Nicht nur eine Frage der Technologie

von Umberto Annino

Der Autor ist Security Project Consultant bei InfoGuard AG.

Mit massivem technischem Aufwand sind Unternehmen bemüht, den steigenden Anforderungen an die Sicherheit der Computersysteme gerecht zu werden. Von Viren und Hackern gehen dabei die grössten Gefahren aus. Verbesserungspotenzial liegt aber auch in den nichttechnischen Bereichen der Unternehmenssicherheit.

Spricht man von den Gefahren bei der Internetnutzung, gelten schon seit längerem Computerviren und Hacker als die Standard-Risiken, von denen die grösste Bedrohung für Betriebe und Unternehmungen ausgehen. Meist wurde versucht, die Schwachstellen mit technischen Massnahmen zu bekämpfen, weshalb viele Unternehmen in den vergangenen Jahren erheblich in Virenschutz und Firewalls investiert haben. Oftmals ging dabei jedoch vergessen, dass die Sicherheit nicht allein nach den Prinzipien des technischen Schutzes gewährleistet werden kann.

Sicherheit beginnt beim Mitarbeiter

Um die Sicherheitskultur eines Unternehmens langfristig sicherzustellen, müssen die Mitarbeiter umfassend darauf ausgebildet und sensibilisiert werden. Der unsachgemässe Umgang mit Informationen stellt in den Unternehmen nach wie vor das grösste Sicherheitsrisiko dar. Wer seine vertraulichen Unternehmensinformationen, seien dies Kundendaten oder Produktinformationen, schützen will, braucht einerseits eine zuverlässige Hard- und Software, andererseits aber auch die volle Unterstützung aller Mitarbeiter.

Informationen sind nicht nur im Netzwerk, sondern auch in den Köpfen der Mitarbeiter vorhanden. Dort werden sie nicht selten von so genannten «Social Engineers» abgeholt. Diese stellen sich etwa die Frage, warum sie die technologisch ausgereifte, wohl konfigurierte Firewall einer Firma in nächtelanger Sisyphusarbeit zu knacken versuchen sollen, wenn doch der Portier am Empfang dem vermeintlichen Techniker den geschützten Zugang zum Serverraum bereitwillig öffnet. Oder weshalb die Abwesenheit des Geschäftsleiters nicht genutzt werden soll – freundlicherweise vom Anrufbeantworter detailliert mitgeteilt –, um vor der wichtigen Kundensitzung in der IT-Abteilung in gespielter Aufregung zu später Stunde die Zugangsdaten für den Remote Access zu erfragen. Wer möchte dem Chef schon einen dringenden Gefallen verweigern?

Der «Social Engineer» nutzt also die psychologischen Schwächen der Menschen für seine eigenen Zwecke aus. Unwissen, Gutgläubigkeit wie auch Hilfsbereitschaft und Hierarchiegläubigkeit der Mitarbeitenden werden skrupellos missbraucht, um an Firmengeheimnisse heranzukommen. Die Techniken, die angewendet werden, um Menschen von den eigenen Wünschen zu überzeugen, sind nicht neu und finden bereits seit Jahrhunderten ihren unrühmlichen Einsatz.

Technische Schutzmassnahmen klar notwendig

Aber auch die sicherste Sicherheitskultur und die Verbesserung des Sicherheitsbewusstseins der Mitarbeiter schützen nicht vor Angriffen und Attacken aus dem Internet.

