user

MAGAZIN April 2005

Sonderausgabe zur user KONFERENZ 2005

user - Das Anwendermagazin des AUGE e.V. - Der Verein der Computeranwender

user KONFERENZ 2005

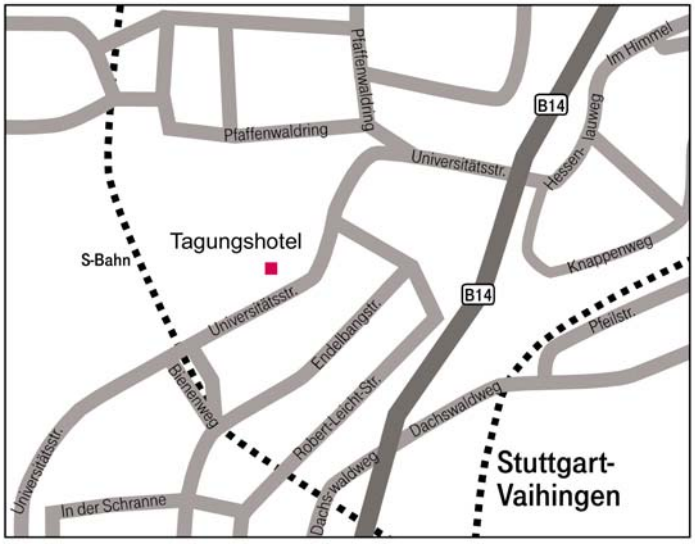
IT Sicherheit - Wen kümmert's?

Samstag, 9. April 2005

Deutsche Telekom
Tagungshotel Stuttgart

Universitätsstraße 34
70569 Stuttgart

Beginn um 14:00 Uhr
Ende gegen 19:30 Uhr



Eine Veranstaltung des AUGE e.V. anläßlich seiner Mitgliederversammlung.

Vortragsprogramm:

➢ **Begrüßung und Einführung**	AUGE e.V.
➢ **Sicherheit unter Linux**	Adrian Reyer LinuxHaus Stuttgart
➢ **WLAN Sicherheit**	Reyk Flöter .vantronix | secure systems GmbH
➢ **Sicherheit im Unternehmen**	NN Internet Security Systems Deutschland
➢ **Daten sichern mit Images**	Heinz Rothkegel AUGE e.V. M2374
➢ **Verschlüsseln und signieren** *Public Key Verfahren verstehen und anwenden*	Michael Schäl AUGE e.V. M6115

user - Das Anwendermagazin des AUGE e.V.

Sonderheft zur user KONFERENZ 2005, 09. April 2005

Das USER MAGAZIN ist eine Publikation des AUGE e.V. und dient der Kommunikation und dem Informationsaustausch innerhalb des Vereines sowie der Erfüllung der Ziele des Vereines. Mitteilungen des Vereines an die Mitglieder, die im USER MAGAZIN veröffentlicht werden, gelten als ordnungsgemäß zugestellt im Sinne der Satzung (unter Wahrung der jeweils geltenden Fristen). Dies gilt auch im Falle einer elektronischen Publikation.

Herausgeber:

AUGE e.V. – Der Verein für Computeranwender
Wielandstr. 41, 60318 Frankfurt/Main
Tel. 069/59795813, Fax 069/552004
E-Mail buero@auge.de, Web http://www.auge.de/

Der AUGE e.V. wird durch seinen Vorstand (E-Mail vorstand@auge.de) vertreten. Namentlich gekennzeichnete Beiträge – so weit es sich nicht um Mitteilungen eines Vereinsorganes handelt - geben stets die Meinung des Autors wieder, nicht die des Vereines; eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion vom Herausgeber nicht übernommen werden. Sämtliche Veröffentlichungen erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes, Warennamen und –zeichen werden ohne Gewährleistung einer freien Verwendung benutzt.

Redaktion:

Redaktion USER MAGAZIN c/o AUGE e.V.
Wielandstr. 41, 60318 Frankfurt/Main
Tel. 069/59795813, Fax 069/552004
E-Mail redaktion@auge.de

Heinz Rothkegel, M2374 (Redaktion)
Michael Welz, M7108 (Layout und Titelbild)
Michael Schäl, M6115 (Layout)

Mit Übergabe der Manuskripte, Abbildungen, Programmlistings etc. an die Redaktion erklärt der Autor, daß er mit einer Veröffentlichung in den Publikationen des AUGE e.V. einverstanden ist und daß sämtliche Materialien frei von Rechten Dritter sind. Der Autor wird insbesondere den Herausgeber von allen Ansprüchen Dritter aus Urheberrechtsverletzungen freihalten, sofern kein eindeutiges Verschulden des Herausgebers vorliegt. Für unverlangt eingesandtes Material wird keine Haftung übernommen. Die Redaktion behält sich das Recht vor, Beiträge zu kürzen, sie auf mehrere Ausgaben zu verteilen oder ggf. auch ganz abzulehnen. Ein Recht der Mitglieder auf Veröffentlichung ihrer Beiträge besteht nicht. Es gilt die jeweils aktuelle Honorarregelung des Herausgebers. Die Richtlinien für Autoren sind unbedingt einzuhalten.

Erscheinungsweise und Redaktionsschluß:

Das USER MAGAZIN erscheint in unregelmäßigen Abständen, je nach Erfordernis. Die Publikation kann entweder durch Versand einer gedruckten/vervielfältigten Ausgabe auf Papier erfolgen oder durch ein elektronisches Medium (Versand einer CD-ROM, Bereitstellung einer Datei zum Download im Web, Versand einer E-Mail). Redaktionsschluß ist in der Regel zwei Wochen vor dem geplanten Erscheinungstermin.

Anzeigen:

Anzeigen in den Publikationen des AUGE e.V. werden nur akzeptiert, soweit sie die Unabhängigkeit des Vereines, seine Ziele und den Grundsatz der Gemeinnützigkeit nicht berühren. Kleinanzeigen von Mitgliedern des AUGE e.V. werden kostenlos veröffentlicht.

INHALTSVERZEICHNIS - AUSGABE April 2005

Magazin

Sicher ist sicher . . . ……...……..…..…… 4
(Florian Delonge, M6285 / Vorsitzender)

IT Sicherheit – Wen kümmert´s? .....…...… 5
(Heinz Rothkegel M2374)

Aktiver Verbraucherschutz – Reg TP ……..… 6
(Manfred Küster, Reg TP)

Spyware – Erkennen und Entfernen …....….……... 7
(Martin Retsch, perComp-Verlag)

Linux – Trügerische Sicherheit ……...….……... 13
(Peter Klein, F-Secure)

Schutz vor Stealth-Viren und Rootkits ……..……... 15
(F-Secure)

True Image 8.0 für Workstations ….……...…..… 16
(Acronis)

Schütze dein eLife ……...……...…..… 17
(Symantec)

Virtual Private Network …….....…… 18
(Thorsten W. Stritzinger, M4066)

Sonstiges

user KONFERENZ 2005 …….....…….. 2

Impressum und Inhaltsverzeichnis ..……..…..…… 3

Aufnahmeantrag .....…….…… 23

Die ausrichtenden Regionalgruppen laden ein ...…. 24

Sicher ist sicher...

Ein Geleitwort von Florian Delonge (M6285), Vorsitzender des AUGE e.V.

In diesem Jahr bietet der AUGE e.V. nun schon zum vierten Mal mit der USER KONFERENZ eine Informationsveranstaltung für Computer-Anwender an, in der ein aktuelles Thema übergreifend über verschiedene Rechnersysteme und Betriebssysteme von verschiedenen Seiten beleuchtet und hinterfragt wird. Dabei ist es ist sicher kein Zufall, dass wieder einmal die Sicherheit der Datenverarbeitung zum zentralen Thema gewählt wurde.

Die Verbreitung ist inzwischen so weit fortgeschritten, dass ein Computer im Haus zum normalen, alltäglichen Gebrauchsgegenstand geworden ist. Diese an und für sich erfreuliche Entwicklung, die ja auch ganz im Sinne der Arbeit des AUGE e.V. ist, hat allerdings auch ihre Schattenseiten. Die Selbstverständlichkeit, mit der heute Computer gebraucht werden, sei es zum Surfen im Web, zum Schreiben von Briefen und Texten, oder auch einfach nur zur Unterhaltung mittels des neuesten Computerspiels, hat auch eine gewisse Gedankenlosigkeit zur Folge, die über tatsächlich vorhandene Risiken leicht hinwegtäuscht.

Wer denkt beim Einschalten eines Rechners denn jedes Mal an die möglichen Gefahren durch Viren, Würmer oder Hacker-Angriffe? Die intuitive Bedienbarkeit, die heute berechtigterweise für Gebrauchsgegenstände – auch technische – gefordert und meist auch realisiert wird, führt andererseits dazu, dass die Gebrauchsanleitung kaum noch gelesen wird und warnende Hinweise auf mögliche Gefahren gar nicht mehr wahrgenommen werden. Das mag bei einem Gerät wie z.B. einem DVD-Player noch relativ unproblematisch sein, bei einem Computer – insbesondere mit Internet-Anschluss, der heute ja die Regel darstellt – kann das fatale Folgen haben.

In Versuchen wurde ermittelt, dass ein Computer, wie er heute schon bei fast jedem Lebensmitteldiscounter um die Ecke mit dem üblichen vorinstallierten Einheitsbetriebssystem günstig erworben werden kann, der ohne weitere Maßnahmen mit dem Internet verbunden wird, innerhalb von weniger als einer halben Stunde von sogenannter „Schadsoftware“ (Malware) befallen wird. Die Zeitspanne, die man benötigt, um den Rechner mit allen notwendigen Sicherheitsupdates und Patches auszustatten, ist aber meist deutlich größer! Dies stellt selbst Computerfachleute manchmal vor Probleme, der normale Anwender ist häufig komplett überfordert.

Da braucht man sich nicht zu wundern, dass nach Computerviren und Würmern, Spyware und Phishing-Attacken nun ein neues Schreckgespenst die Runde macht: Die sogenannten BotNets. Dabei werden Computers mit einer Software „infiziert“, die den Rechner von außen steuerbar macht. Die Ausbreitung erfolgt in der Regel mit Hilfe von Viren bzw. Würmern. Die sogenannten „Zombie-Rechner“ werden dann in Netzwerken, eben den BotNets, zusammengeschaltet und für bestimmte Zwecke eingesetzt, ohne dass der Besitzer des Rechners dies bemerkt. Die Anwendungen reichen vom Versenden von SPAM bis hin zu DoS-Attacken (Denial of Service durch gezielte Überlastung z.B. einer Website). Durch das sogenannte „Honeynet“ Projekt wurden über 100 aktive BotNets festgestellt, die teilweise bis zu 50.000 Rechner umfassten. Die Gesamtzahl der betroffenen Rechner wird auf über eine Million geschätzt.

Aber nicht nur ahnungslose Anwender werden befallen – auch die Kenner der Materie sind nicht völlig sicher. Wer hat nicht schon einmal den Download des neuen Sicherheits-Updates oder auch den laufenden Virenscan abgebrochen, wenn es mal wieder zu lange gedauert hat und dringende Aufgaben zu erledigen waren? Leichtsinn ist neben Unkenntnis die größte Gefahr für die IT-Sicherheit.

Was kann man also tun, um sich gegen derartige Angriffe zur Wehr zu setzen? Gesundes Misstrauen und stete Vorsicht werden gerne empfohlen, natürlich aktuelle Antivirensoftware und Updates des Betriebssystemes. Das ist sicher alles richtig. Was gerne vergessen wird, ist eine aus der Landwirtschaft bestens bekannte Tatsache: Jede Monokultur fördert die Verbreitung von Schädlingen. Man sollte sich also ruhig einmal Gedanken darüber machen, ob es zur üblichen Standard-Software nicht auch Alternativen gibt. Das geht mit dem Betriebssystem los (wie wäre es mit dem MacOS-Betriebssystem des Apple Macintosh oder mit einer der zahlreichen Linux-Distributionen, deren Verbreitung immer weiter zunimmt?) und reicht über das Office-Paket (OpenOffice ist sogar kostenlos) bis hin zum Browser (Firefox!) und Mail-Client (Thunderbird!). Ein anderer guter Rat, der hier gegeben werden kann, gilt der Netzwerkverbindung. Wer eine breitbandige Internetverbindung, z.B. DSL, direkt mit einem Rechner verbindet, der öffnet nicht nur eine Hintertür, sondern gleich ein ganzes Scheunentor für unerwünschte Eindringlinge. Ein Router mit NAT und integrierter Firewall ist nicht nur sicherer, sondern auch komfortabler. Und wer ein drahtloses Netzwerk benötigt, der sollte es auf jeden Fall auch entsprechend absichern.

Kurz gesagt: Über IT-Sicherheit kann man sich gar nicht früh genug und ausführlich genug Gedanken machen. Zum Glück gibt es ja viele Möglichkeiten, sich ausführlich zu informieren, z.B. beim Regionaltreffen oder auf der USER KONFERENZ des AUGE e.V.!

In diesem Sinn bleibt dann eigentlich nur noch übrig, den Organisatoren für ihr Engagement zu danken und den Besuchern eine interessante Veranstaltung zu wünschen!

IT Sicherheit – Wen kümmert´s?

von Heinz Rothkegel , M2374

Unsere erste User-Konferenz im April 2002 stand unter der Überschrift „Datensicherheit“. Damals ging es uns darum, die EDV-Anwender für verschiedene Aspekte dieses wichtigen Themas zu sensibilisieren. Seither ist innerhalb des Vereins auf RG-Treffen und in unserem Internet-Forum immer wieder darüber diskutiert worden. Und auch ich selber, der ich seinerzeit das Thema vorgeschlagen hatte, sehe täglich neue Herausforderungen aus diesem Bereich auf mich zukommen.

Hersteller von Anti-Viren-Programmen geben oft mehrmals täglich neue Signatur-Updates heraus. Und dann kommen neue Hiobs-Botschaften: „Viren, Würmer etc. – ja, das ist schon lästig, aber das haben wir inzwischen ganz gut im Griff. Was viel gefährlicher ist, ist Spyware. Bei manch einem Spyware-Programm, das wir auf einem Testrechner installieren, wissen auch wir nicht, wie wir es wieder los werden sollen.“ Wenn man eine solche Aussage auf einer Tagung von einem hochqualifizierten Anti-Viren-Experten hört, rutscht einem zunächst einmal das Herz in die Hose. Zumindest mir ging das so.

Als nächstes fragte ich mich: „Und jetzt? Wie kann ich meine eigenen PCs und die meiner Kunden so einrichten, daß im Fall des Falles nicht der komplette Datenverlust mit unabsehbaren Folgen droht?“ Ich entschloß mich zum Einsatz von Programmen wie „Norton Ghost“ oder „Acronis TrueImage“. Damit ist es tatsächlich sehr einfach möglich, Images (also Abbilder) der Festplatte zu speichern, die man im Fall des Falles sehr schnell wieder einspielen kann, und zwar bootfähig. Das Backup läßt sich so einrichten, daß es im Hintergrund stattfindet, wenn gewünscht im Stunden-Rhythmus.

Natürlich ist es besser, vorzubauen und es gar nicht erst soweit kommen zu lassen. Ohne Anti-Viren-Programm und eine, wie auch immer geartete, Firewall sollte sich niemand mehr ins Internet trauen. Und regelmäßig Sicherheits-Patches zu installieren, kann man auch nur jedem raten. Aber welcher Anwender ist denn so kompetent und konsequent, das wirklich bestmöglich durchzuführen? Und selbst wenn, dann lauern direkt die nächsten Gefahrenquellen.

