IT-Sicherheit

Folgerungen aus dem Lovsan-Vorfall

21.9.2003, Dietrich Mönkemeyer, D4

Übersicht

- Schwachstelle(n) und Wurm
- Vorfall
- Infektionsweg
- Lehren
- Maßnahmen

Schwachstelle und Wurm

- DCOM-Schwachstelle (MS Bulletin MS03-026)
  - Buffer Overflow Schwachstelle im Windows-Betriebssystem
  - Ausführung beliebigen Codes im RPC Interface möglich
  - Betroffen: XP, W2000, W2003, WNT
- Wurm W32Blaster/W32Lovsan (McAfee)
  - nutzt DCOM-Schwachstelle aus
  - sucht über TCP Port 135 einen angreifbaren Rechner
  - bringt ihn dazu, das Wurm-Programm per tftp vom angreifenden Rechner zu laden
  - Verbreitet sich weiter und verursacht Re-Boots
- Wurm verschont bisher NT-Rechner

Angriff und Abwehr

16.7. MS veröffentlicht Schwachstelle und stellt Patch zur Verfügung

20.7. Patch in neuer Domain via Software Update Service installiert

12.8. Wurm mit DCOM-Exploit im Internet

- Vormittag: Wurm-Warnung von BSI und CERT
- Mittag: Aufforderung von D4, den Virenscanner zu aktualisieren
- Abend: Wurm im internen Netz

12.- 15.8.

- Virenscanner-Updates (ab DAT 4283 wird der Wurm erkannt)
- Patch Installation auf XP und W2000-Rechnern der alten Domain
  - von Laufwerk S:\ (ab 12.8.)
  - per Netinstall-Paket (ab 15.8.)

20.8. Netinstall-Paket auch für WNT

Angriff und Abwehr

- Seit 15.8. regelmäßige Scans
  - Netinstall (XP-Rechner)
    - Patch installiert ?
    - Von Lovsan- oder Nachi-Wurm befallen ?
  - MS-Tool KB823980Scan (alle Rechner)
    - Patch installiert ?
  - Einzelbehandlung der XP-Rechner ohne Patch und/oder mit Wurm
- Seit 12.9. DESY ist zeitweise wurmfrei aber immer noch vereinzelt Rechner mit dem Nachi-Wurm

Weitere Bedrohungen

11.9. Bekanntgabe weiterer DCOM-RPC-Schwachstellen (MS03-039)
- Zwei ermöglichen Ausführung beliebigen Codes
- Eine ermöglicht „Denial of Service“ Angriff
- Bisher kein Wurm bekannt