- Relevante Einsatzfelder bei der Online-Kommunikation bilden E-Mail sowie der Austausch sensibler Unternehmensdaten über das Internet, ferner die Integration von Web-Applikationen wie Online-Shops oder Portale und die Einbindung von Aussenstellen in das Firmennetzwerk mittels VPN-Technologie. Um das Unternehmensnetzwerk wirkungsvoll vor Hacker- und Virenattacken sowie anderen Bedrohungen aus dem Internet zu schützen, ist eine umfassende Internet-Sicherheitslösung unabdingbar.
- Sicherheit wird in der heutigen Form leider viel zu oft als Produkt verkauft, das «out-of-the-box» im Laden erhältlich ist und nachträglich aufgepfropft wird. Ganz nach dem Motto: Firewall einsetzen, Intrusion-Detection-System konfigurieren, Antivirus-Software installieren – fertig ist der Schutz des Netzwerks! Aber so einfach ist es nicht: Sicherheit sollte immer konzeptionell in ein Produkt oder eine Dienstleistung hinein entwickelt und nicht nachträglich aufgetragen werden. Wenn Sicherheitsmassnahmen statisch bleiben, verliert sich die Wirkung innert kürzester Zeit. Da sich die Gefahren ständig ändern, müssen auch die Gegenmassnahmen fortlaufend angepasst werden.

Wirksame Kontrolle mit Firewalls und Virenschutz

Die Hauptaufgabe der Firewalls liegt in der Sicherung von Unternehmens-

netzwerken – seien es Attacken von externen unliebsamen Störenfrieden aus dem Internet oder von Mitarbeitern der eigenen Firma im Intranet. Das interne Netzwerk muss von innen und aussen geschützt werden: vor unerlaubten Zutritten, vor Blockierungsversuchen einzelner Dienste wie Denial-of-Service und dem Absetzen von «Malicious Code» wie Viren, Java Script oder ActiveX. So sollte eine gute Firewall nebst einer Paket-Filterung auch über Application Level Gateways, so genannte Proxies, verfügen. Diese untersuchen die gefilterten Pakete auf deren Inhalte und können so unter anderem auch als Virenschutz oder Spam-Blocker eingesetzt werden.
Im Markt ist zudem der Trend zu beobachten, dass Kunden nach «All-in-one»-Lösungen fragen. Dieser Ansatz mag für Heimanwender sinnvoll sein, die Umsetzung von Sicherheit auf Unternehmensebene sollte jedoch mit dedizierten Systemen erfolgen, um Abhängigkeiten und einen «Single Point of Failure» zu vermeiden.
Obwohl moderne Firewalls zusätzlich Virenschutz-Funktionen übernehmen können, sollte auf eine spezielle Antivirus-Software auf keinen Fall verzichtet werden. Da Viren auf verschiedensten Wegen in ein Unternehmensnetzwerk gelangen, ist eine lokale Virenprüfung für PC, Workstation und Server unabdingbar.

Web-Applikationen als künftige Angriffsziele

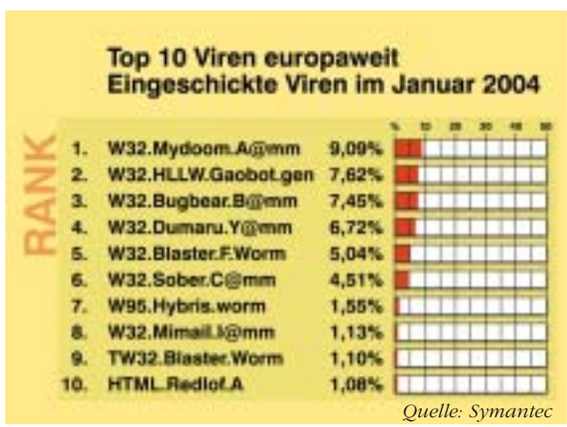
Immer mehr interaktive Applikationen gehen online und sind weltweit von jedem Browser anwählbar. Sie werden zugleich immer komplexer und damit auch anfälliger auf Hackerangriffe. Heutige Web-Applikationen stellen hohe Anforderungen an die generelle Sicherheit und den Datenschutz. Im Hinblick auf Einsatzgebiete wie beispielsweise E-Government oder E-Voting werden diese Anforderungen noch weiter steigen. Mittlere und grosse Unternehmen stehen vor der Entscheidung, ihre IT-Infrastruktur vollständig webfähig zu machen oder aber mittels Middleware den Legacy-Systemen Zugang zum Internet zu verschaffen. Oft wird dabei vergessen, dass solche Systeme vorderhand für den Betrieb in geschützten Umgebungen konzipiert sind und nicht über Sicherheitsmechanismen verfügen, die sie vor zerstörerischen Angriffen aus einem ungeschützten, nicht vertrauenswürdigen Netz bewahren.
Gemäss Untersuchungen des renommierten amerikanischen Research Center für Sicherheit CERT stellen Web-Applikationen das nächste grosse Angriffsziel dar. Auch mit modernen Firewalls ist ein Web-Anwendungsserver jederzeit verschiedensten Attacken auf Anwendungsebene ausgesetzt. Bereits wächst die Anzahl der entsprechenden veröffentlichten Schwachstellen schneller als die Anzahl neu entwickelter Viren: SSL Denial of Service, Cookie Poisoning, SQL und Script Injections sowie Cross Site Scripting (XSS) und Forceful Browsing sind Angriffsmethoden, die von einer Firewall prinzipiell nicht erkannt werden können. Trotzdem werden Sicherheitsmassnahmen im Bereich der Web-Applikationen vorwiegend stiefmütterlich behandelt. Dabei würden Application Security Gateways sehr wirksam und kosteneffizient die entsprechenden Anforderungen erfüllen. Sie werden nach der Firewall als Perimeterschutz vor die Applikationsserver platziert.

