Lange Nacht der Wissenschaften 2007

Gefahr aus dem Internet - Wie kann ich mein Windows-System schützen?

Manuel Selling
Humboldt-Universität zu Berlin
ZE Computer- und Medienservice
Abt. Systemsoftware und Kommunikation
E-Mail: manuel.selling@cms.hu-berlin.de

Agenda

1. Gefahren aus dem Internet
2. Was ist gefährdet?
3. Übersicht Malware
4. Analyse von Malware
5. Schutz-Ebenen
    a. Betriebssystem
    b. Anwendungen
    c. Verhalten

Gefahren aus dem Internet

- Malware:
  - Viren
  - Würmer
  - Trojanische Pferde
  - Backdoor
  - Spyware, Adware, Dialer
- weitere Gefahren
  - Phishing
  - Pharming

Was ist gefährdet?

- E-Mail-Adressen
- Kreditkarteninformationen
- Kontoinformationen
- Zugangsdaten
  - Passwörter und Benutzernamen
- private/geschäftliche Dokumente und Daten
- Surfprofile
- ...

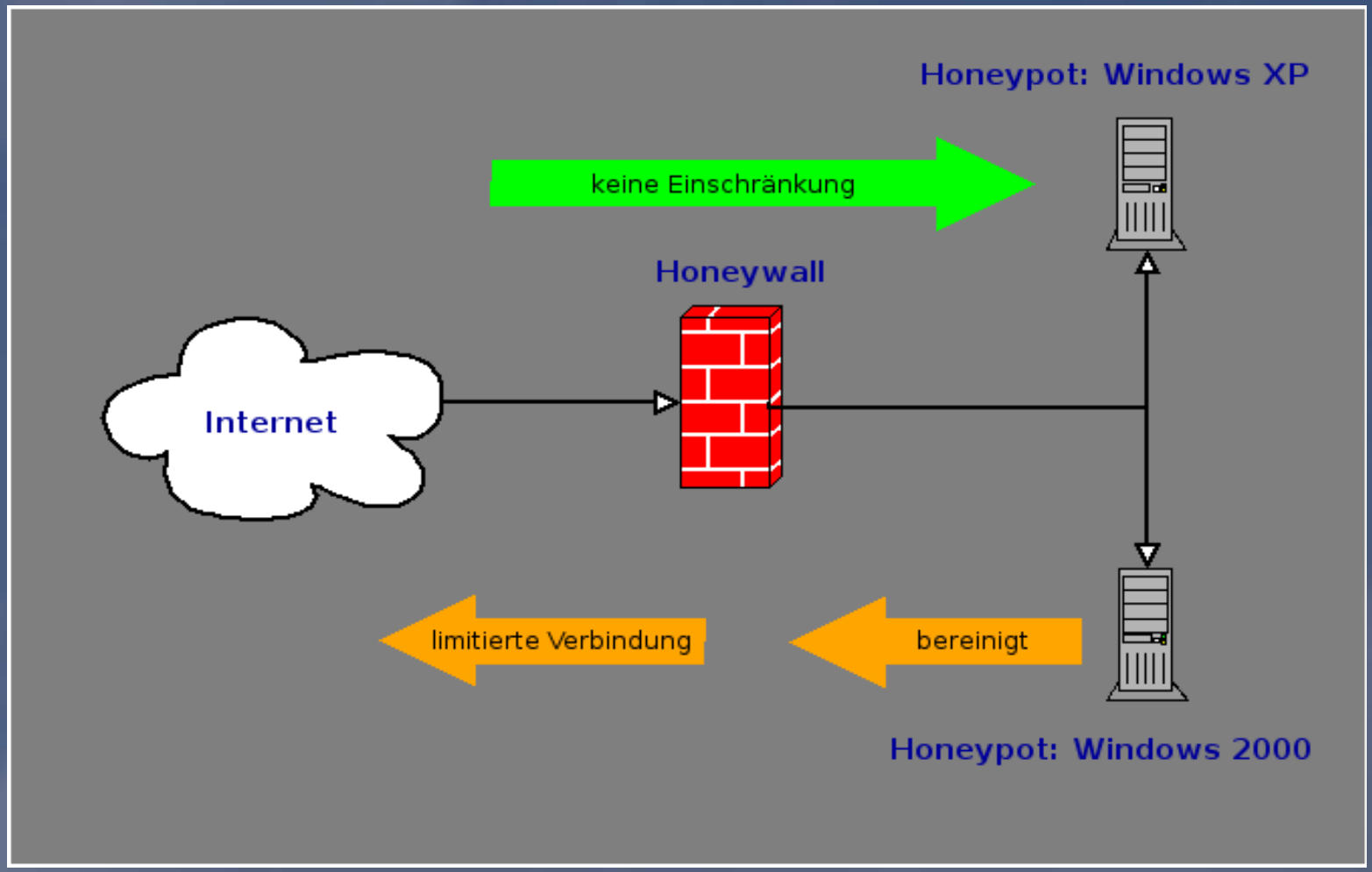
Übersicht Malware

- Entwicklung von Malware 2006[1]
  - 39670 neue Malware (109 pro Tag), Anstieg von 25% im Vergleich zum Vorjahr
  - Rückgang klassischer Viren (-24%)
  - Fokus auf “Ertrag bringende Bereiche”, z.B. Diebstahl + Handel mit Kontodaten/Kreditdateninformationen, Vermietung von Botnetzen
  - Trojan-Downloader (+60%)
  - Ad-/Spyware (+43%)
  - Backdoors (+33%)

The HoneyNet-Project[2]

- Komponenten:
  - Honeywall (Gateway): Roo-1.1
    - Sammlung von Tools zur Protokollierung und Analyse der Netzwerkverkehrs
    - sammelt an zentraler Stelle die Logdaten der integrierten Analyse-Tools
    - Aufbereitung/Auswertung der gesammelten Daten
  - Honeypot(s): Windows XP, Windows 2000
    - anfällige/installierte Betriebssysteme

Aufbau Honeynet



Honeywall Verkehr

The Honeynet PROJECT®

Walleye: Honeywall Web Interface

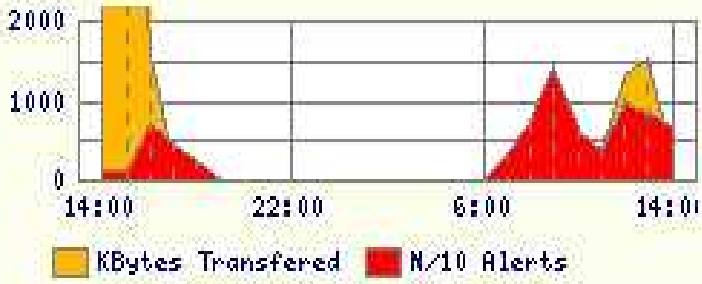
