

# IT-Sicherheit in der Praxis



Ein Fachreferat  
von  
**Ansgar H. Licher**  
Dipl.-Ingenieur der Systemanalyse  
IT-Leiter der MBN Bau AG



Der Einsatz von Informationstechnik schreitet in allen Bereichen der Wirtschaft mit großen und immer schneller werdenden Schritten voran. Durch den Einsatz von E-Mail werden Dokumente blitzartig transportiert, das Internet ermöglicht Kooperationen von räumlich getrennten Personen, Informationen über Dienstleistungen und Produkte sind nur wenige Mausklicks im weltweiten Datennetz entfernt.

Der Wettbewerbsdruck zwingt allenthalben zu Investitionen in Informationstechnik, um mit dem atemberaubenden Arbeitstempo der Mitbewerber mithalten zu können. Immer neue Möglichkeiten zur Reduzierung von Kosten, Zeit und administrativem Aufwand bieten sich an, eingeführt zu werden, um Abläufe zu beschleunigen und alle Informationen zur richtigen Zeit am richtigen Ort vorliegen zu haben.

Die sonnigen Seiten dieser technologischen Neuerungen haben jedoch auch Schattenseiten. In stark zunehmendem Maße tauchen negative Schlagzeilen auf. Es ist die Rede von Viren und Würmern, Hackern und elektronischen Einbrüchen, die zum Verlust von Daten oder zur Kompromittierung von Unternehmen führen. Berichte über „I LOVE YOU“, CodeRed, Nimda und neuerdings sog. Dialer verunsichern Anwender und stellen teilweise erhebliche Gefahrenquellen dar.

Der Wille und die Bereitschaft, dringend notwendige Innovationen in bspw. E-Mail-Systeme und Internet-Zugänge zu investieren, ist in der Wirtschaft durchaus vorhanden. Die Praxis in den Betrieben zeigt dabei jedoch allzu oft, dass das Allerwichtigste in sehr vielen Fällen unberücksichtigt bleibt oder eklatant unterschätzt wird: die Sicherheit der eigenen EDV-Umgebung.

Was für Gefahren drohen Firmen konkret, die E-Mail und Internet einsetzen und wie kann man sich in der Praxis wirksam davor schützen?

Wenn wir die Gefährdungspotenziale näher betrachten und analysieren, müssen wir zunächst eine Unterteilung in die eher sichtbaren und die eher unsichtbaren Gefährdungen vornehmen. Eher unsichtbar sind in diesem Zusammenhang insbesondere alle sog. netzwerkbasierenden Angriffsmethoden, also all das, was man unter den „klassischen“ Hacker-Angriffsmöglichkeiten versteht. Hierbei existiert das Gefahrenpotenzial allein dadurch, dass eine Internet-Verbindung vorhanden ist, die (wie unten beschrieben) geschützt werden muss.

Zu den eher sichtbaren Gefährdungen zählen insbesondere Viren, Würmer, Trojanische Pferde usw. Die Gefahr lauert hier in den Inhalten, also E-Mails, E-Mail-Anlagen, Web-Seiten usw., die vorsätzlich mit schaden-bewirkendem Programmcode ausgestattet sind. Man bezeichnet diese Gefährdungspotenziale auch als inhaltsbezogene (oder Neudeutsch: content-basierte) Gefährdungen.

Im folgenden ist dargelegt, wie sich die Gefährdungspotenziale konkret darstellen und wie praxiserprobte Schutzmechanismen hierzu aussehen.

## **Teil 1: netzwerk-basierende („unsichtbare“) Gefahrenpotenziale**

Der Internet-Zugang aus einem Firmennetzwerk (LAN bzw. Local Area Network) heraus ist keine komplizierte Angelegenheit. Im Gegenteil: Im Prinzip reicht ein analoges Modem oder eine ISDN-Karte und schon kann es los gehen. Die Verbindung zum Internet ist genauso schnell und einfach hergestellt, wie ein Telefonat von A nach B. Ist man mit dem Internet verbunden, kann man bspw. E-Mails austauschen oder im Web surfen usw.

Die Verbindung zwischen einem PC und dem Internet ist vergleichbar mit einem PC in einem LAN. Der PC ist (sobald eine Verbindung zum Internet hergestellt ist) im Internet vollständig sichtbar. Sichtbar heißt in diesem Zusammenhang, dass alle seine Eigenschaften und Leistungsmerkmale



aus dem Internet heraus sichtbar sind (bspw. der Rechnername, Name des angemeldeten Benutzers, freigegebene Verzeichnisse, usw.).

Werden bspw. im LAN Dateien von einem PC zu einem anderen über das Netzwerk kopiert, kann dieses prinzipiell auch zwischen dem PC und dem Internet erfolgen. Ein Windows-PC steht also wie eine offene Tür gegenüber dem Internet da. Dementsprechend ist es sehr einfach, aus dem Internet auf den PC zuzugreifen und diverse Dinge auf dem PC zu tun, bspw. Dateien hin oder herkopieren, etc..