Da schickt mir ein Freund eine Email: „Schau mal, was ich Tolles entdeckt habe! Im Anhang steht mehr.“

Wer platzt da nicht vor Neugier und öffnet umgehend den Anhang? Und tatsächlich, das ist wirklich lustig, was da zum Vorschein kommt. Das muß man direkt an weitere Freunde und Bekannte weiterschicken.

Man mag mich nun für kleinlich halten, aber bei einem solchen Szenario, was durchaus nicht selten ist, sträuben sich mir sämtliche Nackenhaare! Nicht, daß ich irgendeinem meiner Freunde irgend etwas Böses unterstellen wollte, aber woher soll ich wissen, aus welcher Quelle er die lustige Mail hat? Ist diese Quelle vertrauenswürdig? Oder wird da gerade der Versuch unternommen, mir unter dem Deckmantel der Harmlosigkeit etwas unterzuschieben, was ich nicht nur nicht will, sondern was mir früher oder später üble Probleme bereiten wird? Denn alle bisher erwähnten Schutz-mechanismen (AV-Programm, Firewall, Sicherheits-Patch, etc.) greifen an dieser Stelle nicht!

Folgende Fragen stellen sich hier:
- Ist mein Freund wirklich der Absender dieser Mail, oder ist schlichtweg die Adresse gefälscht?
- Ist der PC meines Freundes tatsächlich der Absender dieser Mail, aber mein Freund weiß gar nichts davon, weil sein PC vielleicht mit irgendeinem Virus o.ä. verseucht ist, der eigenständig Mails verschickt.
- Hat mein Freund, blauäugig wie er ist, mir eine „lustige“ Mail weitergeleitet, ohne sich Gedanken über die Vertrauenswürdigkeit der Quelle zu machen?

Man mag mich für kleinlich halten, aber ich traue an dieser Stelle zunächst mal Niemandem! Denn die Kriminalitätsquote im Internet wächst ständig, und die Tricks der Kriminellen (anders kann man es nicht bezeichnen) werden immer raffinierter. Auch ich erwische mich bisweilen dabei, daß ich die eine oder andere Mail öffnen will, weil sie doch erstmal harmlos wirkt. Zum Glück habe ich mich bisher an den richtigen Stellen immer rechtzeitig zurückhalten können.

Denn die Sache kann nicht nur technisch äußerst unangenehm werden. Die Rechtslage ist heute so, daß derjenige, der seinen PC nicht ausreichend gegen Mißbrauch schützt und dadurch (mehr oder weniger unbeabsichtigt) zur Schadensquelle wird, für den entstehenden Schaden in Regreß genommen werden kann. Nicht genug damit, daß man selber Opfer geworden ist und Streß und Kosten hat, seinen eigenen Rechner wieder ans laufen zu bekommen, man wird auf diese Weise auch noch ungewollt zum Täter, mit allen sich daraus ergebenden Konsequenzen.

Aber es gibt auch gute Nachrichten: in den letzten Monaten hat sich die Rechtslage, was die beiden Themen SPAM und Dialer angeht, deutlich zu Gunsten der Verbraucher entwickelt. Und die Organisation, die die Rechte der Verbraucher unbürokratisch aber dennoch mit Nachdruck durchsetzt, ist niemand Geringeres als die „Regulierungsbehörde für Telekommunikation und Post“ (Reg TP).

Auch wir, der AUGE e.V. haben uns in den letzten Jahren immer wieder bei den zuständigen Stellen dafür stark gemacht.

Aktiver Verbraucherschutz - RegTP

von Manfred.Küster, Regulierungsbehörde für Telekommunikation und Post, Bonn

Die Regulierungsbehörde für Telekommunikation und Post hilft dem Verbraucher, bei der Wahrung seiner Rechte.

Unverlangte Werbung/ SPAM

Viele Verbraucher fühlen sich von unverlangter Werbung über elektronische Medien, auch Spam genannt, belästigt. Die Regulierungsbehörde für Telekommunikation und Post (Reg TP) kann unter bestimmten Voraussetzungen beim Abstellen dieser von Vielen als Plage angesehenen Werbung helfen.

Häufig werden Rufnummern über unterschiedliche elektronische Medien mit dem Ziel beworben, letztlich einen Rückruf durch den Verbraucher auf die beworbene Rufnummern zu provozieren. Oftmals handelt es sich bei den offen oder versteckt beworbenen Rufnummern um hochpreisige Rufnummern u.a. in den Bereichen (0)190/(0)900 und 0137, an deren Rückruf der Angerufene verdient.

Unverlangt zugesandte Werbemitteilungen stellen in der Regel einen Verstoß gegen das Gesetzes gegen den unlauteren Wettbewerb (UWG) dar, so dass ein zivilrechtlicher Unterlassungsanspruch besteht. Die Reg TP hat aufgrund des neuen Telekommunikationsgesetzes (TKG) die Befugnis gegen eine derartige, rechtswidrige Bewerbung von Rufnummern vorzugehen. Hierbei differenziert die Reg TP hinsichtlich des Zugangs der unverlangten Werbung derzeit nach vier Medien:

- Telefax
- SMS (auf Handy bzw. Festanschlüsse)
- E-Mail (über das Internet an PC's)
- Ping-Anrufe

Bei Ping-Anrufen wird gezielt nur ein einmaliges Rufzeichen übertragen und danach die Anwahl umgehend beendet. Dies reicht aus, um über die sogenannte Clip-Funktion z. B. eine hochpreisige Mehrwertdiensterufnummer zu übertragen. Diese Rufnummer wird automatisch in die Liste der entgangenen Gespräche eingetragen und soll zu einem Rückruf provozieren.
Erlangt die Regulierungsbehörde von derartigen Sachverhalten z. B. in Form von schriftlichen Beschwerden Kenntnis, ergreift sie Maßnahmen gegenüber den Letztverantwortlichen und den Netzbetreibern, in deren Netzen die entsprechenden Rufnummern geschaltet sind. Vorrausetzung dafür ist eine Bewerbung einer Rufnummer und es darf keine geschäftliche Beziehung zum Absender bestehen bzw. keine Erlaubnis zur Werbung erteilt worden sein. Neben Abmahnungen und Abschaltungsanordnungen der Rufnummer gegenüber den Netzbetreibern erlässt die Regulierungsbehörde in verschiedenen Einzelfällen auch gegenüber dem jeweiligen Inhalteanbieter Unterlassungsverfügungen.
Teilweise erfolgen die Abschaltungen bereits im Rahmen des Anhörungsverfahrens auf freiwilliger Basis durch die Netzbetreiber.
Die Reg TP hat seit August 2003 zahlreiche Abschaltungen von Rufnummern zur Bekämpfung von Spam durchgeführt. Eine Liste der ergriffenen Maßnahmen ist auf der Interseite www.regtp.de veröffentlicht. Voraussetzung für das Einschreitens der Reg TP ist die gesicherte Kenntnis der rechtswidrigen Nutzung von Rufnummern.

Die Reg TP kann natürlich nur eingreifen, wenn sie Kenntnis eines Verstoßes hat. Sollten Sie also außerhalb einer Geschäftsbeziehung und ohne vorher dem Absender Ihre Zustimmung erteilt zu haben über die o. a. Medien unverlangte Werbung, die Sie belästigt erhalten haben und wollen, dass die RegTP im Rahmen ihrer Möglichkeiten hiergegen einschreitet, dann senden Sie uns bitte Ihre aussagekräftigen Unterlagen, an folgende Fax-Nummer: 06321 - 934-111 oder an die Email-Adresse: Rufnummernspam@regtp.de

Dialer

Bei einem Dialer handelt es sich um ein automatisches Anwählprogramm, mit dem bestimmte entgeltpflichtige Dienstleistungen im Internet abgerufen werden können. Weil es in diesem Bereich auch zu Intransparenz und damit zu Missbrauch kommt, hat die Reg TP zum 17. März 2005 nochmals Ihre Regelungen im Bereich Dialer verschärft und damit den Verbraucherschutz gestärkt. Das vor der Herstellung der kostenpflichtigen Verbindung auf dem Bildschirm zu erscheinende Dialer-Zustimmungsfenster wird nunmehr neu für alle Dialer-Anbieter allgemeinverbindlich und graphisch detailliert festgelegt. Weiterhin ist es jetzt verpflichtend, auch in den Zustimmungsfenstern vor Download und Installation/Aktivierung des Dialers den Preis für die Inanspruchnahme anzugeben und es darf keine Kostenfreiheit suggeriert werden. Nicht zuletzt dürfen sich Dialer aufgrund der neuen Reg TP-Vorgaben nicht mehr ohne Zustimmung des Nutzers von dessen Rechner entfernen. Für konkrete Hilfe bei Dialernutzern hat die Reg TP ein Call-Center eingerichtet, dass Sie unter Telefon: 0291 99 55 206 tagsüber erreichen können.

Ausführliche Informationen über die Hilfe durch die Reg TP und Ihre Rechte bei Rufnummernmissbrauch haben wir für Sie in unserer Broschüre **„regtp facts Was tun bei Rufnummernmissbrauch?“** zusammengestellt. Diese Broschüre können Sie im Internet von unserer Homepage www.regtp.de herunterladen, oder als kostenloses Heft bei unserem Druckschriftenversand bestellen:

Telefon: 0361 7398-272, Telefax: 03617398-184,
E-Mail: Druckschriften.Versand@regtp.de

Spyware – Erkennen und Entfernen

von Dipl. Inform. M.Retsch, perComp-Verlag GmbH

Dienstleistungen wie z.B. E-Mail-Service und Software wurden im Internat anfangs kostenlos angeboten. Mit der Zeit kamen schlaue Zeitgenossen auf die Idee, Geld dadurch zu erwirtschaften, indem die kostenlos zur Verfügung gestellten Dienste und Programme mit Werbung gespickt wurden. Schnell sprach sich herum, dass auf diese Art und Weise nicht unerhebliche Mengen Geld zu verdienen waren. Hierdurch entwickelte sich eine ganze Industrie, die mit Adware und Spyware versuchte mehr oder weniger gezielt an Kundeninformationen zu gelangen. Diese wurden anschließend gewinnbringend vermarktet. Laut einer Analyse von Benjamin Edelman wurden im Jahr 2004 allein in die 4 größten Spyware-Software-Firmen in den USA knapp 140 Millionen $ investiert [1]. Auch wenn der eigene PC nur einer von vielen Millionen im Internet ist und die Angriffe auf Ihn inklusive der damit verbundenen Datenverluste selten persönlich zu verstehen sind, können die Folgen der Datenspionage sehr wohl mit persönlichen Konsequenzen verbunden sein.

Spyware ist kein neues Problem. Beispielsweise gibt es Keylogger zum Ausspähen von Passwörtern schon lange. Diese mussten früher vom Spion jedoch manuell und heimlich auf dem Zielrechner installiert und die gesammelten Daten später auf die gleiche Weise wieder über direkten Zugriff abgeholt werden. Für eine weite Verbreitung solcher "Malware" war dies natürlich hinderlich.

Aber wozu gibt es das Internet, mit dessen Hilfe sich Spyware bequem verteilen lässt und die gesammelten Informationen bequem frei Haus geliefert werden? Die AOL/NCSA Online Safety Studie von Oktober 2004 [2] aus den USA zeigt auf, dass inzwischen 80% aller privat genutzten PCs mit Spyware und Adware befallen sind. Zwischen Dezember 2003 und September 2004 verzeichnete das Computer Associates Security Advisory Team einen Anstieg der Spywaremeldungen von ca. 500 % [3]. Beide Quellen belegen, dass Spyware und Adware inzwischen ein ernst zu nehmendes Problem sind.

Definition von Spyware und deren Einordnung

Grob gesagt ist *Spyware* jede Art von Software, welche die Internetverbindung eines Benutzers im Hintergrund (den sogenannten “Backchannel”) ohne sein Wissen und ausdrückliche Genehmigung nutzt [4].

Spyware kann allgemein mit Spionage-Software übersetzt werden. Diese Software besteht meist aus mehreren Komponenten, welche ohne Kenntnis und Zustimmung des Computerbenutzers Informationen und Daten über diesen oder dessen Verhalten auf dem PC sammeln und an eine dritte Person oder Institution (den Initiatoren der Software) weiterleiten. Die gesammelten Informationen können z.B. Tastatureingaben, benutzte Programme, Daten über angewählte Web-Seiten und deren Besuchsdauer, E-Mails, Passwörter und PIN-Daten, Kreditkarteninformationen und Informationen aus dem Instant Messenger beinhalten.

Zu unterscheiden ist hier ferner zwischen kommerziell vertriebener Software, die regulär gekauft werden kann und Spyware, die man sich quasi kostenlos einfängt. Erstere dient zur gezielten Überwachung bestimmter Personen am Arbeitsplatz unter dem Deckmantel der Zeiterfassung oder in privater Umgebung, z.B. zur Überwachung des Ehepartners oder des Nachwuchses am PC. Insight oder Spector CNE sind professionelle Lösungen, die die gesammelten Daten direkt in Datenbanken erfassen und die zentral gesteuert und ausgewertet werden können. Als Beispiel für den privaten Bereich sei hier das Produkt LoverSpy genannt, welches sämtliche Aktivitäten wie E-Mails, besuchte Web-Seiten, Instant Messaging, Kommunikation, Passwörter und vieles mehr auf dem zu überwachenden PC protokolliert und in regelmäßigen Abständen an eine gewünschte Mailadresse weiterleitet. Einen Überblick über diese Art von kommerzieller Spyware findet der interessierte Leser in der ct [5].

Die kommerziell vertriebene Software soll hier außer Acht gelassen und der Focus mehr auf die Spyware gerichtet werden, die ungewollt und ohne Kenntnis des Nutzers zum Beispiel per Huckepack mit Freeware oder durch den Besuch von Webseiten auf den Rechner gelangt. Diese Art der Spyware eignet sich weniger für den Angriff auf gezielte Personen, da nicht bekannt ist, wer wann diese Software herunterlädt und installiert. Das Ziel ist aber auch hier das Sammeln sensitiver und demographischer Daten. Meist werden diese Informationen aus kommerziellem Interesse gesammelt, über das Internet automatisch weitergeleitet und entsprechend durch den Hersteller der Spyware selbst verwertet oder weiterverkauft. Es sind daher große Ressourcen zum Erstellen von Methoden zum Verstecken von Spyware auf dem Rechner und zum Verhindern der Deinstallation verfügbar.

Abgrenzung zu Adware und anderer lästiger Malware

Adware - Der Übergang zwischen Spyware und Adware vollzieht sich fließend. Schwarz oder Weiß wie bei Computerviren gibt es nicht. Der Begriff Adware steht für Advertising Supported Software, welche der Benutzer bewusst installiert. Adware ist also im ursprünglichen Sinne eine Kategorie Software die anderen Programmen beigefügt ist, um diese durch eingeblendete Werbung zu finanzieren. Der Benutzer erlangt in der Regel Kenntnis über die Installation dieser Software in den Lizenzbedingungen. „Gute“ Adware läuft im Gegensatz zu „böser“ Adware bzw. Spyware nur dann, wenn die dazugehörige Software, welche finanziert werden soll, ebenfalls gestartet wird. Sobald die eigentlicher

Software deinstalliert wird, wird auch die „gute“ Adware vom Rechner entfernt. Teilweise wertet auch Adware die Surfgewohnheiten des Nutzers aus, um entsprechende Werbe-Pop-Up Fenster gezielt platzieren zu können. Die gewonnenen Erkenntnisse können ebenfalls an Marketingfirmen gesandt werden. Hier wird die Grenze zu Spyware also verwischt. „Böse“ Adware versucht sich genauso wie Spyware möglichst so im System zu verankern, dass der Benutzer diese nicht ohne Probleme entfernen kann.

