IT-Sicherheit – Ja, aber wie?

Dreo, Graf, Seremek, Thalmeier

AK IT-Sicherheit UniBwM

11.05.2005

der Bundeswehr
Universität München

Warum?

Ein ungeschütztes Windows-System am Netz ist nach ca. 20 Minuten infiziert

Feuerwehr? Eigentlich brennt es doch recht selten!

Waffen lässt man auch nicht ungesichert rumliegen!

Würden Sie Ihr Auto unverschlossen im Parkhaus abstellen?

Inhalt

- Warum?
  - Schutzziele
- Datennetze
  - Firewalls / Packet Filter
  - Personal Firewalls
  - Authentifizierter Netzzugang
  - Wireless LAN
  - Intrusion Detection System
- Rechensystem
  - Schutz vor Malware (Viren, Trojanern, Backdoors, Bots,. . .)
  - Passwörter
  - Betriebssystem
  - Windows
- Applikationen
  - Web-Browser
  - E-Mail-Programme
  - Office
  - sichere Protokolle
- Ist das alles?
- Angebote des Rechenzentrums
  - Packet-Filter
  - Mailfilter
  - Sophos
  - Betriebssystem-Update
- Weiterführende Informationen

Schutzziele

Verfügbarkeit	Schutz vor Ausfall der IT-Systeme, Schutz vor Datenverlust
Vertraulichkeit	Schutz vor unbefugter Kenntnisnahme
Integrität	Schutz vor Manipulation
Authentizität	Schutz vor gefälschter Identität / Herkunft
Verlässlichkeit	Schutz vor unerwünschtem Systemverhalten
Verbindlichkeit	Schutz vor Abstreiten durchgeführter Handlungen

(Anonymität/Pseudonymität)

Inhalt

- Warum?
  - Schutzziele
- Datennetze
  - Firewalls / Packet Filter
  - Personal Firewalls
  - Authentifizierter Netzzugang
  - Wireless LAN
  - Intrusion Detection System
- Rechensystem
  - Schutz vor Malware (Viren, Trojanern, Backdoors, Bots,...)
  - Passwörter
  - Betriebssystem
  - Windows
- Applikationen
  - Web-Browser
  - E-Mail-Programme
  - Office
  - sichere Protokolle
- Ist das alles?
- Angebote des Rechenzentrums
  - Packet-Filter
  - Mailfilter
  - Sophos
  - Betriebssystem-Update
- Weiterführende Informationen

Firewalls

- Firewalls sind Netzkomponenten, die unerwünschte Zugriffe abwehren sollen.
- Märchen: "Eine Firewall schützt uns vor den meisten Bedrohungen"
- Firewalls können nur filtern und regeln, was sie auch verstehen. Kommunikation, die über erlaubte Wege und Protokolle läuft, bleibt unkontrolliert (Verschlüsselung!).
- Sicherer Betrieb erfordert das korrekte Zusammenwirken von Firewall, System und Applikation
- Eine schlecht konfigurierte Firewall ist das größte Sicherheitsrisiko
- Nicht alle Denial-of-Service-Angriffe lassen sich abwehren

Personal Firewalls

Personal Firewalls sind Schutzprogramme, die auf dem System selbst laufen, das geschützt werden soll

Unnötig...

- wenn "sichere" Software eingesetzt wird,
- wenn Software richtig konfiguriert wird und
- wenn der Benutzer versteht, was auf seinem System vorgeht

Personal Firewalls...

- filtern das Grundrauschen der Angriffe aus.
- ermöglichen versierten Benutzern eine bessere Kontrolle über ihr System
- sehen die Applikation
- erhöhen den Support-Aufwand signifikant

Authentifizierter Netzzugang

Authentifizierung:

Bestimmung der Identität einer Person mit einem Merkmal (Wissen, Haben, Sein)

IEEE 802.1x

- Zugang zum Netz erst nach Anmeldung
- Ethernet-Frames passieren den Switch erst nach Anmeldung
- Ein ans Netz angeschlossener Rechner kann nicht automatisch mit anderen Rechnern kommunizieren

