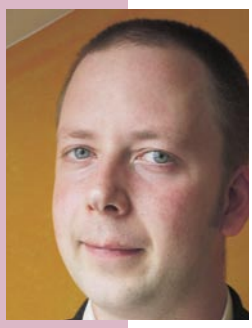
Informations- oder Gefahrenquelle?

Internet am Arbeitsplatz – aber sicher!

Dror-John Röcher, Heidelberg

Die Nutzung des Internets im Unternehmen ist nicht mehr wegzudenken; zu vielfältig sind die Möglichkeiten, die sich bieten: Kommunikation mit Geschäftspartnern und Kunden per E-Mail, Wareneinkauf weltweit, Recherche zu aktuellen Themen und Problemen oder auch Verkauf eigener Leistungen und Waren über die Firmen-Webseite oder über Online-Plattformen. Doch die Nutzung des Internets hat nicht nur handfeste Vorteile, sondern bringt auch Gefahren mit sich, die zum Teil ganz erhebliche Kosten nach sich ziehen können.

zum Autor



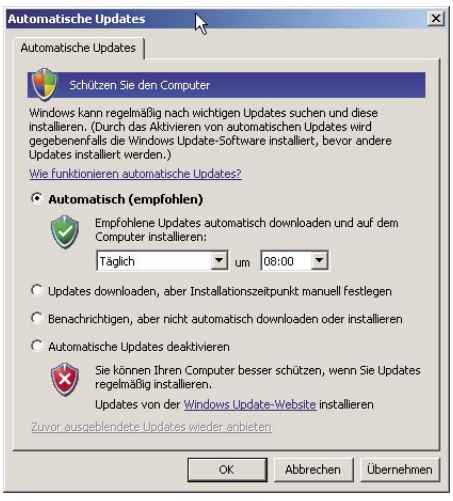
Dror-John Röcher, *Senior IT-Security Consultant bei ERNW – Enno Rey Netzwerke GmbH, Heidelberg. Seine Arbeit umfasst die Erstellung von Sicherheitskonzepten, die Implementierung von IT-Security-Maßnahmen und die Auditierung von IT-Umgebungen u.a. durch gelenkte Penetrations-Tests (Hacking)*

Ein gestohlenes ebay-Passwort oder gestohlene Online-Banking-Zugänge können zum „Einkaufen auf fremde Kosten“ missbraucht werden, ein trojanisierter PC kann zum massenhaften Versenden von Spams benutzt werden und der Zeitaufwand ein viren- oder wurmverseuchtes Netzwerk zu reinigen kann, je nach Schwere der Infizierung und Anzahl der infizierten PCs, einige Manntage betragen.

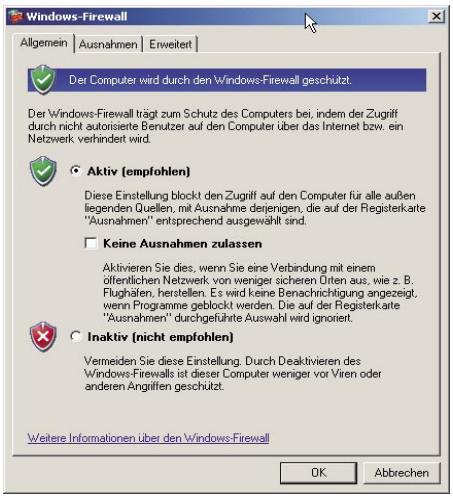
Diesen Gefahren ist der Nutzer aber nicht hilflos ausgeliefert: Mit einigen technischen und organisatorischen Maßnahmen lässt sich das Risiko bei der Benutzung des Internets ohne großen Aufwand und ohne tiefgehende Systemkenntnisse stark reduzieren. Die größten Gefahren und wie ihnen zu begegnen ist werden im Folgenden dargestellt.

