

IT-Sicherheit von PC und Netzwerk

Jeder PC, jedes Netzwerk, jegliche Verschlüsselung sind zu „knacken“. Es kommt nur auf den dazu erforderlichen Aufwand an und die vorhandene kriminelle Energie, die elektronischen Daten von Unternehmen zu schädigen. Bei Angriffen durch Computerviren, Würmer und Trojaner handelt es sich meist um zufällige Attacken, die aber auch gezielt erfolgen können. Mit geeigneten Sicherheitsmaßnahmen sind diese Gefahren aber weitgehend abzuwehren.

Datensicherheit – notwendiger denn je

Das Internet wird zunehmend für die Kommunikation mittels elektronischer Post, zur Informationsbeschaffung, für den Datenaustausch u. a. m. genutzt. Dienstleister bieten zudem ihre Leistungen im Internet an wie beispielsweise Betreiber von Online-Shops. Das kann aber auch Tür und Tor für unberechtigte Zugriffe öffnen. Diese zielen häufig nicht nur darauf ab, z. B. beim Online-Banking am heimischen PC Geldüberweisungen zu manipulieren. Auch geistiges Eigentum, die Privatsphäre, sensible Kundendaten sowie das Image des Unternehmens sind in Gefahr und sollten daher vor Missbrauch, Manipulation, Spionage oder gar Zerstörung bewahrt werden. Um ggf. massive wirtschaftliche Schäden zu vermeiden, ist es für den Unternehmer daher wichtig, diese Risiken zu kennen, einzuschätzen und geeignete Schutzmaßnahmen in der EDV dagegen zu treffen.

Grundsätzlich kann nach vorsätzlichen oder zufälligen Attacken unterschieden werden. Angriffe durch Computerviren, Würmer und Trojaner gehören in der Regel zu den zufälligen Attacken, sind aber auch gezielt einsetzbar.

Viren, Würmer und Trojaner – die häufigsten Angriffe

Viren, Würmer und Trojaner stellen die häufigste Bedrohung für PC-Systeme im privaten sowie im unternehmerischen Umfeld dar. Es handelt sich dabei um winzige schadhafte Computerprogramme, die sich meist an bestehende Programme oder an dessen einzelne Bestandteile in Form

von Dateien anhängen. Durch die Aktivierung der somit infizierten Software werden die elektronischen Schädlinge im Arbeitsspeicher des Computers aktiv. Ihr erstes und gemeinsames Ziel ist meist die Replizierung auf weitere Rechner. Die Verbreitung geschieht auf verschiedene Weise. In der Praxis kommt es häufig vor, dass z. B. Geschäftskunden, die im E-Mail-Adressbuch eines Unternehmens gepflegt wurden, nach geschäftlicher Korrespondenz via E-Mail plötzlich mit Viren- und Spam-Mails überschüttet wurden. Im ungünstigsten Fall wurden beim Versand dieser Mails die Absenderkennungen des von Computerviren infizierten Unternehmens verwendet. Dies schadet nicht nur dem gegenseitigen Vertrauen, sondern kann auch erhebliche Kosten bezüglich der Schadensanalyse und -beseitigung auf beiden Seiten verursachen.

Infizieren durch Viren

Viren verbreiten sich passiv, d. h., sie werden ungewollt kopiert, wenn eine infizierte Datei oder ein infiziertes Programm kopiert wird. Dies geschieht heutzutage oft mithilfe von E-Mails: Ein Bekannter oder ein Geschäftspartner sendet ein Dokument via elektronischer Post. Dieser weiß nicht, dass sein Dokument infiziert ist. Nachdem das Dokument vom Empfänger geöffnet wurde, wird der Schädling aktiv, schleust sich in ein weiteres Programm auf dem Rechner des Empfängers ein oder hängt sich unmerklich an eine auf dem betreffenden Rechner bestehende Datei an. Viren nisten sich auf diese Art gern in Programme ein, die beim Hochfahren des Rechners automatisch gestartet werden – um von nun an regelmäßig aktiv zu

sein. Es ist aber ebenso möglich, dass sich eine infizierte Datei auf einem Wechseldatenträger, wie z. B. einem USB-Stick, einer CD oder auf einer Diskette befindet. Viren verstecken sich häufig in Dateien, die man im Internet downloaden kann. Sobald man die infizierte Datei öffnet, wird das Virus aktiv.