Applikationen von Sicherheitsaufgaben entlasten

Das Ziel der so genannten «Secure Reverse Proxies», wie solche Application Gateways auch bezeichnet werden, ist die Entlastung der Applikationen von Sicherheitsaufgaben. Da die Angriffe ständig ändern, ist es zu aufwändig, jede einzelne Applikation gegen entsprechende Gefahren zu schützen. Zudem darf nicht vergessen werden, dass die Schutzmassnahmen in einer heterogenen Applikationslandschaft ständig auf dem neusten Stand gehalten werden müssen. Der Secure Application Gateway forciert die Authentisierung der Benutzer – im Idealfall über ein bestehendes «Single Sign On» – und übernimmt das sichere Session Handling. Dabei prüft er den Inhalt der übertragenen Pakete und kann so Angriffe, Protokoll-Anomalien und unberechtigte Benutzer ausschliessen.
Zugleich lässt sich in diesem Bereich eine weitere Entwicklung beobachten: Dem IPsec-basierten Virtual Private Network (VPN), das aufwändig zu konfigurieren und nur für bestimmte Einsatzzwecke sinnvoll ist (und das zudem einen korrekt konfigurierter VPN-Client benötigt, um eine Verbindung aufzubauen), steht das neu entwickelte «Extranet» gegenüber – das so genannte SSL-VPN.
Bei diesem erfolgt keine eigentliche Netzwerk-Anbindung, sondern es wird eine sichere Verbindung über einen SSL-basierten HTTP-Verkehr aufgebaut. Die dafür notwendigen Clients sind bereits überall verfügbar und müssen nicht konfiguriert werden: Internet-Browser sind SSL-fähig. So kann der Zugriff auf das Intranet einfach, schnell und vor allem geschützt über das Internet erfolgen – mit Hilfe des Secure Reverse Proxy.

