Wie viel Sicherheit braucht Ihr PC?

Sicherheit ist von individuellen Risiken abhängig. PC Professionell zeigt, welche maximale Security-Konfiguration Sie wirklich benötigen und welche Kosten damit verbunden sind.

Anna Lanvent, Werner Pliegl, Heiko Mergard

Das Angebot an Sicherheits-Software ist unüberschaubar. Firewalls, Antirenprogramme, Security-Suiten oder Malware-Scanner sollen den Anwender vor Viren und Attacken aus dem Web schützen. Für die Anbieter ist das ein gutes Geschäft – auch wenn die IT-Branche noch immer an schwachem Absatz krankt. So hat Symantec, der Marktführer bei Security-Software, bereits im vergangenen Jahr einen Rekordgewinn von über 71 Millionen Dollar eingefahren.

Beim Geschäft mit der Angst vor Viren, Würmern und Hackern zahlt aber meist der Anwender drauf. Viele wissen nicht genau, welche Software sie tatsächlich benötigen und welche schlicht überflüssig ist. Die Sicherheit von PCs, kleinen Workgroups und größeren Netzwerken lässt sich nicht über eine bunte Anhäufung von Sicherheitsprogrammen steigern. Im Gegenteil: Wer wahllos Programme kauft und installiert, verringert nicht nur Leistung und Komfort bei der Bedienung, sondern gefährdet unter Umständen sogar die Integrität des Systems. Hard- und Software-Firewalls im Kombi-Einsatz vertragen sich zum Beispiel oft nicht. Der Einsatz unterschiedlicher Virenscanner im Netzwerk oder auf einer Festplatte verlangsamt das komplette System und irritiert User mit Falschmeldungen. Zwei Virenscanner parallel zu installieren, ist nicht sinnvoll.

Das kostet Sicherheit

Höchste Sicherheit für Endanwender und Unternehmen bedeutet nicht automatisch immense Investitionen. Gerade User, die den PC nicht kommerziell nutzen, können sich oft zum Nulltarif gezielt vor Viren, Würmern und Hacker-Attacken schützen. Auch bei kleinen Unternehmen mit bis zu fünf Mitarbeitern halten sich die Anschaffungskosten mit insgesamt 1500 bis

»PC-Sicherheit erfordert keine teuren Investitionen, sondern exakte Kenntnisse der Gefahren. Wirksame Gegenmittel gibt es auch kostenlos.«

Software-Redakteur **Heiko Mergard**

2000 Euro im Rahmen, wenn sich diese beispielsweise für ein kostengünstiges WLAN entscheiden und die Konfiguration selbst übernehmen.

Große Unternehmen hingegen müssen ihr Netzwerk vor Datenspionage schützen und auch im Falle von Angriffen die ständige Verfügbarkeit der Daten gewährleisten. Dennoch lassen sich auch hier erhebliche Einsparungen erzielen, denn viele Investitionen sind überflüssig.

Anhand dieser drei Szenarien – Profi-User, kleine Netze und große Unternehmen – erläutert dieser Beitrag die Bedrohungen, geeignete Gegenmaßnahmen und die jeweiligen Kosten.

Sicherheit beginnt im Kopf

Wer sich gegen Angriffe wirksam schützen will, sollte sich zunächst mit den vorhandenen PCs und Programmen beschäftigen – und nicht in Panik-Käufe verfallen. Die entscheidenden Fragen lauten: Welchen Gefahren ist mein IT-System ausgesetzt? Welche Gefahren spielen keine Rolle? Datensicherheit, vor allem im IT-Business-Bereich ist immer ein Produkt aus den individuellen technischen Anforderungen und den Risikofaktoren.

Um die individuellen Lücken im System aufzuspüren, sind Security-Audits sinnvoll. Empfehlenswert sind Dienste wie *www.securityspace.com* und *security.symantec.com/de* sowie *www.it-sec.de* – diese bieten auch kostenlose Sicherheits-Checks. Am sparsamsten geht vor, wer die Lücken dann mit Bordmitteln und einer optimalen Konfiguration des Betriebssystems eindämmt. Erst im nächsten Schritt ist zu überlegen, welche Anschaffungen darüber hinaus notwendig sind.

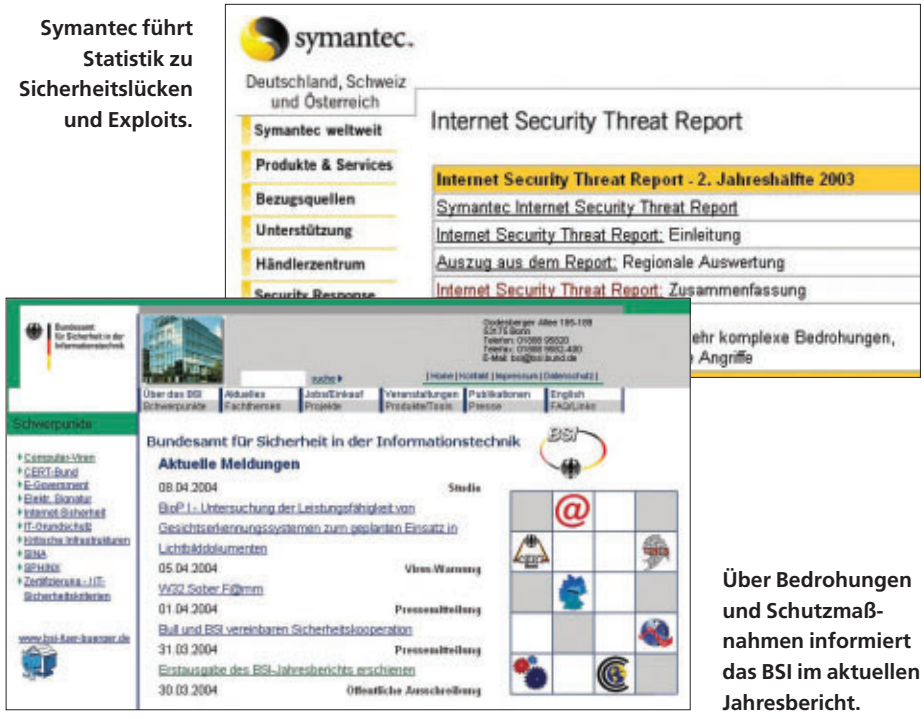
Mit jeder Erweiterung der IT-Infrastruktur potenzieren sich Fehleranfälligkeit und Sicherheitsbedürfnisse. Der Umkehrschluss: Ein Privatanwender mit nur einem PC kann die tatsächlichen Bedrohungen mit wenig Aufwand und fast kostenfrei bannen. Ein Unternehmen muss jedoch in eine zentrale Sicherheitsinfrastruktur investieren, um die Mitarbeiter daran zu hindern, versehentlich einen Virus einzuschleusen. Tipps dazu bietet auch das IT-Grundschutz-Handbuch des Bundesamtes für Sicherheit in der Informationstechnik, kurz: BSI. Interessenten können die CD kostenlos bestellen (siehe *www.bsi.de/produkte/cdrom/index.htm*).