Data Analysis | System Admin | Logout

Online Honeywalls

Honeypot WinXP/W2K

Created: Tue May 29 12:20:55 2007 Last Update: Tue Jun 5 14:33:40 2007

	Bidirectional Flows				Total Flows			
	In		Out		In		Out	
	con	ids	con	ids	con	ids	con	ids
1 Hour	191	109	0	0	2,045	109	0	0
24 Hour	977	602	2,193	169	13,561	602	111,587	169



Auswertung/Übersicht

Activity Report

Top 10 Honeypots

Flags	Host	Connections	IDS events
	141.[redacted]	104,700	150
	141.[redacted]	100	13
	141.[redacted]	1,893	0
	141.[redacted]	544	0
	141.[redacted]	537	0
	141.[redacted]	534	0
	141.[redacted]	528	0
	141.[redacted]	89	0
	141.[redacted]	86	0
	141.[redacted]	85	0

Top 10 Remote Hosts

Host	Connections	IDS events
141.[redacted]	575	425
141.[redacted]	535	177
141.[redacted]	937	0
141.[redacted]	933	0
141.[redacted]	925	0
141.[redacted]	851	0
141.[redacted]	843	0
141.[redacted]	516	0
141.[redacted]	212	0
141.[redacted]	174	0

Top 10 Source Ports

Port	Connections	IDS events
1028	40	12
1036	36	7
2987	35	7
1198	35	7
2959	35	7
2952	35	7
2933	35	7
1290	35	7
2954	34	7
1203	34	7

Top 10 Destination Ports

Port	Connections	IDS events
139	782	746
80	383	13
445	104,437	0
5353	7,483	0
138	6,240	0
137	2,367	0
427	366	0
0	331	0
5355	264	0
14000	224	0

Analyse/Information (1)

- Informationen:
  - Internet Storm Center[3]
  - Computer Emergency Response Team[3]

Port Information

Protocol	Service	Name
udp	netbios-ssn	NETBIOS Session Service
tcp	netbios-ssn	NETBIOS Session Service
tcp	SMBRelay	[trojan] SMB Relay
tcp	Sadmind	[trojan] Sadmind
tcp	Qaz	[trojan] Qaz
tcp	Network	[trojan] Network
tcp	Netlog	[trojan] Netlog
tcp	Msinit	[trojan] Msinit
tcp	GodMessageworm	[trojan] God Message worm
tcp	Chode	[trojan] Chode