Virenschutz

Abhilfe gegen Viren verschaffen so genannte **Virens Scanner**. Diese Programme sind käuflich zu erwerben. Einfache Varianten kann man kostenlos im Internet downloaden.

Funktionsweise. Ein Virens Scanner wird auf dem Betriebssystem eines Rechners installiert. Nach dem Starten des Rechners sollte der Virens Scanner aktiv im Hintergrund laufen und insbesondere den Arbeitsspeicher des Rechners überwachen. Sobald ein Computerprogramm auf dem Rechner aktiviert – in den Arbeitsspeicher geladen – wird, gleicht der Virens Scanner das Verhalten dieses Programms mit seiner internen Datenbank auf bekannte Virensignaturen ab. Gute Virens Scanner erkennen im Falle eines **aktiven Virus** dessen Verhaltensmuster und desinfizieren oder isolieren die betroffenen Dateien.

Ebensoverkehr ein Virens Scanner mit **inaktiven Viren**, die sich auf Datenträgern befinden. Dazu wird mit Hilfe des Scanners ein Prozess gestartet, der sämtliche mit dem Computer verbundenen Medien wie Festplatten, CDs, USB-Sticks und Disketten nach Virensignaturen durchsucht.

Es gibt sogar Virens Scanner, die auf aktiven Netzwerkkomponenten, wie z. B. auf einer Internet-Firewall, laufen und von dort aus den durchlaufenden Datenstrom nach Signaturen durchsuchen. Das ist insbesondere bei Unternehmen interessant, die viele Daten aus dem Internet downloaden. Die aus dem Internet geladenen Dateien werden praktisch auf der aktiven Netzwerkkomponente gescannt, bevor sie auf der Festplatte eines Computers abgelegt werden. Dazu später mehr.

Verbreitung von Würmern

Würmer verbreiten sich im Gegensatz zu Viren aktiv über Netzwerke, z. B. über eine Internetverbindung. Sobald auf einem

Computer ein Programm ausgeführt wird, dass mit anderen Computern kommunizieren, also Daten austauschen möchte, müssen so genannte Softwareports geöffnet werden. Das sind „Türen“ bzw. I/O-Schnittstellen, die das Senden und Empfangen der von den Anwenderprogrammen benötigten Informationen ermöglichen.

Der Wurm ist bereits auf mindestens einem Rechner im Netzwerk, z. B. auf einem Webserver, aktiv und wartet auf eine kommunikative Anfrage eines anderen Computers. Dieser will vielleicht eine Website abrufen, damit diese einem davor sitzenden Benutzer angezeigt wird, und öffnet einen Softwareport, um den Inhalt der Website zu empfangen. Diese für den Moment offene Tür nutzt der Wurm, um neben der eigentlichen Antwort auf die gesendete Anfrage ebenfalls in den Arbeitsspeicher des anfragenden Computers zu gelangen. Dort angekommen, ist der Wurm sofort aktiv und treibt, wie ein Virus, sein Unwesen.

Ein Wurm kann sich ebenso verbreiten, ohne dass vorab eine Anfrage eines Computers an einen anderen stattfindet.

Die verschiedenen Betriebssysteme (Windows, Linux, Mac OS) auf den Computern in Netzwerken stellen von Hause aus bereits offene Softwareports zur Verfügung, die zur Kommunikation mit Netzwerk-Servern, -Druckern oder anderen Netzwerksystemen benötigt werden. Der Wurm kennt diese Standardports und scannt ganze Landschaften von Rechnern nach diesen offenen Ports automatisch ab. Findet er eine offene Stelle, kopiert er sich sofort automatisch in den Arbeitsspeicher des betroffenen Systems – ohne dass ein Benutzer vorher irgendein Programm geöffnet hat.

Schutz gegen Würmer

Um einen Computer vor Wurmern zu schützen, ist ebenso wie bei Viren, ein **Virens Scanner** erforderlich. Der Virens Scanner kann jedoch aus technischen Gründen nicht erkennen, ob der Datenstrom auf einigen Softwareports erwünscht oder unerwünscht ist. Deshalb ist darüber hinaus eine so genannte **Firewall** notwendig. **Die Firewall kann ein Computerprogramm sein, das auf dem zu**

schützenden Rechner unter dessen Betriebssystem installiert wird.