Wachsende Bedrohungen

Eine genaue Kenntnis der Gefahren ist umso wichtiger, je intensiver die Web-Attacken sind. Laut der Sicherheits-Taskforce CERT *(www.cert.org)* haben sich seit 1993 die von Firmen gemeldeten Angriffe und Wurmattacken verzehnfacht. Im letzten Jahr wurden mehr als 100 000 Attacken registriert. Die Dunkelziffer dürfte die Millionengrenze erreichen. HME

Weitere Infos

- **www.microsoft.com/germany/ms/security/guidance/topics/patchmanagement.mspx**
  Anleitungen für zentrales Patch-Management
- **www.microsoft.com/germany/ms/security/guidance/default.mspx**
  Security-Workshops für Firmen und IT-Profis
- **www.microsoft.com/germany/ms/security/winsec.mspx**
  alle aktuellen Security-Bulletins zu Windows XP
- **www.bsi.de/literat/jahresbericht/bsijahresbericht2003b.pdf**
  Sicherheits-Jahresbericht 2003 des BSI
- **www.symantec.com/region/de/pressenter/threat_reports.html**
  Sicherheitsreport für das zweite Halbjahr 2003
- **Vollkasko gegen Viren**
  PC Professionell, Ausgabe 1/2004, ab Seite 144
- **Windows sicher machen**
  PC Professionell, Ausgabe 3/2004, ab Seite 36



Symantec führt Statistik zu Sicherheitslücken und Exploits.

Über Bedrohungen und Schutzmaßnahmen informiert das BSI im aktuellen Jahresbericht.

Sicherheit für Profis

Der Rundum-Schutz, etwa vor Viren- und Hacker-Attacken, ist beim Einzelplatz-PC ohne großen Aufwand realisierbar. Und fast alle wichtigen Gefahren aus dem Internet lassen sich zudem mit kostenlosen Hilfsmitteln ausschalten.

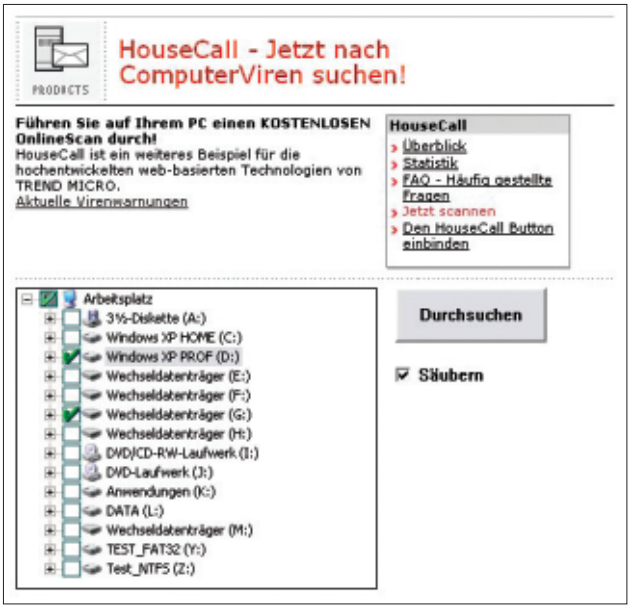
Anna Lanvent

Für Endanwender ist die Zahl der wirklich gefährlichen Sicherheitsrisiken überschaubar. Das macht sich auch bei den nötigen Ausgaben für Sicherheit positiv bemerkbar. Wer in der Lage ist, notfalls selbst eine schadhafte Datei aus dem System zu entfernen, muss nicht einen einzigen Cent ausgeben und schützt den Rechner einfach mit dem kostenlosen Virenscanner Antivir *(www.free-av.de)*, der guten Standard-Firewall von Sygate *(www.sygate.de)* und dem Anti-Dialer-Tool A2 *(www.emisoft.de)*.

Wer es hingegen komfortabler und professioneller mag, setzt bei der Virenerkennung auf das verlässliche Panda Antivirus 7 und wählt am besten die sehr sichere Firewall Sygate 5.5 in der Pro-Edition. Letztere ist zwar relativ kompliziert zu bedienen, erreicht jedoch eine hervorragende PC-Absicherung. Die Suche nach Spyware überlassen Sie am besten dem Profi Pest Patrol *(www.pestpatrol.de)*. Dieses Sicherheitskomplettpaket kostet insgesamt nicht einmal 150 Euro.