Wenn dieser PC nun sowohl eine Verbindung zum LAN wie auch zum Internet hat (bspw. über o.g. Modem oder ISDN-Karte), kann vom Internet aus nicht nur auf den PC, sondern sogar durch ihn hindurch in das gesamte Netzwerk (LAN) zugegriffen werden. Somit steht Hackern das gesamte Netzwerk zum Spionieren und Manipulieren von außen offen. Alle Systeme im Netzwerk sind dann über das Internet von außen zu erreichen: Server, Datenbanken, PCs, Drucker, ...

Ein adäquater Schutz vor solchen unsichtbaren Bedrohungen bieten Firewalls. Eine Firewall ist prinzipiell eine „Brandschutzmauer“. Sie trennt das LAN strikt vom Internet. Jegliche Verbindung zwischen dem Internet und den PCs im Netzwerk wird ausschließlich über die Firewall (statt über einen PC mit Modem oder ISDN-Karte) realisiert.

Dies ist die einzig wirksame und dringendste nötige Schutzvorrichtung, um den unsichtbaren elektronischen Gefahren wirksam vorzubeugen. Hackern wird es somit unmöglich, auf PCs, Server usw. aus dem Internet heraus zuzugreifen. Nur durch den Einsatz einer Firewall ist ein wirklicher Grundschutz gegenüber dem weltweiten Datennetz gegeben.

Allzu oft wird die Anschaffung von Firewall-Systemen vernachlässigt. Oft ist von Dingen wie „Das Netz ist so groß! Wie soll da jemand ausgerechnet unseren PC/unser Netzwerk aufspüren?“ die Rede. In der Praxis ahnen nicht einmal die meisten Privat-Anwender, dass sie mehr oder weniger regelmäßig „abgescannt“ werden.

Unter „abscannen“ versteht man den Vorgang, der quasi immer als erster Schritt eines möglichen späteren Hacker-Angriffs stattfindet. Systematisch werden hierbei alle möglichen auffindbaren Geräte im Internet auf evtl. „offene Türen“ überprüft. Da ein PC (oder ein Netzwerk ohne eine Firewall) etliche „offene Türen“ aufweist, ist so eine Stelle ein idealer Ansatzpunkt für weitere „Nachforschungen“, also eine regelrechte Einladung für potenzielle Hacker.

Das Scannen selber ist so einfach wie wirkungsvoll, zumal es (zumindest heute) keine strafbare Handlung darstellt. Manche Hacker haben sogar fremde Systeme gekapert und diese so manipuliert, dass sie (vom Eigentümer unbemerkt und) vollautomatisch, unauffällig und quasi ständig „scannen“. Sobald sie etwas interessantes entdecken, benachrichtigen solche Systeme den Hacker, der sich dann direkt um die gefundenen interessanten Fälle kümmern kann, ohne seine eigene „Arbeitszeit“ mit der Suche nach Opfern zu „verschwenden“.

Das „Scannen“ kann man sich am einfachsten so vorstellen: In einer Stadt (Internet) befinden sich viele Straßen (Netzwerke). In einer Straße stehen viele große und kleine Häuser (Geräte, bspw. PCs). Jedes dieser Häuser hat einige Türen und Fenster. Bei manchen Häusern sind Türen und Fenster geschlossen, weil der Brandschutz (Firewall) dieses so vorsieht. Bei anderen Häusern stehen einige Türen und Fenster weit offen.

Nun geht jemand zu Fuß durch die Straßen der Stadt und schaut sich die Türen und Fenster an, ob sie geschlossen oder offen sind. Ist das eine strafbare Handlung? Für einen (potenziellen) Einbrecher stellen die offenen Fenster und Türen geradezu eine Einladung dar, oder?

Waren elektronische Einbrüche (Hacks) früher insbesondere nur technisch versierten Freaks mit detaillierten Kenntnissen über die Funktionsweise von Netzwerken usw. möglich, hat sich das Gefahrenspektrum aus dem Internet nun erheblich erweitert. Mittlerweile existieren erhebliche Men-



gen an Tools und Werkzeugen, die das „Fachwissen“ von Hackern auch technischen Laien zugänglich machen: Dank Window-Technik kann heute jeder Laie mit ein paar Mausklicks Systeme scannen, Schwachstellen aufspüren und diese natürlich auch ausnutzen, also hacken.

Die Firewall ist damit *der* zentrale Dreh- und Angelpunkt der grundsätzlichen Absicherung des eigenen EDV-Systems gegenüber dem Internet. Folglich ist dieses auch der wundeste Punkt der eigenen Verteidigungsstrategie. Ist die Firewall überwunden oder ausgetrickst, ist der Weg möglicherweise wieder offen, etwa so, als wäre gar keine Firewall da.

Es kommt also darauf an, ein vernünftiges Konzept aufzubauen, wie man sich effektiv mit einer Firewall schützt. Ebenso ist die regelmäßige Wartung der Firewall sehr wichtig. Die Scan-Methoden der Hacker werden immer ausgefeilter, somit ist auch die Art und Weise, wie die Firewall schützt, den neuen Gegebenheiten anzupassen.