Analyse/Information (2)

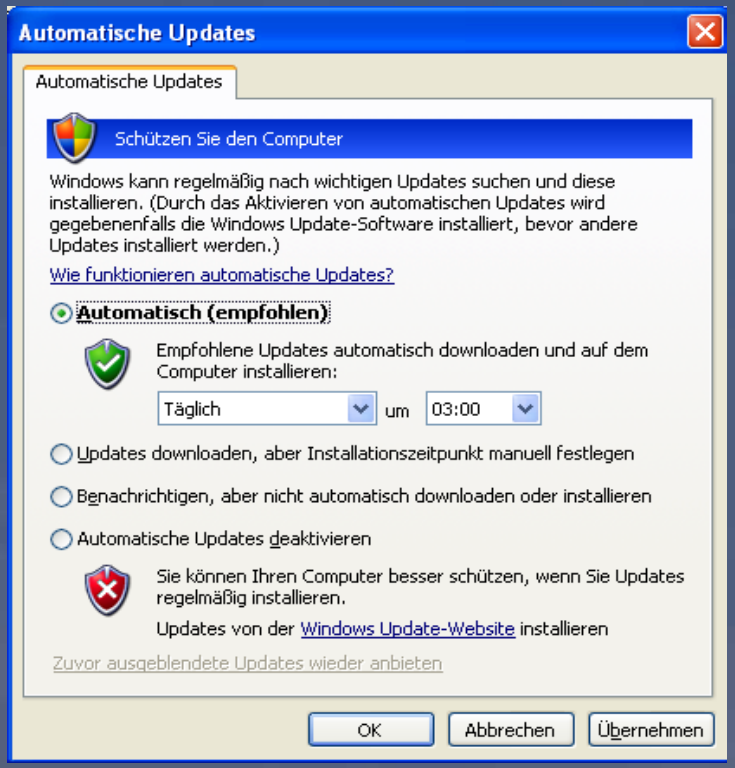
CVE #	Description
CVE-1999-182	"Samba has a buffer overflow which allows a remote attacker to obtain root access by specifying a long password."
CVE-2000-347	"Windows 95 and Windows 98 allow a remote attacker to cause a denial of service via a NetBIOS session request packet with a NULL source name."
CVE-2000-1081	"The xp_displayparamstmt function in SQL Server and Microsoft SQL Server Desktop Engine (MSDE) does not properly restrict the length of a buffer before calling the srv_paraminfo function in the SQL Server API for Extended Stored Procedures (XP)
CVE-2000-1082	"The xp_enumresultset function in SQL Server and Microsoft SQL Server Desktop Engine (MSDE) does not properly restrict the length of a buffer before calling the srv_paraminfo function in the SQL Server API for Extended Stored Procedures (XP)
CVE-2000-1083	"The xp_showcolv function in SQL Server and Microsoft SQL Server Desktop Engine (MSDE) does not properly restrict the length of a buffer before calling the srv_paraminfo function in the SQL Server API for Extended Stored Procedures (XP)
CVE-2000-1084	"The xp_updatecolvbm function in SQL Server and Microsoft SQL Server Desktop Engine (MSDE) does not properly restrict the length of a buffer before calling the srv_paraminfo function in the SQL Server API for Extended Stored Procedures (XP)
CVE-2000-1085	"The xp_peekqueue function in Microsoft SQL Server 2000 and SQL Server Desktop Engine (MSDE) does not properly restrict the length of a buffer before calling the srv_paraminfo function in the SQL Server API for Extended Stored Procedures (XP)
CVE-2000-1086	"The xp_printstatements function in Microsoft SQL Server 2000 and SQL Server Desktop Engine (MSDE) does not properly restrict the length of a buffer before calling the srv_paraminfo function in the SQL Server API for Extended Stored Procedures (XP)
CVE-2000-1087	"The xp_proxiedmetadata function in Microsoft SQL Server 2000 and SQL Server Desktop Engine (MSDE) does not properly restrict the length of a buffer before calling the srv_paraminfo function in the SQL Server API for Extended Stored Procedures (XP)