Information der Administratoren

Bereitstellung der Patches auf Laufwerk S:\

Bereitstellung des Patch Scan-Tools auf Laufwerk S:\

12.9. Neue Domain: Automatische Installation per SUS

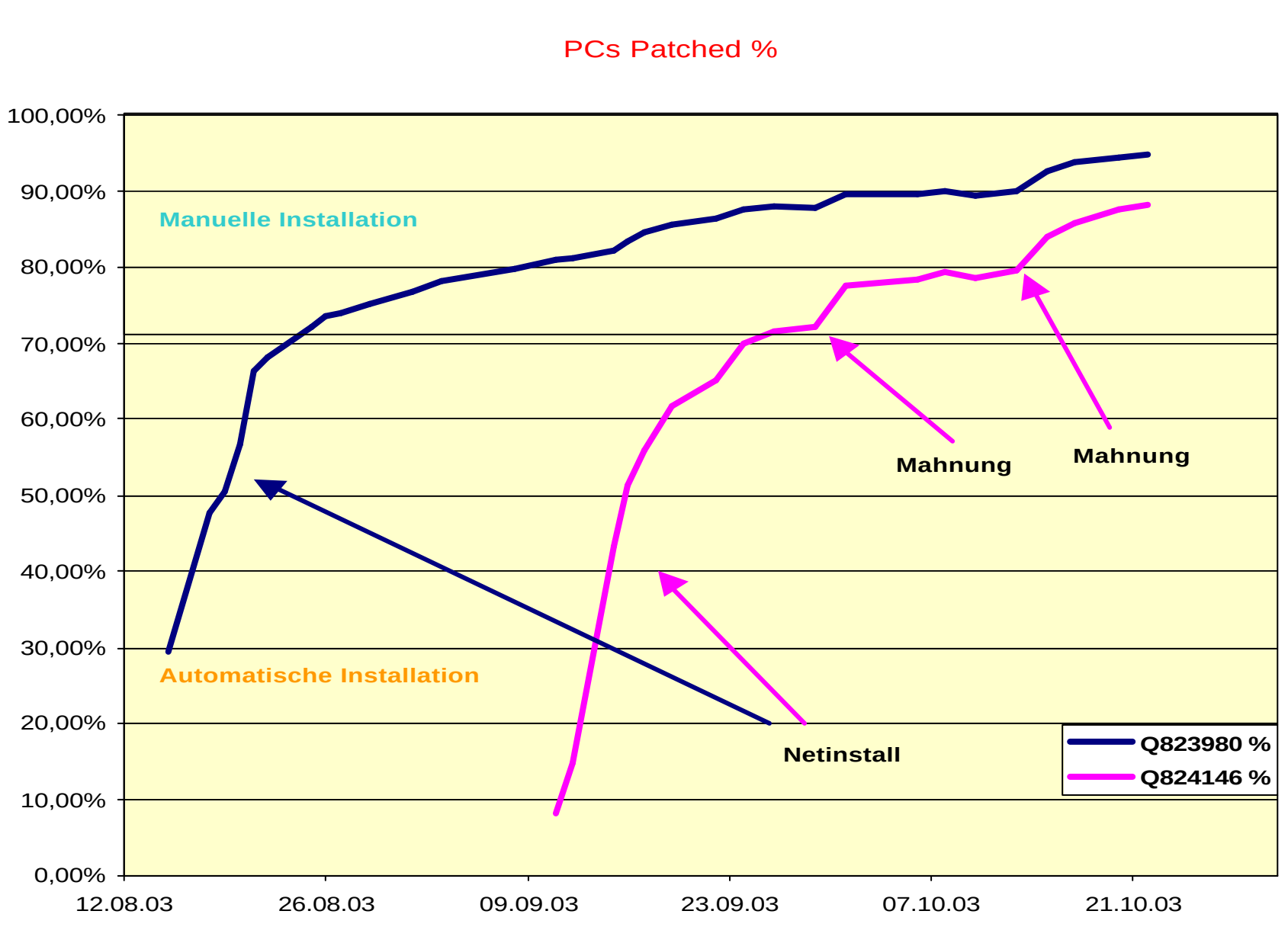
Alte Domain: Automatische Installation per Netinstall auf XP-Rechnern

Regelmäßige Scans aller Windows-Rechner und Bereitstellung der Ergebnisse unter: group/sys/groupadmin/Security Scans

15.9. Automatische Installation per Netinstall auf NT-Rechnern

10.10. Quellcode für Exploit im Internet, soll universell bei mehreren Windows-Versionen funktionieren.

10.10. XP SP1 hat angeblich weitere (von MS noch nicht veröffentlichte) DCOM-Schwachstellen (Multi-Threat Race Condition)


PCs Patched %
100,00%
90,00%
80,00%
70,00%
60,00%
50,00%
40,00%
30,00%
20,00%
10,00%
0,00%
12.08.03
26.08.03
09.09.03
23.09.03
07.10.03
21.10.03
Manuelle Installation
Automatische Installation
Mahnung
Mahnung
Netinstall
Q823980 %
Q824146 %

Infektionsweg

- Firewall schützte uns von außen
  - DCOM-Ports waren geschlossen
- Umgehung war möglich durch Einbringen von verseuchten Rechnern ins Intranet
  - Laptop
  - VPN
  - Maxbox

Defizite

Netzwerk-basierende Sicherheit reicht nicht mehr aus

Durchlöcherung des Netzwerkschutzes

- Schon lange durch Disketten und CDs
- Jetzt massiv durch Laptops, VPN-Zugang etc.

