



sich künftig nicht mehr nur Freaks und Hacker, sondern auch eine kriminelle Szene mit diesem Thema beschäftigen wird. Und der geht es weniger um das öffentlichkeitswirksame Lahmlegen von Millionen Rechnern als vielmehr um den stillen Klau von Konten- oder Kreditkartendaten sowie Unternehmensinformationen, die sich auf dem Schwarzmarkt versilbern lassen.

## Erste Schutz-Maßnahmen

Angesichts dieser Gefahren sind sich die meisten Experten darin einig, dass die bisherigen eindimensionalen Sicherheitsstrategien zu kurz greifen. Da Notebooks und immer kleinere USB-fähige Endgeräte (siehe Kasten: "Die mobile Gefahr") wie selbstverständlich zum Arbeitsalltag gehören, muss das Problem von zwei Seiten angegangen werden: So ist sicherzustellen, dass auf PCs, Notebooks und anderen Endgeräte kein elektronisches Ungeziefer gelangt. Ferner ist zu gewährleisten, dass nur ein geschützter Client von unterwegs über vertrauenswürdige und sichere Verbindungen Zugriff auf die eigene IT erhält. Wenn der mobile Mitarbeiter wieder im Unternehmen ist, muss ein eventuell verseuchter Rechner schnell erkannt und isoliert, also unter Quarantäne gestellt werden.

## Die Gefahr durch elektronische Kleingeräte

Anfangs überwog die Faszination durch die steigende Leistungsfähigkeit elektronischer Kleingeräte wie iPod, USB-Speicherstick, Digitalkamera, PDA oder Smartphone. Mittlerweile warnen aber Beratungshäuser wie die Gartner Group immer eindringlicher auch vor den Gefahren, die von den elektronischen Winzlingen ausgehen. Sie kompromittieren die Unternehmenssicherheit gleich in zweierlei Hinsicht. Einerseits können auf diesem Weg elektronische Schädlinge unter Umgehung der Firewall ins Unternehmensnetz gelangen, andererseits eignen sich die Tools auch hervorragend zum Diebstahl sensibler Daten. Im Gegensatz zum E-Mail-Versand hinterlässt der Dieb dabei nicht einmal Spuren. Bislang stehen die meisten IT-Manager, wie eine englische Studie ergab, diesem Problem ratlos gegenüber. Knapp 84 Prozent der Befragten gaben an, keine geeigneten Tools zu kennen, um die Verwendung dieser Devices zu steuern.

Zudem konterkarieren diese Geräte oft alle Sicherheitsanstrengungen eines Unternehmens, wenn sensible Informationen ungeschützt auf USB-Sticks mit ins Home Office genommen werden. Was passiert mit den Daten, wenn der Stick verloren geht oder gar gestohlen wird? Noch verschlüsselt kaum ein Benutzer die Daten auf den Sticks. Von Reflex Magnetic gibt es nun mit "Disknet USB Control" eine Software, die das Abspeichern von Daten auf den Sticks nur im verschlüsselten Zustand erlaubt.

Die Sicherung der mobilen Rechner beginnt mit ganz banalen Vorsichtsmaßnahmen: etwa der Vergabe von Bios-Passwörtern oder der Verschlüsselung von Datenträgern, um zu verhindern, dass gestohlene oder zeitweise etwa auf Konferenzen unbeaufsichtigte Notebooks von Dritten zum Ausspähen von Zugangsdaten genutzt werden - vom Missbrauch vertraulicher Informationen ganz zu schweigen. Das sind triviale Tipps, die aber in der Praxis gerne vergessen werden, wie Christoph Skornia, technischer Leiter bei Checkpoint, weiß. Ein weiteres Problem ist die ständig verbesserte Connectivity der mobilen Arbeitsgeräte. Dank USB, Firewire und anderen Schnittstellen ist es selbst für den IT-unbedarften Mitarbeiter heute kein Problem mehr, zusätzliche Devices wie Speichersticks, Bluetooth- oder WLAN-Adapter am Rechner anzuschließen, und so eventuell elektronische Schädlinge zu übertragen.

Diese Gefahrenquelle kann unter Umständen bereits mit den Bordmitteln von Windows XP verstopft werden. Mit Hilfe der skriptgesteuerten Installation des Betriebssystems lässt sich verhindern, dass beispielsweise die Treiber für das USB-Interface installiert werden. Allerdings greift diese Massnahme nur, wenn der Anwender unter XP keine Administratorrechte besitzt, sonst kann er die entsprechenden Treiber selbst nachinstallieren. Gepaart mit der aktivierten Personal Firewall des Betriebssystems und einer aktuellen Antivirensoftware, ergibt sich bereits ein Grundschutz. "Ein Ansatz, der in Projekten öfter gefordert wird", beobachtet Microsoft-Sprecher Thomas Baumgärtner. Allerdings, so schränkt er ein, hat das rigorose Abschalten der Schnittstellen auch einen Nachteil.