Die Kombination aus einer (ggf. auch mehrerer) Firewall(s) und einem geeigneten, aufzubauenden Schutzkonzept, gewähren grundsätzliche Sicherheit. Aber auch nur auf der hier beschriebenen untersten (und für den Anwender völlig unsichtbaren) Ebene. Alle weiteren, eher sichtbaren Gefahren, können von Firewalls, die zwar eine sehr wichtige Funktion wahrnehmen, nicht aufgehalten werden. Hier müssen andere Strategien und Werkzeuge her.

Teure Tools und Firewall-Systeme sind nicht immer die Besten, um sich vor den Gefahren aus dem Internet zu schützen. In vielen Fällen kann bspw. eine auf dem quell-offenen Betriebssystem Linux basierende Lösung hinreichend Schutz bieten. Ausgefeilte Firewall-Funktionen sind in Linux bereits implementiert. Hinzu kommt, dass Linux extrem leistungsfähig ist. Eine linux-basierende Firewall für kleine und mittlere Netze kann somit ohne weiteres auf älterer PC-Hardware (bspw. 486er) aufgebaut werden. Linux ist Open Source Software und deshalb völlig kostenlos, was ein weiteres Plus für strapazierte IT-Budgets bedeutet.

## Teil 2: inhalts-/content-basierende („sichtbare“) Gefahrenpotenziale

Um Missverständnisse von vornherein zu vermeiden: Auch inhalts- bzw. content-basierende Gefahren sind ebenfalls überwiegend unsichtbar, wenngleich sich ihre Auswirkungen i.d.R. eher feststellen lassen, als die im ersten Teil genannten netzwerk-basierenden Gefahren.

Das Spektrum der content-basierenden Gefahren ist ausgesprochen vielschichtig. Hierbei handelt es sich im Wesentlichen um gezielte Manipulation von vermeintlich harmlosen Inhalten wie bspw. E-Mails, E-Mail-Anlagen, Web-Seiten und Programmen. Die hier lauenden Gefahren heißen (Makro-)Viren, Würmer, Trojanische Pferde, JavaScript, ActiveX und neuerdings Dialer usw. Ziel dieser Art von Angriffen ist also, einem Anwender vermeintliche Sicherheit vorzutäuschen und ihn zum Anwenden bestimmter Programme oder zum Öffnen bestimmter Dateien zu bewegen, die letztendlich den Schadensmechanismus in Gang setzen.

Die Gefahr, Opfer einer Virenattacke zu werden, ist in den letzten 24 Monaten exponentiell gestiegen. Die Zahl der Virenfunde im eigenen Hause haben allein in den vergangenen 12 Monaten um rd. 250% zugenommen. Insgesamt sind heute weit über 60.000 verschiedene Virentypen und –arten bekannt.

Dass die Virengefahr stetig steigt, liegt nicht erst seit „I LOVE YOU“ auf der Hand: Ähnlich wie bei den netzwerk-basierenden Tools gibt es auch im Virusbereich eine ganze Menge an Werkzeugen, die es dem Anwender erlauben, auf einfachste Weise neue Viren zusammenzubauen. Diese Generatorprogramme ermöglichen, per Mausklick Eigenschaften ein- und auszuschalten, über die der zu generierende Virus verfügen soll.



Während früher im Grunde nur Spezialisten bzw. Leute mit erheblichem Spezialwissen Unruhe im Bereich der IT-Sicherheit stiften konnten, müssen wir heute vor sog. „Skript-Kiddies“ zittern. Oftmals sind dies junge Menschen, die (von „sportlichem“ Ehrgeiz getrieben) agieren. Bestimmtes EDV-Wissen ist (ganz im Gegensatz zu früher) hierfür oft nicht einmal mehr im Ansatz nötig.

Die content-basierte Gefahrenklasse lässt sich prinzipiell in die beiden wesentlichen Gruppen „E-Mail-bezogen“ bzw. „Web-bezogen“ unterteilen:

Viren werden heutzutage weniger über Disketten als vielmehr über E-Mail verbreitet. Schneller und effizienter kann man solche Schädlinge kaum verteilen. Die E-Mail-bezogenen Gefahren sind demnach im wesentlichen Viren, Würmer und Trojaner. Diese haben gemeinsam, dass sie sich nach außen als vermeintlich wichtige oder interessante Datendateien oder Programme darstellen, im Kern aber Böses im Schilde führen, während der Anwender über die wahren Absichten und Umstände im Dunkeln gelassen wird.

Bei den weiter unten beschriebenen web-bezogenen Gefahren handelt es sich i.d.R. weniger um Viren als mehr um sog. „aktive Inhalte“ oder „active content“. Hierunter versteht man Mini-Programme, die (auf Web-Seiten eingebettet) aktiv Dinge ausführen können, wie bspw. Berechnungen durchführen oder Animationen vornehmen (oder auf den Rechner des Surfers zugreifen).

## 2a) E-Mail-basierte Gefahrenpotenziale

Seit auch kleine Betriebe verstärkt E-Mail einsetzen, wissen wir, wie effizient diese neue Kommunikationsform ist. Seit „I LOVE YOU“ wissen wir, wie gefährlich sie sein kann.