Netzwerksicherheit als

- Erst- oder Notmaßnahme
- Ergänzung einer host-basierenden Sicherheit

Host-basierende Sicherheit unterentwickelt

Probleme

- Fehlende Informationen
- Vielfalt an Software (-ständen)
- Automatische Installationsverfahren nur für Teilbereiche
  - Netinstall
  - Neue Domain (Software Update Service)

Defizite

Ineffiziente Wartungs-Methoden behindern schnelles Reagieren

Rechner sind vielfach auf einem alten und insgesamt sehr unterschiedlichen Software-Stand

- XP-Rechner mit deutscher Version (Probleme bei automatischer Patch-Installation)
- Viele NT-Rechner benötigen ein neueres Service Pack (NT Patch setzt SP 6 voraus)

Software Update ist schwerfällig, langsam und ineffektiv

- Ca. 100 Administratoren müssen mitwirken
- In kleinen Gruppen fehlt es oft an Know How
- Dezentrale Windows-Struktur stößt an ihre Grenzen

Kurzfristige Maßnahmen

Sicherheitsstandard von Rechnern, die auch mit fremden Netzen verbunden werden, verbessern

- Laptops, die auf Reisen waren und danach direkt ans Intranet angeschlossen werden
- Laptops oder Desktops, die z.B. auf Reisen oder von zu Hause Zugang zum Internet hatten und sich danach per VPN oder Maxbox mit dem Intranet verbinden

Aktueller Softwarestand inkl. Sicherheits-Patches

Aktueller Virenscanner mit Tages-aktuellen Signaturen

Personal Firewall (in fremden Netzen zu aktivieren)

Kurzfristige Maßnahmen

Virenschutz verbessern

- Mailserver

  Alle Mailserver mit Virenscannern ausstatten

- Anordnung bzgl. Virenscannern auf PCs

  auf allen Windows-PCs muss ein aktueller Virenscanner mit Tages-aktuellen Signaturen aktiviert sein

  es ist unzulässig, ihn eigenmächtig zu deaktivieren

  eventuelle Ausnahmen sind mit D4 abzusprechen

- Voraussetzung: umfassendes Betriebskonzept für den Einsatz von Virenscannern

Kurzfristige Maßnahmen

Wichtige Rechner gesondert sichern

Sicherheits-Patches zeitnah einspielen

Soweit wie möglich Abschottung gegen den Rest des Intranets

Informationsstand verbessern

Alle Rechner inkl. Software erfassen (*AMS*?)

Regeln für Rechner im Intranet erlassen

Werden vom RSR in Kürze verabschiedet

Mittel- und langfristige Maßnahmen

Ordnung schaffen

Rechner-Klassen definieren

- jeweils definierter Stand von Hardware und (Basis-) Software (z.B. Bürorechner, Kontroll-Rechner, Laptops etc.)
- Erleichtert auch das Austesten von neuen Versionen, Patches etc.

Automatische Update-Verfahren auf breiter Basis

Software Update Service für Betriebssystem inkl. IE (verfügbar in Windows-2003 Domain)

Netinstall für Applikations-Software

Migration in Windows-2003 Domain vorantreiben

- Alle Rechner mit *Netinstall* ausstatten
- Alle Rechner mit *AMS* scannen

Mittel- und langfristige Maßnahmen

Windows Struktur und Software Update
Zusammenspiel IT und Administratoren

Einheitliche Bereitstellung von Software Update-Verfahren durch IT

Durchführung von Software Updates für *Betriebssystem* und *Standard-Applikationen* zentral durch IT in Absprache mit den Gruppen-Administratoren

- für kleine Gruppen (zbau, zmx, d0x, l00, pr, w50 etc.)
- für Standard-Rechner (Bürorechner, Laptops etc.)

Software Updates für Nicht-Standard Rechner durch die jeweiligen Gruppen mit den von IT bereitgestellten Verfahren

Rechner nach Klassen ordnen und in dedizierten Subnetzen anschließen

- Spezifischer Netzwerkschutz möglich

Kompetente Gruppen-Administratoren erforderlich

Gruppen sind zuständig und verantwortlich

Informationen an zentraler Stelle

Gruppen-Administratoren als Ansprechpartner für Gruppenmitglieder und IT unverzichtbar

Restrisiko

- Gäste im internen Netz
- Rechner mit externem Zugang
- Großflächige Härtung hilft
  - In vielen Fällen können sich nur die unsicheren gegenseitig gefährden
  - Trotzdem: Szenarien mit großem Schadenspotential sind denkbar
  - Deshalb: Zahl unsicherer Rechner muss so klein wie möglich gehalten werden