

Sicherheit für Windows-Clients

Winfried Naumann

w.naumann@cms.hu-berlin.de

Viren und Würmer verschlingen unsere Arbeitszeit. An diesem Problem kommt (fast) keiner mehr vorbei – nicht als PC-Benutzer, Techniker oder Server-Administrator:

Viele, die verantwortungsbewusst mit dem Thema Sicherheit umgehen, müssen die Suppe auslöffeln, die von anderen angerichtet wurde. Für einen Teil der PC-Benutzer ist das Thema mit dem Satz »ich habe keine Geheimnisse auf meinem PC« schon erledigt. Eine andere Gruppe glaubt, keine Zeit zu haben, sich um die Sicherung ihres PCs zu kümmern. Eine weitere Gruppe (häufig dort zu finden, wo IT-Entscheidungen zu treffen sind) glaubt, da könnte der (nebenamtliche) DV-Beauftragte des Instituts mal ab und zu ein Auge darauf werfen oder das sei überhaupt eine Aufgabe, die nur im CMS gelöst werden könnte. Aber alle verlangen die sofortige Behebung des Schadens, wenn ihr eigener PC betroffen ist. Träumereien, Gedankenlosigkeit, Ignoranz – wesentliche Voraussetzungen für die enorme Wirksamkeit der Schädlinge.

Was alles passiert, wenn ein PC durch Viren oder Würmer infiziert wird:

- Daten aus der täglichen Arbeit (Texte, Präsentationen, Mess-Ergebnisse, Planungen, Bestellungen) werden gelöscht, verfälscht oder an beliebige Empfänger verschickt. Einige Mitarbeiter/innen tragen hier besondere Verantwortung, weil ihnen Personaldaten oder Forschungsdaten von Industriepartnern anvertraut sind.
- Nachdem Ihr infizierter PC fleißig Spam verschickt hat und dabei als Absender E-Mail-Adressen aus Ihrem Adressbuch verwenden konnte, werden die Eigentümer dieser Mail-Adressen nun mit Nachrichten überhäuft, in denen behauptet wird, sie hätten virenverseuchte E-Mails verschickt. Danke, Mail-Partner!
- Der infizierte PC wird als Zwischenlager für gecrackte Software, raubkopierte Filme, Kinderpornos, gestohlene vertrauliche Dokumente u. a. missbraucht oder in internationale Tauschbörsen eingebunden, ohne dass Sie es wissen. Mit den Adressen derart manipulierter PCs wird gehandelt. Können Sie in so einem Fall beweisen, dass Sie das Material nicht selbst auf Ihren PC heruntergeladen haben?

- Ihr PC ist der Ausgangspunkt für Angriffe auf andere PCs oder Server im Internet, bei denen Spam an Millionen von Empfängern verschickt wird, Daten gelöscht, gestohlen oder Server lahmgelegt werden. Bei den Nachforschungen der Betroffenen oder der Ermittler stellt sich heraus, dass der Angriff von Ihrem PC bzw. einem PC der Universität ausging. Wie viel Schadensersatz könnten Sie oder die Universität der betroffenen Firma zahlen? Wie lange könnten Sie auf Ihren PC zu Hause verzichten, wenn die Polizei ihn zur Beweissicherung eingezogen hat?

Sie haben Recht. So etwas ist Ihnen noch nicht zu Ohren gekommen. Einige Dinge passieren noch zu selten. Bisher hat es eher nur dazu geführt, dass Ihr DV-Beauftragter weniger Zeit für andere Aufgaben hatte, weil er Viren entfernen, PCs neu installieren und Dateien wiederherstellen musste. Glauben manche Benutzer wirklich, Administratoren müssten ihnen Viren beseitigen, die sie sich unzweifelhaft auf Servern mit Sex-Seiten eingefangen haben? Ihr Institut arbeitet noch mit Banyan VINES? Solche Probleme vergeuden Arbeitszeit der Administratoren, die ihnen für die Vorbereitung der Umstellung fehlt.

Da es in diesem Beitrag nicht um Polemik sondern um den praktikablen Umgang mit dem Problem Sicherheit gehen soll, nun die Lösungsvorschläge:

Auf allen Ebenen muss etwas getan werden, damit das HU-Netz und der Übergang zum Internet für alle Beteiligten sicherer wird: am PC des Benutzers, im lokalen Netz des Institutes, auf den zentralen Servern und an den Übergangspunkten (Gateways) zum Internet. Ganz bewusst habe ich mich auf Maßnahmen beschränkt, die wenig Zeitaufwand und kein besonderes Fachwissen erfordern oder bereits gut beschrieben wurden. Weitere Verbesserungen sind auf jeden Fall möglich, erfordern aber deutlich mehr Kenntnisse und mehr Zeit beim Anwender oder mehr Unterstützung durch den DV-Beauftragten.