Browser Hijacker - Beim Hijacking werden die Einstellungen des Browsers sowie die von diesem verwendeten DNS-Einstellungen so abgeändert, dass Benutzer auf bestimmte Web-Seiten gelotst werden (wodurch der Traffic auf dieser Webseite ansteigt und der Besitzer dies für höhere Werbeeinnahmen verwenden kann) oder bestimmte Pop-Up-Werbefenster eingeblendet werden, sobald der Browser genutzt wird. Browser Hijacking ist ein Methode, die gerne von „böser“ Adware genutzt wird, um den Benutzer mit Werbung zu „beglücken“ oder um diesen dazu zu veranlassen, „etwas“ auf dem PC zu installieren.

Spam – Hierbei handelt es sich um unerwünscht per Mail versandte Werbe-E-Mails. Diese werden ohne spezielle Kenntnisse über die Empfänger an Zieladressen gesandt. Der Rücklauf ist zwar nur gering, aber aufgrund des geringen Kostenaufwands meist völlig ausreichend; um Profit zu erzielen. Auch über Spam kann man zu Spyware gelangen, wenn beispielsweise diese den Benutzer dazu verleitet, auf bestimmte HTML-Links zu klicken.

Viren - Ein Computer-Virus ist ein in ein Wirtsprogramm eingebettetes oder mit einem Wirtsprogramm verbundenes, sich selbst reproduzierendes Computer-Programm bzw. Stück ausführbarer Programmcode.

Zur Reproduktion modifiziert ein Virus andere Programme in einer Weise, dass diese eine (möglicherweise abgewandelte) Kopie seiner selbst enthalten. Durch den Aufruf des Wirtsprogramms wird eine Ausführung des Virus verursacht. Dies kann und soll (aus der Sicht des Viren-Autors) eine Ausbreitung des Virus bewirken. Viren können eine explizite Schadensroutine haben, müssen es aber nicht. Viren nutzen diverse Verfahren wie Stealth-Techniken oder Polymorphismus, um ihre Entdeckung zu erschweren. Einige Spyware hat solche Verfahren inzwischen ebenfalls adaptiert.

Trojanisches Pferd (kurz: Trojaner) - Ein Trojanisches Pferd ist ein Programm, das eine nicht dokumentierte Routine enthält. Diese führt eine unerwartete, meist destruktive Aufgabe durch und versucht den PC-Anwender zu täuschen. Ein Trojanisches Pferd reproduziert oder „bewegt“ sich im Gegensatz zu Viren nicht. Der Ort der Manipulation ist zugleich auch der Ort seiner Wirkung.

Eng verwandt mit den Trojanern sind die *Backdoors*, welche auf dem befallenen Rechner eine „Hintertür“ öffnen, über welche ein Angreifer Zugriff auf den PC erlangen kann. Backdoors können beispielsweise dazu missbraucht werden, weitere Trojaner auf dem PC zu installieren. Wenn ein Trojaner ferngesteuert werden kann, spricht man von einem *RAT* (Remote Access Trojan). Diese bestehen in der Regel aus einer Server-Komponente, die auf dem Opferrechner installiert wird und einer Client-Komponente, die der Angreifer zum Verbinden nutzt. RATs verhalten sich auf dem Wirtsrechner so lange ruhig, bis sie eine Anweisung von ihrem Besitzer empfangen, bestimmte Aufgaben auszuführen. Es lassen sich so bei erfolgreicher Verbreitung ganze sogenannte Bot-Netze aufbauen. Dabei handelt es sich um über das Internet zusammen geschaltete Rechner in aller Welt, die sich jederzeit auf Knopfdruck zu kriminellen Zwecken mobilisieren lassen und auch vermietet werden können. Je nach Funktionalität lassen Sie sich zum Beispiel für das Versenden von Spam-Mail oder für verteilte „Denial of Service“-Angriffe auf Webserver oder andere Server im Internet nutzen. Da sehr viele verschiedene Rechner bei solchen Angriffen involviert sind, kann sich der Angegriffene meist schlecht wehren. Spyware kann im Prinzip als eine spezielle Art von Trojanischem Pferd bezeichnet werden, da sie im verborgenen arbeitet und ihre destruktive Aufgabe darin besteht, unerlaubt Daten zu sammeln und zu verschicken.

Phishing – Phishing bezeichnet das Versenden von Mails mit gefälschten Inhalten an ahnungslose Benutzer mit dem Ziel, diese zum Besuch einer bestimmten Webseite zu verleiten und zum Übermitteln von Daten zu veranlassen. Meist sehen diese Mails so aus, als ob Sie von einem Finanzinstitut oder anderen kommerziellen Anbietern kommen. Sie enthalten den Hinweis, dass Aufgrund eines aktuellen Anlasses die persönlichen Benutzerdaten überprüft oder neu angegeben werden müssen. Der Benutzer soll diese dann auf der in der Mail angegeben Webseite eingeben. Diese gehört dem Angreifer, die der original Webseite des Anbieters täuschend ähnlich sieht. Mit den so erhaltenen Daten werden vom Angreifer dann beispielsweise Kreditkartenbetrug oder andere finanzielle Betrügereien oder Identitätsdiebstahl durchgeführt. Im Gegensatz zu Spyware übermittelt der Benutzer die Daten aktiv an den Angreifer, auch wenn er keine Kenntnis hat, dass er von diesem unter Vorspiegelung falscher Tatsachen hereingelegt wird.

Wie fange ich mir Spyware ein?

Es gibt viele Wege, ungewollt an Spyware zu gelangen. Die häufigsten Wege sind über das Internet per HTTP, per E-Mail über POP3 , über IRC und über den Instant Messanger.

Spyware versteckt sich in ActiveX-Komponenten genauso wie in .exe-Dateien oder Installationspaketen von regulärer Freeware oder Shareware, Patches und Softwarecracks.

Es werden Schwachstellen im Betriebssystem genauso wie im Internet Browser direkt durch Exploits ausgenutzt, damit sich die Spyware automatisch auf dem System installiert. Meist ist kein bewusstes oder vorsätzlich falsches Handeln notwendig, um einen Rechner mit Spyware zu infizieren. Es reicht schon aus, bestimmte Webseiten anzuwählen und unbedacht auf etwas zu klicken. Alternativ wird die Neugierde der Opfer

ausgenutzt, damit sie das Programm herunterladen und starten, welches mit Spyware gespickt ist.

Über E-Mail wird versucht, den Benutzer auf bestimmte Webseiten zu locken oder eingebettete Dateianhänge werden so dargestellt, dass der Benutzer über den tatsächlichen Dateityp getäuscht wird, wenn er nicht die entsprechenden Browser-Patches installiert hat. Nicht immer wurden im Outlook beim Dateinamen mehrere Datei-Endungen angezeigt, so dass die als ungefährlich erscheinende Datei Harmlos.bmp in Wirklichkeit die Datei Harmlos.bmp.exe sein kann. Ein weiterer Trick ist die Verwendung vieler Leerzeichen zwischen der ersten und zweiten Extension, so dass nur die erste Extension auf dem Bildschirm sichtbar ist. Einige E-Mail-Würmer nutzen diese Tricks im übrigen ebenfalls aus.

Wie arbeitet Spyware?

Ist die Spyware erst einmal auf dem Rechner installiert, so werden fleißig Daten gesammelt, lokal gespeichert und an den Initiator meistens per FTP oder Mail versandt. So ist es möglich, dass protokolliert wird, welche Programme gestartet und beendet wurden. Schnappschüsse des Bildschirms können als Reaktion auf bestimmte Ereignisse oder in festgesetzten Intervallen ebenso erstellt werden, wie die aufgerufenen Internetseiten, die dazugehörigen Fensternamen und auf welche Daten zugegriffen wurde.

Wie verstecke ich mich?

In der Regel möchte die Spyware möglichst lange auf dem Rechner bleiben, um möglichst viele Daten sammeln zu können. Hierzu bedient Sie sich einiger Tricks, die zum Teil von anderer Malware übernommen wurden.

Zu den einfacheren und weniger wirkungsvollen Maßnahmen gehören beispielsweise das Setzen der Dateiattribute auf „versteckt“, damit der Benutzer die Dateien beim Verwenden des „Dir“-Befehls auf der Konsole oder im Windows Explorer nicht angezeigt bekommt. Zur weiteren Verschleierung werden häufig Dateinamen gewählt, die denen von Systemdateien sehr ähneln, so dass der Benutzer keinen Verdacht schöpft, wenn er diese erblickt. Teilweise werden hier auch die exakten Namen von echten Systemdateien genutzt, diese aber dann z.B. im Verzeichnis c:\windows statt im Verzeichnis c:\windows\system32 abgelegt. Als weitere Verfeinerung dieser Technik, werden Namen von Systemdateien von Windows 95 für Spyware-Dateien unter Windows 2000 genutzt.

Die Dateinamen können aber auch per Zufallsgenerator erzeugt werden, was die Erkennung durch Anti-Spyware-Programme erschwert, sofern diese sich auf Dateinamen verlassen.

Auch die Ausnutzung von „alternativen Datenströmen“ (Alternate Data Streams, ADS) unter NTFS kann erfolgen. Existierende Dateien und Verzeichnisse können hier mit zusätzlichen Daten verknüpft werden, die normalerweise im Explorer nicht mit angezeigt werden. Ein Aufruf der Datei erfolgt dann zum Beispiel mit dem Befehl „start c:\windows\calc.exe:spyware.exe”. Es gibt spezielle Tools wie LADS [6], welche die in ADS abgelegten Dateien anzeigen können.

Zum Austricksen von Anti-Spyware-Programmen können auch polymorphe Verfahren eingesetzt werden. Diese bewirken, dass die Spyware-Dateien in jeder Instanz anders aussehen, indem zum Beispiel in die Datei zusätzlich Konfigurationsinformationen und Datenmüll mit abgespeichert werden.

Der Einsatz zweier Prozesse ermöglicht eine gegenseitige Veränderung der Dateien während der Laufzeit, die gegenseitige Überwachung der Prozesse sowie das gegenseitige Starten und Nachladen fehlender Komponenten aus dem Internet, falls ein Prozess vom Benutzer erkannt und beendet oder die dazugehörige Datei gelöscht werden sollte.

Einige Spyware verfügt über eine angebliche Deinstallationsroutine, welche jedoch, sofern Sie vom Benutzer erkannt und gestartet wird, nicht die Spyware deinstalliert, sondern stattdessen die Installation repariert oder weitere Komponenten hinzufügt.

Ähnlich wie einige Viren gibt es auch Spyware, die versucht, laufende Prozesse von Anti-Viren-Programmen und Anti-Spyware-Programmen oder auch dem Registry Editor zu beenden, um eine Erkennung und Deinstallation zu erschweren.

Die Spyware/Adware-Familie **CoolWebSearch** setzt in ihren unzähligen Varianten unter anderem folgende Techniken ein [7]:

- Benutzer Style Sheets mit Java Script Code
- Browser Helper Objects

- Hinzufügen von Domänen in „Vertrauenswürdige Zone“
- Hinzufügen von Favoriten in den Internet Explorer
- Manipulation der Browsereinstellungen in der Registry
  HKCU\Software\Microsoft\Internet Explorer
  HKLM\Software\Microsoft\Internet Explorer
- Manipulation der „about:blank“-Seite
- Manipulation der Winsock LSP
- Manipulation der Hosts Datei
- Tarnung als Treiberaktualisierung
- Einträge in die „Run“- Keys der Registry
- Starteinträge in der Win.ini, System.ini
- Verwendung der Autostart Verzeichnisse
- Starteintrag in HKLM\Software\Microsoft\Windows NT\CurrentVersion\WinLogon\UserInit=
- Verwendung von exakten oder ähnlichen Systemdateinamen z.B. ctfmon32.exe statt

ctfmon.exe (Teilweise werden die Original-Dateien überschrieben)
- Verwendung von .hta Dateien im geschützten Fonts Folder
- Einsatz .reg Dateien regedit –s sys.reg
- Verwendung von .dll-Dateien in Verbindung mit Windows rundll32
- Verwendung mehrere Prozesse zum gegenseitigen Überwachen und Nachladen
- Hijack von Standard URL Prefixes -> Adressen die im Browser ohne http:// eingegeben werden, werden auf andere Webseiten umgeleitet
- Erstellung von Kontextmenü-Einträgen
- Verwendung von Rootkit-Technologie zum Verbergen von laufenden Prozessen

Erkennung von Spyware

Der Benutzer merkt es oftmals nicht, dass sein Rechner mit Spyware verseucht ist, solange es zu keinen unerklärlichen Problemen im laufenden Betrieb kommt. Wenn ein Auto gestohlen wurde, ist es weg, die von der Spyware gesammelten Daten werden hingegen nur kopiert und anschließend nicht vermisst, da sie noch auf dem Rechner vorhanden sind.

Je mehr Spyware und Adware sich auf dem Rechner befindet, desto wahrscheinlicher kommt es zu Problemen und Konflikten mit anderer Software auf dem PC. Die Zahl der Pop-Up Fenster beim Surfen im Internet steigt an, der Browser wird langsam und bleibt häufiger hängen. Es kommt vermehrt zu Abstürzen einzelner Anwendungen bis hin zum gesamten System.

Oftmals speichert Spyware die gesammelten Daten in regelmäßigen Abständen auf der Festplatte ab. Wenn Sie also auf der Festplatte in einem Verzeichnis auf fortlaufend nummerierte Dateien in gleichmäßigen Abständen treffen, können diese von Spyware stammen. Sind solche Dateien entdeckt, kann man über das Tool Filemon [8] protokollieren, welcher Prozess diese erstellt.

Besonders hilfreich ist bei der Erkennung von Spyware eine lokale Firewall, die ausgehenden Netzverkehr filtert und festlegt, welche Applikation eine Netzverbindung aufbauen dürfen (application control). So lässt sich leicht erkennen, ob eine unbekannte Routine senden möchte, oder wenn plötzliche Öffnungsversuche von Internetverbindungen erfolgen. Dann kann mit dem Befehl Nslookup oder Internetdiensten wie http://www.dnsstuff.com ermittelt werden, zu wem oder welcher Webseite die vermeintliche IP-Adresse gehört, zu der ein Verbindungsversuch erfolgt.

Wurde eine verdächtige oder unbekannte Datei identifiziert, so hilft es unter Umständen, im Explorer über das Kontextmenü den Dialog „Eigenschaften/Version“ aufzurufen um nachzuschauen von wem diese Datei kommt. Bei regulären Systemdateien stehen hier unter Firmenname immer Einträge, wie zum Beispiel „Microsoft Corporation“. Ist der Herstellereintrag leer, so ist dies schon einmal verdächtig. Als nächstes sollte nach dem Dateinamen im Internet mit der Suchmaschine Google, bei www.sysinfo.org oder in der Prozessdatenbank von Uniblue Systems [9] nachgeforscht werden, ob es sich um eine reguläre Systemdatei oder eine Komponente einer bekannten Spyware oder Malware handelt. Wenn eine unbekannte DLL entdeckt wird, kann mit dem Tool „Process Explorer“ [10] aufgelistet werden, welche laufenden Prozesse diese DLL nutzen.

Werden gar keine Informationen gefunden, so kann eventuell die Analyse der Datei mit einen Hex-Editor nach verdächtigen Klartexteinträgen weiterhelfen.