Gefahren im E-Mail-Verkehr meist unterschätzt

Nebst der steigenden Zahl von Web-Applikationen hat heute die E-Mail im Geschäftsbereich längst eine Vormachtstellung eingenommen. Gerade bei der Geschäftskommunikation werden zahlreiche vertrauliche Daten wie Bestellungen, Angebote, Geschäftsbriefe, Verträge oder Dateien mit vertraulichen Kundendaten mittels E-Mail versandt. Dabei werden immer noch in vielen Fällen vertrauliche E-Mails unverschlüsselt über das Netz geschickt, da die Gefahren des Mitlesens beim E-Mail-Verkehr weitgehend unterschätzt werden. Vielen Benutzern ist nicht einmal bekannt oder bewusst, dass der Inhalt einer E-Mail im Klartext via Internet übertragen wird.
Seit vergangenem Jahr sind zudem sämtliche Schweizer Provider verpflichtet, den E-Mail-Verkehr ihrer Kunden aufzuzeichnen. Die Internetanbieter müssen hin und her geschickte E-Mails registrieren, sechs Monate lang aufbewahren und bei konkretem Tatverdacht den Behörden mittels richterlicher Verfügung aushändigen. Weiterhin wird in den meisten Unternehmen die Gefahr der Spionage des internen E-Mail-Verkehrs ignoriert, obwohl es heute ein Leichtes ist, sich via Internet kostenlos entsprechende Programme zu beschaffen.
Das auf dem Markt erhältliche Angebot an Firewalls, Intrusion-Detection- und Prevention-Systemen, Anti-Virus-Software und E-Mail-Verschlüsselung ist gross, was unweigerlich die richtige Entscheidung erschwert. Es gilt daher immer abzuklären, welche Anforderungen gegeben sind, wer in die Lösung eingebunden werden muss und an welcher Stelle die Sicherheit ansetzen soll. Anhand dieser Vorgaben muss die passende Lösung evaluiert und mit organisatorischen Massnahmen zu einem umfassenden Informations-Sicherheits-System ergänzt werden. ◆



Quelle: Symantec

INFORMATIONEN ÜBER DIE AKTUELL AM HÄUFIGSTEN AUFTRETENDEN VIREN

www.symantec.de/region/de/avcenter/index.html

«Neue Technologien ziehen auch neue Bedrohungen nach sich.»

Interview mit Kevin Hogan zur Internetsicherheit 2004

«Einen rückläufigen Trend beim Hacken kann ich nicht ausmachen. Der Trend zu einer Vermischung von Hacking und Virenschreiben wird sich weiter fortsetzen.»

Kevin Hogan,
Senior Security Manager Symantec AG

Kevin Hogan leitet als Senior Manager im Virenforschungszentrum von Symantec in Dublin ein Team von Sicherheitsexperten, die Viren und andere bösartige Codes analysieren sowie neue Bedrohungen im Bereich der IT-Sicherheit erforschen.

Herr Hogan, ein kurzer Rückblick ins Jahr 2003: Haben sich Ihre Prognosen bewahrheitet?
Im Wesentlichen ja. Wir haben Ende 2002 bereits vor dem Auftauchen komplexer Bedrohungen gewarnt. Zudem haben wir auf immer häufiger auftretende Schwachstellen und die immer schnellere Ausnutzung solcher Schwachstellen durch Virenschreiber hingewiesen. Die Wirksamkeit und die schnelle Verbreitung von Slammer, Blaster und Welchia haben die damaligen Vermutungen bestätigt. Der Schaden war enorm.

Was bedeutet die Entwicklung im Bereich der Schwachstellenausnutzung für Computeranwender?
Neben der Installation leistungsfähiger Sicherheitslösungen und deren automatischer Aktualisierung dürfen die Schwachstellen in Betriebssystemen und Anwendungen nicht aus den Augen verloren werden. Das regelmässige Einspielen von Patches trägt erheblich zu einem höheren Sicherheitsniveau bei. Genügte es früher, dass man ein bis zwei Mal im Jahr Patches von den Websiten der Hersteller heruntergeladen hat, so ist dies mittlerweile in Abständen von zwei bis drei Wochen ratsam – ein erheblicher Mehraufwand also.

Lange Zeit kursierte die Sicherheitsempfehlung, niemals E-Mails zu öffnen, die einen bekannten Absender mit einer Betreffzeile in einer Fremdsprache kombinieren. Würden Sie diesen Hinweis heute noch so unterschreiben?
Ich fand diesen Tipp nie sonderlich nützlich. Bereits Sober arbeitete mit einer Betreffzeile in der Muttersprache des Empfängers. Und vor ihm gab es Virdem, der sowohl in einer englischen als auch in einer deutschen Version in Umlauf war. Massenmailer haben heute zahlreiche Tricks auf Lager, um den Empfänger zum Öffnen der Nachricht und der Anlage zu bewegen. In manchen Fällen erzeugen Würmer die Betreffzeile und auch den Dateinamen der Anlage aus Stichwörtern, die sie im System aufschnappen.

