Absicherung von Windows-Clients

Hergen Harnisch

harnisch@rrzn.uni-hannover.de

1 Installation & Setup

2 Firewall

3 Anti-Malware

4 Update

5 Backup

R|R|Z|N

XP & 2003

frisch installiert aber ungepatcht $\wedge$ Internet $\Longrightarrow$ infiziert

- etwas entspannter seit Windows-Firewall, nach Installation aber nur automatisch aktiv bei XP-SP2/SP3 und 2003-SP2
- nur Installationsmedium mit $\geq$SP2 verwenden, ggf. per Slipstreaming neu erstellen[1]
- bei der Installation (zunächst) ohne MS-Netzdienste und mit aktivierter TCP/IP-Filterung arbeiten

  http://www.uni-muenster.de/ZIV.RainerPerske/Sicherheit/WindowsXPInstallation.shtml
- besste Lösung:
  1. offline installieren
  2. „WSUS-Offline"-CD/DVD zum Patchen verwenden
     http://www.rrzn.uni-hannover.de/update_cd.html

[1] ob Bereitstellung durch RRZN möglich ist, ist zu klären

R|R|Z|N

Netzwerkeinstellungen

Einige Dinge sind Standardumfang, aber für Clients unnötig

Systemsteuerung → Einstellungen → Netzwerkverbindungen; Verbindung wählen, Eigenschaften-Knopf

- Deaktivieren Sie NetBios

  … Eigenschaften des TCP/IP-Protokolls, Erweitert, WINS-Karteikarte
- Entfernen oder Deaktivieren Sie die Datei- und Druckerfreigabe für Microsoft-Netzwerke

  … Häkchen entfernen oder Deinstallieren-Knopf
- QoS-Paketplaner ist ebenso unnötig

Autorun deaktivieren

- dient dem Autostart von CD-Roms
- kann Programme starten und das Kontextmenü ändern, jeweils in Datei `autorun.inf` auf dem Datenträger definiert
- funktioniert auch auf Festplatten und USB-Sticks
  - Malware nutzt z.T. Autorun auf Festplatten als Aktivierungs-Hook
  - über USB-Sticks u.Ä. kommt Malware (z.B. Conficker)
- Deaktivierung über Gruppenrichtlinien (alle Laufwerke!)
  (vgl. Sicherheitstage WS2006/07, Windows-Richtlinien, Folie 10:
  `http://www.rrzn.uni-hannover.de/fileadmin/it_sicherheit/pdf/SiTaWS06-Policies.pdf`)
- … aber leider hat Windows bis zu einem Patch im März/April die Einstellung nicht immer vollständig beachtet
  (vgl. `http://support.microsoft.com/kb/967715/`)

Nutzer ohne Administrator-Rechte

Vorteil

Je weniger Rechte desto weniger Schaden, auch

- schwierigere Festsetzung von Schadsoftware,
- Schutzsoftware schwerer aushebel- oder abschaltbar.

Nachteil

- Software-Installationen und sogar -Updates schwierig
- schlechte / alte Software läuft evt. nicht ohne Manipulation
- teils weitergehende Rechte trotzdem nötig, z.B. Netzwerk am Notebook
  (Gruppe Netzwerkkonfigurations-Operatoren)

... richtig gut nutzbar erst ab Windows-Vista oder in der Domäne

R|R|Z|N

Fortgeschritten: Scan-Linux

Wie das Booten von einem Scan-Medium (CD, USB-Stick), ein immer verfügbares Scan-Linux kann im Betrieb die Hürde Aufwand senken.

- Bei Partitionierung des Systems dran denken, 2 Möglichkeiten
  - separate Linux-Partition mit Dual-Boot
  - separate Boot-Partition, die wie USB-Stick Live-System enthält
- Netzwerk-Boot im LAN anbieten

⟶ Beides erfordert Admin-Aufwand und gute Linux-Kenntnisse.

Windows-Firewall

- Standard Windows-Firewall meist völlig ausreichend
  (dürfte Masseninfektionen in Conficker-befallenen LANs verhindert haben)
- filtert nur von Außen initiierten Datenverkehr
- Filterung nach
  - Daemon-Programm (Dienst) oder
  - UDP/TCP-Port

  und das je Netzwerkanschluss und ggf. für bestimmte Quell-IP-Bereiche
  - ICMP separat & global (Echo-Request sollte man zulassen)
- Einstellung mit Gruppenrichtlinien zementiert Konfiguration gegenüber Nutzern

(vgl. http://www.rrzn.uni-hannover.de/fw_windows.html)