Spätestens jetzt ist es auch an der Zeit, einen Blick auf den Taskmanager zur Kontrolle der laufenden Prozesse zu werfen. Gibt es hier Einträge mit merkwürdigen Prozessnamen zum Beispiel auch mit Sonderzeichen, die denen von verdächtigen Dateinamen entsprechen? Die Starteinträge des Systems in der Registry, dem Autostartordner sowie der Datei System.ini oder Win.ini (unter Windows 9x) sollten ebenfalls nach neuen, unbekannten Anwendungen kontrolliert werden. MSCONFIG oder WINMSD liefern Informationen zu den Startverzeichnissen und Systemdiensten. Experten können direkt in der Registry mit „regedit“ die folgenden Einträge inspizieren, über welche beim Start des Rechners Dateien automatisch ausgeführt werden können:

HKEY_CURRENT_USER\
Software\Microsoft\Windows\CurrentVersion\

Run
RunOnce
RunOnceEx
RunServices
RunServicesOnce

HKEY_LOCAL_MACHINE\
Software\Microsoft\Windows\CurrentVersion\

Run
RunOnce
RunOnceEx
RunServices
RunServicesOnce

HKEY_LOCAL_MACHINE\Software\Microsoft\
Windows NT\CurrentVersion\Winlogon\Userinit

HKEY_LOCAL_MACHINE\
System\Current ControlSet\Services
[11]

Im letzten Eintrag werden die im System verzeichneten Dienste und Ihre dazugehörigen Parameter aufgelistet und ob diese automatisch gestartet werden. Einfacher ist es allerdings einen Blick in Systemsteuerung/Verwaltung/Dienste zu werfen, um zu sehen, welche Dienste gestartet sind.

Eine detaillierte Liste aller Autostart-Möglichkeiten unter Windows kann im Internet bei Heise abgerufen werden [12].

Erscheinen beim Surfen im WWW häufig Seiten, die gar nicht angewählt wurden oder können manche Seiten gar nicht mehr erreicht werden, so sind eventuelle Einträge in der Hosts Datei vorgenommen wurden. Die Hosts-Datei dient als eine Art Adressbuch zur Umsetzung von Domänen Namen in IP-Adressen. Hierbei haben die Einträge der Hosts Datei Vorrang vor den DNS Einträgen, die der ISP liefert. Gewisse Einträge in der Hosts Datei können somit dazu führen, dass der Browser beim Aufruf einer Web-Seite eine ganz andere IP-Adresse ansteuert, welche zu einer anderen Domäne gehört und eine andere Webseite beinhaltet. So könnte der Eintrag für www.tagesschau.de auf die IP-Adresse www.amazon.de verweisen, welche dann angesteuert wird, wenn der Benutzer www.tagesschau.de im Browser eingibt.

Hier kann also Missbrauch getrieben werden, um zum Beispiel den Download von Updates für Anti-Viren-Programme zu verhindern oder um auf Webseiten zu verlinken, über die weiterer schadhafter Code heruntergeladen wird.

Als sehr hilfreich für die Systemanalyse hat sich das Tool Hijackthis [13] erwiesen, welches die gesamten für Spyware und Adware relevanten Informationen aus dem System herausfiltert und übersichtlich gruppiert zusammenfasst. Zu den aufgeführten Einträgen ist meist eine Hilfe verfügbar. Allerdings sind bei weitem nicht alle aufgelisteten Einträge auch wirklich mit Spyware in Verbindung zu bringen. Für den Laien ist es schwer, zwischen guten und schlechten Einträgen zu filtern. Selbst versierte PC-Nutzer stoßen hier an Ihre Grenzen und müssen ausgiebige Recherchen nach den Einträgen im Internet durchführen. Achten Sie aber auch auf die Vertrauenswürdigkeit der so erlangten Informationen.

Wie werde ich die Plagegeister wieder los?

Hier hilft oftmals nur eine Kombination aus Anti-Viren-Programmen, Anti-Spyware-Programmen sowie die Zuhilfenahme oben aufgeführter Tools zur manuellen Analyse und Reinigung. Die Reinigung ist aufgrund der Verzahnung mit dem befallenen System und der oftmals tiefgehenden Eingriffe meist unvollständig und zudem nur unter Einsatz hoher Benutzerkompetenz durchführbar. Erschwerend kommt hinzu, dass die Erkennungs- und Beseitigungsraten der Anti-Spyware-Programme im Vergleich zu Anti-Viren-Programmen bei Viren, Würmern und Trojanern bislang recht lückenhaft sind. Vereinzelte Testberichte von Mary Landesman [14] und Eric L. Howes [15] mit Anti-Spyware-Programmen haben ergeben, dass selbst die Kombination mehrerer Anti-Spyware-Programme nicht immer alle Komponenten einer Spyware auf dem PC erkennen und entfernen kann. Häufig werden nicht alle Teile der Spyware identifiziert und bereinigt. Sobald aber ein Startvektor oder Prozess bei der Reinigung übersehen wird, kann es zu einer Reinitialisierung der Spywareinfektion auf dem PC kommen.

Sicherheitshalber sollte daher grundsätzlich immer eine Neuinstallation des Systems erfolgen oder ein Backup zurückgespielt werden. Sollte dies aus irgendwelchen Gründen nicht praktikabel sein, so können Sie unter Einsatz diverser Analysetools eine Desinfektion angehen.

Nehmen Sie zunächst den Rechner vom Netz. Starten Sie dann einen Scanlauf mit einem Anti-Viren-Programm welches auch die Alternate Data Streams prüfen kann und einem oder mehreren Anti-Spyware-Programmen. Dateien sollten zunächst nur isoliert werden. Auf diese Weise können Sie kontrollieren, ob das System noch einwandfrei funktioniert. Die Dateien können zu einem späteren Zeitpunkt immer noch endgültig gelöscht werden.

Als nächsten Schritt setzen Sie das Tool Hijackthis ein, um sämtliche für Spyware relevanten Systembereiche zu analysieren. Seien Sie aber vorsichtig beim Löschen von Einträgen in der Registry oder Dateien, von denen Sie nicht sicher sind, was diese bewirken. Legen Sie von der Registry eine Sicherheitskopie an. Dateien sollten Sie zunächst nur umbenennen. Eventuell müssen Sie hierzu den Rechner im „abgesicherten Modus“ starten, oder Sie versuchen, vorher den Prozess zu beenden, der den Zugriff auf die Datei verhindert.

Wenn alle Dateien und Registry-Einträge bereinigt sind, kontrollieren Sie, ob sich der Spion einen eigenen Zugang zu Ihrem Rechner angelegt hat. Schauen Sie über die Systemsteuerung in der Benutzerkontenverwaltung nach unbekannten Benutzern und deaktivieren oder löschen Sie diese gegebenenfalls.

Kontrollieren Sie, ob eventuell Netzwerkfreigaben auf Ihrem Rechner angelegt wurden. Dieses kann über Netzwerk-umgebung / Eigener Computername festgestellt werden.

Aktualisieren Sie alle Ihre Sicherheitsprogramme und ändern Sie letztendlich sämtliche Passwörter für Ihre Internet Accounts, Web-Seiten, E-Mail, lokaler Rechner usw.

Beachten Sie aber bitte auch, dass nach Entfernung von Adware die mit dieser Software finanzierte Freeware evtl. nicht mehr funktioniert bzw. das Entfernen der Werbekomponente gegen die Lizenzrichtlinien verstößt.

Vorbeugende Gegenmaßnahmen

Damit der Kampf von David gegen Goliath (Enduser gegen Spyware Hersteller) nicht eintritt, können Sie eine Reihe von Vorsichtsmaßnahmen ergreifen.

Setzen Sie aktuelle Anti-Viren-Programme, eine lokale Firewall mit Applikationskontrolle und ein oder mehrere Anti-Spyware-Programme wie zum Beispiel Spybot, Ad-Aware, Pest Patrol, Spybot Search and Destroy oder Microsoft Antispyware Beta1 zur Abwehr ein. Die professionellen Versionen verfügen oftmals über einen permanenten Hintergrundschutz. Halten Sie diese Programme durch regelmäßige Updates auf dem aktuellen Stand. Da Spyware versucht, Daten in das Netz „nach Hause“ zu übermitteln, ist

es besonders wichtig, auf jedem einzelnen Computer den ausgehenden Datenverkehr zu filtern. Die Application Kontrolle sollte vorhanden sein, damit zwischen den Prozessen, die versuchen Daten zu senden, unterschieden werden kann. Im Zweifellsfall können Sie einen Prozess dann immer blockieren und schauen, ob etwas nicht mehr funktioniert.

Aktualisieren Sie zusätzlich Ihr System und den Internet Explorer regelmäßig mit den neuesten Patches von Microsoft. Schalten Sie in Ihrem Internet Browser ActiveX und Java Script ab oder verwenden Sie diese nur nach Eingabeaufforderung auf vertrauenswürdigen Web-Seiten. Öffnen Sie hierzu im Internet Explorer „Extras/ Internetoptionen/Sicherheit“.

Wählen Sie in der Zone „Internet“ die Option „Stufe anpassen“ zum Anpassen der Einstellungen für den Internet Explorer:

- ActiveX Steuerelemente ausführen, die für Scripting sicher sind = Eingabeaufforderung
- ActiveX Steuerelemente initialisieren und ausführen, die nicht sicher sind = deaktivieren
- ActiveX Steuerelemente und Plugins ausführen = Eingabeaufforderung
- Download von signierten ActiveX-Steuerelementen = Eingabeaufforderung
- Download von unsignierten ActiveX-Steuerelementen = deaktivieren
- Installation von Desktopobjekten = Eingabeaufforderung
- Programme und Dateien in einem IFRAME starten = deaktivieren
- Active Scripting = Eingabeaufforderung
- Scripting von Java Applets = Eingabeaufforderung

Sicherer ist es, wenn Sie einen anderen Browser als den Internet Explorer einsetzen.

Wenn Sie vom Internet Explorer keinen Abstand nehmen möchten, so können Sie sich IE-Spyad [16] installieren. Hier bei handelt es sich um eine Liste bekannter Domänen, welche dazu neigen Adware und Spyware verteilen. Die Webseiten werden im Internet Explorer in die Sicherheitszone „Eingeschränkte Sites“ eingetragen, wodurch beim Besuch einer dieser Domänen verhindert wird, dass Cookies, ActiveX Controls , Java Applets oder Scripting zur Kompromittierung des PCs genutzt werden können. Diese Liste kann allerdings nur manuell aktualisiert werden.

Installieren Sie keine Freeware und Shareware aus zweifelhafter Quelle. Lesen Sie sich vor der Installation die Lizenzbedingungen genau durch. Oftmals befinden sich die Hinweise tief darin versteckt, wenn darauf auch nicht immer Verlass ist. Meiden Sie die Software, wenn in den Lizenzbedingungen das Recht zur Übermittlung von Daten an Dritte oder die Möglichkeit zum automatischen Nachladen von Komponenten oder Software von Drittanbietern festgehalten wird. Vermeiden Sie die Installation von File-Sharing Software wie z.B. Kazaa, da viele dieser Applikationen in Verbindung mit Adware und Spyware kommen.

Surfen Sie ordentlich und klicken Sie auf Webseiten nur überlegt. Gehen Sie sparsam mit dem Einsatz von Browser-Erweiterungen und Toolbars um. Klicken Sie in unbekannten Pop-Up-Fenstern niemals auf Buttons, sondern schließen Sie diese über das „x“ in der oberen Fensterleiste oder mit der Tastenkombination „STRG“ + „F4“.

Zusätzlich sollte die Daten- und die Systempartition auf dem Rechner voneinander getrennt werden, damit ein regelmäßiges Backup des Systems und der Daten einfach durchgeführt werden kann. Im Ernstfall kann dann der Ursprungszustand der Systempartition wieder schnell hergestellt werden.

Literatur und Verweise

[1] Benjamin Edelman, Investors Supporting Spyware, http://www.benedelman.org/spyware/investors/

[2] AOL/NCSA (National Cyber Security Alliance) Online Safety Studie, Oktober 2004, http://www.staysafeonline.info/news/NCSA-AOLIn-HomeStudyRelease.pdf

[3] CA Security Advisory Team, Center for Pest Research
Dirk Schadt: Spyware - Ungebeten und unerwünscht
http://www.eicar.org/wg2/20041109/Spyware_ungebeten_und_unerwuenscht_09112004.pdf

[4] Steve Gibson, http://grc.com/optout.htm

[5] Detlef Borchers , „Überwachung Total“, c´t 23/2004, S.146

[6] Frank Heyne, LADS, www.heysoft.de

[7] Merijn Bellekom, The CoolWebSearch Chronicles, http://www.spywareinfo.com/~merijn/cwschronicles.html

[8] Mark Russinovich, Filemon von Systeminternals, http://www.systeminternals.com/

[9] Prozessdatenbank von Uniblue Systems, http://www.liutilities.com/products/wintaskspro/processlibrary/

[10] Mark Russinovich, Process Explorer von Systeminternals, http://www.sysinternals.com/ntw2k/freeware/procexp.shtml

[11] Microsoft Knowledgebase Artikel über CurrentControlSet\Services Schlüssel Einträge, http://support.microsoft.com/kb/103000/en-us

[12] Autostarts unter Windows, http://www.heise.de/security/artikel/49573

[13] Merijn Bellekom, HijackThis, http://www.merijn.org/files/hijackthis.zip

[14] Mary Landesman , Review: Microsoft AntiSpyware (beta1) http://antivirus.about.com/od/antivirussoftwarereviews/a/msantispy.htm?nl=1

[15] Eric L. Howes, http://spywarewarrior.com/asw-test-guide.htm

[16] Eric L. Howes, IE-SPYAD, https://netfiles.uiuc.edu/ehowes/www/resource.htm

Linux – Trügerische Sicherheit

von Peter Klein, System Engineer bei F-Secure

Viren, Würmer und andere Schädlinge verbreiten sich über Internet und E-Mail immer stärker. Trotzdem wägt sich die Open-Source-Gemeinde in Sicherheit. Linux haftet hartnäckig der Ruf an, immun zu sein gegen Malware-Infektionen. Ein Irrtum: Denn Linux-Viren sind – zugegebenermaßen selten – auch schon „In-the-Wild“ aufgetaucht. Von größerer Bedeutung ist aber, dass durch den zunehmenden Einsatz von linux-basierten Servern für Windows-Clients Viren Tür und Tor geöffnet werden. Um der Ausbreitung von Schädlingen in Unternehmensnetzwerken vorzubeugen, empfiehlt sich der Einsatz eines Linux-Virenscanners.

Schreckensmeldungen über neue, sich schnell verbreitende Malware, die Rechner infiziert, Daten stiehlt und Hackern eine Hintertür auf das System öffnet, lassen Linux-Anwender meist völlig kalt. Viren und Würmer werden immer noch als reines Problem für Benutzer von Windows-Rechnern angesehen. Und tatsächlich scheinen die letzten großen Virenepidemien – verursacht durch Mydoom, Sobig, Lovsan oder Slammer – diese landläufige Meinung zu bestätigen. Dass Linux momentan noch als vergleichsweise sicher gelten kann, hat mehrere Ursachen. Zwar hat Linux seinen Exoten-Status längst verloren, doch ist die Verbreitung des quelloffenen Betriebssystems noch relativ gering. Sein Marktanteil im PC-Markt beträgt laut Analysten der Gartner Group gerade mal 1,5 Prozent, im Serverbereich nur gut 20 Prozent (Quelle: IDC). Das schafft wenig Anreiz für Virenautoren, deren Ansehen in der Hacker-Szene sich vor allem daran misst, wie viele Rechner ein in Umlauf gebrachter Virus infiziert und wie viel Schaden er anrichtet. Windows mit Installationen auf vielen Millionen Clients und Servern bietet daher eine wesentlich attraktivere Angriffsfläche.