Was empfehlen Sie den Computernutzern im Umgang mit E-Mails?
Viele Würmer verbreiten sich nicht, weil sie mit neuen Techniken oder Tricks daher kommen, sondern einfach, weil die Leute immer noch vollkommen arglos E-Mails und Dateianhänge öffnen. Eine gesunde Portion Skepsis ist also angebracht. Das heisst: Nicht jede E-Mail einfach öffnen und schon gar nicht die angehängten Dateien. Ich kann mich als PC-Nutzer auch nicht mehr auf mir bekannte Absender verlassen, denn viele Würmer arbeiten mit gefälschten Adressen. Also: Besser einmal zu viel löschen als einmal zu wenig.

Erleiden Privatuser tatsächlich finanzielle Verluste durch Viren, Würmer und Hackerattacken oder ist das alles nur Panikmache?
Es kommt immer darauf an, wie der Computer eingesetzt wird. Hat ein Privatanwender tatsächlich vertrauliche Informationen im Computer gespeichert oder wird der PC als Arbeitsmittel eingesetzt, dann kann der PC-Nutzer auch ernste oder besser gesagt wirtschaftliche Schäden durch Viren davontragen. Nehmen Sie als Beispiel den Blaster-Wurm: Der Wurm hinterliess eine sogenannte «Backdoor» (Hintertür) auf der infizierten Maschine. So konnten Dritte den infizierten PC ganz nach Belieben fernsteuern – ohne Wissen des Besitzers. PCs mit dem Betriebssystem Windows XP liefen überdies Gefahr, in einen Reboot-Cycle zu geraten. Für PC-Nutzer ohne besondere Computerkenntnisse kann sich daraus schon ein beträchtlicher Schaden ergeben.

Wie sieht es mit den Schäden für Unternehmen aus?
Da Unternehmen sich noch stärker auf Computer verlassen, um ihre Geschäfte zu führen, kann jeder Zwischenfall mit Schadenscode zu einem finanziellen Verlust führen. Die meisten Unternehmen sind sich dieser Tatsache bewusst. Um mit der technologischen Aufrüstung von Hackern und Virenschreibern Schritt zu halten, setzen daher immer mehr Firmen auf den Einsatz integrierter Sicherheitslösungen oder auf die Auslagerung der kompletten IT-Sicherheit.

Welche weiteren Bedrohungen werden in naher Zukunft auf Computernutzer zukommen?
Cyberbedrohungen werden immer komplexer, sprich Virenschreiben und Hacken sind schon seit einiger Zeit eine Symbiose eingegangen. Slammer, Blaster und Welchia sind die ersten Anzeichen für diesen Trend und es ist wahrscheinlich, dass wir im Jahresverlauf weitere Beispiele erleben werden. Die Wirksamkeit dieser Cyberschädlinge hängt dabei stark davon ab, wie verbreitet die Schwachstelle ist, die sie ausnutzen, und wie leicht es ist, sie auszunutzen.

Wie sieht es mit Sicherheitsrisiken für die Nutzer von WLANs aus? Steigt mit der kabellosen Verbindung das Risiko, Opfer eines Lauschangriffs zu werden?
Das grösste Sicherheitsrisiko, das Nutzer von kabellosen Netzwerken haben,

ist der Daten- und Vertraulichkeitsverlust durch Lauschangriffe. Die Möglichkeit von Dritten, sich Zugang zu Funknetzwerken zu verschaffen, sind beachtlich. Das blosse Vorhandensein einer WLAN-Karte auf dem PC stellt allerdings noch kein Sicherheitsrisiko dar. Wer jedoch die Datenübertragung per kabellosem Netzwerk wählt, sollte neben den üblichen Vorsichtsmassnahmen wie Virenschutz, auch eine speziell für Notebooks konfigurierbare Firewall und – besonders bei sensiblen Daten – eine Verschlüsselung benutzen.