Schadprogramm – Malware[1]

Unter dem Begriff „Malware[2]“ wird eine ganze Reihe unerwünschter Schadprogramme zusammengefasst: Computerviren, Würmer, Trojanische Pferde (Trojaner) und Spyware. Die Schadfunktion kann von „einfacher Verbreitung“ über „Ausspähen von sensiblen Daten“ (Passwörtern, Bankdaten, etc.), der „Installation einer Hintertür[3]“ oder „Versand von Spam“ bis zur „Manipulation oder dem Löschen von Daten“ reichen. **Computerviren** sind die älteste Form der Schadprogramme. Sie verbreiten sich, indem sie eine Kopie von sich selbst an Dateien anhängen – wird die infizierte Datei weitergegeben und auf einem PC ausgeführt, so wird der PC vom Virus befallen, die Schadroutine wird ausgeführt und weitere Dateien auf dem PC werden mit dem Computervirus befallen. **Würmer** hingegen verbreiten sich selbstständig aktiv über Computernetzwerke und befallen anfällige PCs ohne weiteres menschliches Zutun. **Trojanische Pferde** entstehen aus der Kombination eines interessanten oder nützlichen (oder scheinbar nützlichen) Wirtsprogramms mit einer versteckten Schadroutine, die häufig eine Hintertür oder Spyware im System installiert. Sobald ein Benutzer das Wirtprogramm installiert, wird im Hintergrund auch gleichzeitig die Schadroutine installiert. Dabei verbreitet sich der Trojaner nicht selbstständig, sondern „wirbt“ mit dem Nutzen des Wirtsprogramms, um sich zu verbreiten. **Spyware** zielt darauf, ab Informationen über den Benutzer zu sammeln (z.B. Passwörter, Bankdaten oder einfach „nur“ Verhaltensmuster) und weiterzugeben. Dabei verbreitet sich Spyware nicht aktiv selbst, sondern wird häufig als Schadroutine Trojanischer Pferde in Umlauf gebracht. **Adware** sind in der Regel kostenlose Programme, die sich über die Einblendung von Werbung finanzieren. Häufig ist eine werbefreie Version des Programms käuflich erhältlich. Adware wird oft als eine Form von Spyware klassifiziert, da nicht selten Informationen über das Benutzerverhalten gesammelt werden,



Automatische Updates bei Windows XP

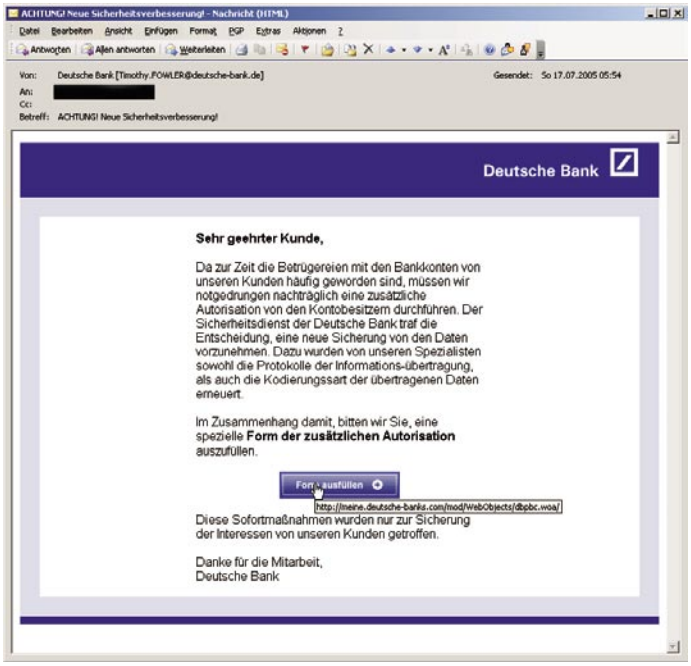


Einstellungen der Windows-Firewall

1 Die allgemeine Umgangssprache im Internet ist Englisch und auch die meisten Fachbegriffe stammen aus dem Englischen. Wenn möglich werden die deutschen Begriffe im Artikel bevorzugt und neben die englischen Begriffe gestellt.

2 Eine gute Übersicht über die Definition der verschiedenen Kategorien von Schadprogrammen im Internet bietet Wikipedia: http://de.wikipedia.org/wiki/Malware

3 Eine Backdoor oder Hintertür ermöglicht es einem Angreifer immer wieder mit speziellen Programmen auf den PC zuzugreifen und ihn komplett fernzusteuern. Dadurch ist es z.B. möglich neue oder weitere Schadfunktionen nachzuinstallieren. Siehe auch: http://de.wikipedia.org/wiki/Backdoor



Phishing-E-Mail. Der Link in der E-Mail führt auf eine Seite, die nicht zur Deutschen Bank gehört

Aktuelle Warnung über bösartige E-Mails mit Trojanern

um die Werbung zielgerichteter gestalten zu können. Ob Adware automatisch als Spyware zu klassifizieren ist, ist durchaus strittig.