Wireless-Security

- Jeder kann ein ungeschütztes WLAN nutzen
- Der Verkehr in einem ungeschützten WLAN kann abgehört oder manipuliert werden
- Schutz durch IEEE 802.11i (WPA2 / AES / IEEE 802.1x) auf Schicht 2 möglich
- Andere Strategie: "Beschränkung auf sichere, verschlüsselte Protokolle" ist nur sinnvoll, wenn kein Übergang zum Internet besteht. (Kosten, Missbrauch)
- Virtual Private Network (VPN) / IPsec als Schutz auf IP-Ebene durch Authentifizierung und Verschlüsselung

Intrusion Detection System

- Alarmanlage für IT-Systeme
- Bietet keinen unmittelbaren Schutz, sondern erkennt Angriffe
- $\longrightarrow$ Intrusion Prevention
  Rückkopplung mit anderen Komponenten, um begonnene Angriffe zu vereiteln

- Network-based
- Host-based
- Application-based

Inhalt

- Warum?
  - Schutzziele
- Datennetze
  - Firewalls / Packet Filter
  - Personal Firewalls
  - Authentifizierter Netzzugang
  - Wireless LAN
  - Intrusion Detection System
- Rechensystem
  - Schutz vor Malware (Viren, Trojanern, Backdoors, Bots,. . .)
  - Passwörter
  - Betriebssystem
  - Windows
- Applikationen
  - Web-Browser
  - E-Mail-Programme
  - Office
  - sichere Protokolle
- Ist das alles?
- Angebote des Rechenzentrums
  - Packet-Filter
  - Mailfilter
  - Sophos
  - Betriebssystem-Update
- Weiterführende Informationen

Wie schützt man ein Rechensystem?

- "Entschärfung" bekannter Schwachstellen
  - Patchen, Updaten, Deinstallieren
  - Umkonfigurieren
- "Entschärfung" unbekannter Schwachstellen?
  - Minimale Rechte
  - Failsafe Defaults
  - Erlaubnisprinzip
  - Gehärtete Software
- Schutz vor Viren, Würmern, Trojanischen Pferden . . .

Schutz vor Malware (Viren, Trojanern, Backdoors, Bots,. . .)

- aktuellen Virenschutz (z.B. Sophos) einsetzen und aktuell halten (z.B. Sophos-Update)
- zentrales Management mehrerer Rechner mit Sophos-Enterprise-Manager
- oft entscheiden wenige Stunden oder Minuten
- Eine sichere Rechtevergabe lähmt bereits manche Viren
- Nicht als Administrator arbeiten

Passwörter

Passwörter gut wählen

- gut merken, gut tippen
- Keine Eigennamen, bekannten Abk. usw.
- Nicht zu kurz
- Buchstaben (groß+klein) + Sonderzeichen + Zahlen
- `iAwdW>J1`
- regelmäßig wechseln
- bei Security-Vorfall *immer alle* wechseln

Betriebssystem

- Rechteverwaltung verwenden
- Minimale Rechte verwenden
- Aktuelle Software verwenden / Patches einspielen
- Sicherheits-Updates durchführen
- Konfigurationsmöglichkeiten nutzen
- Nicht benötigte Funktionen deaktivieren oder deinstallieren

Windows

- Windows-Update oder WSUS
- Microsoft Baseline Security Analyzer
- Nicht als Administrator arbeiten
  Legen Sie sich einen Benutzer an, der weniger Rechte hat. Somit kann Software, die ihnen untergeschoben wurde, weniger Schaden anrichten.
- Deaktivieren und entfernen Sie nicht benötigte Programme und Dienste
  Bedenken Sie immer: Was nicht installiert ist, kann nicht angegriffen werden.

