Eingabeüberprüfung in Webanwendungen
- Downloads prüfen
- regelmässige Back-ups
- Test Restore
- Installation relevanter Patches und Updates
- Schreibschutzschalter bei Disketten
- kritische Anwendungen ohne Internetanschluss
- zentraler Ansprechpartner in Firmen
- aktuelle Sicherheitsinformationen, z.B. vom Computer Emergency Response Team CERT

Schutz der Verfügbarkeit

- physische Sicherheit: Zugang, Strom, Katastrophen
- ausreichend dimensionierter Webserver
- Proxy-Server
- Netzwerkanalysetools: Schwachstellen-Suche
- Sicherheitskonzept
- Notfallplan

Schutz der Authentizität

- Authentifizierungsverfahren
  - Identifikation (Benutzermanagement)
  - Authentifizierung
  - Autorisierung (Rechtemanagement)
- Single Sign On SSO
- Hashing-Verfahren
- digitale Signatur
- IPsec

Schutz der Verbindlichkeit

- Überwachung
- Protokollierung
- garantierter Timestamp

Schutz der Vertraulichkeit

WSEC

Serverkonfiguration

- minimales Betriebssystem
- Beschränkung auf notwendige Dienst- und Benutzerkonten
- Passwort- und Zugriffsschutz
- Autorisierung: restriktive Zugriffsberechtigungen für Dateien und Verzeichnisse mit access control lists ACL
- Deaktivierung nicht benötigter Netzdienste und -protokolle
- Schliessen nicht benötigter Ports
- Überwachung der offenen Ports
- Administration nur über eine sichere Verbindung
- Verzeichnisinhalt auflisten deaktivieren
- Option “Symbolische Links“ deaktivieren

E-Mail-Sicherheit

- Mails von unbekannten Absendern sofort löschen
- nur vertrauenswürdige Anhänge öffnen, z.B. nach telefonischer Absprache
- Mails nur im Plain Text-Format lesen und schreiben, nicht im HTML-Format
- Virenwarnungen an Sicherheitsbeauftragten senden, sind oft Falschmeldungen (Hoax)

Firewall

- nicht benötigte Ports schliessen
- IP-Masquerading mit Network Address Translation NAT
- Filter: nur zum WLAN gehörende MAC-Adressen
- Paketfilter-Einstellungen: Abblocken nicht erlaubter Protokolle, Verhinderung von IP-Spoofing
- Modems auf der unsicheren Seite der Firewall installieren

Intrusion Detection System IDS

Überwacht Netzwerkaktivitäten in Echtzeit und spürt ungewöhnliches Verhalten auf, aber teuer in Anschaffung und Unterhalt.

- Wiederholte Einlogversuche mit falschem Passwort
- Einloggen zu ungewöhnlichen Zeiten
- unerwartetes Verhalten des Systems oder einzelner Programme
- neue oder veränderte Dateien
- hohe Netz- oder Speicherauslastung
- Dateien mit geänderten Zugriffsrechten
- Portscan
- Inkonsistenzen oder Lücken in den Logdateien

Intrusion Response System IRS

Überwacht Netzwerkaktivitäten in Echtzeit und reagiert auf ungewöhnliches Verhalten.

- Abschalten betroffener Dienste
- Information von Verantwortlichen

Pretty Good Privacy PGP

Öffentlich verfügbares asymmetrisches Verschlüsselungsverfahren für E-Mail und Dateien und zur elektronischen Signatur.

Funktionsweise:
Web of Trust, vernetztes Vertrauensmodell ohne Oberinstanz, öffentliche Schlüssel von Bekannten signieren oder an “Key Signing Parties” Fingerprints vergleichen

WLAN

- Standard-Passwort im WLAN-Router ändern
- Access-Point-Name verstecken
- Zugriff auf Access-Point beschränken: Adapter-MAC-Adressen im MAC-Adressfilter erfassen
- Verschlüsselung aktivieren
- Client mit Benutzername und Passwort beim Access-Point anmelden

Aktive Inhalte

- Java-Applets:
  vorkompilierte Java-Programme
  kein Zugriff auf fremde Speicherbereiche (Sandbox)
- Authenticode (für ActiveX):
  Verfahren zur Software-Authentifikation von Microsoft
  - Zertifikat: geladenes Objekt noch im Originalzustand
  - digitale Signatur: von wem stammt Objekt
- JavaScript:
  Code-Analyse vor Ausführung

Virenschutzprogramm

- automatische Aktualisierung
- zentral beim File- und Mailserver:
  on demand, zeitgesteuert oder on access
- lokal beim Client zum Schutz bei verschlüsselter Kommunikation