Betriebssystem

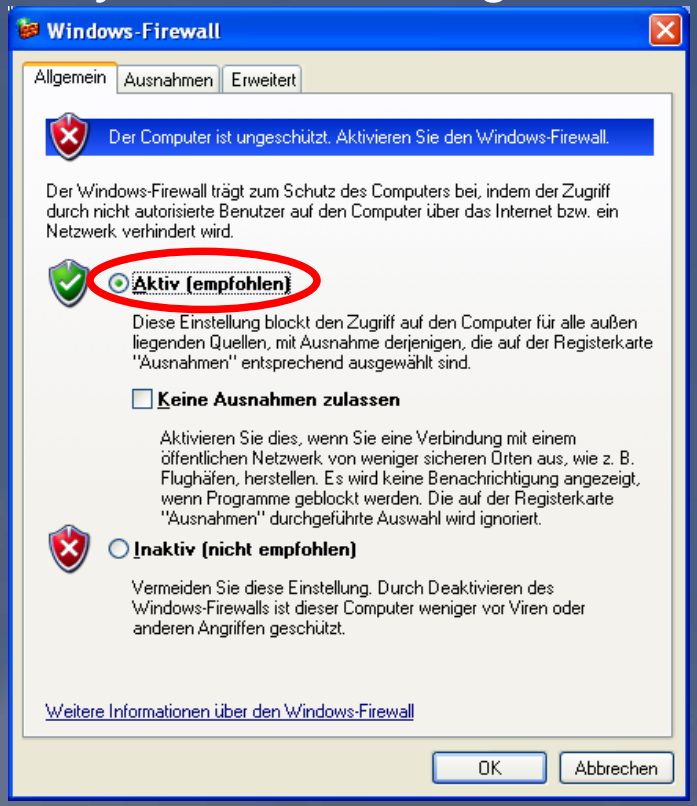
Betriebssystem

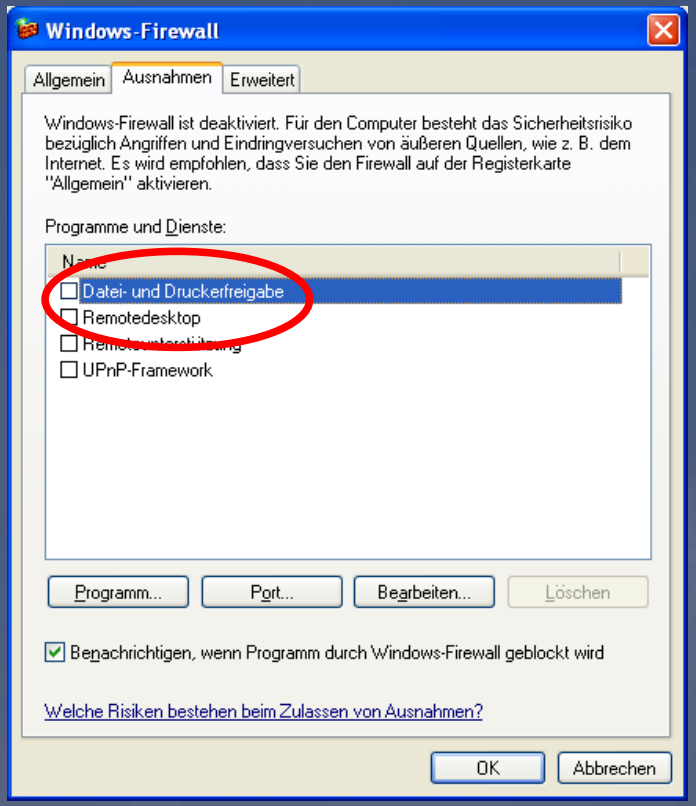
- mit eingeschränktem Account arbeiten
  - nicht als Administrator
- sichere/gute Passwörter wählen[4]
  - mindestens 8 Zeichen
  - Kombination aus Groß- und Kleinbuchstaben, Ziffern, Sonderzeichen
  - kein Wort einer bekannten Sprache
    - z. B. “von 8 bis 16 Uhr: Schlafen verboten!“
      = v8b16U:Sv!
  - regelmässig Passwörter wechseln

- Betriebssystem aktuell halten
  - Windows Update/Microsoft Update konfigurieren
    - Systemsteuerung-->Sicherheitscenter-->automatische Updates



- Windows-Firewall aktivieren/konfigurieren
  - aktivieren und bei Bedarf Ausnahmen definieren
    - Systemsteuerung-->Sicherheitscenter-->Windows-Firewall





Betriebssystem

- Dienste abschalten, die nicht benötigt werden[5]
- WLAN konfigurieren
  - keine “automatische Konfiguration von Drahtlos-Netzwerken“
  - Parameter des WLAN manuell konfigurieren
  - keine WEP-Verschlüsselung, besser WPA2