Hinken Sicherheitslösungen nicht immer einen Schritt hinter Hackern und Virenschreibern her? Wie kann man da Sicherheitslösungen noch voll vertrauen?
Auch Sicherheitsgurte im Auto geben Fahrern keinen «Freischein», die Geschwindigkeit zu überschreiten oder auf der falschen Seite zu fahren. Auf Computer übertragen heisst das: Egal, welche Sicherheitslösung installiert ist, PC-User sollten sich umsichtig im Internet bewegen. Um bei der Analogie mit der Autosicherheit zu bleiben: Die meisten Autos haben zusätzlich zum Sicherheitsgurt Airbags. Als Computernutzer sollte man sich nicht ausschliesslich auf Virenschutzlösungen verlassen, sondern auch eine Firewall installieren. Eine Firewall auf Desktop-Ebene kann einen PC gegen Bedrohungen wie Slammer oder Blaster schützen. Sie kann jedoch nichts gegen Sobig ausrichten, so dass man eben auch den Virenschutz braucht. ◆

«Wir sollten uns das selbstverständliche Sicherheitsbewusstsein zum Schutz gegen Angriffe von aussen auch für solche von innen aneignen. Vor allem wenn es um die Verteilung der Budgets geht. Es kann nicht Aufgabe der Firma sein, jeden Mitarbeiter zum Sicherheitsexperten auszubilden oder nur noch hochqualifizierte Mitarbeiter zu beschäftigen.»

Harry Galli,
Geschäftsleiter Checkpoint Schweiz AG

«Intrusion-Detection-Systeme decken unberechtigte Zugriffe aller Art auf, können aktiv eingreifen und helfen, den Angriff im Nachhinein nachzuvollziehen. Sie werten Alarmmeldungen jedoch nicht automatisiert aus, können Sicherheitslöcher und Programmfehler nicht aufdecken, Hacker-Aktivitäten nicht unterbinden und schützen nicht vor Viren und Würmern. Für einen optimalen Schutz ist eine Rund-um-die-Uhr-Überwachung der Netzwerke durch Sicherheitsspezialisten daher unerlässlich.»

Dr. Matthias Rosche,
Manager Security Consulting, Integralis GmbH

USER AUTHENTICATION ZUM KLEINEN PREIS

Aussendienst und Heimanwender wählen sich immer häufiger über Internet-VPN oder direkt per Modem-Verbindung in eine Firma ein, um auf Datenressourcen zuzugreifen. Diese Remote-Zugriffe werden aber oft nur mittels schwacher Benutzerpasswörter oder durch statische Schlüssel geschützt – eine Schwachstelle, die Hacker ausnutzen können, um sich Zugriff auf sensitive Firmendaten zu beschaffen, mutwillig Daten zu zerstören oder Firmenrechner als Zwischenstation für Attacken auf weitere Angriffsziele zu benutzen.
Für Sicherheit sorgt hier die sogenannte Zwei-Faktoren-Authentifizierung, die bisher nur in Form von teuren, hardware-basierenden Tokens erhältlich war. Eine Alternative bietet jetzt die IT-Security-Spezialistin Celeris mit ihrem «Strong-User-Authentication»-Produkt Pampin, das mit den gängigen Firewalls, VPN- und RAS-Lösungen kompatibel ist.
Pampin basiert auf der vom Online-Banking her bekannten Streichlisten-Methode. Diese kombiniert einen statischen PIN mit einem dynamischen numerischen Code, dessen Gültigkeit jeweils nach der Benutzung verfällt. Die reine Software-Lösung ist laut Anbieter hochsicher, einfach zu handhaben und auch für grosse User-Gruppen geeignet. Ihre Flexibilität und Skalierbarkeit macht sie sowohl für den Mittelstand als auch für Grossunternehmen zu einer effizienten und kostensparenden Alternative zu SecurID-Lösungen.

Info: www.cetus.ch