„Es ist sicherzustellen, dass die Software auf dem aktuellen Stand ist und der User unbedenkliche Kommunikationswege nutzt.“

Florian Schiebl, Ipass

## Risiko USB-Schnittstelle

Mobile Drucker und andere Endgeräte wie beispielsweise Beamer oder USB-Tokens, die diese Schnittstellen benötigen, können nicht genutzt werden. Im Alltag dürften deshalb zusätzliche Tools wie etwa der "Interface Manager" der Bonner Comma Soft AG, "Drivelock" von Centertools in Ludwigsburg oder der "USB Blocker" des Instituts für System Management GmbH in Rostock die praktikablere Lösung sein. Diese Werkzeuge erlauben eine genauere Festlegung, wofür etwa die USB-Schnittstelle genutzt werden darf.

Die Idee, ein Notebook mit der integrierten Firewall von Windows XP vor unerwünschter Kommunikation zu schützen, trifft jedoch nicht überall auf ungeteilte Zustimmung. Kritiker geben zu bedenken, dass das Microsoft-Tool für systemnahe Dienste wie den Windows Messenger zusätzliche Kommunikations-Ports öffnet und so Angreifern unnötige Einfallspforten bietet. Hersteller wie Checkpoint ("Secure Client") oder Symantec ("Client Security 2.0") setzten deshalb auf eigene Firewall-Lösungen auf dem Notebook in Verbindung mit Antivirensoftware und Werkzeugen zur Intrusion Detection und Prevention.

## Aktuellen Patch-Level erzwingen

Die Kombination aus Intrusion Detection, Personal Firewall und Antivirensoftware ist auch für Florian Schiebl, Director of Business Development beim Connectivity-Lösungsanbieter Ipass in München, die Basis einer ausgefeilten Sicherheitsstrategie: "Das reicht aber nicht, denn zusätzlich ist sicherzustellen, dass die Software automatisch auf dem aktuellsten Stand ist und der User nur unbedenkliche Kommunikationswege benutzt." So überprüft der Ipass-Client auf dem Rechner auch, über welches Netzwerk und über welchen Zugang ein Benutzer online geht. Nur wenn beides den definierten Sicherheitsregeln entspricht, erhält der Anwender einen Zugriff auf die Unternehmens-IT.

Dieses Prinzip hat auch Microsoft im eigenen Konzern realisiert: Die Mitarbeiter erhalten über eine E-Trust-Lösung von CA in Verbindung mit einer Smartcard einen Fernzugriff (Remote Access Service = RAS) auf das Unternehmensnetz. Will sich ein Mitarbeiter auf diese Weise einklinken, überprüft im Hintergrund ein SMS-Server den aktuellen Softwarestand und stellt entsprechende Updates zur Verfügung. "Weigert sich ein Anwender die Updates zu installieren", so berichtet Baumgärtner, "wird die MAC-Adresse des entsprechenden Endgerätes gesperrt, und der Benutzer hat keinen Zugriff mehr."

## 10 Sicherheitsregeln

- Bios-Schutz verwenden;
- Festplatte verschlüsseln;
- USB-Schnittstellen kontrollieren;
- Antivirensoftware einsetzen;
- Personal Firewall installieren und aktivieren;
- Intrusion Detection auf dem Endgerät;
- Updates erzwingen und Release-Stände überprüfen;

- Remote Access nur über VPN;
- Einhaltung der Sicherheitsregeln im Netz aktiv überprüfen;
- suspekta Endgeräte vom Netz trennen beziehungsweise isolieren.

### Kontrolle vor der Einwahl

Ähnlich rigide Überprüfungs-konzepte verfolgen auch Checkpoint, Ipass und andere Hersteller. Allen gemeinsam ist der Gedanke, dass das sicherste virtuelle private Netz (VPN) beim Remote Access auf das Unternehmensnetz nichts nützt, wenn das Notebook bereits vorher manipuliert wurde, weil es nicht den aktuellen Sicherheitsstandards entspricht. Stellt etwa Checkpoints Lösung, bestehend aus dem "Secure Client" und "Zonelabs Integrity", eine Verletzung der Sicherheitsregeln fest, so erhält der Client keinen Netzzugriff mehr. Gleichzeitig konfiguriert die Firewall den Rechner so um, dass nur noch Verbindungen zum Administrator zulässig sind, damit dieser die Probleme beseitigen kann. Noch restriktiver geht Ipass bei der Überprüfung der mobilen Geräte vor.

### Sicherheit im Unternehmensnetz

Bevor der Mitarbeiter unterwegs eine VPN-Verbindung zum Unternehmensnetz bekommt, kontaktiert das Endgerät einen Ipass-Server, auf dem die Sicherheitsregeln (erlaubte Netzadapter, Verbindungen, geforderte Softwarestände) des Unternehmens hinterlegt sind. Erst wenn der Rechner diese Überprüfung erfolgreich besteht, baut Ipass eine Verbindung zum Unternehmensnetz auf.