Das Problem bei E-Mails sind nicht die E-Mails selbst, sondern zwei wesentliche Faktoren: die Neugier des Empfängers über das Erhaltene und die schlampige Programmierung des am meisten verbreiteten und deswegen in die Schlagzeilen geratenen E-Mail-Programms Outlook bzw. Outlook-Express.

Bei „I LOVE YOU“ haben wir erlebt, wie schnell und massiv ein Virus wirken kann (der so schädlich nicht einmal war, verglichen mit Nimda und Co. Der SIRCAM-Virus bspw. sendet beliebige Anwenderdateien per E-Mail an Wildfremde in der ganzen Welt).

Viren dieser Art werden oft in VisualBasic-Script entwickelt. Diese Programmiersprache hat vollen Zugriff auf alle Komponenten des Systems, kann also bspw. die Festplatte formatieren, E-Mails versenden, Dateien ausspähen, manipulieren oder löschen usw.

Neben den vorgenannten Viren sind insbesondere noch sog. Backdoor-Programme (also: Hintertüren) hervorhebenswert. Backdoor-Programme (bspw. „NetBus“ oder „Back Orifice“, um nur die bekanntesten zu nennen), kommen bspw. in einer unauffälligen E-Mail verpackt daher. Startet der Anwender das vermeintlich nützliche Programm aus der E-Mail, wird (ohne dass der Anwender etwas davon bemerkt) die Hintertür eingerichtet. Der Hacker im Internet hat dann jederzeit, wenn der PC mit dem Internet verbunden ist, die Möglichkeit, den gesamten (!) PC vollständig zu kontrollieren: Keine Datei und keine Systemeinstellung bleibt ihm verborgen. Natürlich kann er alles, was er sieht, auch manipulieren. Der Anwender ahnt, wie gesagt, überhaupt nichts davon.

Eine spezielle „Virenattacke“ sind sog. „Hoaxes“, also üble Scherze. Es handelt sich hierbei in Wirklichkeit gar nicht um Viren, sondern um Warnungen vor angeblichen Viren. Trittbrettfahrer schreiben solche Warnungen, die dann bspw. vor E-Mails mit einem bestimmten Betreff und einer bestimmten Anlage warnen. Dort sei dann ein sehr gefährlicher Virus enthalten. Ziel ist hierbei nicht, einen tatsächlichen Virus zu verbreiten, sondern Verwirrung zu stiften und Irritationen auszulösen. Diese Hoaxes sind reine Textmitteilungen und samt und sonders harmlos.



## 2b) Web-basierte Gefahrenpotenziale

Auf Web-Seiten werden heute zunehmend nicht nur statische Informationen feilgeboten, sondern auch Funktionen zur Verfügung gestellt, mit denen Anwender aktiv Dinge tun können, wie bspw. Zinsberechnungen, Routenberechnungen usw. vornehmen. Neben Nützlichem kommen auch rein kosmetische Animationen zum Tragen.

Zur Realisierung dieser Merkmale werden i.d.R. Mini-Programme entwickelt, die statt auf dem Server des Anbieters auf dem PC des Surfers ablaufen. Hierzu stehen verschiedene Technologien (von Java über JavaScript bis hin zu ActiveX) zur Verfügung. Während Java auf Grund seiner Architektur noch einigermaßen sicher ist, kann dieses für die sog. abgespeckte Version von Java (JavaScript) nicht gelten: Beide Programmtypen laufen auf dem PC des Anwenders, jedoch hat JavaScript (im Gegensatz zu Java) Zugriff auf eine Vielzahl von Eigenschaften des PCs. Bspw. können JavaScript-Programme Systemeinstellungen des PCs ändern, auf dem sie laufen, usw.

Bei ActiveX sieht die Gefahrenlage noch viel verheerender aus. Diese von Microsoft entwickelte Technologie hat Zugriff auf den gesamten PC mit *allen* seinen Eigenschaften, Ressourcen und Funktionen. Was seinen Ursprung nahm als „Klebstoff-Programm“ zwischen Softwarekomponenten auf verschiedenen PCs in einem LAN wurde ohne jegliche Einschränkung auf das Internet übertragen. Somit kann ein ActiveX-Programm auf den gesamten PC und all seine Ressourcen, bis hin zum angeschlossenen Netzwerk zugreifen und *alles* (!) damit tun.

Genau an dieser Stelle liegt das große Problem der Web-Sicherheit: Der Anwender hat (bei ActiveX bspw. trotz möglichen Sicherheitszertifikaten) keinerlei Chance zu überprüfen, ob das Programm (egal, ob Java, JavaScript oder ActiveX) nichts schadhaftes anrichten kann. Er muss darauf vertrauen, dass das Programm „sauber“ ist, hat aber niemals eine Garantie dafür. Eben dieser Treuglaube wird von böswilligen Seitenanbietern immer wieder ausgenutzt und unterlaufen. Gerade die berühmten 0190-Dialer lassen sich per ActiveX auf's einfachste über die Menschheit verteilen.