Schadprogramme kommen auf verschiedenen Wegen auf den PC des Anwenders. Jede Datei, egal woher sie stammt, kann mit einem Virus verseucht sein. Insbesondere Programmen aus dubiosen Quellen im Internet sollte man grundsätzlich misstrauen, denn Trojaner und Spyware sind oft unerwünschte Begleiter solcher Programme. Würmer verbreiten sich selbstständig über das Internet oder über das Firmennetzwerk. Oft genügt es, dass ein unachtsamer Mitarbeiter einen Wurm einschleppt und in Windeseile sind alle Computer befallen.

E-Mail-Spam[4] und Phishing[5]

E-Mail-Spam hat sich zum aktuell größten Problem im Internet entwickelt. Dabei ist Spam nicht gleich Spam; eine Unterscheidung verschiedener Kategorien von Spam ist hilfreich bei der Abwehr von Spam. **Unverlangte Werbemails** (UCE) beinhalten Werbung im weiteren Sinn für Produkte (die oft „Wunder“ versprechen und in der Regel an die niederen Instinkte appellieren: dem Wunsch nach mehr „Manneskraft“ oder „Haarwuchs“, oder der „perfekten Figur“) oder dubiose Angebote, die häufig viel Geld für eine vergleichsweise geringe (und somit risikoarme?) Vorausleistung versprechen[6]. Neben diesen Werbemails werden häufig auch **Viren und Würmer** als Dateianhänge in Massenmails versendet, der Inhalt dieser E-Mails besteht oft aus so genannten „**Hoaxes**[7]“, die den Empfänger veranlassen sollen den Dateianhang zu öffnen, wodurch der PC des Benutzers infiziert wird.

Phishing-E-Mails sind eine moderne Version des Trickbetrugs, die versucht die Leichtgläubigkeit und Unwissenheit der Benutzer auszunutzen, um an vertrauliche Zugangsdaten (zum Onlinekonto, Login-Daten für ebay, etc.) zu gelangen. Phishing-E-Mails werden massenhaft versendet, in der Gewissheit, dass einige Menschen auf den Betrug hereinfallen werden. Die E-Mails scheinen z. B. von der eigenen Bank zu kommen, imitieren den Stil der Bank und sind häufig auf den ersten Blick nicht von echten E-Mails der Bank zu unterscheiden. Jede E-Mail, die von einem unbekannten Absender stammt, den Empfänger auffordert vertrauliche Informationen preiszugeben oder einen Link auf eine Website enthält ist grundsätzlich verdächtig. Auch im Internet gilt: Keiner möchte ihnen etwas schenken – erst recht kein Unbekannter.

Schutz vor Schadprogrammen

So schützen Sie sich vor Würmern:

Würmer nutzen zur Verbreitung Fehler in installierter Software aus; das können Fehler im Betriebssystem sein, aber auch Fehler in installierten Anwendungen oder Serverdiensten. Zwei technische Maßnahmen helfen dem Wurmbefall einen Riegel vorzuschieben: **Softwareaktualisierungen** und **Firewalls**.

Sobald Sicherheitslücken in einer Software bekannt werden, stellt der Hersteller in der Regel kurzfristig eine Aktualisierung (sog. „**Patches**“) bereit, die die Lücken schließen. Computer, die auf dem aktuellsten Softwarestand sind, sind weniger anfällig gegen Würmer, als PCs, deren Software nicht „gepatcht“ ist. Insbesondere ist es wichtig, dass das Betriebssystem selbst und der benutzte Browser auf dem aktuellsten Stand sind. Microsoft hat für die Windows-Betriebssysteme „Automatische Updates“ eingeführt, die das Betriebssystem automatisch aktualisieren. Der Computer sucht in vorgegeben Zeitintervallen auf http://windowsupdate.microsoft.com nach verfügbaren Aktualisierungen und untersucht, welche Aktualisierungen für den PC relevant sind. Die Funktion ist über die Systemsteuerung aufrufbar, die Einstellungen sollten so gewählt werden, dass der Computer täglich nach Aktualisierungen sucht und diese automatisch installiert. In kleineren Windows-Netzwerken bietet sich das kostenlose Programm „Microsoft Baseline Security Analyzer[8]“ an, welches alle PCs des Netzwerkes auf fehlende Patches untersucht. Neben dem Betriebssystem ist es wichtig Applikationen, die mit dem In-