Die Benutzer und ihre PCs bzw. Notebooks

Es gibt einfache Maßnahmen, die wenig Aufwand verlangen, aber die meisten Bedrohungen von den Rechnern fernhal-

ten. Die gehören für jeden Benutzer im HU-Netz zum Pflichtprogramm.

7 Regeln für grundlegende Sicherheit (Stufe 0):

- Halten Sie Ihr Windows-Betriebssystem und Ihre Anwendungen (z. B. Browser, Office-Software) auf dem aktuellen Stand. Auch in Programmen wie Winzip oder Acrobat Reader gab es gefährliche Sicherheitslücken. Updates schließen solche Lücken. Der Rechner wird weniger angreifbar. Systeme ab Windows 2000 Service Pack 3 können automatisch aktualisiert werden (zurzeit nur Sicherheits-Updates), wichtige Updates für Microsoft Office findet man bei *Office Update* [1].
- Installieren Sie einen Virens Scanner: Die Software McAfee VirusScan Enterprise 7.1 kann auf jedem PC im Campus-Netz der HU installiert werden [2]. Schalten Sie den On-Access Scan (Scannen beim Zugriff auf Dateien) ein und lassen Sie die Dateien mit den Virendefinitionen (DAT) täglich automatisch aktualisieren [3].
- Führen Sie regelmäßig (mindestens einmal pro Woche) auf allen Festplatten Ihrer PCs einen gründlichen Virentest durch (automatisierbar).
- Konfigurieren Sie Ihr Mailprogramm so, dass Anhänge (*Attachments*) oder Nachrichten im HTML-Format nicht automatisch geöffnet werden. Öffnen Sie nur E-Mails oder Anhänge von bekannten, vertrauenswürdigen Absendern und nur dann, wenn die Nachricht mit großer Wahrscheinlichkeit von dort stammen könnte (Absender werden oft gefälscht). Siehe z. B. c't-Emailcheck [4].
- Speichern Sie keine Passwörter auf Ihrer Festplatte, sei es auch noch so bequem (z. B. automatische Anmeldung beim Betriebssystem, bei der Einwahl von zu Hause, im Mailprogramm, beim Online-Banking, ...). Solche Passwörter werden von schädlichen Programmen leicht ausgelesen und dann für weitergehende Angriffe missbraucht. Benutzen Sie keine einfachen Passwörter!
- Eigentlich selbstverständlich: Meiden Sie wenig vertrauenswürdige Server im Internet (Cracker-/Warez-Sites, Sex-Seiten). Beteiligen Sie sich nicht an File-sharing-Netzen.

- Installieren Sie nur Software, die Sie wirklich (und längere Zeit ...) brauchen und die lizenziert ist. Widerstehen Sie den Verlockungen durch CDs aus irgendwelchen Zeitschriften.

Regeln für verbesserte Sicherheit (Stufe 1):

Die folgenden Vorschläge erfordern einige Änderungen in der Arbeitsweise. Der relativ geringe Aufwand lohnt sich, wenn der PC dafür sicher bleibt:

- Benutzen Sie die in Ihrem Browser gebotenen Möglichkeiten zur sicheren Konfiguration: Blocken Sie Pop-up-Fenster, erlauben Sie die Nutzung von Skriptsprachen nur vertrauenswürdigen Sites. Nutzen Sie verschlüsselte (SSL-) Verbindungen, wenn sie angeboten werden. Siehe u. a.: c't-Browsercheck [5].
- Konfigurieren Sie den Spam-Filter Ihres Mailprogramms oder wechseln Sie zu einem Programm, das diese Funktion enthält (z. B. Mozilla Mail). Viren und Spam treten immer häufiger zusammen auf.
- Arbeiten Sie auf Ihrem Rechner nicht als Mitglied der Administrator-Gruppe, sondern höchstens als Mitglied der Gruppe *Hauptbenutzer* (nur Installationen und manche Konfigurations-Änderungen erfordern Administrator-Rechte). Alle Schädlinge haben sonst die gleichen (Administrator-) Rechte wie Sie. Einige wenige Anwendungen werden möglicherweise nicht mehr richtig funktionieren wollen (weil die Hersteller sich nicht an die Standards halten). Es gibt jedoch die einfache Möglichkeit, nur diese Anwendungen dann unter dem Administrator-Account zu starten – das minimiert die Risiken erheblich. Lassen Sie sich von Ihrem Administrator zeigen, wie das geht.

Die Administratoren der Institute und ihr Netz

6 einfache Regeln:

- Betreiben Sie nur solche Dienste und Server, für deren Betreuung Sie ausreichendes Wissen, genügend Zeit und eine Vertretung haben. Benutzen Sie sonst die zentralen Angebote des CMS oder verzichten Sie auf diesen Dienst! Sicherheit erfordert kontinuierliche Administration (z. B. das rechtzeitige Einspielen von Sicherheits-Updates, die Überwachung der verschiedenen Logs auf dem Server), keine einmalige Installation! In jede Projektplanung gehören Kosten für die Administration der benötigten Computer und Dienste!
- Planen Sie neue Dienste und Server mit Mitarbeitern des CMS. Lassen Sie sich

vorher beraten, auch bei der Hardware-Beschaffung.