Bugs beheben ohne bürokratische Hürden

Einen nicht unerheblichen Beitrag zur Sicherheit von Linux liefert auch das Prinzip offener Quellcode. Die Linux-Anwender bilden eine eingeschworene Gemeinschaft und kommunizieren aktiv über mögliche Gefahren und Gegenmaßnahmen. Sind Sicherheitslücken bekannt, läuft im Gegensatz zu kommerzieller Software sofort und völlig umkompliziert das Bug-Fixing an. Viele Hände arbeiten gleichzeitig an einem Patch und stellen diesen wieder allen zur Verfügung. So existieren bereits zahlreiche kostenlose Mailscanner wie AMaViS (A Mail Virus Scanner), die E-Mails auf Viren überprüfen.

Die Zugangsbeschränkungen unter Linux stellen bislang noch die größten Hürden für das Eindringen von Malware dar. Zwar können unter Linux prinzipiell alle Dateien ausgeführt werden – während unter Windows nur Dateien mit bestimmten Endungen wie EXE zulässig sind – doch passiert nichts, so lange nicht die Ausführ-Flag der Datei gesetzt ist. Schutz bieten auch die Root-Rechte, die für viele Aktionen unter Linux notwendig sind. Root-Rechte besitzt in der Regel nur der Administrator. Wer sich mit einem ganz normalen User Account anmeldet, hat keinen Zugriff auf zentrale System- und Konfigurationsdateien. Auch ein vom Anwender gestarteter Virus könnte daher keinen großen Schaden anrichten, da er nur auf Daten zugreifen kann, für die der User Zugriffsrechte hat. Damit Angreifer sich unter Linux keine Root-Rechte verschaffen und so alles lesen, schreiben und löschen könnten, steht frei zugänglich auch LIDS (Linux Intrusion Detection System) bereit. LIDS schützt Dateien und Verzeichnisse, indem es die Root-Rechte exakter festlegt und die uneingeschränkte Allmacht aufhebt. Wird gegen eine LIDS-Regel verstoßen, schließt LIDS die Shell, von der aus die Verletzung ausging, und informiert den Systemadministrator darüber.

Viren unter Linux

Die Sicherheit, die das Linux-Betriebssystem ausstrahlt, ist trügerisch. Sie setzt nämlich voraus, dass der Systembetreuer keine Konfigurationsfehler macht, viel Zeit in die Administration investiert und größte Sorgfalt beim Aufspielen aktueller Patches walten lässt. Dass das in der Vergangenheit nicht immer reibungslos geklappt hat, zeigen verschiedene Beispiele. Der Wurm Ramen brachte es 2001 zu einiger Berühmtheit, als er Red Hat Linux befiel und die bekannten Sicherheitslücken in *wu-ftpd*, *rpc.statd* und *lpd* ausnutzte . Erfolgreich war auch der im selben Jahr aktive Linux-Wurm Lion. Die Payload des Wurms sieht vor, verschiedene Systemdienste unter Linux auszutauschen, um seine Verbreitung zu sichern und sich zu tarnen. Zudem ersetzt Lion *login*, so dass sich Passwörter ausspionieren lassen und eine Hintertür auf das System geöffnet werden kann. Eine Schwachstelle, die im August 2002 in OpenSSL Libraries bekannt wurde, verhalf dem Wurm Slapper am 13. September 2002 zu einer raschen Verbreitung auf Linux-Rechnern.

Attacken über Buffer Overflow

Wenn Programmierer es versäumen, Pufferlängen zu begrenzen, kann diese Nachlässigkeit von Hackern leicht zum Einfall in ein Linux-System genutzt werden. Buffer Overflows können Daemons wie Sendmail zum Absturz bringen. Anstatt den Puffer nur mit unsinnigen Daten zum Überlaufen zu bringen, kann ein Virenautor auch schadhaften Code in die Zeichenkette, die den Buffer Flow verursacht, einbauen. Sendmail wird als Root ausgeführt und stürzt nun das Programm ab, verändert die Malware das System so, dass eine Shell mit Root-Rechten gestartet wird. Der Hacker kann dann mit unbeschränkten Root-Privilegien auf das System zugreifen. Auf diese Weise könnten dann auch ELF-

Binaries andere Dateien patchen und infizieren. Besonders prekär ist, dass der Virus in diesem Fall schon dann eingeschleppt wird, wenn der Anwender seine Mails abruft und nicht erst beim Ausführen einer Datei.

Gefahrenpotenzial heterogene Netzwerke

Noch sind Linux-Viren oder gezielte Angriffe auf Linux-Systeme eher eine Seltenheit. Sicherheitsrisiken entstehen aber schon jetzt durch die Popularität des quelloffenen Betriebssystems. Linux hat sich im Serverbereich als feste Größe in Unternehmen und Behörden etabliert. Zuverlässig und unschlagbar günstig arbeitet es als Mail- und Dateiserver. Integriert in solche meist heterogene IT-Landschaften sieht sich auch das Open Source-Betriebssystem massiv dem Virenproblem ausgesetzt: Denn die auf Linux-Servern gespeicherten Dateien werden in der Regel für Windows Clients zur Verfügung gestellt. Sind diese Dateien mit zum Beispiel mit Windows- oder Makro-Viren verseucht, besteht zwar für Linux keine Gefahr, aber die Malware kann sich rasch im Netzwerk verbreiten. Abhilfe schaffen hier Virenscanner wie F-Secure Anti-Virus für Linux.

So tappen Viren unter Linux in die Falle

E-Mails sind immer noch der Hauptübertragungsweg für Viren. Die Schädlinge befinden sich in Attachments, die die User öffnen und damit unbeabsichtigt den Virus aktivieren. Um effizient zu arbeiten, sollte der Virenscanner die Nachrichten schon vor Auslieferung an den Empfänger überprüfen. F-Secure Anti-Virus für Linux – umfangreich getestet unter unter Red Hat (Versionen 7.3, 8.0 und 9), Red Hat Enterprise Linux (Versionen 2.1 AS und 3 AS), Debian GNU/Linux 3.0r1, SuSE Linux (Versionen 8.1, 8.2 und 9) sowie SuSE Linux Enterprise Server 8 – kann mit einem Mail Transport Agent (MTA) wie postfix, sendmail oder qmail eingesetzt werden. Die Integration des Virenscanners erfolgt über AMaViS.

Zunächst muss aber F-Secure Anti-Virus für Linux installiert werden. Die Software verfügt über mehrere Scan-Engines, die Linux-, Windows-, DOS-Dateiviren und Makroviren in infizierten MS Office-Dateien erkennen. Diese Engines werden als Daemon dauerhaft in den Arbeitsspeicher geladen. Hierfür muss die Datei *fsavd* aus dem Standard-Installationsverzeichnis */opt/f-secure/fsav/etc* nach */etc/init.d* kopiert werden. Um sicher zu stellen, dass das System das Skript beim Systemstart lädt, kann zum Beispiel unter Red Hat folgender Befehl ausgeführt werden:

```
$ cp /opt/f-secure/fsav/etc/fsavd /etc/init.d $ /sbin/chkconfig fsavd
```

Schließlich muss noch die Variable *fsavuser* in *amavis* umgeändert werden.

Nach der Installation des F-Secure Virenscanners, kann AMaViS installiert werden. Dazu müssen manuell eine Group ID und User ID, die von amavisid genutzt wird, erstellt, Verzeichnisse angelegt sowie die Rechte vergeben werden. Die Installation von AMaViS kann dann durch Ausführen der folgenden Befehle erfolgen:

```
$ /bin/gzip -dc amavisd-new-20030616-p6.tar.gz | /bin/tar xf -
$ cd amavisd-new-20030616
$ /usr/sbin/groupadd amavis
$ /usr/sbin/useradd -M –d /var/amavis -g amavis –s /sbin/nologin amavis
$ mkdir /var/amavis
$ chown amavis:amavis /var/amavis
$ chmod 750 /var/amavis
$ cp amavisd /usr/sbin/amavisd
$ chown root /usr/sbin/amavisd
$ chmod 755 /usr/sbin/amavisd
$ cp amavisd.conf /etc
$ chown root /etc/amavisd.conf
$ chmod 644 /etc/amavisd.conf
$ mkdir /var/virusmails
$ chown amavis:amavis /var/virusmails
$ chmod 750 /var/virusmails
```

Nach erfolgreicher Installation von AMaViS erfolgt noch die Anpassung von */etc/amavisid.conf*. Dazu muss */etc/amavisid.conf* in einem beliebigen Texteditor geöffnet werden und *$mydomain* durch einen für die individuelle Installation sinnvollen Eintrag ersetzt werden. *$daemon_user* und *$daemon_group* müssen mit *amavis* ersetzt werden. Da F-Secure Anti-Virus für Linux sämtliche Nachrichten eigenständig scannen kann und keine Extrahierung durch AMaViS nötig ist, muss die Umleitung *$bypass_decode_parts* mit # auskommentiert werden. Schließlich muss in der Datei den Kommandozeilen-Parametern von *fsav* noch *--mim*e hinzugefügt werden. Auch das Scannen von Spam mit Hilfe von SpamAssassin sollte durch auskommentieren der Befehlszeile *$bypass_spam_checks_acl* deaktiviert werden.

Kommt als MTA Postfix zum Einsatz müssen in den Konfigurationsdateien zwei Änderungen vorgenommen werden. Der Datei *master.cf* muss Folgendes hinzugefügt werden:

```
smtp-amavis unix - - n - 2 smtp
-o smtp_data_done_timeout=1200
127.0.0.1:10025 inet n - n - - smtpd
-o content_filter=
-o local_recipient_maps=
-o relay_recipient_maps=
-o smtpd_restriction_classes=
-o smtpd_client_restrictions=
-o smtpd_helo_restrictions=
-o smtpd_sender_restrictions=
-o smtpd_recipient_restrictions=permit_mynetworks,reject
-o mynetworks=127.0.0.0/8
-o strict_rfc821_envelopes=yes -o smtpd_error_sleep_time=0 -o smtpd_soft_error_limit=1001
-o smtpd_hard_error_limit=1000
```

Am Ende der Datei *main.cf* wird angefügt:

```
content_filter = smtp-amavis:[127.0.0.1]:10024
```

Durch diese beiden Einträge wird ein Transport (smtp-amavis) erzeugt, über den E-Mails an AMaViS weiter geleitet und nach Prüfung durch den F-Secure Scanner über einen zusätzlichen *smtpd* wieder an Postfix zurück geschickt werden. Auch die Alias-Datei muss geändert und das E-Mail-Konto aufgenommen werden, das die Benachrichtigungen über Viren, die beim Scannen gefunden werden, erhalten soll:

```
virusalert: <mailbox>
```

Welche Maßnahmen für infizierte Dateien ergriffen werden sollen, gibt der Systemadministrator über den Daemon *fsav* vor. Eine Desinfizierung erfolgt mit *--disinf*. Dafür muss *fsav* mit Schreibrechten für die betreffende Datei ausgestattet sein. Über *--rename* können befallene Dateien umbenannt werden in <Ursprungs_Dateiname>.virus und ausführbare sowie SUID-Bits entfernt werden. Die Option *--delete* ermöglicht auch ein sofortiges Löschen einer infizierten Datei. Die Default-Einstellung von F-Secure Anti-Virus für Linux sieht dabei vor, dass diese Aktionen vor der Ausführung nochmals bestätigt werden.

Das A und O für eine erfolgreiche Abwehr von Malware sind die regelmäßigen Aktualisierungen der Virendefinitions-Datenbanken. *dbupdate* ist ein Shell Skript für F-Secure Anti-Virus für Linux, das das Herunterladen der neuesten Updates der Virensignaturen vereinfacht. Um diesen Prozess zu automatisieren steht Anwendern das Shell Skript *fsavschedule* zur Verfügung, das zudem auch zeitgesteuertes, automatisches Scannen über cron jobs ermöglicht.

Fazit

Das Schattendasein für Linux ist längst vorbei. Gerade im Serverbereich ist das freie Betriebssystem eine beliebte Alternative. Und mit zunehmender Popularität und Verbreitung steigt die Virengefahr. Zuverlässigen Schutz bieten kommerzielle Virenscanner für Linux, die Malware auf Servern und Workstations erkennen und entfernen. Von einem sicheren Netzwerk profitieren Unternehmen in mehrerer Hinsicht:
Sie beugen Imageschäden sowie finanziellen Einbußen durch Systemausfallzeiten und der kostspieligen Wiederherstellung infizierter Netzwerke vor

Schutz vor Stealth-Viren und Rootkits

F-Secure Blacklight bekämpft die neuste Generation von Schädlingen

von F-Secure GmbH

Kriminelle Eindringlinge und Hacker erfinden laufend neue Methoden für Angriffe auf Computer und Server. Der neueste Trend sind fortschrittliche Stealth-Techniken in Form von Rootkits. Diese können beispielsweise Trojanische Pferde und Keylogging-Komponenten unsichtbar auf dem Computer platzieren, um so den PC zu überwachen und wichtige Daten zu stehlen. Der bösartige Code ist so gut versteckt, dass er weder vom Betriebssystem noch von den derzeit erhältlichen, konventionellen Sicherheitsprodukten wie Viren- und Spywareschutz oder IDS-Lösungen (Intrusion Detection System) aufgespürt wird. F-Secure arbeitet bereits mit Hochdruck an der Entwicklung neuer Techniken zum Erkennen und Beseitigen von Kernel-Rootkits. Die erste Beta-Version der F-Secure BlackLight-Technologie zur Entfernung von Rootkits wurde auf der diesjährigen CeBIT vorgestellt.

Unsichtbare Formen von bösartigem Code werden sich in Zukunft mehr und mehr zu einem handfesten Problem auswachsen. Im Rahmen der vor kurzem abgehaltenen RSA-Sicherheitskonferenz in San Francisco drückten die Microsoft Corporation und führende Sicherheitsexperten der Branche ihre Besorgnis hinsichtlich des aufkommenden Rootkits-Problems aus. Das Betriebssystem Windows XP ist beispielsweise bei zahlreichen Kernel-Rootkit-Programmen nicht in der Lage, die zugehörigen Dateien oder Prozesse darzustellen. Der Benutzer oder Administrator weiß daher nichts von ihrer Existenz. Es wird vermutet, dass diese Art von Stealth-Spyware-Programmen an einigen bekannten Fällen von Industriespionage beteiligt waren.
„Leistungsstarke Windows-Rootkits können sich künftig zu einem echten Problem entwickeln“, befürchtet Mikko Hyppönen, Chief Research Officer bei F-Secure. „Rootkit-Programme knacken den Zugang zu allen Informationen auf dem System und können unbeobachtet auf Computern agieren. Diese Angriffsprogramme dringen über Viren oder Sicherheitslücken in PCs und Server ein. Sobald das Rootkit seinen Inhalt abgeladen hat, sind konventionelle Sicherheitsprogramme – auch Virenschutz- und Spywareschutz-Programme – nicht in der Lage, diesen zu erkennen oder zu entfernen“, so Hyppönen weiter. F-Secure BlackLight kann Dateien, Verzeichnisse und Prozesse erkennen und beseitigen, die dem Betriebssystem und auch anderen Sicherheitsprodukten verborgen bleiben. „Die derzeit erhältlichen Virenschutz- und Spywareschutz-Produkte können die nächste Welle von Stealth-Viren und Spyware weder erkennen noch aufhalten. Und darum gehen wir zuversichtlich davon aus, dass Administratoren und IT-Spezialisten diese neue Art der Sicherheit zu schätzen wissen“, erläutert Pirkka Palomäki, Vice President für F&E bei F-Secure. „Die BlackLight-Technologie und ihre vielfältigen Möglichkeiten sind wirklich aufregend.“ Für das Jahr 2005 kündigt F-Secure verschiedene Produkte und Lösungen mit BlackLight-Technologie an. Damit wird das bestehende Sicherheitsangebot des Unternehmens – zentral verwaltete Lösungen im Bereich Virenschutz, Desktop-Firewall, Intrusion Detection und Schutz vor Spyware – weiter gestärkt.