Professionelle Anti-Viren-Software enthält heutzutage oft einen Virens Scanner und eine Software-Firewall. Einige Betriebssysteme verfügen bereits über eine vorinstallierte Firewall.

Funktionsweise. Die Firewall sperrt offene Softwareports für Netzwerkbereiche, aus denen diese Ports nicht benutzt werden sollen. So kann man eine Firewall beispielsweise so einstellen, dass offene Ports für alle Rechner, Drucker und Server innerhalb eines Büros erreichbar sind. Rechner, mit denen man im Internet kommuniziert, können jedoch nur explizit jene Ports ansprechen, die z. B. für E-Mail- oder sonstige Internetdienste erforderlich, also gewollt sind. Welche Ports mit welchen Funktionen hierbei interessant sind, wird in einem separaten Beitrag erläutert.

Gefahr durch Trojaner

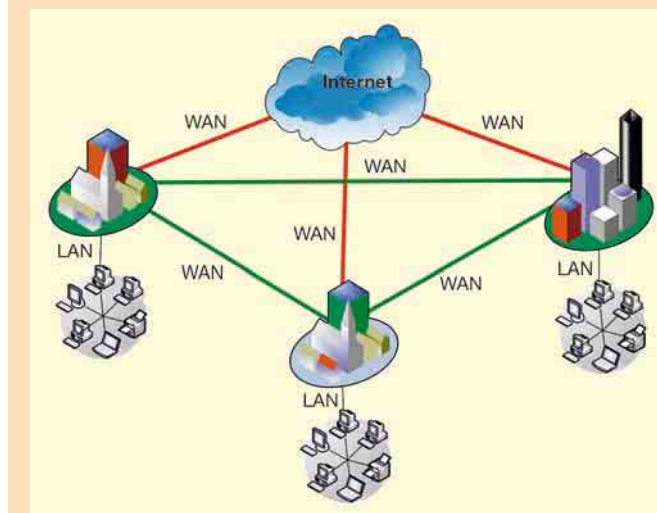
Als Trojaner bezeichnet man Computerprogramme, die auf einem betroffenen Rechner dem Anwender unbekannte oder ungenannte Funktionen ausführen. Diese Programme werden vom Anwender geöffnet und führen im Hintergrund Aktionen aus, die nicht Bestandteil der eigentlichen Funktion des ausgeführten Programms sind.

Trojaner verbreiten sich auf die selbe Art wie Computerviren oder werden vorsätzlich auf Computersystemen eingeschleust.

Oft verbergen sich diese Programme hinter nützlichen Erweiterungen für Anwendersoftware wie z. B. Internetbrowser (Plug-In's) und stehen im Internet zum Download „zur Verfügung“. Trojaner replizieren sich im Gegensatz zu Computerviren nicht selbst.

Typische Angriffsszenarien

Installation von Schadprogrammen. Der Trojaner an sich schädigt den betroffenen Rechner in der Regel nicht. Allerdings installiert er auf dem System selbstständig weitere Programme, die z. B. bekannte Passwort-Dateien ausspionieren (Spyware), als „Keylogger“ fungieren (Malware). Dabei werden sämtliche Tastatureingaben mitgeschnitten, Programme wie Virens Scanner ausgeschaltet, bestehende Dateien sa-



1 LAN- und WAN-Verbindungen

botiert oder die Netzwerkkommunikation zwischen verschiedenen Anwenderprogrammen aufgezeichnet (Sniffer).

Die gesammelten Informationen werden dann, z. B. per E-Mail, durch die schadhafte Programme an einen potentiellen Angreifer gesendet.

Netzwerkverbindungen zu Fremdsystemen. Diese schadhafte Programme können auch eigene Netzwerkverbindungen zu fremden Systemen aufbauen. Über diesen Kommunikationsweg, der praktisch von einem betroffenen Rechner in einem lokalen Netzwerk, beispielsweise im Büro, zu einem fremden Rechner in einem anderen Netzwerk – z. B. im Internet – initiiert wird, ist es möglich, den betroffenen Rechner komplett fernzusteuern und auszuspionieren.