4 SPAM („spiced ham“ – gewürzter Schinken) bezeichnet eine Marke für Dosenfleisch der Firma Hormel Foods Inc., Spam hingegen massenhaft zugesandte, unerwünschte (Werbe)-E-Mails. Der offizielle Begriff für Spam lautet „unsolicited bulk email“ (UBE – unverlangte Massenmail) bzw. „unsolicited commercial mail“ (UCE – unvererlangte Werbemail). Der Begriff Spam stammt aus einem Sketch der Comedy-Gruppe „Monty Pythons Flying Circus“.
Siehe auch: http://de.wikipedia.org/wiki/UBE

5 Phishing hat sich als Begriff mittlerweile auch im Deutschen etabliert. Dabei leitet sich der Begriff vom „Fischen“ (engl. Fishing) ab. Gefischt wird nach persönlichen Daten, die Ersetzung von „f“ durch „ph“ ist bei Hackern üblich.

6 In diesem Kontext hat sich die „Nigeria Connection“ eine besondere Stellung „erarbeitet.“ Eine typische „Nigeria-Connection“-E-Mail involviert große Geldbeträge (häufig mehrere Millionen USD) auf einem afrikanischen Konto, die der Absender der E-Mail (häufig ein Staatsbediensteter in hoher Stellung) nur mit Hilfe des Empfängers in den Westen transferieren kann. Als Entschädigung für die Mitarbeit werden dem Empfänger Anteile vom Gesamtbetrag in Aussicht gestellt. Eine schöne Zusammenfassung verschiedener Nigeria-Connection E-Mails findet sich unter http://www.nigeria-connection.de/ und auch das Auswärtige Amt weist mittlerweile auf die Nigeria-Connection hin: http://www.auswaertiges-amt.de/www/de/laenderinfos/419_html

7 Ein Hoax ist eine (sensationelle) Falschnachricht, ein aufregendes Gerücht oder auch eine (falsche) Virenwarnung. Siehe auch http://www.trendmicro.com/vinfo/hoaxes/default.asp

8 http://www.microsoft.com/technet/security/tools/mbsahome.mspx

ternet kommunizieren über Softwareaktualisierungen zu schützen. Insbesondere Browser (Internet Explorer, Netscape, Firefox, Opera) beinhalten immer wieder schwerwiegende Fehler, die es einem Angreifer ermöglichen, unbemerkt Schadprogramme auf dem PC des Benutzers zu installieren. Dazu ist oft nicht mehr als das reine Betrachten einer speziell vom Angreifer präparierten Webseite nötig[9]. Aber auch Anwendungen, die scheinbar nichts mit dem Internet zu tun haben, können als Einfallstor für Würmer dienen und sollten deswegen auf dem aktuellsten Stand gehalten werden. Mittlerweile hat fast jede Software eine „Auto-Update"-Funktion, und es ist dringend empfohlen, von dieser Funktion regen Gebrauch zu machen.

Grundsätzlich gibt es zwei Stellen, an denen **Firewalls** sinnvoll sind: Zum einen auf dem Router, der die Verbindung ins Internet herstellt und zum anderen auf jedem PC und Server. Die Firewall auf dem Router verhindert, dass Würmer übers Internet ihren Weg auf die PCs der Anwender finden. Fast alle gängigen DSL-Router bieten mittlerweile grundlegende Firewall-Funktionalitäten, die in der Regel ausreichen, falls keine eigenen Dienste im Internet publiziert werden (sollte dies der Fall sein, führt kein Weg an einer professionellen Firewall-Lösung herum). Dabei ist zu beachten, dass vom Router kein Verkehr aus dem Internet an die PCs weitergeleitet wird, es sei denn, es handelt sich um Antwortverkehr auf Anfragen, die von den PCs gestellt worden sind. So genanntes „Port-Forwarding[10]" und „statische NAT-Einträge", wie sie häufig vorgenommen werden, um besseren Durchsatz bei File-Sharing-Programmen oder Tauschbörsen[11] zu erreichen, bilden ein ideales Einfallstor für Würmer und sollten nicht eingerichtet werden. Windows XP bringt von Haus aus eine Firewall mit, die für die allermeisten Zwecke ausreicht und den PC schützt, falls sie konfiguriert und aktiviert ist.