Weitere Informationen zu F-Secure BlackLight sowie eine kostenlose Beta-Version sind im Internet unter www.f-secure.com/blacklight zu finden. .

Acronis True Image 8.0 für Workstations

umfassender Schutz für Workstations

von Acronis

Acronis, Technologieführer bei Lösungen zur Speichermedienverwaltung und Datensicherheit, hat im Acronis True Image 8.0 für Workstations veröffentlicht. Acronis True Image 8.0 ist die neueste Version innerhalb einer preisgekrönten Produktpalette für Festplatten Imaging auf Workstations und Servern, für Backups und Wiederherstellung auf unvorbereitete Datenträger.

Mit Acronis True Image 8.0 für Workstations können Anwender im laufenden Betrieb ein exaktes Abbild von Festplatten oder Partitionen für ein komplettes Backup erzeugen und so alle Inhalte, einschließlich der Betriebssysteme, der Programme und der persönlichen Dateien und Einstellungen für eine Wiederherstellung sichern.

Im modernen Geschäftsleben ist der Faktor Zeit beim Herstellen verlorener Daten von größter Wichtigkeit. Basierend auf der exklusiven Imaging-Technologie Acronis Drive Snapshot ermöglicht Acronis True Image die Erstellung von Online-Images im laufenden Betrieb ohne Neustart des Rechners. Außerdem beeinflusst die Datenmenge die Größe des Abbilds und damit auch die Geschwindigkeit, mit der ein Image erstellt und wiederhergestellt wird. Die neuen Funktionen von Acronis True Image 8.0 schließen deshalb bei der Sicherung Auslagerungs- und Ruhezustandsdateien vom Image aus und verteilen die PC-Leistung optimal zwischen den Prozessen zur Sichern der Festplatten und den gleichzeitig aktiven Anwendungen. Nach einer erfolgten Komplettsicherung können die Archive inkrementell erweitert werden – ein weiteres Plus für Zeit- und Kostenersparnis. Dank schnellster Wiederherstellungstechnologien werden die Ausfallzeiten bei einem Systemcrash und die damit verbundenen IT-Kosten erheblich reduziert.

Darüber hinaus ist die neue Version in der Lage, ein Image zu prüfen, bevor die eigentliche Wiederherstellung beginnt. Ebenso ist eine Kontrolle des Dateisystems nach der Wiederherstellung möglich. Diese Funktionen erhöhen die Sicherheit für den Benutzer, wirklich exakte und funktionstüchtige Abbilder seiner wertvollen Daten zu besitzen und zuverlässig wiederherzustellen.

Zusätzlich zu seinen Image-Fähigkeiten bietet Acronis True Image 8.0 für Workstations alle Funktionen, die für das Klonen, Ersetzen und Aufrüsten von Festplatten-Laufwerken nötig sind. Anwender verfügen mit Acronis True Image 8.0 für Workstations über ein umfassendes und kostengünstiges Datensicherungssystem, das einfach und sicher zu bedienen ist.

Systemanforderungen

Acronis True Image 8.0 kann auf Computern mit Betriebssystem Windows XP (Home oder Professional), Windows 2000 Workstation, Windows NT Workstation, Windows Me oder Windows 98 installiert und ausgeführt werden.

Acronis True Image 8.0 kann Bootdisketten und bootfähige CD-R/W erstellen. Mit diesen können Computer mit beliebigen PC-basierten Betriebssystemen (einschließlich LINUX) gesichert und wiederhergestellt werden.

Acronis True Image 8.0 speichert Festplatten- und Partitionsabbilder auf Festplatten, Disketten, CD-R / CD-RW, DVD-R / DVD-RW, DVD+R / DVD+RW, ZIP®, Jaz® und andere Wechseldatenträgern und Netzwerklaufwerken
Acronis True Image 8.0 unterstützt IDE, SCSI, USB 1.0/2.0, FireWire und PCCard-Geräte.

Für die volle Leistungsfähigkeit von Acronis True Image 8.0 wird ein IBM PC/AT kompatibler PC mit CPU der Pentium-Klasse, mindestens 32 MB RAM, VGA-Monitor und Maus benötigt.

Über Acronis

Acronis bietet Programme zur Datenträgerverwaltung, die technisch hoch entwickelt, aber einfach zu nutzen sind. Mit umfassenden Systemlösungen für Geschäfts- und Privatkunden ist Acronis technologisch führend im Bereich Verwaltung von Partitionen, Boot-Management, Disk-Editing, Datenlöschung, anderen Aufgaben zur Datenträgerverwaltung sowie weiteren Kerntechnologien. Acronis verfügt über Büros in den USA, Europa und Asien und vermarktet seine Produkte im Handel und über Wiederverkäufer sowie im Internet. Produkte von Acronis sind in 10 Sprachen weltweit verfügbar und werden über verschiedene Vertriebskanäle angeboten. Qualität und Resonanz der Produkte spiegeln sich in einer Reihe von Testsiegen und Auszeichnungen wider, unter anderem der von der PC Professional erhaltenen Auszeichnung "Innovation des Jahres 2002/2003" für Acronis True Image. Weitere Informationen finden Sie unter http://www.acronis.de.

Schütze Dein eLife

von Symantec GmbH

Ach Du Schreck, alles weg! Der PC stürzt ab und plötzlich sind die Hochzeitsfotos verschwunden oder das letzte Kapitel der Seminararbeit fehlt. Doch der Verlust von unwiederbringlichen Erinnerungsfotos und wichtigen Dokumenten muss nicht sein: Entsprechende Software, zum Beispiel zum Erstellen von Sicherungskopien, schafft hier Abhilfe.

Digitalfotografie, Internetnutzung, Downloads von Musik, Videos und Spielen - durch immer mehr digitale Anwendungen mausert sich der PC vom reinen Arbeitsgerät zum vielseitigen Multimedia-Tool im Haushalt. Oft ersetzt der Computer bereits Fotoalbum, Musikanlage, Spielekonsole oder auch den Dokumentenordner im Regal. Doch damit steigt auch das Risiko, durch Systemabstürze neben wichtigen Daten unwiederbringliche Erinnerungen zu verlieren. „Ein Computercrash kann verschiedene Ursachen haben, wie eine Überlastung des Rechners, oder auch Schadprogramme. Zudem kann das Installieren eines neuen Programms oder Computerspiels, das der Anwender schnell einmal ausprobieren möchte, Grund für einen Absturz sein“, erklärt Patrick Heinen, IT-Sicherheitsexperte bei Symantec. Umso ärgerlicher, wenn hierdurch neben Daten auch Programme und Anwendungen verloren gehen. Abhilfe schaffen hier Softwarelösungen, die zum einen einem Crash vorbeugen, zum anderen im Notfall die Daten wiederherstellen können.

Mehr als speichern

So genannte Back-Up-Lösungen, wie beispielsweise Norton Ghost 9.0 erstellen Sicherungskopien der Festplatten – sogar während des laufenden Betriebes. Funktionieren nach einem Absturz auch einzelne Programme nicht mehr so, wie sie sollen, und sind ganze Datensätze in den „Untiefen des PCs“ verschwunden, kann diese Kopie, das so genannte „Image“, schnell und einfach helfen, den Zustand des Rechners wiederherzustellen. Die Kopie der Daten kann auch unbeaufsichtigt, zum Beispiel nachts erstellt werden. Und wenn gar nichts mehr geht, hilft die Rettungs-CD: Mit ihrer Hilfe kann ein Neustart des Rechner erfolgen, auch wenn das Betriebssystem nicht mehr reagiert. Zudem können damit Systemkorrekturen und Virenprüfungen ausgeführt sowie verloren gegangene Daten wiederhergestellt werden.

Das Risiko eines Datenverlustes minimiert der Anwender auch durch Anlegen von mehreren definierten Bereichen (Partitionen) auf der Festplatte. Für jedes Thema, wie Musik, Programme, Videos, Dokumente oder Spiele, sollte im Idealfall ein eigener Bereich angelegt werden. Dabei helfen Programme wie Norton PartitionMagic 8.0, mit dem die Festplatte schnell und einfach zu strukturieren ist. Ein Assistent hilft dem Benutzer schrittweise bei der Erstellung der Sicherungspartitionen. Die Daten werden getrennt vom Betriebssystem des Computers erstellt, so dass Sicherungen leichter und schneller angefertigt und Systemabstürze verhindert werden.

Anwenderfehler ungeschehen machen

Wenn mehrere Personen einen Computer nutzen oder die Kinder öfters am Rechner sitzen, empfehlen sich Komplettpakete wie Norton SystemWorks 2005. Sie beinhalten eine ganze Reihe an Helfern und Datenwächtern, wie beispielsweise Norton GoBack 4.0. Damit kann der Anwender versehentliche Änderungen rückgängig machen und sogar Dateien oder Ordner, die gelöscht wurden, wiederherstellen.

Zusätzliche Funktionen sorgen für einen stabilen Zustand des Systems: Norton Utilities beseitigt Probleme auf dem Computer und optimiert die Leistungsfähigkeit. Das Feature CleanUp bereinigt den Rechner von unerwünschten Überbleibseln aus dem Internet, wie Cookies, die unnötig Speicherplatz beanspruchen und so die Systemleistung mindern können. Für PC-Gamer kann der SafeTry-Modus ein Segen sein: Über einen temporären Status können neue Programme und Spiele ausprobiert werden, ohne negative Auswirkungen befürchten zu müssen. Und um Gefahren aus dem Internet keine Chance zu geben, ist im Paket auch ein Virenschutzprogramm dabei.

Da der PC immer mehr zum Archiv für Persönliches wird, sollte er dementsprechend gepflegt und gesichert werden, damit wichtige Dokumente oder einfach schöne Erinnerungen an Kindertage, Urlaube oder Familienfeste lange erhalten bleiben.

Über Symantec

Symantec ist weltweit marktführend auf dem Gebiet der Informationssicherheit. Die umfangreiche Angebotspalette umfasst Software- und Appliance-Lösungen sowie Services, die Privatanwendern, Unternehmen und Internet-Dienstleistern helfen sollen, ihre IT-Infrastruktur zu sichern und zu verwalten. Die Konsumentenmarke Norton ist weltweit marktführend auf dem Gebiet der Sicherheits- und Systempflegeprodukte für Endanwender. Das Unternehmen hat seinen Hauptsitz in Cupertino, Kalifornien und ist in mehr als 35 Ländern vertreten.

Virtual Private Network (VPN)

von Thorsten W. Stritzinger, M4066

Laut einer Umfrage der IDC zur Nutzung des Internets unter den weltweit Top-1000 Firmen trauen diese Firmen dem Internet nicht. Vielleicht verändert sich diese Einstellung ja durch eine ganz neue Art des Tunnelbaus - das VPN. Außerdem integrieren VPNs unterschiedlichste Netzwerktechnologien und Protokolle, dabei lockt diese Technologie auch noch mit Kostenvorteilen und mehr Produktivität im Netz der Netze. Der folgende Artikel soll ein wenig Licht in die Welt der virtuellen privaten Netzwerke bringen.

Öffentliche und private Netze

Bisher konnte man eindeutig zwischen öffentlichen und privaten Netzen differenzieren. Auf der einen Seite existieren öffentliche Netze, wie beispielsweise das Telefon-Netz der Deutschen Telekom AG oder das Internet. Diese Netzwerke zeichnen sich durch zahlreiche Teilnehmer aus, die in keiner festen Beziehung zueinander stehen und verhältnismäßig ungehindert Daten austauschen. Personen mit Zugang zu einem öffentlichen Netz weisen nicht unbedingt gemeinsame Eigenschaften auf und kommunizieren fast immer nur mit einem sehr kleinen Teil aller möglichen Benutzer.

Ein privates Netzwerk dagegen besteht nur aus Rechnern einer bestimmten Organisation, die hauptsächlich untereinander Informationen austauschen. Die Benutzer können sich sicher sein, daß das Netz ausschließlich von ihnen genutzt wird und die ausgetauschten Informationen selbst im schlimmsten Fall (worst case) nur den anderen Teilnehmern bekannt werden. Ein Exempel für ein privates Netzwerk ist das lokale Firmen-Netzwerk (kurz: LAN: local area network) oder das firmeninterne Weitverkehrsnetzwerk (kurz: WAN: wide area network). Der Wechsel zwischen privatem und öffentlichem Netz passiert eigentlich immer am Gateway-Router. Dort wird eine Firewall eingerichtet, die Eindringlinge aus dem öffentlichen Netz fernhält und verhindert, daß die eigenen internen Netz-Teilnehmer sich das öffentliche Netz genauer anschauen.

Noch vor kurzem konnte es sich ein Unternehmen erlauben, seine LANs als völlig unabhängige Einheiten zu betreiben. Jede Niederlassung besaß ein eigenes LAN mit individuellen Namensvereinbarungen, eigenem Mail-System und sogar speziellem Netz-Protokoll, die mit denen anderer Filialen nicht zwangsweise kompatibel waren. Mit wachsender Veränderung der Ressourcen auf elektronische Datenverarbeitung wurde es allerdings immer wichtiger, die unterschiedlichen Außenstellen miteinander zu verbinden. Hierfür verwendete man meistens Standleitungen verschiedenster Bandbreite, die permanent verfügbare und daneben auch vertrauliche Verbindungen garantieren. Standleitungen sind aber eigentlich immer eine teuere Lösung, da man eine monatliche Grundgebühr plus Basisanschluß und eine entfernungsabhängige Komponente zahlen muß. Für ein Unternehmen mit vielen landesweiten Geschäftsstellen sind diese Gebühren ziemlich hoch, wodurch natürlich die Lösung über Standleitungen schnell kostenintensiv wird.

Bei privaten Netzwerken erleichtern die mobilen Benutzer die Problematik ganz und gar nicht. Außendienst-mitarbeiter, die permanent unterwegs sind, müssen die Möglichkeit besitzen, per Modem mit dem Firma zu kommunizieren. Wenn sich diese Mitarbeiter nicht in der Nähe eines firmeneigenen Rechners befinden, sind für die notwendige Kommunikation Ferngespräche notwendig, die auf lange Sicht extrem teuer sind.

Vorteile des VPN

Das Konzept des virtuellen privaten Netzwerks beseitigt die Grenze zwischen öffentlichem und privatem Netz. VPNs besitzen die Möglichkeit, in einem öffentlichem Netz wie dem Internet ein sicheres, privates Netz zu etablieren. Zum Schutz werden Techniken wie Verschlüsselung, Authentifizierungen, Paket-Tunneling und Firewalls verwendet. Weil VPNs sich das Internet als WAN zu Nutze machen und nur kurze Standleitungen zwischen einem Firmenstandort und dem nächsten Einwahlknoten (PoP = Point of Presence) erfordern, stellen sie für große Unternehmen eine kosteneffektive Alternative dar. und sind heute auch für kleinere Firmen bereits erschwinglich.