Angriffe auf fremde Websites und Rechner. Unter den Schädlingen befinden sich oft auch Programme, die nicht dem infizierten System schaden, sondern automatisch andere Rechner, z. B. die Webserver eines Unternehmens im Internet, angreifen oder mit Werbemails (Spam) überschütten. Der Benutzer des eigentlich infizierten Systems ist sich meist gar nicht dessen bewusst, dass sein Rechner anderen Schaden zufügen kann. Deshalb ist es besonders wichtig, auch an die Datensicherheit, beispielsweise der seiner Lieferanten und Kunden, zu denken. Man darf keinesfalls davon ausgehen, dass die eigenen Systeme keines Schutzes bedürfen, da auf ihnen keine relevanten Funktionen laufen oder sensiblen Daten liegen.

Überwachen des Surf- und Kauf-

verhaltens. Diese „Spyware“ und „Malware“ wird auch oft genutzt, um das Surf-Verhalten oder das Shopping-Verhalten eines Anwenders im Internet aufzuzeichnen, damit dieser dann effizienter mit Werbung zu „ködern“ ist oder um Statistiken anzulegen.

Interne Status- oder Fehlermeldungen. Teilweise werden Trojaner sogar für „friedliche Absichten“ verwendet. So kann es sein, dass ein Programmierer eine Funktion in seiner Anwendersoftware integriert, die ihm Status- oder Fehlermeldungen sendet. Solange der Anwender über solche Funktionen nicht in Kenntnis gesetzt ist, fällt diese Funktion in die Kategorie Trojaner.

Erkennen von Trojanern

Trojaner werden ebenso wie Viren und Würmer von **Virens Scannern** erkannt. Darüber hinaus gibt es spezielle Software, die explizit „Malware“ und „Spyware“ auf PC-Systemen erkennt und deinstalliert. Oftmals ist diese Art von „**Bereinigungssoftware**“ effektiver zur Bekämpfung dieser Schädlinge als der eigentliche Virens Scanner. Solche Software sollte in regelmäßigen Abständen auf dem zu schützenden System gestartet werden.

Um unerwünschte Funktionen, die von Trojanern installiert werden, zu unterbinden, empfiehlt sich ebenfalls dafür eine **Software-Firewall**. Diese regelt, wer mit wem auf welchen Wegen kommunizieren darf und wer nicht.

Computer als Bots

Etliche Computer im Internet fungieren darüber hinaus, freiwillig

oder unfreiwillig, als Roboter (Bots) und durchsuchen andere Rechner, die mit dem Internet verbunden sind, permanent nach Schwachstellen. Sobald diese gefunden sind, werden diese protokolliert und automatisch angegriffen, z. B. mittels Würmern.

Es ist ebenso wahrscheinlich, dass insbesondere Trojaner vorsätzlich in Computersysteme eingeschleust werden, um Spionage oder Sabotage zu betreiben.

Angriffsziele. Im privaten Bereich ist insbesondere das „Online-Banking“ davon betroffen.

In Unternehmen sind vor allem solche sensiblen Daten wie Aufträge, Preiskalkulationen, Kundendaten, Unternehmensstatistiken und Patententwicklungen usw. für den Angreifer interessant. Ebenso kann es dessen Ziel sein, das Image einer Firma zu schädigen oder deren produktive Abläufe zu sabotieren.

Zu empfehlende Sicherheitsmaßnahmen

Sicherheits-Software. Auf PC-Systemen im privaten Bereich sollten mindestens eine Software-Firewall, ein Virens Scanner sowie ein Programm zur Bekämpfung von Spy- und Malware installiert sein. Diese Programme müssen durch den Benutzer stetig aktuell gehalten werden und ggf. wöchentlich manuell ausgeführt oder kontrolliert werden. Am einfachsten ist es, diese Prozesse zu automatisieren. Benutzerfreundliche Software stellt dafür entsprechende Installationsassistenten bereit.

Hardware. Für kleine und mittlere Unternehmen empfiehlt sich zusätzlich zu diesen Schutzmechanismen der Einsatz von Security-Komponenten in Form von Hardware. Diese wird von einem IT-Fachmann, dem Security-Fachmann, installiert und gewartet. Der erhöhte Aufwand ist insbesondere dann zu empfehlen, wenn die möglichen Auswirkungen von angerichteten Schäden im Vergleich zur Installation dieser Security-Komponenten exorbitant hoch wären. Dabei sollte man auch das Image seines Unternehmens sowie die Verantwortung gegenüber Dritten im Auge behalten.