Sophos-Anti-Virus

LUH hat Lizenz für Sophos-Antivirus, auch zur Privatnutzung

⟶ unbedingt auch zuhause einen Virenscanner verwenden (lassen)

- Performance-Impact ist heute kein Grund mehr gegen On-Access-Scanning
  - On-Access-Scanning ist Pflicht in Windows-Systemen
  - Netzlaufwerke ruhig ausnehmen, wenn Server scannt
  - Messdaten oder große Dateien ggf. in ausgenommenem Verzeichnis
- Behavioral Genotype Protection / HIPS evt. deaktivieren, erzeugt teilweise Last & Fehlalarme, schützt aber auch
- Aktualisierung alle 15 Minuten empfehlenswert
- zentrale Meldung bei Fund eher nur uniweit sinnvoll (ist ja keine Infektion, gibt übergreifend ein Lagebild), per SNMP ans RRZN ist in Planung, Institute können SMTP nutzen

Sophos & Notebooks

Notebooks bewegen sich auch außerhalb des Uni-Netzes
⟶ wie externe Rechner konfigurieren

- Update-Server `sophosupd1.rrzn` ist überall erreichbar
- derzeit zu installieren per Offsite-Installer
- bestehende LUH-interne-Konfig (`luhsau.exe`) lässt sich umstellen
  - (Update-)Konfiguration steht in einer Ini-datei (Text)
    `C:\Programme\Sophos\AutoUpdate\Config\iconn.cfg`
  - Nicht-Änderbarkeit in GUI ist nur Konfig-Einstellung
    `AllowLocalConfig = 0` (auf 1 umeditieren)

Sophos

Problem

Zentrales Monitoring der (Signatur-) Update-Verteilung (welcher Client ist nicht mehr versorgt) ist ein ungelöstes Problem.

zu beachten

Nur einige Mitarbeiter des RRZN sind für den Sophos-Support eingetragen & berechtigt, bitte immer erst das RRZN kontaktieren (Sicherheit, User-Support) und nicht selbst den Sophos-Support.

WSUS

- zentrale Bereistellung von Patches
  - schneller Download im Uni-Netz
  - reduziert Traffic
- umfasst auch MS-Zusatzprodukte wie Office
- aber nur für deutsch & englisch
- Deployment via Gruppenrichtlinien, Installer oder Registry