Topaktuell: Virenschutz online

Der Einsatz eines Virenscanners ist unentbehrlich. Im *PC-Professionell*-Test in Ausgabe 1/2004 erreichte Panda Antivirus 7 die beste Platzierung *(www.panda-software.de)*. Aber auch Norton Antivirus *(www.symantec.de)* und Gdata Antivirenkit Pro 2004 *(www.gdata.de)* erzielten gute Noten. Kostenlos verfügbar ist Antivir Personal Edition von H&B EDV.



Der Online-Virenscanner von Trend Micro überprüft Partitionen und Ordner kostenlos per Internet-Zugriff.

Im Gegensatz zum pflegebedürftigen Programm auf der Festplatte arbeitet das kostenlose Housecall mittels Online-Scan per ActiveX-Control *(de.trendmicro-europe.com/enterprise/products/housecall_it.php)*. Der Vorteil: Housecall scannt immer mit aktuellsten Signaturen. Der Nachteil: Bei einem Virenfund muss sich der Anwender unter Umständen selbst um die Desinfektion kümmern.

Tipp: Virenschutz ohne Tools

Ein Virenscanner gilt gemeinhin als Garant für PC-Sicherheit. Tatsächlich ist aber die Wahrscheinlichkeit, Opfer einer Virenattacke zu werden, für verantwortungsbewusste Privatanwender relativ klein. Das hat zwei Gründe: Zum einen kommen die meisten Viren noch immer als E-Mail-Anhang. Wer also grundsätzlich keine PIF-, SCR- oder EXE-Dateien öffnet, die er nicht ausdrücklich angefordert hat, schaltet bereits einen Großteil der Gefahren aus, die etwa auch von bekannten Würmern wie Netsky ausgehen.

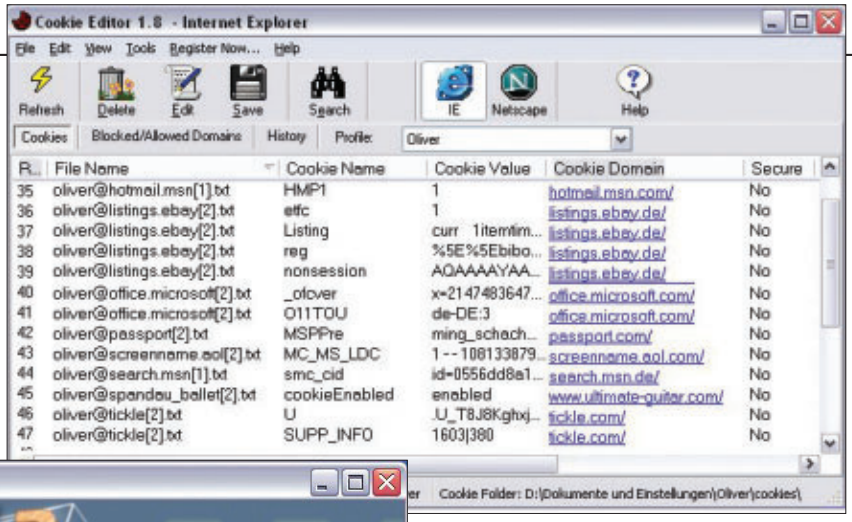
Die zweite wichtige Gruppe von noch immer aktuellen Wurm-Virus-Kombinationen schlüpft durch bekannte Sicherheitslecks wie das ungepatchte RPC-Modul (Remote Procedure Call). Was Blaster im Sommer letzten Jahres vorgemacht hat, ahmen jetzt dessen Enkel, zum Beispiel Gaobot, nach. Nichts zu befürchten hat demnach, wer regelmäßig die Patches von Microsoft einspielt. Am einfachsten ist dies mittels *Systemsteuerung/Automatische Updates*. Hier legen Anwender fest, nach welchem Modus neue Updates eingespielt werden sollen, beispielsweise automatisch oder nach Rückfrage.

Firewalls – die beste ist gratis

Auch der Einsatz einer sicheren Firewall ist auf Einzel-PCs unverzichtbar. Der steigende Anteil von Privatanwendern, die etwa per Highspeed-DSL ins Web gehen, eröffnet Angreifern gute Aussichten: Denn aufgrund der hohen Übertragungsgeschwindigkeiten sind diese User lohnende Opfer für Hacker, die über Trojaner, Backdoor-Viren oder verseuchte Webseiten versuchen, Malware einzuschleusen. Im schlimmsten Fall missbraucht der Angreifer sein Opfer als Proxy-Server, indem er über dessen IP-Adresse Viren verteilt oder weitere Hacker-Attacken vorbereitet.