Weitere Angriffsszenarien gegen Computersysteme

Angriffe gegen Computersysteme richten sich in der Regel nach deren Schwächen. Die Betriebssysteme auf PCs oder Anwenderprogramme bergen jede Menge Schwachstellen in sich, da deren grundsätzliche Aufgaben nicht die Abwehr von Angriffen ist. Insbesondere jene Komponenten, die über das Netzwerk kommunizieren sind ggf. manipulierbar. Ein Angreifer kann den Kommunikationsschnittstellen, die Softwareports, gezielt Informationen übertragen, die das System veranlassen, vom Benutzer ungewollte Funktionen auszuführen. **Phishing.** So ist es z. B. möglich, den PC dazu zu bringen auf eine andere Website zu springen als die, die vom Benutzer aufgerufen wurde – das so genannte Phishing. Sehr beliebt ist das beim Online-Banking. Der Anwender wird auf eine Website geleitet, die genauso aussieht, wie seine gewohnte Online-Banking-Seite.

Dort wartet ein potentieller Angreifer nur noch auf die Eingabe von Kontonummer, PIN und TAN durch den Benutzer.

„Deny of Service“. Ebenso beliebt sind „Deny of Service“ (DoS)-Angriffe. Hierbei geht es darum, ein System mit Anfragen oder Antworten zu „überfüttern“. Der Computer kann den überhäuft und fehlerhaften Netzwerkstrom nicht mehr verarbeiten und „stürzt ab“ oder führt Fehlfunktionen aus.

„Man in the Middle“. Eine weitere Bedrohung ist ein Angriff namens „Man in the Middle“. Hierbei wird ein Computer dazu veranlasst, über einen bestimmten Netzwerkknoten mit seinem eigentlichen Ziel zu kommunizieren. An diesem Netzwerkknoten zeichnet ein Angreifer den durchgehenden Netzwerkverkehr auf (Sniffen) und gelangt so an den Inhalt von E-Mails, an Passwörter und an den Inhalt sonstiger Kommunikation.

Derartige Angriffsszenarien sind heutzutage größtenteils automa-

tisiert. Die dahinter steckenden Personen werten die gesammelten Informationen aus und missbrauchen diese dann ggf.

„Rootkids“. Bisweilen versuchen sich potentielle Angreifer auch persönlich im „Hacken“, um ihr Know-how zu trainieren. Hierbei spricht man von Angriffen durch so genannte „Rootkids“.

Beispiel. Insbesondere Unternehmen mit Patententwicklungen oder sensiblen Kundendaten sind häufig Opfer von Industriespionage und -sabotage. So kam es vor, dass ein mittelständisches Unternehmen sein über mehrere Jahre entwickeltes Patent anmelden wollte. Dieses wurde jedoch abgelehnt, da es zuvor bereits durch ein anderes Unternehmen angemeldet worden war – mit ähnlichem Wortlaut und fast identischen Grafiken. Die Ingenieure des geschädigten Unternehmens waren sich bis dahin nicht darüber im Klaren, dass E-Mails im Internet wie Postkarten lesbar und duplizierbar sind. Da ihre Kommunikation größten-

teils via unverschlüsselter E-Mails stattfand, hatte offensichtlich ein Spion keine große Mühe, an die wertvollen Informationen zu gelangen.

Der Aufwand, mehrere Computer oder gar komplexe Netzwerke aus mehreren Computersystemen mithilfe der bisher aufgeführten Maßnahmen zu schützen und stetig aktuell zu halten, ist recht hoch und steigt mit jedem neu hinzukommenden System. Wesentlich günstiger und sicherer ist ein System aus Schutzkomponenten, das Angriffe oder Viren bekämpft, bevor diese ins lokale Netzwerk eindringen.

Schutz von lokalen Netzwerken

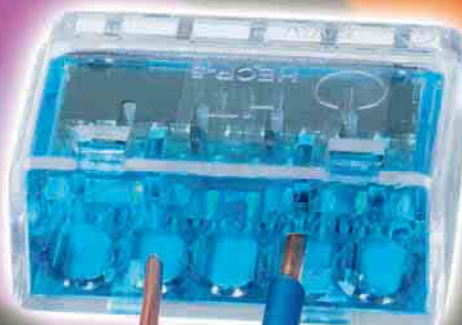
Als lokale Netzwerke, auch LAN (Local Area Network) genannt, bezeichnet man Computersysteme, Netzwerkdruker, Server und sonstige Netzwerkkomponenten, die innerhalb eines Standortes eines Unterneh-

Anzeige

Kabel lieben HelaCon.