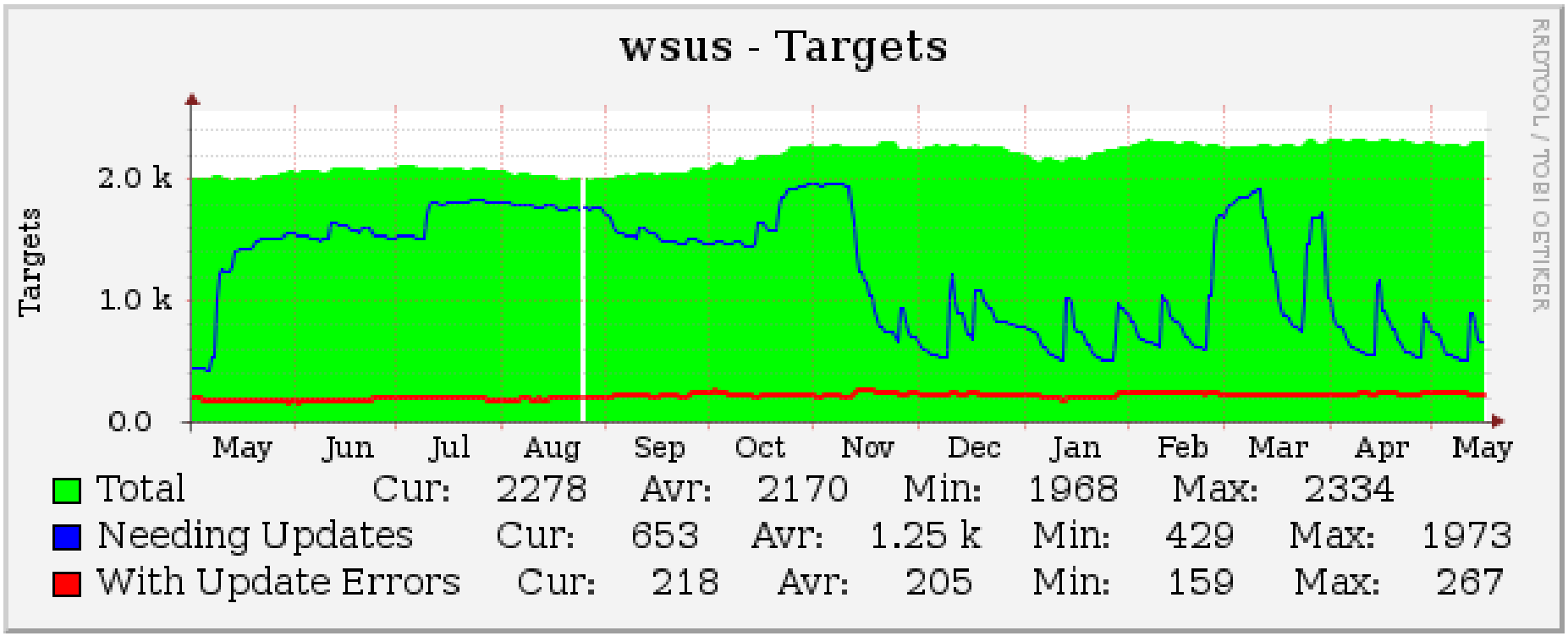
Reporting

Zentrales Monitoring der Patchstände ist wahrer Vorteil. Reportzustellung zu OU-Admins steht leider nochimmer aus.

http://www.rrzn.uni-hannover.de/its_sus.html

R|R|Z|N

WSUS-Clients in der LUH



XP-SP3 wurde wg. Problemen mit Zenworks erst verspätet freigegeben (Plateau von Mai bis November) ... und man erkennt die Patchdays

Zahl der Rechner mit Fehlern ist zu hoch! Zu wenige WSUS-Nutzer.

R|R|Z|N

alte SUS-Nutzer

- Umstellung von SUS auf WSUS war Ende 2005,
  aber trotz mehrfacher Ankündigungen über verschiedene Kanäle …
- nochimmer gibt es Clienten, die SUS-nutzen wollen
- fiel nun durch Zufall in Apache-Logs auf
  - SUS-Anfragen laufen auf Sophos-Update-Server auf:
  - Wir haben bis zu diesem Zeitpunkt nicht an Auswertemöglichkeit gedacht, das aber am 2.2.09 nachgeholt und alle Betroffenen per Mail verständigt.
  - Einige haben nicht reagiert, SUS-Anfragen gibt es nochimmer.
- 3 Jahre keine Patches:
  Eigentlich müsste man diese Rechner umgehend sperren …

Windows-Updates & Notebooks

Der WSUS-Dienst ist nur aus dem LUH-Netz erreichbar, kommt für Notebooks daher nicht in Frage.

- Nutzen Sie WSUS nicht für Notebooks, verlassen Sie Sich nicht auf regelmäßigen Netzkontakt / VPN-Nutzung.
- Aktivieren Sie die automatische Update-Suche.
- Je nach Nutzer: aktivieren Sie das automatische Einspielen der Updates oder verpflichten Sie den Nutzer.

Einstellungen eigentlich wie bei WSUS, aber ohne Setzen eins Update-Servers, vgl. Registry oder Richtlinien-Doku auf RRZN-Webseite
http://www.rrzn.uni-hannover.de/wsus_gpo.html

R|R|Z|N

Update von Nicht-MS-Software

Lage

- wohl größte Bedrohung beim Surfen etc.: Adobe-Reader, Flash, Video-Codecs & -Programme, Java, ...
- zunehmend eigene Update-Routinen, aber nicht immer
- kein zentrales Patchmanagement (durchführen, monitoren)

Lösung

- zentrale Softwareverteilung
  - schwierig, Aufwand
  - ganz schwierig für Notebooks, die länger außerhalb des LANs
- Nutzer einweisen & dazu anhalten (ebenfalls schwierig)

Backup

Der Sicherheitsvorfall kann immer eintreten, Vorbereitung mildert Auswirkung.

Backup

Die eigentlichen Daten müssen in ein Backup (z.B. Angebot des RRZN), schwierig für Notebooks.

disaster recovery

meint etwas anderes als Backup: Wiederherstellung der Rechner-Funktionalität. Ist nicht unbedingt für einfache Clients / Setups nötig, bewusst entscheiden.

Proben Sie das Restore: Keiner will Backup, alle wollen Restore

R|R|Z|N

„mündiger Nutzer“

überspitzt

Bei aller Technik bleibt das größte Sicherheitsproblem der Nutzer:

- Er kennt die Gefahren nicht oder ignoriert sie.
- Er ist kreativer als der Programmierer oder Admin vorher denkt.
- Er will ein Ziel erreichen, Sicherheit stört dabei.

Aufklärung

ist die größte Aufgabe, die

- hauptsächlich dezentral in den „OUs“ erfolgen muss,
- vom RRZN nur mittelbar angegangen werden kann.