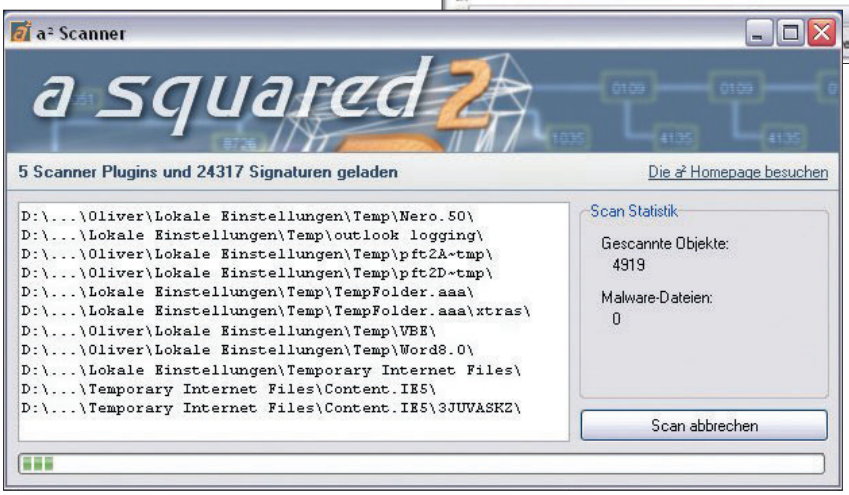
Schutzmaßnahmen

- **Virensendung per E-Mail**
  Panda Antivirus kontrolliert POP3-Accounts
- **Hacker-Angriffe, Port-Scans**
  Sygate Personal Firewall schließt offene Ports
- **Spionage über Webbugs**
  Malware-Scanner wie beispielsweise Spybot finden Spy-Cookies
- **Dialer**
  Dialer-Scanner wie A2 enttarnen Dialer
- **Browser-Hijacking**
  Pest Patrol findet schädliche ActiveX-Controls



Nicht alle Cookies sind harmlos. Inhalt und Wirkung der Text-Spione verrät die Shareware Cookie-Editor.

Nach Dialern, Spionage-Programmen und Würmern sucht die Freeware A2.



Der Testsieger aus *PC Professionell* 3/2004, die Sygate Firewall *(www.sygate.de)*, ist als Standard Edition kostenlos. Ferner erreicht auch die gut ausgestattete Norman Personal Firewall 1.4 *(www.norman.de)* eine noch gute Leistung im Bereich Sicherheit.

Spam & Spionage

Werbetreibende haben es mit perfiden Mitteln auf die PC-User abgesehen. Einige Cookies von manipulierten Web-Inhalten sind in der Lage, private Informationen des Anwenders an einen zentralen Server zu senden. Die Rede ist von Web-Bugs. Das sind winzige GIF-Dateien, die mit CGI-Skripten versehen sind und dynamisch Daten an den Ursprungs-Server zurücksenden.

Abhilfe schaffen hier Spionage-Abwehrprogramme wie die Freeware Spybot Search and Destroy 1.23 *(www.safer-networking.org)*. Das Programm sucht die Registry nach verräterischen Spuren ab und überzeugt mit sehr guten Erkennungsraten. Deutlich schneller gelingt die Suche über den Online-Privacy-Dienst Pestscan *(www.pestscan.de)*. Der einzige Nachteil dieser kostenlosen Lösung: Die gefundenen Spyware-Programme werden nicht automatisch eliminiert. Wer es komfortabler mag, sollte zur Vollversion von Pest Patrol für rund 50 Euro greifen (*www.pestpatrol.de*).

Sowohl Pestscan als auch Pest Patrol kümmern sich zudem um so genannte Spyware-Cookies. Diese protokollieren ebenfalls das Surf-Verhalten des Users und geben den gesammelten Datenbestand an andere Server weiter. Der Internet Explorer verbirgt eine rudimentäre Cookie-Verwaltung unter *Datenschutz/Erweitert*. Wesentlich mehr Informationen zum Inhalt und der Wirkungsweise der geladenen Cookies verrät die Shareware Cookie-Editor *(www.spychecker.com,* 12 US-Dollar).

Dialer & Browser-Hijacking

Noch immer ein Thema sind Dialer. Zwar hat die Rechtsprechung mittlerweile klargestellt, dass ein versehentlich installierter Dialer nicht automatisch zur Zahlungsverpflichtung führt. Dennoch gilt es, diese Gefahr im Vorfeld auszuschalten. Anwender, die nicht über DSL- oder Kabel ins Internet gehen, sollten einen Dialer-Scanner mit der Systemwartung beauftragen. Empfehlenswert sind die Freeware-Tools A2 *(www.emsisoft.de/de/software/free/)* sowie der 0190-/0900-Warner *(www.wt-rate.com)*. A2 hat den nützlichen Nebeneffekt, dass es auch nach weiterer Spyware Ausschau hält.

Browser-Hijacking bezeichnet das Umleiten von Startseiten oder Suchanfragen im Internet auf bestimmte, meist mit Malicious-Code manipulierte Webseiten. In der Regel ist ein Javascript oder ein lokal installiertes ActiveX-Control dafür verantwortlich. Malware-Scanner wie Pest Patrol sind jedoch in der Lage, Übeltäter dieser Art auf dem System zu finden und verlässlich zu löschen. HME

Checkliste Bedrohungen und Gegenmittel

Bedrohung	Maßnahme	Programmempfehlung	Preis	Info
Virensendung	Virenscanner, Online-Scan der verdächtigen Datei	Panda Antivirus Platinum 7, lokal/ Housecall von Trend Micro, online	70 Euro/kostenlos	www.panda-software.de, www.trendmicro.de
Hacker-Attacken	Firewall	Sygate Firewall Standard/5.5 Pro	kostenlos/34 Euro	www.sygate.de
Web-Bugs	Malware-Scanner	Pest Patrol, lokal/Pestscan, online	40 Euro/kostenlos	www.pestpatrol.de, www.pestscan.de
Spyware-Cookies	Cookie-Verwalter	Cookie-Editor (Shareware)	12 US-Dollar	www.spychecker.com
Dialer	Dialer-Scanner	A2	kostenlos	www.emsisoft.de
Browser-Hijacking	Malware-Scanner	Pest Patrol	50 Euro	www.pestpatrol.de

Sicherheit für kleine Netzwerke

Drei oder mehr vernetzte PC-Arbeitsplätze benötigen bereits ein zentrales Sicherheitskonzept. Der dafür nötige Aufwand und die entsprechenden Kosten bleiben etwa dank WLAN und Netzwerk-Scanner überschaubar. Anna Lanvent, Heiko Mergard

Die Preise für drahtlose Netzwerke (WLAN) fallen. Nicht zuletzt deshalb bieten sich WLANs für kleinere Büros an. Die Kosten liegen bei rund 150 Euro für einen DSL-WLAN-Router mit Firewall. Gut beraten sind Anwender mit dem Belkin F5D7630-4B. Das mit 130 Euro sehr günstige Gerät bietet neben WPA-Verschlüsselung und einer Stateful Inspection Firewall auch Ping-Blocking sowie Paket- und URL-Filter (siehe auch ab Seite 86).