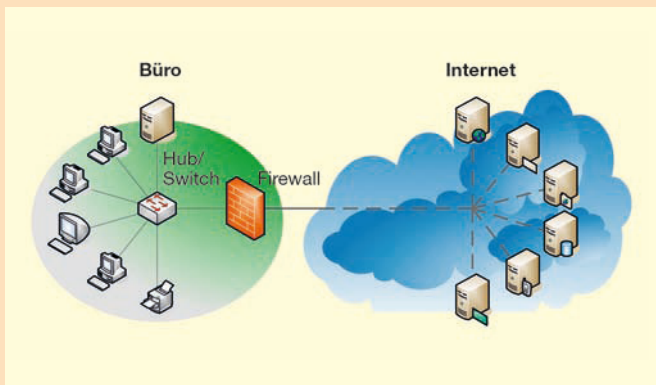
Für Kabel ist es eine sichere Lösung. Für Profis eine innovative Verbindungsklemme, die jeder Situation gewachsen ist. Denn mit **HelaCon Plus** und **HelaCon Easy** stehen Ihnen hochentwickelte Steckklemmen für die professionelle Kabelverarbeitung in der Haus- und Gebäudeinstallation zur Verfügung. Die neu entwickelte Doppelfeder von HelaCon Plus ermöglicht Ihnen eine einfache Verarbeitung und entlastet Sie auch in besonders schwierigen Situationen wie der Überkopf-Montage.



Besuchen Sie uns auf der
Light & Building, Frankfurt
in **Halle 9.0, Stand B50**
(06. – 11.04. 2008)

www.HellermannTyton.de/HelaCon

HellermannTyton



② durch Hardware-Firewall geschützte Internetanbindung

mens, innerhalb eines Büros oder auch innerhalb der eigenen vier Wände miteinander vernetzt sind (Bild ①).

Das LAN an einem weiteren Standort eines Unternehmens, betrachtet man für sich als eigenständiges LAN. Verbindet man die lokalen Netze verschiedener Standorte miteinander, so spricht man bei dieser Verbindung von einem WAN (Wide Area Network). Eines der größten und bekanntesten WANs ist das Internet. Größere Unternehmen vernetzen die LANs ihrer Filialen über WAN-Verbindungen mitunter weltweit.

Um die Computersysteme und elektronischen Daten in lokalen Netzwerken zu schützen, verwendet man in der Praxis verschiedene Security-Hardware.

Hardware-Firewall

Das sind Rechnersysteme die als aktive Netzwerkkomponenten ins bestehende Netzwerk eingebunden werden und auf denen entsprechend ihrer Funktion eine Security-Software läuft.

Eine Hardware-Firewall (Bild ②) fungiert hauptsächlich als Filter zwischen mindestens zwei verschiedenen Netzen. Das können WANs und LANs oder verschiedene LANs untereinander sein (Bild ①). Die gesamte Kommunikation der einzelnen Computersysteme in diesen verschiedenen Netzen wird reglementiert durch die Firewall geleitet.

Am häufigsten werden Firewalls als Schutzkomponente vor Angriffen aus dem Internet eingesetzt. Die Firewall wird hierbei in die Verbindung zwischen dem lokalen Netzwerk und dem Internet eingebunden (LAN-WAN). Sie ist dadurch im Internet als aktive Komponente zu sehen und somit direkt angreifbar, verbirgt jedoch

das lokale Netzwerk hinter sich. **Funktionsweise.** Auf einer Firewall wird geregelt, wer mit wem wie kommunizieren darf. Jeglicher Netzwerkstrom, der durch die Firewall fließt, wird auf Grundlage entsprechend definierter Kriterien geprüft. Wenn es keine Regel für eine bestimmte Verbindung gibt, wird der Informationsfluss auf dieser Verbindung verworfen.

Darüber hinaus laufen insbesondere auf Hardware-Firewalls Mechanismen, die z. B. reglementieren, dass grundsätzlich kein Netzwerkstrom aus Netzen mit niedriger Vertrauensstufe (Internet, WAN) ohne Weiteres in ein Netz mit hoher Vertrauensstufe (LAN) fließt. Sobald z. B. ein Computer aus dem LAN eine Verbindung zu einem Internetserver aufbaut, öffnet die Firewall einen Tunnel für diese Verbindung, sofern ihre vorab definierten Regeln dies zulassen. Die Antwort des Internetserver darf ausschließlich durch diesen Tunnel zurück an den Computer erfolgen, der die Anfrage startete. Bekannte Angriffsmechanismen, bei denen ein Internetserver beim Antworten auf eine Anfrage parallel weitere Verbindungen zur Quelle aufbaut, werden somit von vornherein unterbunden. Außerdem sind diese Geräte in der Lage, Angriffe, die gegen sie selbst gerichtet sind, abzuwehren.