Insbesondere JavaScript wird auf vielen Web-Seiten gerne für programmtechnische Kleinigkeiten verwendet. Aber genau diese Skriptsprache verfügt über eklatante Sicherheitsmängel, die es für Angreifer interessant machen, harmlos aussehende Web-Seiten mit gefährlichen JavaScript Programmen auszustatten, die teilweise erhebliche Kontrolle über den PC übernehmen können.

Vor dem tödlichen Gefahrenpotenzial von ActiveX kann nur eindringlichst gewarnt werden! Ebenso aber darf JavaScript aus sicherheitstechnischer Sicht nicht unberücksichtigt bleiben und muss auf Grund immer wieder auftretender eklatanter Sicherheitsverletzungen ebenfalls als sehr kritisch betrachtet werden.

## Schutzmaßnahmen gegen inhalts-/content-basierende Gefahrenpotenziale

Nachdem eine Firewall Grundsicherheit in bezug auf den Netzwerkverkehr herstellt, ist nachstehend beschrieben, welche Maßnahmen betreffs Schutz vor Viren, Würmern und gefährliche Web-Seiteninhalte getroffen werden müssen.

Ob ein einzelner PC oder ein gesamtes Firmennetzwerk mit direkter Internet-Anbindung zu schützen ist, kann im Grunde vernachlässigt werden. Beide Seiten sind absolut gleichzusetzen! Ein Virus auf einem Aussendienst-Notebook kann nicht nur dort Schaden anrichten, sondern auch sehr leicht auf das Firmennetzwerk übergreifen und umgekehrt.

Für einzelne PCs bspw. gibt es Kompakt-Lösungen, die einfach zu installieren sind und den PC sowohl gegen Disketten-Viren als auch gegen E-Mail-Viren schützen. Darüber hinaus bieten die Produkte oft auch Schutz beim Surfen im Internet.



Um das eigene Firmennetzwerk (LAN) effektiv zu schützen, sind ein paar mehr Dinge erforderlich. Hier gilt es, ein ganzes Netzwerk mit mehreren Geräten (PCs, Servern, Druckern, usw.) zu schützen. Neben dem Schutz vor netzwerk-basierenden Angriffen, der durch eine o.g. Firewall erfolgen muss, ist hier beschrieben, wie ein wirksamer Schutz vor inhalts-/content-basierten Angriffen aufgebaut werden sollte.

Die einzig wirksame Sicherheitsphilosophie ist, grundsätzlich sämtliche Datenströme, die egal von welchen externen Quellen und egal auf welchen Wegen in das eigene Unternehmen gelangen, zunächst ausnahmslos unter Generalverdacht zu stellen. Niemand kann sagen, ob bspw. eine Datei wirklich das enthält, was erwartet wird, ohne sie zu öffnen. Das Öffnen selbst ist aber der Gefahrenpunkt. Dementsprechend müssen alle eingehenden Daten (egal von wo und egal mit welchem Transportmedium sie in das Unternehmen gelangen) auf potenzielle Viren, Würmer, Trojaner etc. überprüft werden.

Die Eindringpunkte externer Daten in das Unternehmen sind relativ klar: Disketten, CDs, Bänder, Wechselplatten, E-Mail, World Wide Web (WWW, surfen). Nur wenn es gelingt, wirklich alle Eintrittspunkte zu kontrollieren, ist ein wirklicher Schutz vor Viren und anderem böswilligen Code gewährleistet, wenngleich die Internet-basierenden Eintrittspunkte (E-Mail, WWW) heute die gefährlichsten sind.

Die Aufgabe, alle Daten, die das Unternehmen betreten, zu kontrollieren, scheint angesichts der Komplexität der Aufgabe unvorstellbar. Jedoch gibt es exakt auf dieses Problem zugeschnittene Lösungen. Wir selbst setzen das Produktportfolio der Firma TrendMicro ein, einem führenden Hersteller von Anti-Virenprodukten. Der vollständige Schutz vor Viren, Würmern, usw., ist gewährleistet, weil die einzelnen Produkte nahtlos ineinander greifen und alle kritischen Bereiche hervorragend abdecken. Konkret ist der Virenschutz wie folgt aufgebaut:

## Schutz vor E-Mail-basierenden Gefahren:

Alle aus dem Internet eingehenden E-Mails betreten das Unternehmen an einer zentralen Stelle. Sie gelangen aus dem Internet zunächst in eine Durchgangszone zwischen dem Internet und dem LAN. Hier befindet sich ein E-Mail-Virenschanner, der jede E-Mail nebst Anlagen auf Virenbefall oder anderweitigen böswilligen Programmcode untersucht. Nur wenn keinerlei Beanstandungen festgestellt werden, wird die überprüfte E-Mail aus der Durchgangszone zwischen Internet und LAN in das LAN gelassen. Sie gelangt dort dann in das Postfach des Anwenders.

Wir setzen an mehreren Standorten Mail-Server ein. Dennoch existiert nur ein einziger zentraler Zugang zum Internet. Um auszuschließen, dass Viren per E-Mail von einem Standort zu einem anderen gelangen (egal wo und wie sie in das Mailsystem gelangen könnten), sind auch alle Mail-Server mit einem eigenen Virenschutz (ScanMail) ausgestattet.