Downloads

- Grösse, Prüfsumme, Signatur prüfen
- vor Installation mit Virenschutzprogramm prüfen

Notfallplan

- Zuständigkeiten, Netzwerkplan
- Zuständigkeiten:
  - Einschätzung der Schwere des Angriffs
  - Sicherstellung von Beweismitteln
  - Analyse des Angriffs
- Vorgehen je nach Art und Schwere des Angriffs
- Eskalationsplan
- Information, Lautsprecherdurchsagen
- Wiederherstellung eines sicheren Zustands mit Test
- Dokumentation und Bewertung
- Optimierung des Sicherheitskonzepts

Proxy-Server

- weniger Internet-Zugriffe durch Cache-Verzeichnis:
  - reduzierter Netzwerkverkehr
  - kürzere Übertragunszeit
- Protokollierung der Zugriffe

Schutz der Authentizität

WSEC

Identifikation

Prüfung der Identität:
- Benutzername
- Nummer
- E-Mail-Adresse
- synthetische UserID (enthält Benutzerinformationen)

Identifikationsmerkmale:
- eindeutig
- dauerhaft: für Nachvollziehbarkeit, nicht löschen oder wiederverwenden
- sprechend (falls möglich)

Benutzermanagement

Benutzer eruieren:
- bestehender Kundenstamm
- Umfrage
- Logfile-Auswertung, automatisch mit Logfile-Analyzer

Benutzersegmentierung für Webauftritt:
- Marketingaspekte: Zielgruppen für CRM
- Kundensegmentierung: individualisierter Webauftritt
- Herkunft: Sprache, Cookie
- unerwünschte Besucher

Benutzergruppen:
- Rollen: Sachbearbeiter, Abteilungsleiter, Entwickler
- Technisch: Server, Drucker, ERP-System

Authentifizierung

Prüfung der Echtheit der Identifikation.

- logische Merkmale, was man weiss:
  Passwort, Einmalpasswort, Algorithmus (Securitas), Spezialwissen (Challenge/Response)
- physische Merkmale, was man hat:
  Schlüssel, Badge, Streichliste, Hard Token (Smart Card), Token-Generator (SecureID), Dongle, Chip-, Magnetkarte
- biometrische Merkmale, was man ist:
  Fingerabdruck, Netzhautmuster, Spracherkennung, Gesichtserkennung, Schrifterkennung, Eingaberhythmus, Verhaltenserkennung, DNA
- geographische Merkmale: IP-Range, Call Back
- Spezialverfahren: CGI, Kerberos, SSO, VPN

Passwörter

Empfehlungen:
- Passwörter für Login, Dateien, Applikationen, Bildschirmschoner, Access-Point
- keine Wörterbuch-Passwörter
- Passwort nie aufschreiben, nie weitergeben
- Anmeldeinformationen immer verschlüsseln
- Einmalpasswort braucht physisches Merkmal wegen Verteilung

Autorisierung

Berechtigung auf Applikationsebene aufgrund Identifikation. Regelt erlaubte Tätigkeiten von Subjekten (können auch Applikationen sein) bezogen auf Objekte.

Grundrechte im File-Umfeld:
- r=read, lesen
- w=write, schreiben (erstellen, ändern, löschen)
- x=execute, ausführen

Grundrechte im applikatorischen Umfeld:
- create
- read
- update
- delete

Rechtemanagement

Gruppenbildung aufgrund von Rollen zur Vereinfachung.

Hierarchie der Rechteverwaltung
(evtl. mit automatischer Konsistenzprüfung):
- Benutzer
- Gruppe
- Allgemein

Stellvertreter-Problematik:
- Ausnahmeregeln auf Benutzerebene: wird unübersichtlich
- Benutzer in beiden Gruppen: zuviele Rechte
- Stellvertreter Gruppe: nur benötigte Rechte zusätzlich

Single Sign On SSO

Einmalige Authentifizierung für verschiedene Applikationen.

Funktionsweise:
- SSO-Client verbindet sich mit SSO-Server
- SSO-Server prüft Logon-Daten mit Verzeichnisdienst
- SSO-Client erhält Session ID
- SSO-Server propagiert Session ID an Applikationen

Directory Services (Verzeichnisdienst, hierarchische DB):
- Lightweight Directory Access Protocol LDAP: vermittelt Kommunikation zwischen SSO-Server und Directory Server
- DNS, soll durch LDAP abgelöst werden
- Active Directory: Microsoft, zu 98% kompatibel zu LDAP