Betriebssystem

Anwendungen

Anwendungen

- Virenschutz/Viren-Scanner installieren[6]
  (z.B. Avira AntiVir PersonalEdition Classic)
  - neueste Version: Programm/Engine
  - regelmässiges Update der Viren-Signaturen, Scan der Festplatten
- Ad- und Spyware-Scanner installieren[7]
  (z.B. Spybot Search&Destroy)
  - neueste Version: Programm
  - regelmässiges Update der Signaturen
  - regelmässiger Scan der Festplatten, Immunisierung

Anwendungen

- Web-Browser (z.B. Internet Explorer, Firefox)[8]
  - neueste Version, regelmässig Sicherheitsupdates einspielen
  - sichere Konfiguration:
    - wenn möglich: **kein** JavaScript, Java, ActiveX, Cookies
    - keine Passwörter speichern
    - Phishing-Schutz aktivieren
    - empfohlene Einstellungen für die gängigsten Browser: c't-Browsercheck[9]

Anwendungen

- E-Mail Programme (z.B. Outlook, Thunderbird)[10]
  - neueste Version, regelmässig Sicherheitsupdates einspielen
  - sichere Konfiguration
    - wenn möglich: **keine** HTML-Darstellung
    - verschlüsselte Kommunikation zum Mail-Server
    - Spam- und Phishingschutz aktivieren
    - automatische Prüfung der eingehenden Mails auf Viren
    - keine Passwörter speichern
    - empfohlene Einstellungen für die gängigsten E-Mail Clients: c't-Emailcheck[11]

Anwendungen

- generelle Empfehlungen:
  - installierte Programme/Plugins aktuell halten
    - z.B. Auflistung/Überprüfung installierter Programme, ggf. Aktualisierung
    - Überprüfung der Konfiguration (Sicherheit)
  - installierte Treiber überprüfen/aktualisieren
  - nicht benötigte Programme deinstallieren

Anwendungen

Verhalten

Anwendungen

Verhalten

- gesundes Misstrauen gegenüber fremden Inhalten
  - Mails/Dateien von bekannten Personen nicht unbedingt vertrauen
  - umsichtige Installation von Programmen/Freeware
  - Vorsicht bei unseriösen Angeboten (kostenlos/extrem günstig...)
  - niemals per Mail sicherheitsrelevante/kontobezogene Daten an Kreditinstitute verschicken
- sicherheitsrelevante Aktionen (z.B. Online-Banking)
  - immer verschlüsselt durchführen, Zertifikate auf Echtheit prüfen

Verhalten

- Schutz der Privatsphäre
  - regelmässiges Löschen von Cookies, Browser-Cache und temporären Internet-Dateien
- Kleiner Tipp gegen Spam:
  - mehrere E-Mail-Adressen benutzen (Bestellungen, Newsletter, Foren-Accounts, Privat)

Geschütztes System

Link-Liste

- 1 - Malware-Report 2006
  - http://www.antiviruslab.com/whitepapers/AnnualReport.Malware2006DE.pdf
- 2 - Honeywall:
  - http://www.honeynet.org/
- 3 - Malware-Infos:
  - http://isc.sans.org
  - http://www.cert.org/advisories/
- 4 - Passwörter:
  - http://www.rrzn.uni-hannover.de/pw_used.html
- 5 - Dienste:
  - http://www.tecchannel.de/client/sicherheit/401894/
- 6 - Virenscanner:
  - Avira AntiVir PersonalEdition Classic (kostenlos): http://www.free-av.de/
- 7 - Ad- und Spyware-Scanner:
  - Spybot Search&Destroy (kostenlos): http://www.safer-networking.org/
  - Ad-Aware 2007 Free (kostenlos): http://www.lavasoft.de/products/ad_aware_free.php

Link-Liste

- 8 - Browser
  - Firefox: http://www.mozilla-europe.org/de/products/firefox/
- 9 - Browser-Einstellungen:
  - C't-Browsercheck: http://www.heise.de/security/dienste/browsercheck/
- 10 - E-Mail Programm
  - Thunderbird: http://www.mozilla-europe.org/de/products/thunderbird/
- 11 - E-Mail-Client Einstellungen:
  - C't-Emailcheck: http://www.heise.de/security/dienste/emailcheck/
- 12 - Windows Sicherheit Checkliste:
  - SecurityFocus: http://www.securityfocus.com/columnists/220
- 13 - Allgemeine Sicherheitsinformationen
  - Heise Security: http://www.heise.de/security/

Vielen Dank für Ihre Aufmerksamkeit!

Download des Vortrages:

http://www.clauman.de/Indw2007_WindowsSicherheit.pdf