## Schutz vor Web-basierenden Gefahren:

Wie bei den E-Mails kommen auch hier ausnahmslos alle Daten aus dem Internet zunächst in die Durchgangszone. Hier befindet sich ein zentraler Proxy-Server, der all diese Daten annimmt. Auf dem Proxy wiederum ist die sog. „VirusWall“ (also der Virenschanner) installiert, die nun alle eingehenden Daten (Webseiten, Downloads, etc.) aus dem Web auf Virenbefall oder anderweitigen böswilligen Programmcode untersucht. Nur Unbeanstandete Daten werden von der VirusWall durchgelassen und gelangen dann im LAN in den Browser des Anwenders.

Bevor der Datenstrom aus dem Internet jedoch in die VirusWall gelangt, kommt vorher eine wesentliche Eigenschaft des Proxy-Servers zum Tragen: Alle aktiven Inhalte (Java, JavaScript und ActiveX) werden vom Proxy Server aus dem Datenstrom aus dem Internet herausgefischt und gelöscht. Erst diese bereinigten Daten gelangen danach in die VirusWall. Somit kann kein noch so ausgeklügeltes JavaScript-Programm den Virenschanner umgehen: Es wird bereits vorher gelöscht.



Auf manchen Seiten ist der Einblick in Informationen manchmal unmöglich, wenn bspw. kein JavaScript in den Browser des Anwenders gelangt. Um dieses Problem zu umgehen, kann der Administrator bestimmte Web-Seiten explizit als vertrauenswürdig und zuverlässig einstufen. Das führt dazu, dass aktive Inhalte von diesen explizit erlesenen Seiten durch den Proxy durchgelassen werden. Sie gelangen dann zum Virensch scanner und werden (sofern es keine Beanstandungen gibt) zum Browser des Anwenders durchgelassen.

Schutz vor Gefahren durch verseuchte Datenträger auf PCs:

Disketten, CDs und Wechsellplatten spielen dank der heutigen Datenaustauschvielfalt eine große Rolle. Der Schutz ist an dieser Stelle jedoch so einfach wie wirkungsvoll: Auf jedem Anwender-PC ist der PC-Scanner von TrendMicro (OfficeScan) installiert. Er scannt automatisch jede Datei auf dem PC, sobald diese geöffnet wird. Falls ein Virus o.ä. vorliegt, wird entweder das Öffnen der Datei verhindert oder die Datei desinfiziert. Die Gefahr ist damit gebannt.

Schutz vor Gefahren durch verseuchte Datenträger auf Servern:

Hier stellt sich die Situation im Prinzip ähnlich dar. Disketten, CDs und Bänder können direkt auf Servern aufgespielt werden. Da Server zudem zentrale Datenspeicher sind, ist auf jedem Server ein Virensch scanner (ServerProtect) installiert, der analog dem PC-Scanner alle Dateien vor dem Öffnen überprüft.

Daneben führen alle Server in den Nachtstunden einen vollautomatischen Virencheck aller vorhandenen Dateien durch, so dass ständige Virenüberprüfung und –sicherheit vorliegt.

All diese Schutzmaßnahmen ergeben in Summe einen vollständigen Schutzschild gegen das Eindringen von Viren, Würmern, Trojanern und anderem schädlichen Programmcode. Es gelangt nicht ein einziges Bit von Extern in das Unternehmen, ohne auf Viren oder böswilligen Code überprüft worden zu sein.

Abgerundet wird dieser Rund-Um-Schutz durch die zentrale Administrierbarkeit der Lösung. Alle beteiligten Programmkomponenten sind in einer zentralen Virenschutz-Konsole integriert. Somit laufen alle Virenalarme an einer einzigen zentralen Stelle zusammen, wo sie protokolliert werden und bspw. per E-Mail oder SMS an den EDV-Verantwortlichen weitergeleitet werden können.

Diese zentrale Verwaltung hat neben dem Komfort der Übersicht den unschlagbaren und unersetzlichen Vorteil, das alle Viren-Scannerupdates (sowohl Virenpattern- als auch Programmupdates!) für alle beteiligten Programmteile (E-Mail-, Web-, Dateivirenschutz, usw.) vollautomatisch vorgenommen werden. Die zentrale Virenschutz-Konsole holt sich in definierbaren Intervallen alle notwendigen Updates selbständig aus dem Internet und verteilt diese dann vollautomatisch an alle beteiligten Programmteile des Virenschutzsystems. Das gesamte Viren-Abwehrsystem ist jederzeit vollautomatisch auf dem aktuellsten Stand. Völlig ohne manuelles Zutun. Niemand muss sich um die Virenabwehr kümmern, das alles geschieht automatisch. Der Aufwand an Arbeitszeit für die Virenabwehr liegt bei null. Einzig die Alarm-Meldungen und die Protokolle sollten im Auge behalten werden. Damit hat man die Gewähr, dass alles auf dem aktuellsten Stand ist und nichts anbrennt.