Die weiteren Kosten für eine notwendige Sicherheitsinfrastruktur hängen von der Zahl der vernetzten Workstations ab. Auf jedem Rechner sollte ein Virenscanner installiert sein. Dabei scheiden im Büro wegen kommerzieller Nutzung Freeware-Tools aus. Panda Antivirus Platinum 7 zeigt sehr gute Leistungswerte (*PC-Professionell*-Test 1/2004, Seite 144) und lässt sich als 5er Lizenz für Peer-to-Peer-Netze für 240 Euro erwerben.

Zusätzlich sind ein Image- sowie ein Verschlüsselungs-Tool unverzichtbar, um sich gegen hohe Verluste im Falle von Datensabotage zu wappnen. Pro Workstation entstehen damit Kosten von rund 200 Euro.

Verzicht auf teure Server

Kleine und mittlere Unternehmen, die nur wenige Arbeitsplätze ausstatten, können in der Regel auf eine teure Server-Infrastruktur verzichten. Sofern die Clients im Peer-to-Peer-Netz nach einheitlichen und genau überwachten Regeln konfiguriert werden. Das verlangt von allen Anwendern hohe Disziplin bei der Pflege des Systems mit Patches und Security-Updates. Denn die Integrität der installierten Betriebssysteme folgt dem Prinzip des kleinsten gemeinsamen Nenners. Jeder Rechner gewährt nur so viel Schutz wie der schwächste PC im Netz.

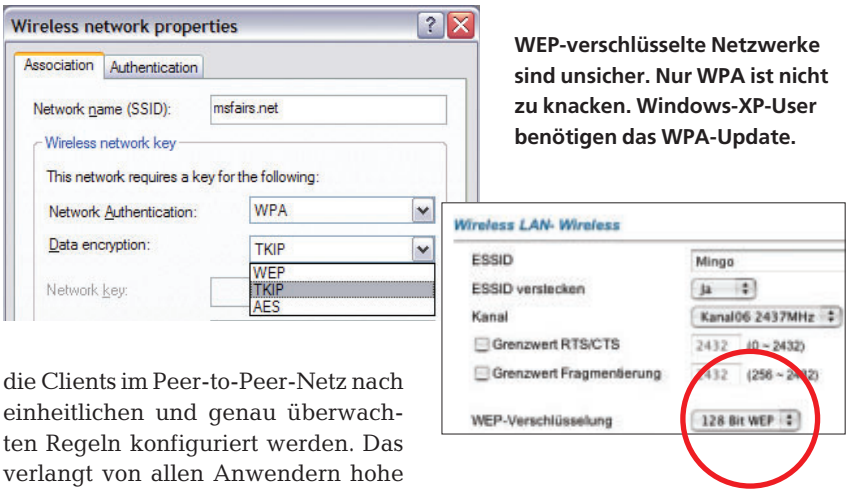
Die Internet-Sicherheit muss gleichwohl ein zentraler Router sicherstellen, der die Zugangskontrolle der Clients übernimmt, die Firewall-Funktionalität bereitstellt und die Verschlüsselung des Datenverkehrs sicherstellt. Damit ist der Router der Grundstein für eine sichere IT-Infrastruktur.

WLAN richtig absichern

Drahtlose Netzwerke sind beliebte Ziele von Hackern und Datenspionen. Daher sollten Sie auf jeden Fall alle möglichen Sicherheitsmaßnahmen ausschöpfen. Einen ersten Grundschutz bieten folgende Maßnahmen:

Mit aktiviertem MAC-Adressfilter sollten nur zugelassene Clients auf das WLAN zugreifen können. Doch Hacker umgehen die entsprechende Konfiguration schnell. Auch das Abschalten der SSID (Service Set Identifier, Netzwerk-Kennung) reicht nicht aus, um unautorisierte Benutzer vom WLAN auszuschließen.

Ebenfalls nicht hinreichend schützt die WEP-Verschlüsselung (Wired Equivalent Privacy) vor fremden Horchern im kabellosen Netzwerk. Verbreitete Cracker-Tools wie Kismet und Wepattack gewähren Hackern direkten Zugriff auf verschlüsselte Daten. Da WEP nur maximal 16,7 Millionen Schlüssel ermöglicht, wiederholen sich bereits verwendete Schlüssel nach etwa 25 GByte Datentransfer im Netzwerk. Nach spätestens 13 Stunden haben Hacker die vorhandenen Schlüssel geknackt.



WEP-verschlüsselte Netzwerke sind unsicher. Nur WPA ist nicht zu knacken. Windows-XP-User benötigen das WPA-Update.

Auf die erwähnten Security-Funktionen sollten Anwender dennoch nicht verzichten. Denn je mehr Verteidigungslinien an den WLAN-Grenzen errichtet sind, desto höher der Aufwand für Hacker.