So schützen Sie sich vor Viren:

Der beste Schutz vor Viren ist ein **Virenscanner** gepaart mit einem ehrlichen **Misstrauen gegenüber Dateien** unbekannter Herkunft. Viren verbreiten sich, weil Menschen zu unachtsam mit fremden Dateien umgehen und ohne nachzudenken beliebige E-Mail-Anhänge öffnen und alle möglichen Programme aus dem Internet auf ihren PCs installieren. Ein Virenscanner gehört heutzutage zur Grundausstattung eines jeden PCs – unabhängig davon ob der PC eine Verbindung zum Internet hat oder nicht. Doch der beste Virenscanner nützt nichts, wenn er nicht benutzt wird oder nicht aktualisiert wird. Mittlerweile bieten fast alle bekannten Virenscanner automatische Aktualisierungen der Virensignaturdateien, automatische, regelmäßige Überprüfungen des gesamten PCs und auch Untersuchungen der Postfächer der gängigen E-Mail-Clients (Outlook, Eudora, Netscape Mail, etc.). Wichtig ist weiterhin ein „Echtzeitschutz", der jede Datei beim Zugriff, z. B. im Windows Explorer, auf Viren überprüft. Diese Einstellung kann auf älteren PCs allerdings zu spürbaren Leistungseinbußen führen und sollte dort nur vorsichtig eingesetzt werden. Viele Virenscanner bieten mittlerweile weit mehr Funktionen als nur die Suche nach Schadprogrammen. Häufig sind mittlerweile Anti-Spam-Filter, Firewall-Funktionalitäten und Spyware-Suche in einem Produkt integriert[12].

So schützen Sie sich vor Spyware:

Spyware findet auf verschiedenen Wegen auf den PC eines Benutzers: Als unerwünschte Dreingabe bei der Installation von Software, in E-Mail-Dateianhängen oder auch über ungepatchte und schlecht konfigurierte Browser. Auch hier ist der wichtigste Schutz das eigene Verhalten: Keine unbekannten Dateianhänge öffnen und keine Hyperlinks aus E-Mails öffnen. Neben diesen Verhaltensregeln kann auch hier wieder mit Werkzeugen gegen Spionageprogramme und „Tracking Cookies[13]" vorgegangen werden. Aktuelle Virenscanner haben mittlerweile häufig Komponenten zur Aufspürung und Beseitigung von Spyware, doch gibt es auch spezialisierte Programme, die diese Aufgabe in der Regel besser erledigen. Besonders empfehlenswert ist das kostenlose Programm „**Spybot Search & Destroy**[14]".

So schützen Sie sich vor Trojanern:

Aktuelle Browser bieten mittlerweile weit mehr Möglichkeiten als „nur" unbewegliche HTML-Seiten anzuzeigen; Interaktion mit dem Anwender über „aktive" Inhalte (ActiveX, Java, JavaScript, etc.[15]) gehört mittlerweile zum „guten Ton" und wird vielmals auch von Anwendern erwartet – über spezielle Erweiterungen (Browser-HelpObjects oder Plug-Ins) lässt sich oftmals auch die Funktionalität der Browser erweitern, um zum Beispiel pdf-Dateien direkt im Browser anzeigen zu können. Allerdings beinhalten viele dieser aktiven Technologien große Sicherheitsrisiken. So können bösartig programmierte Webseiten den PC des Besuchers angreifen und dort Software installieren, die dem Betreiber der Webseite die volle Kontrolle über den PC ermöglicht. Anstatt diese Inhalte von allen Webseiten zu akzeptieren, sollte die **Browserkonfiguration** so angepasst werden, dass diese nur von vertrauenswürdigen (vom Benutzer als vertrauenswürdig eingestuft) Webseiten entgegengenommen werden. Eine detaillierte Anleitung zur sicheren Konfiguration aktueller Browser findet sich unter http://www.heise.de/security/dienste/browsercheck/anpassen/.

9 Der Heise-Zeitschriftenverlag, Herausgeber der C't und IX, hat unter http://www.heise.de/security/dienste/browsercheck/ eine Browser-Online-Überprüfung, die den Browser des Benutzers auf aktuelle Sicherheits-Probleme überprüft.