Einfacher und sicherer kann die Abwehr von Viren, Würmern, Trojanern und anderem schädlichem Programmcode heute nicht mehr sein. Dass es ohne Rund-Um-Schutz heute nicht mehr geht, belegen die (vorgenannten bzw. nahezu täglich zu erlebenden) Tatsachen.



## Teil 3: Die Gefahrenpotenziale des eigenen EDV-Systems

Das Bedrohungspotenzial erweitert sich in allerjüngster Zeit zusehends in die Richtung, dass das eigene EDV-System zum sicherheitskritischen Faktor wird. Waren es anfangs Hacker, die auf Grund enormen Fachwissens elektronische Einbrüche verüben konnten, leiden wir seit geraumer Zeit zunehmend unter dem Einfluss von Skript-Kiddies. Heute entwickeln sich Unzulänglichkeiten der eigenen EDV-Infrastruktur zu einem sehr ernstzunehmenden Gefahrenpotenzial.

Dass die jüngsten Wurm-Attacken („Code Red“ und vor allen Dingen „Nimda“) durchschlagenden Erfolg hatten, ist einzig und allein darauf zurückzuführen, dass diese beiden Würmer Sicherheitslücken in dem Web-Server „Internet Information Server“ (kurz: IIS) von Microsoft ausgenutzt haben, die teilweise bereits seit einigen Monaten bekannt waren und längst von den Administratoren hätten geschlossen werden können. Mit anderen Worten: Schlampige Programmierung ergibt Software mit teilweise eklatanten Sicherheitslücken, die nach und nach aufgedeckt und von Hackern schamlos ausgenutzt werden. Nach und nach liefern die Hersteller solcher Software zwar Korrekturupdates aus, aber teilweise kommen mehrere Sicherheitslöcher pro Woche zum Vorschein, so dass teilweise mehrere Updates je Woche installiert werden müssten. Welcher Administrator hat aber die Zeit, derart viele Updates allein nur für Web-Server zu installieren? Abgesehen davon vergehen i.d.R. einige Tage bis mehrere Wochen, bis ein Korrekturupdate fertiggestellt ist. Was aber kann man in der Zwischenzeit tun, wenn eine Sicherheitslücke bekannt, aber eine Korrektur noch nicht verfügbar ist?

Bereits das Erscheinen von „I LOVE YOU“ hat berechtigte Fragen in bezug auf die Qualität von Microsoft-Software aufgeworfen. „Code Red“ und „Nimda“ hätte es ohne den IIS nie gegeben. Mittlerweile äußern sich selbst sehr renommierte Marktforschungsunternehmen wie die Gartner Group sehr distanziert zum IIS: Demnach sollen die IIS-Anwender ernsthafte Anstrengungen unternehmen, den IIS aufzugeben und stattdessen alternative Produkte verwenden. Das alles klingt doppelt eindringlich, wenn man im Hinterkopf hat, dass Gartner üblicherweise mit Microsoft schmeichelt. Scott Blake, ein hochrenommiertes amerikanischer IT-Sicherheitsspezialist, wird hierzu in einer deutschen Fachzeitschrift mit den Worten „Am besten hätte man den IIS von Microsoft gar nicht erst eingeführt.“ zitiert. Dies macht die Tragweite von Angriffsflächen durch schlechte Softwarequalität deutlich.

Sicherheitslücken sind auch in PC-Software zu finden. Web-Browser wie der „Internet Explorer“ von Microsoft sind in der Hacker-Szene so etwas wie ein „Quell steter Freude“. Immer wieder werden in diesen Programmen Sicherheitslücken entdeckt, die sich insbesondere unter Zuhilfenahme von aktiven Inhalten (Java, JavaScript, ActiveX) ausnutzen lassen. Allein schon aus diesem Grunde sind die beiden kritischsten Vertreter dieser Programmier Technologie (JavaScript und ActiveX) unbedingt aus dem Internet-Datenstrom beim Eintritt in das Unternehmen zu eliminieren (s.o.).

Aber auch an anderen, eher unscheinbaren Stellen treten immer wieder Sicherheitslücken auf. Ein Paradebeispiel dafür ist der sog. „Remote Access Service“, einem Dienst von Windows NT/2000, mit dem sich bspw. Aussendienstler per Modem oder ISDN in das LAN einwählen können. Diesen Service kann man bspw. auch über das Internet ausführen. Dabei kommt eine speziell verschlüsselte (sog. getunnelte) Verbindung zum Tragen, damit die Unternehmensdaten nicht von Unbefugten eingesehen werden können. Als diese Technik von Microsoft veröffentlicht wurde, dauerte es nicht einmal 2 Tage, um die Verschlüsselung zu knacken. Das Verfahren ist damit völlig wertlos.

Wir selbst setzen zur Lösung der Aussendienst-Anbindung eine internet-basierte Tunnel-Lösung von F-Secure ein. Die Aussendienst-Notebooks sind damit auch von der Baustelle aus transparent in das Netzwerk eingebunden und haben Zugriff auf alle Ressourcen, einschließlich E-Mail und Virenschutz.