Moderne Sicherheitslösungen berücksichtigen nicht nur die Endgeräte, sondern statten auch die Unternehmensnetze mit entsprechenden Features aus. Neueste Security-Lösung, wie sie etwa Ipass mit "Policy Orchestration" erst letzte Woche vorstellte, gehen deshalb dazu über, auch im Unternehmensnetz selbst die Sicherheitsintegrität der Rechner zu prüfen und sie im Zweifelsfall vom Netz zu trennen. Die Überprüfung muss dabei nicht auf PCs, Notebooks oder PDAs beschränkt bleiben.



Der kalifornische Hersteller Sygate hat beispielsweise mit "Magellan 1.0" ein Tool im Programm, das alle mit einem Netzwerk verbundenen IP-Geräte erkennt und auf ihr Kommunikationsverhalten hin überwacht. Neben den kleineren Playern wie Ipass oder Checkpoint, Sygate oder Symantec haben mittlerweile auch IT-Größen wie Microsoft oder Cisco die Vorteile dieses Konzepts erkannt.

So propagiert etwa Microsoft unter dem Schlagwort "Network Access Protection"(NAP) eine entsprechende Lösung. Diese Technologie soll mit dem R2-Update des Windows Server 2003 im ersten Halbjahr 2005 erhältlich sein. Neben einem Policy-Connecticon-Server-Dienst für Windows Server 2003 will Microsoft bis dahin die entsprechenden Application Programming Interfaces (APIs) veröffentlichen, damit sich beispielsweise Antivirensoftware- und Netzhersteller in das NAP-Konzept einklinken können. Bislang haben 25 Firmen ihre Unterstützung angekündigt.

Grob vereinfacht, basiert dieses Prinzip darauf, dass ein Client - bevor er einen allgemeinen Zugriff auf das Netz oder Unternehmensanwendungen erhält - von einem Server auf die Einhaltung definierter Sicherheitsregeln überprüft wird. Dabei kann beispielsweise die Aktualität der Antiviren-Software oder der Patch-Stand des Betriebssystems kontrolliert werden. Entspricht ein Rechner nicht der geforderten Security-Policy, so wird er isoliert.

Ein ähnliches Konzept verfolgt Cisco mit dem Network Admission Control Program (NAC). Ein wichtiger Bestandteil dieser Lösung ist der "Cisco Trust Agent" (CTA), der auf den Endgeräten installiert werden muss und dort den Sicherheitsstatus ermittelt. Diese Informationen liefern etwa Antivirenprogramme. Die so gewonnenen Daten erhalten dann Ciscos Netzkomponenten, die dann entscheiden, ob ein Netzzugriff zulässig ist oder nicht.

Allerdings haben diese Verfahren, so überzeugend sie in der Theorie klingen, in der Praxis einen Nachteil: Ihr Erfolg steht und fällt mit der Unterstützung der Dritthersteller, die in ihre Software oder Netzkomponenten entsprechende APIs einbauen. Ferner ist offen, ob kleinere Hersteller die Ressourcen haben, um sowohl für das Microsoft- als auch das Cisco-Konzept Interfaces zu entwickeln.

PDA's und Handys nicht vergessen

Zudem stellt Checkpoint-Manager Skornia die nicht unberechtigte Frage, ob es wirklich sinnvoll ist, im Problemfall den Client-Port am Switch abzuschalten. Denn dadurch habe auch ein Administrator keinen Zugriff mehr auf das betroffene Endgerät, womit wieder Turnschuhsupport angesagt sei. In den Augen von Skornia erfordern diese Konzepte letztlich bis zum Desktop Netzkomponenten, die den Verkehr auf Layer-4-Ebene überwachen, um in der Praxis sinnvoll angewendet werden zu können.

Angesichts dieser offenen Fragen erscheinen derzeit (noch) Lösungen, die direkt am Client die Netzverbindungen überprüfen und eventuell blockieren, als die praxisgerechteren Verfahren. Zumal wenn etwa eine intelligente Firewall auf den Rechnern erkennt, ob sich der Client wie ein Trojaner verhält und zum Beispiel im Netz die unterschiedlichsten Ports absucht.

Unabhängig davon, welchem Ansatz ein Systemadministrator letztlich den Vorzug gibt, sollte bei der Wahl der Sicherheitslösung auch ein Blick in die Zukunft geworfen werden: Die steigende Zahl an PDA's und Smartphones, die etwa mit privaten lediglich 30 Euro teuren Bluetooth-Adaptoren mit dem PC oder Notebook gekoppelt werden, erhöhen die Security-Risiken.

---

IDG Business Media GmbH

Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Business Media GmbH. DPA-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass in Computerwoche unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von Computerwoche aus gelinkt wird, übernimmt die IDG Business Media GmbH keine Verantwortung.