- Installieren Sie alle Computer (Arbeitsplatz-Rechner *und* Server) inklusive Sicherheits-Updates und Virens Scanner *offline* – d. h. ohne Anschluss an das Netzwerk. Viele Rechner werden schon während der Installationsphase infiziert.
- Halten Sie sich an die Installations-Empfehlungen des CMS.
- Versuchen Sie, auf allen Arbeitsplatz- Rechnern Ihres Verantwortungsbereiches die grundlegenden Sicherheits-Einstellungen durchzusetzen (Stufe 0, siehe oben).
- Benutzen Sie nur dann Administrator-Rechte, wenn sie unbedingt erforderlich sind! Arbeiten Sie sonst mit gewöhnlichen Benutzerrechten. Administrieren Sie nur von Computern der Stufe 1 (siehe oben).

Zentrale Dienste im CMS

Maßnahmen, die zur Verbesserung der Sicherheit eingeführt wurden oder geplant sind:

- Sperrung des Zugangs zu allen nicht benötigten Ports (von außerhalb des HU-Netzes). Der Blaster-Wurm gelangte im Sommer des letzten Jahres also nicht über Netzverbindungen ins HU-Netz, sondern wurde mit Notebooks eingeschleppt.
- Betrieb eines zentralen Spam-Filters [6].
- Bereitstellung von Patch-Prozeduren, die die Offline-Installation der Server und Clients erleichtern (für Windows-Server vorhanden, für Windows-Clients geplant).

Alle Anstrengungen für mehr Sicherheit im HU-Netz sind nur wirksam, wenn auf allen genannten Ebenen Verbesserungen erreicht werden. Die Nutzung der verfügbaren technischen Mittel würde die Sicherheit unserer PCs und unseres Netzes schon deutlich verbessern. Das Problem mit den Viren, Würmern und anderen Schädlingen ist aber mit technischen Mitteln allein nicht zu lösen. Nur die Kombination aus technischen Maßnahmen und vernünftiger Arbeitsweise ist erfolgreich. Ist an einer Stelle eine Einstellung vergessen worden oder konnte ein Sicherheits-Update aus Zeitmangel noch nicht eingespielt werden, dann sorgen in der Regel die anderen Maßnahmen dafür, dass kein oder nur geringer Schaden entsteht.

Gibt es weniger unsichere Computer im Netz, gibt es auch weniger Risiken und mehr störungsfreie Arbeitszeit.

Noch einmal ganz deutlich: die Zugänge aus dem Internet und die zentralen Server werden so konfiguriert und überwacht, dass Schädlinge eigentlich nicht in unser Netz gelangen könnten. Warum passiert es trotzdem?

Die drei *wichtigsten* Ursachen:

- Benutzer öffnen unüberlegt zweifelhaftes Mailanhänge oder HTML-Mails *und* haben außerdem keinen aktivierten oder aktuellen Virens Scanner *und* keine Sicherheits-Updates eingespielt (fast immer kommt es nur in dieser Kombination zum Schaden!).
- Die Verbreitung von Notebooks hat zugenommen. Manche wählen sich zu Hause über die Netzverbindungen anderer Provider ein und überlassen ihr Gerät Familienmitgliedern oder Freunden zum Spielen, zum Surfen, um E-Mails abzurufen usw. – und das wiederum mit deaktiviertem oder veraltetem Virens Scanner. Die eingefangenen Schädlinge nimmt man dann unter den Arm und trägt sie ins HU-Netz.
- Es werden Server beschafft bzw. installiert, für deren Administration man weder Mittel noch Zeit hat. Weil diese Server nach der Installation sich selbst überlassen bleiben, werden sie häufig nach einiger Zeit erfolgreich angegriffen und attackieren dann weitere Rechner – leider die typische Entwicklung vieler Projekte.

Für die eben genannten Probleme gibt es keine (oder nur sehr restriktive) technische Lösungen. Auch die Empfehlung von Personal Firewalls für PCs wäre nicht hilfreich. Wir müssen die Sicherheitsprobleme zur Kenntnis nehmen und unsere Arbeitsweise darauf einstellen.

Literatur

- [1] <http://office.microsoft.com/officeupdate/default.aspx>
- [2] <http://amor.cms.hu-berlin.de/software/nai/> (nur HU-intern)
- [3] <http://amor.cms.hu-berlin.de/software/nai/#win7auto>
- [4] <http://www.heise.de/security/dienste/emailcheck/>
- [5] <http://www.heise.de/security/dienste/browsercheck/>
- [6] Schmidt, B.: Spam-Abwehr – Möglichkeiten und Grenzen. (in diesem Heft)