Das Surfen im Internet im Aussendienst geschieht ausschließlich über die Tunnel-Verbindung zu unserem LAN und von dort aus über die Firewall ins Internet, nicht direkt vom Notebook aus. Damit ist der vollständige Schutz vor allen Internetgefahren auch mobil problemlos gewährleistet.

Fazit: Angesichts der Bedrohungslage mag sich nun mancher Leser fragen, ob es nicht einfach besser wäre, die Finger vom Internet und seinen Möglichkeiten zu lassen. Dies kann nur strikt verneint werden! Das Internet ist Motor und Drehscheibe unserer informations-gestützten Geschäftsabwicklung. In vielen Bereichen ist es nicht mehr wegzudenken, sogar nahezu unmöglich ohne auszukommen. Die Bereiche, in denen das Internet noch keine so gravierende Rolle spielt, werden in wenigen Jahren ebenfalls integriert sein.

Gegen diese stille Revolution können wir uns nicht auflehnen oder sie ablehnen. Im Gegenteil: wir sind aufgefordert, seine Möglichkeiten auszuschöpfen, bevor der Mitbewerb den Vorteil längst nutzt, während wir noch darüber nachdenken. Die Frage der Nutzung stellt sich nicht, wohl aber die Frage der Art und Weise der Nutzung.

Das Gefahrenpotenzial aus dem Internet ist wahrlich nicht klein und wächst eher ständig, anstatt zu schrumpfen. Aber die für die Herstellung von Sicherheit notwendigen Werkzeuge sind verfügbar. Es gibt also keine Ausrede mehr, auf diese neuen Techniken zu verzichten. Wir sollten sie nutzen, aber keinesfalls zum Preis mangelnder Sicherheit!

Der Autor:

Dipl.-Ingenieur Ansgar H. Licher wurde am 21.05.1965 in Georgsmarienhütte geboren. Nach einer Berufsausbildung und einem Fachabitur im Bereich Maschinenbau studierte er von 1986 bis 1989 Systemanalyse/Wirtschaftsinformatik an der Hochschule Bremerhaven, das er als Dipl.-Ingenieur abschloss. Nach seinem Studium arbeitete er bis 1993 als wissenschaftlich-technischer Mitarbeiter und Junior-Unternehmensberater für „EDV und Organisation“ zunächst im Bereich Technologietransfer an der Hochschule Bremerhaven und anschließend in einer norddeutschen Unternehmensberatung.

Seit 1993 leitet er die Abteilung Datenverarbeitung + Informationssysteme bei der MBN Bau Aktiengesellschaft in Georgsmarienhütte. Der Autor kann unter der E-Mail-Adresse a.licher@mbn.de erreicht werden.

Glossar:

- LAN (auch Local Area Network) ist das EDV-Netzwerk eines Unternehmens (Firmennetzwerk) an einem Standort.
- WAN (auch Wide Area Network) verbindet mehrere Standorte (also LANs) eines Unternehmens miteinander.
- Viren sind Programme, die sich auf einem PC einnisten und dort Schaden anrichten.
- Makroviren sind spezielle Virenarten. Diese wirken nur innerhalb bestimmter Programme, die Makros (Befehlsfolgen) verarbeiten können, also bspw. Microsoft Word, Excel, PowerPoint etc.
- Würmer sind im Prinzip Viren, breiten sich jedoch völlig selbständig in Datennetzen (z.B. LAN, Internet) per E-Mail oder über andere Wege weiter aus.
- Trojanische Pferde leiten sich aus dem alten Troja ab: Das geschenkt bekommene Pferd entpupperte sich später als böse Überraschung; im übertragenen Sinn bedeutet das heute: ein als nützlich



betrachtetes Programm (bspw. aus dem Internet) entpuppt sich im Nachhinein als böse Überraschung, da es z.B. Passwörter oder Kontonummern sammelt und diese (z.B. per E-Mail) an einen Hacker schickt etc.

- Backdoor-Programme gehören im Grunde zur Klasse der Trojanischen Pferde bzw. Trojaner, sammeln jedoch keine Informationen sondern dienen als Hintertür. Ein Hacker kann sich so perfider Weise unbemerkt und hinterrücks uneingeschränkten Zugang zu PCs usw. verschaffen.
- JavaScript ist eine Skriptsprache, mit der man kleine, begrenzte Programme schreiben kann. Leider ist JavaScript der Grund für vielerlei Sicherheitsprobleme in Zusammenhang mit Web-Seiten und E-Mails.
- VisualBasic-Script (VB-Script, VBS) ist ebenfalls eine Programmiersprache unter Windows mit Zugriff auf alle Systemressourcen des PCs, weshalb sie auch bevorzugt als Programmiersprache für Viren und Würmer verwendet wird.
- ActiveX ist eine Komponententechnologie von Microsoft, die es ermöglicht, Aktionen auf mehrere PCs zu verteilen, die miteinander in Verbindung stehen. Da ActiveX ursprünglich für LAN-basierte Anwendungen geschrieben wurde, gibt es keine wirklichen Sicherheitsfeatures. Ebenso fehlen Beschränkungen bzgl. des Zugriffs auf fremde PCs. Daher ist diese Technologie (im Internet eingesetzt) aus Sicherheitssicht katastrophal.