10 http://de.wikipedia.org/wiki/Port_Forwarding

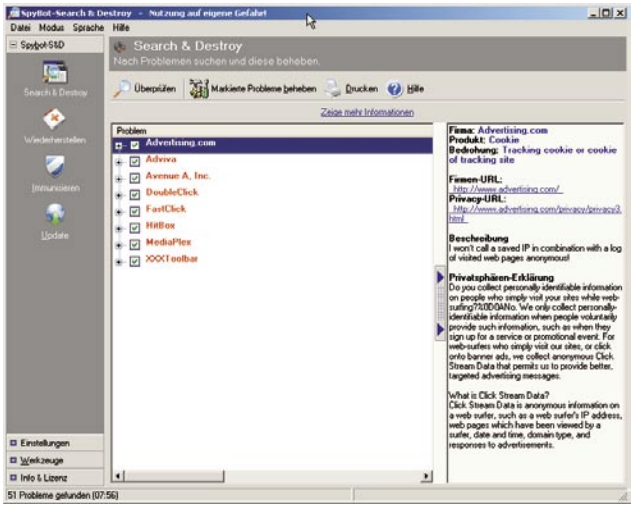
11 Tauschbörsen ermöglichen das direkte „Teilen" oder „Tauschen" von Dateien zwischen (fremden) Anwendern. Dazu werden Verbindungen zwischen den PCs der Teilnehmer hergestellt, die ein so genanntes „peer-to-peer" Netzwerk bilden. Neben den rechtlichen Aspekten, die beim Tausch z.B. geschützter Software oder Musik eine Rolle spielen, werden Dateien in diesen Netzwerken häufig absichtlich infiziert um Schadprogramme möglichst schnell und weiträumig zu verteilen.

12 Aktueller Test zu 11 Antivirus-Produkten: http://www.chip.de/artikel/c1_artikel_15037118.html

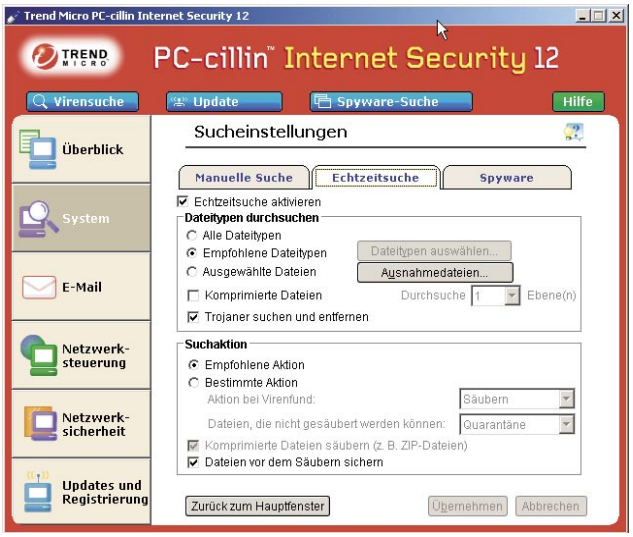
13 http://www.computer-greenhorn.de/cookies.htm

14 http://www.spybot.info/

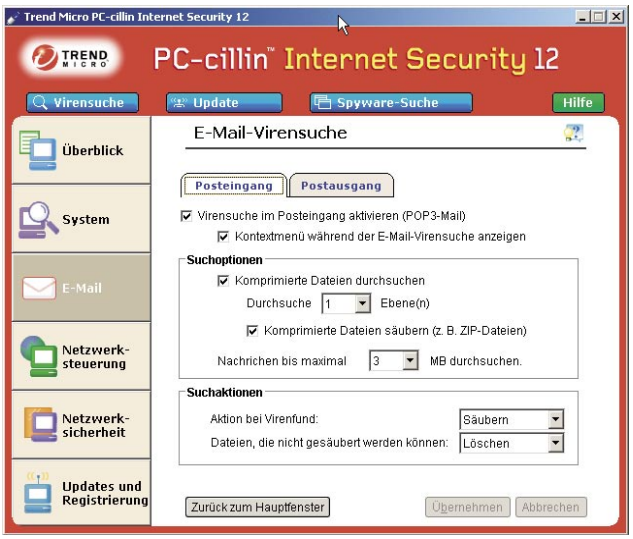
15 Überblick über „aktive Inhalte": http://www.bsi-fuer-buerger.de/browser/02_03.htm



Spybot S&D findet Spyware und entfernt sie vom PC



Die Echtzeitsuche eines Virenscanners untersucht Dateien bei jedem Zugriff auf Viren



Die E-Mail-Virensuche untersucht alle ankommenden und ausgehenden E-Mails nebst Anhängen auf Viren

Trojaner finden aber auch über vom Benutzer installierte Programme auf den PC – deswegen sollte grundsätzlich keine Software aus nicht vertrauenswürdigen Quellen eingesetzt werden. Die großen Softwarehersteller können in diesem Kontext als vertrauenswürdig angesehen werden.