Ein virtuelles privates Netzwerk ist eine Methode, in einem öffentlichen Netz wie dem Internet ein privates Netz zu simulieren. Man bezeichnet es als virtuell (virtual), da es auf virtuelle Verbindungen aufbaut oder anders formuliert, sich auf temporäre Verbindungen stützt, die sich nicht durch ihre physikalisches Präsenz definieren, sondern nur aus Paketen bestehen, welche über verschiedene Rechner im Internet ohne fest vorgegebene Route transferiert werden. Sichere virtuelle Verbindungen können zwischen zwei Rechnern, zwischen einem Rechner und einem Netz oder zwischen zwei Netzen etabliert werden.

Die Nutzung des Internet zum Zugriff auf entfernte LANs verringert die Kosten deutlich. Man kann sich überall einwählen, sofern der eigene Internet Service Provider (ISP) einen PoP anbietet. Besitzt ein ISP landesweit Einwahlknoten, ist das eigene LAN aller Wahrscheinlichkeit nach auch zum Ortstarif erreichbar. Einige ISPs operieren auch international oder kooperieren mit ISPs im Ausland. Viele kleinere ISPs offerieren dem ungeachtet gebührenfreie Nummern für mobile Benutzer. Schaut man sich die gegenwärtig sehr günstigen Geschäftsbedingungen

für Wahlzugänge an, sind geeignete ISP-Accounts in jedem Fall preisgünstiger als ein Modem-Pool für den Fernzugriff inklusive der Kosten der Fernverbindungen mobiler Teilnehmer. Ebenfalls ist der gebührenfreie Zugriff auf einen ISP üblicherweise günstiger als eine eigene gebührenfreie Nummer, weil der ISP meist bessere Konditionen von der/den Telefongesellschaft(en) eingeräumt bekommt.

Fernverbindungen von Netzen werden vielfach mit einer Standleitung, einem Anschluß an ein Frame-Relay-Netz oder ISDN bewerkstelligt. Wie schon erwähnt wurde, ist eine Standleitung mit hoher Bandbreite sehr kostspielig. Ebenfalls kann man einen hohen Datendurchsatz mit Frame-Relay-Verbindungen erzielen, wobei die Kosten entfernungsunabhängig sind. Bei dieser Technik erwirbt man einen Anschluß an eine Frame-Cloud, welche über Switches die Verbindung zu dem Zielrechner schafft. Im Gegensatz zur Standleitung hängen die Kosten nicht von der Distanz, sondern rein von der Bandbreite und dem Datenvolumen ab, die der Verbindung zugeordnet worden ist. Frame-Relay-Verbindungen sind dennoch sehr teuer. Bei ISDN existieren wie beim altbewährten Telefonsystem entfernungsabhängige Kosten. In Deutschland werden (anders als in den Staaten) auch bei Ortsgesprächen (local calls) Gebühren pro Minute erhoben, was die Unkosten dementsprechend vergrößert. Falls sich die Netzwerke eines Unternehmens in unterschiedlichen Städten befinden, ist es erheblich kosteneffektiver, jede Außenstelle über Frame-Relay- oder ISDN-Verbindung an den lokalen Einwahlknoten eines ISPs anzubinden, als jedes Mal zwei Außenstellen mit diesen Verfahren zu verbinden. Zwischen den Routern der beiden Geschäftsstellen kann über das Internet sodann ein VPN installiert werden. Ein solches virtuelles privates Netzwerk bietet überdies den Vorteil, daß die Internet- und WAN-Verbindungen in einem einzigen Router und einer Leitung zusammengefasst werden kann, womit sich die Kosten für die Infrastruktur und Hardware weiter reduzieren.

VPN und Intranet

Allgemein bekannt sind inzwischen auch Intranets, die bei Unternehmen eingesetzt werden. Man betreibt hierfür ein TCP/IP-Netz, veröffentlicht Informationen auf den internen Web-Servern und installiert für alle Benutzer Web-Browser. Ein gutes Beispiel für eine Intranet-Anwendung ist eine Datenbank, die über das Web erreichbar ist. Außendienstmitarbeiter können eine solche Datenbank nutzen, um Kunden über neue Artikel zu informieren und/oder Angebote abzugeben. Die Datenbank kann mit einem HTML-Frontend ausgestattet werden, so daß man mit einem ganz normalen Web-Browser (Internet Explorer, Netscape) auf die Datenbank zugreifen kann. Die Entwicklung von Intranets hängt dabei eng mit der Ausbreitung des Internet und den beliebten Informationsdiensten im WorldWideWeb (WWW) zusammen - es handelt sich ja letztlich nur um Internet-Technik bzw. -Techniken, die nun in einem privaten Netz verwendet werden.

Mit VPN-Technologie läßt sich der Aktionsradius eines Intranets stark erhöhen. Intranets sollten eigentlich nur für firmeninterne Informationen benutzt werden, daher dürfen sie im Grunde auch nicht vom Internet erreichbar sein. Oft ist es jedoch vorteilhaft, Daten auch zusammen mit weit entfernten Außenstellen zu nutzen oder isolierten Benutzern über das Internet Zugriff auf das Intranet zu gestatten. VPNs bieten sichere Verbindungen zum Intranet an und garantieren zudem, daß vertrauliche Informationen das Netz nicht ungeschützt verlassen. Die meisten Außendienstmitarbeiter sind ständig unterwegs, andere Mitarbeiter sind Teleworker und arbeiten von zu Hause aus. Es spricht nun nichts mehr dagegen, daß diese Personen über das Internet auf den firmeninternen Web-Server zugreifen, auf dem sich beispielsweise die Kundendatenbank befindet. Wichtige bzw. empfindliche Informationen können so berechtigten Benutzer auch im Fernzugriff zugänglich gemacht werden. Mit einem VPN ist es möglich, eine sichere Verbindung zwischen dem Laptop eines Mitarbeiters und dem im Intranet befindlichen Web-Server mit Datenbankzugriff herzustellen und die zu übertragenden Daten daneben noch verschlüsseln. VPNs bieten Standortunabhängigkeit und gestatten, praktisch jeden firmeninternen Dienst oder besser Netzwerk-Dienst sicher über das Internet zu nutzen.

Sicherheit

Jedem Internet-Benutzer dürften die Risiken bewußt sein, die mit der Nutzung des Netzes aller Netze verbunden sind. Laufend entstehen neue Gefahren, wie private Daten (Gesundheitsstatus, Kreditkarten-Nummern, etc.) im Internet in die falschen Hände geraten können. Unternehmen werden durch diese Gefahren jedoch noch viel direkter bedroht. Erspähte oder gelöschte Firmendaten können Einzelpersonen schaden und einem Unternehmen die Existenz kosten, falls beispielsweise Projektdateien oder die Kundendaten gestohlen werden.

Dieses Risiko besteht bei jedem ans Internet angeschlossene System, da das Internet ein öffentliches Netz ist. Bisher mußte sich ein Eindringling bzw. Hacker erst einmal in Ihr Netz einwählen, bevor es überhaupt möglich war, ein System knacken zu können. Der Hacker musste sich zuerst eine Telefonnummer für den entsprechenden Modem-Pool beschaffen und riskierte ein Zurückverfolgen der Verbindung. Falls nun das Unternehmensnetz über das Internet verbunden ist und die Sicherheitsmaßnahmen zu schlampig sind, erhält der Hacker vielleicht schon Einlass zu ihrem Netz, indem er den gewöhnlichen Zugang eines beliebigen ISP gebraucht. Sogar unerfahrene Benutzer können sich Tools für die automatische Sicherheitslückenüberprüfung wie zum Beispiel SATAN beschaffen und damit Sicherheitslücken in einem Unternehmensnetz ausfindig machen. Schwerwiegender ist jedoch, daß man hiervon unter Umständen gar nichts bemerkt. Bevor vertraulichen Daten durch das Internet geschickt werden, sollte man also sicher sein, daß sie durch ein VPN angemessen geschützt sind.

Welche Daten gilt es eigentlich zu schützen? Diese Frage sollte man sich immer stellen. Dem Verantwortlichen einer Firma werden sicherlich zuerst die Dateien auf den vernetzten Rechnern einfallen, solche Dateien können höchstempfindliche Daten beinhalten wie beispielsweise Dokumente mit Unternehmensstrategien, Tabellenkalkulationen mit Finanzanalysen einer geplanten Produkteinführung, Datenbanken mit Informationen zu Gehältern und Steuern oder vielleicht auch eine Sicherheitsanalyse des Firmen-Netzes. Man muss jedoch auch an die weniger gegenständlichen Dinge denken, die ebenfalls eine Verbindung zum Internet besitzen. Hierzu zählen die Dienste, die Mitarbeitern und Kunden zur Verfügung stehen, ferner die Rechnerkapazität, die bereitgestellt wird, und last but not least die Reputation einer Firma. Das Ausnutzen einer Sicherheitslücke könnte dazu führen, daß Benutzer zeitweise keine Verbindung zu anderen Standorten etablieren können oder die elektronische Post (email) von allen Händlern als unzustellbar zurückgeschickt wird.

Am einfachsten und sichersten wäre es sicherlich alle wichtigen Daten gesondert und total isoliert zu speichern. Dies ist jedoch in der modernen Welt mit Telekommunikation, Außendienstmitarbeitern und Fernarbeit nicht mehr ganz so einfach, da beispielweise der Geschäftsführer in der Lage sein muß, unterwegs Finanzdaten abzufragen, genauso wie die Mitarbeiter in der Lage sein müssen, von zu Hause aus auf wichtige Information zugreifen zu können.

VPN Techniken

VPN verwenden verschiedene Techniken zum Schutz der Datenübertragung über das Internet, hierzu zählen besonders Firewalls, Authentifizierung, Verschlüsselung und Tunneling:

Firewalls

Es gibt verschiedene Arten von Firewalls, alle dienen jedoch dem gleichen Zweck, ein bestimmtes wohldefiniertes Gebiet zu schützen. Eine Firewall überprüft zum Beispiel die Internet-Adresse von Paketen oder die Ports, die in eingehenden Verbindungen angefordert werden, und beschließt aufgrund dieser Informationen, welche Daten ins Netz gelassen werden oder halt auch nicht.

Obgleich die meisten VPN-Pakete an sich keine Firewall-Funktionalität aufweisen, stellen Firewalls doch einen integralen Bestandteil von VPNs dar. Das Konzept besteht darin, unerwünschte Besucher wie Hacker durch eine Firewall vom Netz fernzuhalten, VPN-Benutzer andererseits dürfen die Feuerwand unbeschadet passieren. Bevor man ein virtuelles privates Netzwerk aufbauen kann, muß man sich zunächst einmal eine Firewall besorgen, falls man nicht schon längst eine besitzt.

Der gebräuchlichste Firewall-Typ arbeitet mit Paketfilterung, wodurch bestimmte IP-Dienste an bestimmten Portnummern am Durchlaufen des Gateway-Router gehindert werden. Die meisten Router, die VPN-Techniken unterstützen, besitzen auch die Möglichkeit der Paket-Filterung. Ebenso werden Proxies häufig verwendet, um ein Netz abzusichern und nur VPN-Dienste passieren zu lassen. Bei einem Proxy-Server handelt es sich meist um eine Softwarelösung, die in der Anwendungsschicht auf einem Netzbetriebssystem gestartet wird.

Authentifizierung

Die Authentifizierung stellt ein weiteres überaus wichtiges Element von VPNs dar, da sie dafür gerade stehen muß, daß die Kommunikation wirklich zwischen den gewünschten Parteien erfolgt. Die meisten VPN-Authentifizierungssysteme beruhen auf gemeinsame Schlüssel. Die Schlüssel durchlaufen einen Hash-Algorithmus, der einen Hash-Wert generiert. Die zweite Partei, die dieselben Schlüssel ihr eigen nennt, erzeugt ebenso einen Hash-Wert und vergleicht diesen mit dem Wert, den sie von der anderen Seite bekommen hat. Der über das Internet transferierte Hash-Wert ist für Lauscher nutzlos, so daß beim Abhören des Netzverkehrs kein Passwort erschnüffelt werden kann. Das Challenge Handshake Authentication Protokoll (kurz: CHAP) ist ein gutes Beispiel für ein Authentifizierungsverfahren, das genau dieses Konzept verwendet.

Authentifizierung wird gewöhnlich zu Anfang einer Sitzung gemacht und danach in wahllosen Abständen wiederholt, um garantieren zu können, daß sich kein Betrüger in die Kommunikation eingeschlichen hat. Authentifizierung kann auch als Garantie der Datenintegrität verwandt werden, hierbei durchlaufen die eigentlichen Daten einen Hash-Algorithmus, dessen Resultat als Prüfsumme an die Nachricht angehängt wird. Falls nun die gesendete von der am Zielort berechneten Prüfsumme differiert, ist es unverkennbar, daß die Daten beim Transfer beschädigt oder abgehört und verändert wurden.

Verschlüsselung

Alle VPNs unterschützen Verschlüsselung, hierbei werden die Daten in ein sicheres Packet verpackt. Verschlüsselung ist ebenso bedeutsam wie Authentifizierung, da sie die Daten beim Transfer vor Paketschnüfflern absichert. In VPNs werden hauptsächlich zwei Verfahren benutzt, nämlich die Secret-Key-Verschlüsselung und die Public-Key-Verschlüsselung.

Bei der Secret-Key-Verschlüsselung gibt es ein gemeinsames geheimes Passwort, das allen Benutzern bekannt ist, die Zugriff auf die verschlüsselten Informationen benötigen. Mit diesem Schlüssel werden die Informationen codiert und decodiert. Das wohl bekannteste Beispiel für ein Secret-Key-Verfahren ist der Data Encryption Standard (DES).

Die Problematik der Secret-Key-Verschlüsselung besteht nun darin, daß alle Benutzer den geheimen Schlüssel kennen müssen, um auf die verschlüsselten Daten zugreifen zu können. Für einen kleinen begrenzten Kreis ist dies kein Problem, in einem großen Netzwerk mit vielen Benutzern hingegen ist dieses Verfahren jedoch überhaupt praktikabel. Man muß sich nur den Aufwand vor Augen führen, falls sich irgendetwas an der Personalstruktur ändert. Beispielweise hört 3jemand bei der Firma auf, dann muß der alte gemeinsame Schlüssel schnellstmöglich entfernt, ein neuer Schlüssel installiert und alle Benutzer auf sicherem Wege davon benachrichtigt werden.

Einen Ausweg aus der Misere bietet die Public-Key-Verschlüsselung. Hier gibt es einen öffentlichen Schlüssel und einen privaten Schlüssel. Den öffentlichen Schlüssel kann man allgemein bekannt geben, wohingegen der private Schlüssel geheim bleiben muß. Um einem anderen Teilnehmer empfindliche Daten zu zusenden, codiert man diese mit einer Kombination aus dem eigenen privaten und dem öffentlichen Schlüssel des Empfängers. Dieser decodiert die Daten anhand des öffentlichen Schlüssels des Senders und seines privaten Schlüssels. Je nach eingesetzter Software, differieren die Schlüssellängen des öffentlichen und privaten Schlüssels, welche recht groß sein können, so daß man sie sich nicht einprägen kann. Daher speichert man sie meist auf dem Rechner der Person, die das Verschlüsselungsverfahren benutzt. Die privaten Schlüssel ihrerseits werden normalerweise mittels Secret-Key-Verfahren wie DES und eines einprägsamen Passworts gespeichert. Hierdurch wird verhindert, daß ein Hacker im System private Schlüssel im Klartext lesen kann. Wohl das bekannteste Programm zum Datenschutzt, das mit Public-Key-Verschlüsselung arbeitet, ist Pretty Good Privacy (PGP). Der größte Nachteil der Public-Key-Verschlüsselung besteht allerdings darin, daß die Codierung im Vergleich zur Secret-Key-Methode in der Regel viel langsamer ist.