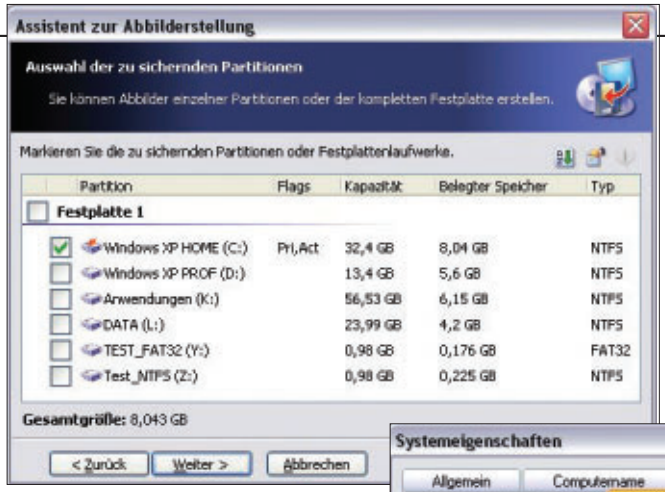
Professionelle Sicherheit

Zuverlässige Sicherheit im WLAN ist aber möglich: Bis heute gilt die WPA-Verschlüsselung (Wi-Fi Protected Access) als nicht zu knacken. Dieser abwärtskompatible WEP-Nachfolger basiert auch auf dem RC4-Algorithmus, unterstützt jedoch bis zu 500 Billionen Schlüssel, die zudem komplexer ausfallen als bei WEP (Details siehe *PC Professionell* 5/2004, ab Seite 164).

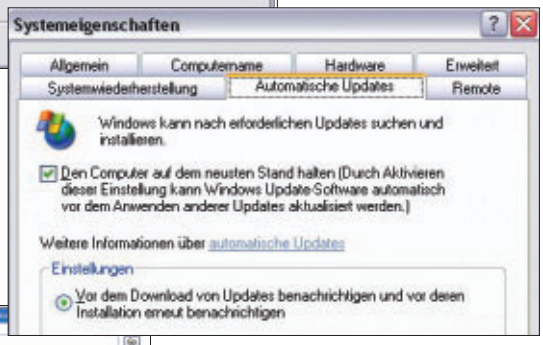
Ein hohes Maß an Sicherheit bringt auch VPN-Tunneling. Dabei findet der Datenaustausch im Netzwerk über verschlüsselte Pipelines zwischen den Rechnern statt. Üblicherweise sind dafür jedoch Server-Infrastrukturen

Schutzmaßnahmen

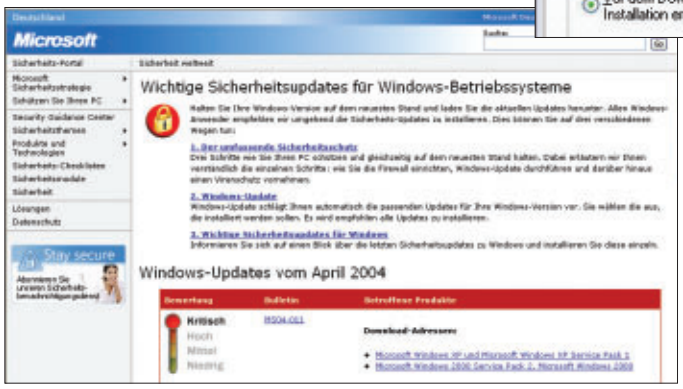
- **Virensendung per E-Mail**
  Panda Antivirus Platinum für Peer-to-Peer-Netze
- **Hacker-Angriffe, Port-Scans**
  WLAN-DSL-Router mit Firewall
- **Sicherheitslücken der Clients**
  zentrale Update-Politik
- **Datenspionage**
  Verschlüsselung mit PGP Workgroup Desktop
- **Datensabotage**
  regelmäßige Datensicherung mit Images, beispielsweise mit True Image 7



Die Trennung von Anwendungen, System und Daten auf der Festplatte ist die Voraussetzung einer wirksamen Image-Strategie.



Der Anwender sollte sich über verfügbare Updates unbedingt von Microsoft automatisch informieren lassen.



Vor allem für PCs im Netzwerk sind die kritischen Sicherheits-Updates von Microsoft überlebenswichtig. Diese sollten regelmäßig installiert werden – am besten automatisch.

notwendig. Geräte wie das Lancom 1821 Wireless ADSL verfügen jedoch bereits über einen integrierten VPN-Server, so dass keine weitere Hardware gekauft werden muss. Solche Sicherheit inklusive Stateful Packet Inspection hat allerdings ihren Preis: Rund 800 Euro kostet das Gerät. Zwar unterstützt der WLAN-DSL-Router kein WPA, Lancom verspricht seinen Kunden aber ein Fimware-Upgrade, das dies nachrüstet.

Um WPA auch unter Windows XP nutzen zu können, müssen Anwender ein Update von Microsoft einspielen. Zu finden ist der wichtige Download unter *support.microsoft.com/?kbid=815485* in der Knowledge Base.

Alle Clients absichern

Auch in serverlosen Netzwerken sind zentrale Sicherheitspolicies unerlässlich. Das beginnt bei der Wahl sicherer Passwörter für das gesamte Netzwerk und alle lokalen Accounts. Von enormer Bedeutung ist zudem eine konsequente Benutzerverwaltung, die etwa die Freigaben lokaler Ressourcen im Netz auf ein Minimum begrenzt. Der Beitrag »Individuelle Benutzerrechte« in *PC Professionell*, Ausgabe 5/2004 (ab Seite 158) informiert ausführlich und praxisnah über die wichtigsten Schritte.