Zum Umgang mit E-Mail

E-Mail ist eines der großen Einfallstore für Schadprogramme und die Flut an unerwünschter Werbung und Phishing-E-Mails nimmt täglich zu. Eine technische Maßnahme zur Reduzierung der täglichen Spamflut besteht in der Installation einer Filtersoftware, die die ankommenden E-Mails automatisch untersucht und Spam entweder direkt löscht oder in einen separaten Ordner verschiebt. Viele Virenscanner bringen mittlerweile Spamfilter mit; anstatt die E-Mails lokal auf dem PC des Benutzers zu filtern, bietet sich in Unternehmen die Installation eines zentralen Spamfilter[16] auf dem E-Mail-Server an.

Neben dem Filtern kann aber jeder Benutzer durch sein Verhalten aktiv daran mitwirken, dass er wenig(er) Spam erhält. Einige wichtige Regeln zum Umgang mit E-Mail und der eigenen E-Mail-Adresse:

- Die E-Mail-Adresse nicht zur Registrierung für Mailinglisten, Gewinnspiele, etc. benutzen, wenn der Anbieter keine eindeutige Aussage zum Umgang mit den gespeicherten Daten trifft. Die Datenschutzgesetze in Deutschland sind im Vergleich zu ausländischen Gesetzen sehr restriktiv. Deswegen gilt besondere Vorsicht bei ausländischen Angeboten – viele „Info-Angebote“ dienen unter anderem dem Sammeln und Vermarkten von gültigen E-Mail-Adressen.
- Niemals auf „Abmelde“-Links in Spam-E-Mails klicken. Diese Links dienen nur der Verifikation gültiger E-Mail-Adressen. Eine derart „validierte“ E-Mail landet in Spam-Datenbanken und wird anschließend mit noch mehr Spam überhäuft.
- E-Mails nicht im HTML-Format anzeigen lassen. In HTML-Mails können Bilder integriert sein, die beim Betrachten von einem Server im Internet nachgeladen werden. Der Server registriert diesen Vorgang und validiert auf diese Weise gültige E-Mail-Adressen.
- Niemals auf einen Link in einer E-Mail klicken, die eine Phishing-E-Mail sein könnte. Links in Phishing-E-Mails verweisen auf gefälschte Seiten, die die Original-Seiten nachbauen, um den Benutzer zur Eingabe von Usernamen und Passwort zu verleiten. Beim Online-Banking z. B. immer die Adresse der Bank von Hand im Browser eintragen oder die Lesezeichen-Funktion des Browsers verwenden.
- Niemals Anhänge von unbekannten Absendern öffnen. Diese Anhänge können mit Schadprogrammen verseucht sein, die beim Ausführen den PC infizieren.
- Anhänge immer vor dem Öffnen auf Viren untersuchen. Dies gilt auch für Anhänge, die von Freunden oder Kollegen kommen; Viren unterscheiden nicht zwischen „Freund und Feind.“

Fazit

Mit der Kombination einiger technischer Maßnahmen und Verhaltensweisen ist die Benutzung des Internets auch für technische Laien auf einem hohen Sicherheitsniveau möglich. Insbesondere sollten ein Virenscanner (nebst aktuellen Signaturen), eine Anti-Spyware-Software und eine Firewall auf jedem PC installiert sein. Viele Produkte vereinen diese Funktionalitäten mittlerweile in einer einzelnen Anwendung, wodurch sich die Wartung und die Benutzung vereinfacht. Zusätzlich müssten das Betriebssystem und die installierten Anwendungen regelmäßig aktualisiert werden.

Die Benutzer sollten im Umgang mit der Sicherheits-Software geschult werden und für das Thema „Sicherheit im Internet“ und „Umgang mit E-Mail“ sensibilisiert werden. ■

16 Wenn der E-Mail-Server von einem Provider betrieben wird, so bietet der Provider in der Regel gegen eine geringe Gebühr die Installation und Wartung eines zentralen Spamfilters an. Wenn der E-Mail-Server im eigenen Unternehmen betrieben wird, kann dort ein Spamfilter & zentraler E-Mail-Virenscanner installiert werden.