Im Gegensatz zu PGP, wo die codierten Daten als Datei gespeichert werden, findet in einem VPN eine Verschlüsselung der Daten in Echtzeit statt. Aus diesem Grund werden Nachrichten, die in VPNs übertragen werden sollen, mit Secret-Key-Verfahren und Schlüsseln codiert, die nur für die Dauer der momentanen Sitzung gültig sind. Der sogenannte Sitzungsschlüssel, der meist kürzer als die Daten ist, wird vor dem Transfer mit einem Public-Key-Verfahren codiert.

Das nächste und meiner Ansicht nach wichtigste Verfahren ist IPSec (secure IP). IPSec oder RFC-1825, ist ein Standard, der IP-Pakete schützt und Sicherheit transparent für Anwendungen ermöglicht, es besteht aus einer Vielzahl von Empfehlungen der IETF für ein sicheres IP-Protokoll für IPv4 und IPv6. Hierbei handelt es sich um Verschlüsselung, die bereits in der IP-Schicht und nicht erst in höheren Schichten stattfindet, wie es bei SSL und den meisten VPN-Produkten der Fall ist. IPSec erzeugt einen offenen Standard für VPNs. Momentan werden in einigen der wichtigsten VPN-Produkten herstellerspezifische Verschlüsselungsmethoden oder offene Standards eingesetzt, an die sich allerdings nur wenige Hersteller halten. Die meisten Hersteller sehen in IPSec jedoch keine Konkurrenz, sondern vielmehr die Möglichkeit, Sicherheitsmaßnahmen zu verbessern und die Tunneling- und Verschlüsselungsverfahren um ein kompatibles Element zu erweitern.

Tunneling

Eigentlich alle VPN-Produkte setzen das Tunneling-Verfahren zur Etablierung eines privaten Netzes ein. VPNs bieten die Möglichkeit, sich über das Internet, das im Grunde ein gigantisches IP-Netzwerk darstellt, mit einem entfernten Netz zu verbinden. Viele (firmeninterne) LANs verwenden jedoch nicht nur TCP/IP. Bei Netzwerken mit Windows NT Servern kommt beispielsweise NetBEUI zum Einsatz, Novell-Server benutzen das IPX-Protokoll. Tunneling bietet die Aussicht, ein Paket in ein anderes Paket zu kapseln und damit inkompatible Protokolle zusammenzubringen. Das gekapselte Paket kann demselben, aber auch einem völlig anderen Protokoll angehören. Durch Tunneling können zum Beispiel IPX-Pakete über das Internet gesendet werden, so daß ein ferner Benutzer auf einen Novell-Server zugreifen kann.

Mit dieser Methode lässt sich ein IP-Paket in ein anderes IP-Paket kapseln. Dies hat den Vorteil, Pakete mit willkürlichen Ziel- und Quell-Adressen im Internet zu versenden, da diese wiederum in Paketen untergebracht sind, deren Ziel- und Quelladresse geroutet werden können. Man kann demnach auch den reservierten IP-Adressbereich, also dem im Internet nicht routing-fähigen Adressbereich, benutzen, der von der IANA (Internet Assigned Numbers Authority) für private Netze vorgesehen ist.

Tunnel durch das Internet lassen sich auf Basis unterschiedlicher Protokollstandards verwirklichen. Microsoft entwickelte beispielsweise die PPTP-Technologie (Point-to-Point Tunneling Protocol), das für die Einwahl zum ISP eingesetzt wird. Das alternative Tunneling Protokoll L2F (Layer 2 Forwarding) wurde von Cisco entwickelt. Beides sind zwar Protokolle der Ebene 2 nach dem OSI-Schichtenmodell, allerdings verhalten sie sich nicht kompatibel zueinander. Dieses Manko wird durch L2TP (Layer 2 Tunneling Protocol) behoben, da der von der PPP Working Group (Microsoft, Cisco, Ascend, 3COM) definierte L2TP-Standard die beiden Protokolle L2F und PPTP miteinander verbindet. Weitere Standards, die in VPNs zum Einsatz kommen, sind X.509-Zertifikate, das Lightweight Directory Access Protocol (LDAP) und Radius zur Authentifizierung.

Die Bandbreite an VPN-Produkten geht inzwischen von reinen Software-Lösungen, die auf oder besser in Abstimmung mit einem Netzbetriebssystem ausgeführt

werden - ein gutes Beispiel hierfür ist der AltaVista Tunnel - über Hardware-Router/Firewalls bis zu integrierten Hardware-Lösungen, die speziell für den VPN-Einsatz konzipiert worden sind. Dazu zählt beispielsweise VPNet oder Bay Networks Extranet Switch. Einige VPN-Protokolle wie SSH oder SSL sind bereits in anderer Funktion bekannt geworden, werden inzwischen aber genauso in VPNs verwandt.

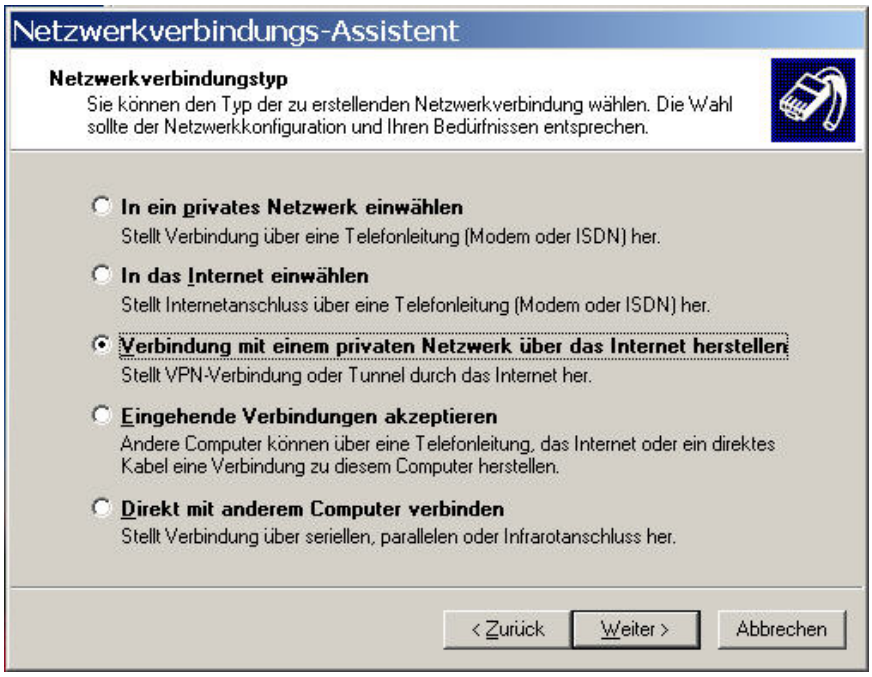


Bild: VPN Zugang einrichten unter Windows 2000

Mittlerweile bieten übrigens auch verschiedene ISPs VPN-Dienste an. Das Tunneling beispielsweise wird meist auf den Geräten des ISP durchgeführt. Diese Variante besitzt noch einige weitere Vorteile, auf die aber hier nicht näher eingegangen werden soll.

Zuverlässigkeit

Eine ganz wichtige Frage beim Einsatz von VPNs ist die nach der Zuverlässigkeit. Das Internet ist leider nicht unbedingt für seine Zuverlässigkeit bekannt. Auf ihrem Weg durch das Internet passieren die Pakete oft mehrere Netze mit ganz unterschiedlicher Geschwindigkeit, Zuverlässigkeit und Funktionalität. All diese verschiedenen Netze stellen potentielle Problemfelder dar. Die fehlende Zuverlässigkeit des Internet und das Faktum, daß es von keiner definierbaren Instanz kontrolliert wird, macht es einem Netzadministrator relativ schwer, VPN-Probleme zu analysieren bzw. zu beheben. Falls sich ein Benutzer nicht per remote access in den Server einwählen kann oder die Verbindung über eine Standleitung Probleme bereitet, weiß der Administrator, daß hierfür nur eine limitierte Anzahl von möglichen Ursachen in Frage kommt.

Hingegen bei einem VPN über das Internet könnte das Problem bei dem Rechner am anderen Ende, beim ISP am anderen Ende, bei einem der zwischenliegenden Netze, beim ISP der Firma oder beim Server oder Router in der Firma liegen. Einige große ISPs offerieren gewisse Sicherheiten für einen glatten VPN-Service, sofern alle beteiligten Parteien an deren Netz angeschlossen sind. Der Netzadministrator wird jedoch immer wieder in Situationen geraten, wo er auf seine eigenen Möglichkeiten, Fähigkeiten und Erfahrungswerte angewiesen ist.

Planung

VPNs bieten eine große Anzahl an Vorteilen, allerdings verlangen sie auch Experten. Dies fängt schon bei der Implementierung an. Der verantwortliche Netzwerkplaner muß hierbei zahlreiche Faktoren ins Kalkül ziehen. Einleitend sollte eine Einschätzung der Benutzer und der Art der zu transferierenden Daten erfolgen, da infolgedessen die richtige VPN-Lösung zusammenzustellen ist. Bei jeder Fernzugriffslösung sind die Benutzer und ihr Arbeitsverhalten ein bestimmender Faktor bei der Definition der Systemanforderungen.

Beim Direktwahlzugang stellt sich die ausschlaggebende Frage, wie viele Anschlüsse erforderlich sind, bei VPN kommt dies der Anzahl der Sessions gleich, die parallel unterstützt werden können. Unter allen Umständen schlagen sich die Sessions/Anschlüsse in Kosten für notwendige Hardware sowie für die damit verbundene Pflege und Erhaltung nieder. Das Unternehmen muß ein Verhältnis von Benutzern pro Anschluß bestimmen und bekommt somit den Leistungsgrad für den Fernzugriff.

Je mehr Teilnehmer pro Anschluß, desto höher die Wahrscheinlichkeit, daß einer von ihnen keine Verbindung erhält, während im umgekehrten Fall die Kosten für die Ausrüstung steigen. Ratsam ist zirka ein Verhältnis von einem Anschluß/Sitzung pro zehn Benutzer. Ferner ist die leichte Implementierung eines VPN-Gateways zu erwähnen. Längst konfigurierte Router, Firewalls und Sicherheitspakete lassen sich unverändert beibehalten, womit keine zusätzliche Arbeit anfällt.

Fazit

Speziell in den Bereichen E-Commerce, Internet-Shopping oder beim Transfer sensibler Informationen stellen VPNs die bestmögliche Technologie dar. Da es sich bei diesen meist um IPSec-Verbindungen handelt, die IP-Pakete übertragen, besteht für den Endbenutzer vollkommene Transparenz. Mit Hilfe der 168-Bit-Verschlüsselung (TripleDES) befindet man sich auf alle Fälle auf der "sicheren Seite". •

Sonderaktion!
befristet bis 30.04.2005

Jetzt Mitglied werden im AUGE e.V.!

Bitte nachstehenden Aufnahmeantrag ausfüllen und unterschrieben einsenden an das Vereinsbüro:

AUGE e.V.
Wielandstr. 41
D-60318 Frankfurt a. M.

AUGE

Der AUGE e.V. bietet Kontakt und Wissensaustausch mit anderen Mitgliedern durch:

- Regelmäßige Regionaltreffen an verschiedenen Orten in Deutschland (vielfach mit Vorträgen)
- Publikationen des Vereines per Newsletter, CD-ROM und als Online-Magazin
- Arbeitsgemeinschaften zu speziellen Schwerpunktthemen
- Online-Community im Web mit Forum, Kleinanzeigen etc.
- Kostenloser Web-Space und E-Mail Account
- **Prämie bei Neueintritt: MP3-Player für SD Card und SD-Card 256MB**

[ ] Aufnahmeantrag
[ ] Änderungsmitteilung (nur für Mitglieder) zu Mitgliedsnummer: .....

Bitte verwenden Sie dieses Formular auch dann, wenn sich Ihre Anschrift oder Kontoverbindung geändert hat.

Bitte füllen Sie die folgenden Felder vollständig aus:

Name .....

Vorname .....

Firma (falls Firmenantrag) .....

Straße, Hausnummer .....

Nationalität ..... Postleitzahl ..... Ort .....

Geburtsdatum .....

Bitte füllen Sie diese Felder aus, wenn Sie per Lastschrift zahlen wollen (siehe nebenstehenden Text):

Kontonummer ..... Bankleitzahl .....

Geldinstitut, Ort .....

Kontoinhaber (falls vom Antragsteller abweichend) .....

Hiermit ermächtige ich/wir den Verein AUGE e.V. widerruflich, die von mir/uns zu entrichtenden Zahlungen bei Fälligkeit zu Lasten meines / unseres nebenstehend angegebenen Kontos mittels Lastschrift einzuziehen. Wenn das angegebene Konto die erforderliche Deckung nicht aufweist, besteht seitens des kontoführenden Geldinstituts keine Verpflichtung zur Einlösung. Teileinlösungen sind bei Lastschriften ausgeschlossen.

Freiwillige Angaben:

Beruf .....

Telefon (privat) ..... Telefax (privat, 24 Std.) .....

E-Mail-Adresse .....

Mit der Angabe meiner E-Mail-Adresse stimme ich der Einrichtung eines E-Mail-Alias in der Form <vorname>.<nachname>@auge.de und der Eintragung in den E-Mail-Verteiler des AUGE e.V. zu.

Hiermit beantrage ich die Aufnahme in den AUGE e.V. unter Anerkennung der Vereinssatzung und der für die Gewährung der Prämie im Rahmen dieser Sonderaktion geltenden nachstehenden Zusatzbedingungen:

- Die Mitgliedschaft ist erstmalig nach Ablauf eines Jahres kündbar.
- Es handelt sich um einen Neueintritt, nicht um einen Ersatz für eine bereits bestehende Mitgliedschaft, d.h. in den vergangenen 12 Monaten ist kein Austritt aus dem Verein erklärt worden.
- Es wird mindestens ein voller Mitgliedsbeitrag geleistet, d.h. Beitragsermäßigungen können frühestens nach 12 Monaten geltend gemacht werden

Der Weitergabe meiner Kontaktdaten an andere Mitglieder stimme ich zu *(falls unzutreffend, bitte streichen).*

Ort, Datum Unterschrift

.....
(bei Minderjährigen auch die Unterschrift des gesetzlichen Vertreters)

Der Mitgliedsbeitrag beträgt derzeit pro Jahr 54,- EUR für natürliche und 96,- EUR für juristische Personen/Firmen. Für Schüler und Studenten gilt gegen Nachweis bis zum vollendeten 27. Lebensjahr ein ermäßigter Beitrag von 30,- EUR.

Die auf diesem Antrag gemachten Angaben werden elektronisch gespeichert und nach Beendigung der Mitgliedschaft gelöscht.

Der Verein für Computeranwender

Information und Erfahrungsaustausch
Regionale Treffen

Mehr unter: www.auge.de

Treffen in der Region Stuttgart

Regionalgruppe Stuttgart

www.auge.de/rg700

Regionaltreffen

Letzter Freitag im Monat
um 19:00 Uhr
in Stuttgart
Sportgaststätte West
Herderplatz
an der U-Bahn Haltestelle
Herderplatz

Kontakt

Michael Schäl
Wolfmahdenstraße 12
70563 Stuttgart
Tel.: 0 711 / 9 01 83 04
rg700@auge.de

Regionalgruppe Ostalb

www.auge.de/rg735

Regionaltreffen

3. Samstag im Monat
um 14:30 Uhr
in Schwäbisch Gmünd
Vereinsheim der Naturfreunde
Hintere Schmiedgasse 16

Kontakt

Michael Welz
Scheffelstraße 7
73540 Heubach
Tel.: 0 71 73 / 7 16 33 55
rg735@auge.de