Proxy-Server

Ein Proxy-Server ist ein Rechner, der die Internetanfragen von lokalen Rechnern entgegennimmt und sich stellvertretend für diese im Internet bewegt.

Moderne Firewalls verfügen bereits über integrierte Proxy-Funktionen, man spricht hierbei von „Application-Layer-Firewalls“. Die Proxy-Funktion kann stellverte-



③ durch IPS und Firewall geschützte Internetanbindung einschließlich DMZ

tend als E-Mail-Empfänger und -Sender fungieren, wobei gleichzeitig die Möglichkeit besteht, die E-Mails auf Spam und Viren zu prüfen und zu filtern – in moderneren Versionen diese sogar zu ver- oder entschlüsseln.

Mit einem Proxy kann man den Internetverkehr auf Inhalte (Content-Filter) und Kategorien wie z. B. Pornographie, Waffen, Drogen, Alkohol usw. filtern, um den Anwendern den Zugang zu unsicheren oder fragwürdigen Websiten zu verwehren. Das ist besonders auch in Ausbildungsbetrieben für den Jugendschutz wichtig.

Besonderer Schutz bei Internetdiensten

Eine besonders ernstzunehmende Konstellation in punkto Sicherheit tritt ein, wenn ein Unternehmen einen Dienst oder eine Anwendung für Nutzer aus dem Internet bereitstellen will – z. B. ein eigener Webserver, auf dem ein Onlineshop läuft. Dieser Server soll im eigenen Netzwerk stehen und trotzdem im Internet zu erreichen sein.

DMZ. Alle Systeme, die aus dem Internet erreichbar sein sollten, müssen in eine so genannte DMZ („Demilitarisierte Zone“) integriert werden. **DMZ– das ist ein lokales Netzwerksegment, das separat über einen eigenen Anschluss mit der Firewall verbunden ist.** Das Segment ist dann aus dem lokalen Netz sowie aus dem Internet erreichbar und wird auf der Firewall möglichst sensibel bewacht. Für einen Webserver oder ähnliche Anwendungen ist es aber erforderlich, dass Anwender im Internet diese Dienste direkt durch die Firewall abrufen können. Es muss auf der Firewall mindestens eine Regel existieren, die den direkten Zugriff vom Internet in die DMZ ermöglicht.

Auf dieser Verbindung ist jedoch auch ein Angriff möglich, z. B. indem spezielle Programmcodes an ein automatisches Onlineformular auf diesem Webserver übergeben werden, um diesen zum Ausführen ungewollter Funktionen zu bringen.

IPS. Um diesen Netzwerkstrom dennoch zu überwachen und zu sichern, ist der Einsatz eines IPS (Intrusion Prevention System) notwendig (Bild ③). **Dieses System besteht aus Security-Software, die auf einem gesonderten Rechner oder auf einer Application-Layer-Firewall läuft.**

Funktionsweise. Ein IPS kann den durchlaufenden Netzwerkstrom mit Hilfe einer integrierten Datenbank nach Angriffsmustern oder Unregelmäßigkeiten durchsuchen und Gegenmaßnahmen einleiten, wie z. B. das Aussperren des Angreifers oder das Verwerfen der Verbindung zum angreifenden Computer. Der sonstige Nutzdatenverkehr bleibt davon unberührt.

Fazit

Mit diesen Sicherheitsvorkehrungen – in Abhängigkeit von den jeweiligen Risiken – kann sich ein Unternehmen grundsätzlich vor äußeren Angriffen auf seine internen elektronischen Daten schützen.

Zusätzliche Maßnahmen sind darüber hinaus empfehlenswert, wenn beispielsweise Außendienstmitarbeiter einen Zugriff auf Daten im Firmennetzwerk benötigen. Dann ist es unter Umständen sinnvoll, die Einwahl via VPN (Virtual Private Network) durchzuführen. Das wird Gegenstand eines weiteren Beitrags im **ep** sein.

D. Schubert