Inhalt

- Warum?
  - Schutzziele
- Datennetze
  - Firewalls / Packet Filter
  - Personal Firewalls
  - Authentifizierter Netzzugang
  - Wireless LAN
  - Intrusion Detection System
- Rechensystem
  - Schutz vor Malware (Viren, Trojanern, Backdoors, Bots,...)
  - Passwörter
  - Betriebssystem
  - Windows
- Applikationen
  - Web-Browser
  - E-Mail-Programme
  - Office
  - sichere Protokolle
- Ist das alles?
- Angebote des Rechenzentrums
  - Packet-Filter
  - Mailfilter
  - Sophos
  - Betriebssystem-Update
- Weiterführende Informationen

sichere Applikationen

- Aktuelle Software verwenden
- Sicherheits-Updates durchführen
- Konfigurationsmöglichkeiten nutzen
- Nicht benötigte Funktionen deaktivieren oder deinstallieren

Web-Browser

- aktuell halten
- sinnvoll konfigurieren

  `http://www.heise.de/security/dienste/browsercheck/`
- nicht notwendige Funktionen abschalten/deinstallieren
  - ActiveX
  - Plugins
  - Java
  - Javascript
  - Visual Basic Script
- Sparsam sein mit Cookies

E-Mail-Programme

- SSL aktivieren
- Vorschaufunktionen ausschalten

Auch bei eigenen Mails meiden:

- HTML
- Attachments
- Links

Office

- Makroviren
- Dokumentaustausch möglichst ohne Makro-fähige Formate (.txt .pdf .rtf)
- Office-Viewer verwenden
- OpenOffice (?)

sichere Protokolle

- Verschlüsselte Protokolle lösen unverschlüsselte ab
  - https://
  - POPs / IMAPs
  - SSH (scp / sftp)
  - ...
- Welchen Schlüsseln vertraue ich?

Ist das alles?

Nein, das sind die ersten Schritte

- Mächtigkeit von IT-Systemen wächst schneller als linear
- Software-Altlasten kommen nur nach und nach ans Licht, wenn überhaupt
- Computer-Kriminalität ist zum lohnenden Geschäft geworden
- Es gibt kaum Bereitschaft für sichere Software erheblich mehr Geld zu bezahlen

Inhalt

- Warum?
  - Schutzziele
- Datennetze
  - Firewalls / Packet Filter
  - Personal Firewalls
  - Authentifizierter Netzzugang
  - Wireless LAN
  - Intrusion Detection System
- Rechensystem
  - Schutz vor Malware (Viren, Trojanern, Backdoors, Bots,...)
  - Passwörter
  - Betriebssystem
  - Windows
- Applikationen
  - Web-Browser
  - E-Mail-Programme
  - Office
  - sichere Protokolle
- Ist das alles?
- Angebote des Rechenzentrums
  - Packet-Filter
  - Mailfilter
  - Sophos
  - Betriebssystem-Update
- Weiterführende Informationen

Packet-Filter

- Anti-Spoofing-Filter
- Email-Verkehr nur über RZ-Mailrelays
- News nur über registrierte Server
- Windows-Ports: 135, 137-139, 445
- Konfigurationsports: TFTP, BOOTP, OSPF, SNMP
- Aufgrund von Angriffen gesperrt (MS-SQL, 42, . . .)
- Von außen nur über RZ-bekannte DNS-Server
- Abschirmung von Sonderbereichen (z.B. Verwaltung)

Mailfilter

- Spammarkierung
- Virenfilterung

Juristische Fragestellungen!

Sophos

- Wird von Rechenzentrum auf CD angeboten
- Remote-Update über Web an http://semsrv.rz.unibw-muenchen.de
- Mit Sophos Enterprise Manager lassen sich ganze Windows-Domänen auf einmal installieren

Betriebssystem-Update

- Windows Server Update Services (im Testbetrieb) spiegelt Microsoft-Patches für das Campus-Netz
- Offline-Update-CD für
  - Windows 2000 und
  - Windows XP (momentan nur SP1!)

Weiterführende Informationen

- BSI Leitfaden IT-Sicherheit
  `http://www.bsi.de/gshb/Leitfaden/`
- `http://isc.sans.org/presentations/first_things_first.php`
- Rüdiger Dierstein: IT-Sicherheit und ihre Besonderheiten
  `http://wwwbode.cs.tum.edu/zope/lectures/courses/WS04/itsicher`
- `http://www.unibw-muenchen.de/campus/RZ/Security/`