Zudem ist eine konsequente Update-Politik Pflicht. Sinnvollerweise wird jeder Anwender im WLAN automatisch benachrichtigt, wenn neue Patches zur Verfügung stehen. Die entsprechenden Einstellungen befinden sich in den *Systemeigenschaften* unter *Automatisches Update*. Alle aktuellen Security-Bulletins zu Windows XP liefert *www.microsoft.com/germany/ms/security/winsec.mspx*.

Datensicherheit durch Datensicherung

Wird nicht ein Server zentral mit der Sicherung der Daten beauftragt, ist mindestens wöchentlich ein Image von der System- und täglich von der Datenpartition anzulegen. True Image 7 *(web.acronis.de)* ist dabei die beste Wahl. Praktisch und unkompliziert: Die Sicherungen, auch der Systempartition, lassen sich nebenbei im laufenden Betrieb durchführen.

Für die Verschlüsselung des Datentransfers sorgt etwa PGP Workgroup Desktop, das nicht nur E-Mails, sondern auch lokale Files codiert. Einzelplatzlizenzen gibt es ab 66 Euro (*www.pgp.com/products/desktop/workgroup/datasheet.html*). HME

Checkliste Bedrohungen und Gegenmittel

Bedrohung	Maßnahme	Programmempfehlung	Preis	Info
Virenangriff	netzwerkfähiger Virenscanner	Panda Antivirus 7 Platinum, 5 Lizenzen, Peer-to-Peer im Büro/Gdata Antivirenkit 2004, Heimnetz	240 Euro/100 Euro	www.panda-software.de, www.gadata.de
WLAN-Attacke	WLAN mit Router abschotten	Belkin F5D7630-4B/Lancom 1821 Wireless ADSL	130 Euro/800 Euro	www.lancom.de, www.belkin.de
Sicherheitslücken im System	konsequente Update-Politik	kein Programm erforderlich	kostenlos	www.microsoft.com/germany/ms/security/winsec.mspx
Datenspionage	Verschlüsselung von Mails und lokalen Files	PGP Workgroup Desktop	ab 66 Euro, Lizenz	www.pgp.com
Datenverlust /Datensabotage	regelmäßige Datensicherung mit Image-Programm	Acronis True Image 7	50 Euro	www.acronis.de
Browser-Hijacking	Einsatz eines Malware-Scanners	Pest Patrol	40 Euro	www.pestpatrol.de

Sicherheit für große Netzwerke

Großes Netzwerk – großes Risiko. Der Administrator muss täglich Hacker und Web-Attacken abwehren – und die eigenen Mitarbeiter daran hindern, versehentlich Viren einzuschleppen.

Werner Pliegl

Ab etwa zehn Arbeitsplätzen lässt sich ein Netzwerk aus Performance- und Sicherheitsgründen nicht mehr als Peer-to-Peer-Lösung realisieren. Kleine und mittelständische Unternehmen kontrollieren daher die Netze meist über Windows-, Linux- oder Unix-Server. Die Angriffsabwehr muss am Server erfolgen. Hierzu ist eine Kombination von serverseitiger Firewall, Spam- und Virenfilter notwendig.

Das lässt sich nicht mehr mit Freeware-Tools oder Endanwender-Programmen erledigen. Ein Netzwerk mit 100 Usern lässt sich ab etwa 7500 Euro absichern – pro Jahr. Darin enthalten sind die Lizenzen für den Einsatz eines unternehmensweit eingesetzten Virenscanners, eine professionelle Hardware-Firewall sowie Content-Filtering-Software im Mail-Server. In den Folgejahren fallen dann, abhängig von den eingesetzten Produkten, weitere Kosten für Updates, Support und Systempflege an, die in diesem Beispiel bei knapp 1000 Euro liegen.

Highend-Firewalls schützen sicher vor Server-Attacken

Besonders gefährlich für Firmen sind Denial-of-Service-Angriffe (DoS), bei denen Hacker den Server so lange mit Datenpaketen bombardieren, bis dieser die Anfragen nicht mehr beantworten kann. Im Extremfall führt das dazu, dass ein ganzes Unternehmen zeitweise keinen Zugriff auf Server und Netzwerk hat. Das bringt immense Folgekosten mit sich. Eine serverseitig gesteuerte Gateway-Firewall verhindert solche Übergriffe. Allerdings reduziert eine Firewall gleichzeitig die Routing-Leistung.

Microsoft Software Update Services helfen bei einer zentralen Patch- und Update-Politik.

Der Administrator lässt sich mit Hilfe der Überwachungsrichtlinien über fehlgeschlagene und erfolgreiche Active-Directory-Zugriffe informieren.

Mindestanforderungen an eine Firewall sind Filterung von IP-Adressen und Ports, Port-Blockierung, Network Adress Translation (NAT) zum Verbergen interner IP-Adressen und Stateful Inspection. Stateful Inspection sorgt dafür, dass der TCP-Header eines Datenpaketes durchleuchtet wird. Das verhindert den Eingang von Viren- oder Trojaner-Sendungen.

Mit diesen professionellen Features werden Port-Scanning, IP-Spoofing und DoS-Attacken entschärft. Noch höhere Sicherheit bringt allerdings eine Firewall, die zusätzlich auch FTP- oder Mediadatenströme filtert.

Je größer das Netzwerk ist, desto höher fallen auch die Anforderungen an den Datendurchsatz der Firewall aus. Empfehlenswert ist daher der Einsatz einer Hardware-Firewall, etwa von Zyxel *(www.zyxel.com)*, Fortinet *(www.fortinet.com)* oder Checkpoint *(www.checkpoint.com)*. Im *PC-Professionell*-Test (Netzwerk-Ausgabe 5/2004, ab Seite N2) konnte sich die Firewall-Appliance mit 1120 Euro relativ günstige Fortigate 60 von Fortinet durchsetzen. Als Highend-Lösung empfiehlt sich dagegen das Modell Checkpoint Sun Fire V60X. Dafür fallen jedoch bereits 5200 Euro an.

Systemsicherheit: Aktualität entscheidet

Absolut sicher vor einem Hacker-Angriff ist ein Unternehmen trotz dieser Maßnahmen noch nicht. Denn Hacker entdecken in Server-Systemen und Anwendungen täglich neue Programmfehler, die einen Pufferüberlauf erzeugen können. In der Folge lässt sich beliebiger Programm-Code auf dem Server ausführen. Gegen einen solchen Angriff hilft eine Firewall nur dann, wenn diese auch den dafür benutzten Port blockiert.

Schutzmaßnahmen

- **DoS-Attacken**
  Einsatz einer Gateway-Firewall
- **Spam-Bombardements**
  Content Filtering
- **Viren**
  Netzwerk-Virenscanner
- **Angriffe auf Anwendungsebene**
  Zugriffsbeschränkung durch Active Directory
- **Fehlbedienungen**
  Zugriffsbeschränkung durch Active Directory

Der Microsoft Baseline Security Analyzer zeigt Sicherheitslücken bei Servern und Desktops.

Der beste Schutz gegen solche Angriffe sind tagesaktuelle Security-Updates. Dazu lassen sich zwei kostenlose Microsoft-Tools netzwerkweit einsetzen. Der Baseline Security Analyzer identifiziert Sicherheitslücken und fehlgeschlagene Updates *(www.microsoft.com/technet/security/tools/mbsahome.mspx)*. Die Software Update Services dienen zum automatischen Download und zur Verteilung von Updates im Netzwerk *(www.microsoft.com/downloads/details.aspx?FamilyId=A7AA96E4-6E41-4F54-972C-AE66A4E4BF6C&displaylang=en)*.

Spam: größter Kostenfaktor

Spam ist zwar nicht per se destruktiv, führt aber bereits bei einem Unternehmen mit nur 100 Mitarbeitern zu erheblichen Produktivitätsverlusten und damit zu Kosten in fünfstelliger Höhe pro Jahr. Deshalb muss auch Spam bereits am Gateway geblockt werden. Dafür reicht die Funktionalität eines Mailservers wie etwa Exchange Server 2003 oder Domino-Server nicht immer aus. Deren Filtermöglichkeiten beschränken sich weitgehend auf den Vergleich des Absenders mit Black- und Whitelists.

Spezielle E-Mail-Filter für Gateways nutzen heuristische Analysen und greifen in Echtzeit auf so genannte Realtime Blackhole Lists im Web zu, um mit hoher Wahrscheinlichkeit unerwünschte Werbebotschaften von regulären Nachrichten zu unterscheiden. Im *PC-Professionell*-Vergleichstest (Ausgabe 2/2004) erwiesen sich als empfehlenswert die Lösungen E-Mail-Filter for SMTP von Surfcontrol *(www.surfcontrol.com)* sowie Mailsweeper for SMTP 4.3 von Clearswift *(www.clearswift.com)*. Die Preise beginnen – abhängig von der Anzahl der Clients – bei etwa 1500 Euro.

Viren müssen draußen bleiben

Viren dürfen erst gar nicht ins Netz gelangen, deshalb muss der Riegel schon auf dem Server vorgeschoben werden. Guten Schutz bietet etwa Trend Micro Interscan Web Security *(de.trendmicro-europe.com/enterprise/products/groups.php?prodgroup=1&family=26)*. Die 1-Jahres-Lizenz inklusive Updates kostet für 100 Arbeitsplätze 1430 Euro. Serverseitige Virenscanner mit vergleichbaren Erkennungsleistungen gibt es zudem von NAI, Panda, Sophos und Symantec. Entscheidend ist, dass die Hersteller täglich ein Update der Virensignaturen mit automatischem Download anbieten.

Desktop-Zugriffsrechte

Nicht weniger gefährlich als externe Angriffe sind Attacken von innerhalb des Unternehmens. Diese lassen sich aber ohne zusätzliche Tools durch eine optimale Netzwerk-Konfiguration ausschalten. Bei Windows-Netzwerken mit Active Directory definiert der Administrator einfach die Rechte aller Mitarbeiter zentral über die Gruppenrichtlinienkonsole *(gpedit.msc)*. Damit kontrolliert er die Authentifizierung, Passwortregeln, Schreib- und Leserechte sowie den Zugriff der Anwender auf Directories. HME

Checkliste Bedrohungen und Gegenmittel

Bedrohung	Maßnahme	Programmempfehlung	Preis	Info
Viren-Angriff	serverseitiger Virenscanner	Trend Micro Interscan Web Security	1430 Euro (1-Jahres-Lizenz für 100 User, inkl. Viren-Update)	www.trendmicro.de
Spam	serverseitiger Spamfilter	Surfcontrol E-Mail Filter for SMTP	ab 1500 Euro (abhängig von der Zahl der User)	www.surfcontrol.com
Hacker-Attacken	Hardware-Firewall	Fortigate 60	1120 Euro	www.fortinet.com
Netzwerk-Attacken	Intrusion Detection System installieren	Snort	kostenlos	www.snort.org
Angriffe auf Anwendungsebene	Sicherheits-Patches einspielen	Microsoft Software Update Services und Baseline Security Analyzer	kostenlos	www.microsoft.com/technet/security
Passwortspionage	Gruppenrichtlinien	Bestandteil von Verzeichnissystemen wie Active Directory	kostenlos	www.microsoft.de