


# Internet-Sicherheit

Internet-Sicherheit muss kein "Räuber und Gendarm"-Spiel zwischen Hackern und Sicherheitsexperten bleiben. Es gibt auch für den findigsten Hacker nur wenige Kanäle, über die er angreifen kann, und diese Kanäle lassen sich vollständig schließen. Ein so gesichertes System erlaubt eine risikolose Internetnutzung und ist auch ohne ständige Anpassungen zuverlässig gefeit vor dem nächsten "Sicherheitsskandal".

Für einen normalen Internetnutzer gibt es 3 Angriffskanäle, die "gestopft" werden müssen: die Transportschicht (= die Funktionen unterhalb der Applikationen wie Browser oder E-Mail), das Surfen und der E-Mail-Bereich.

Die **Transportschicht** lässt sich durch Firewalls einfach absichern. Auch das **Surfen** kann abgesichert werden, indem z. B. Surf-PCs genutzt werden, die physisch vom Firmennetz getrennt sind, oder beim Surfen aus dem Firmennetz heraus alle aktiven Inhalte z. B. über die Firewall herausgeschnitten werden. So wird verhindert, dass Angreifer Browserfehler benutzen können, um einen Zugriff auf das Firmennetz zu erhalten. Diese beiden Kanäle können also mit Standardmitteln erfolgreich "gestopft" werden. (Mehr hierzu im Artikel "Tipps zur Internet-Sicherheit" unter "http://www.redtenbacher.de/support/security.htm".)

Beim **E-Mail-Verkehr** ermöglichen die derzeit üblichen Standardmittel jedoch **keine wirkliche Sicherheit**. Dort findet täglich ein Wettlauf zwischen neu aufgetretenen Viren und der rechtzeitigen Bereitstellung eines Schutzes in Form eines aktualisierten Virenscanners statt. Dabei vergehen manchmal Tage, bis ein Virus als solcher erkannt und gemeldet wird, und anschließend weitere Zeit, bis Abhilfen zur Verfügung stehen. Spionagesoftware, die sonst keinen Schaden anrichtet, bleibt oft sogar lange Zeit unentdeckt. Diese Zeitverzögerung wird bei der heutigen Bedeutung von E-Mail zu einem wachsenden Risiko, denn bis zur jeweiligen Abhilfe bleibt ein Netzwerk, das seine Sicherheit auf Virenscanner abstützt, einem neuen Angriff gegenüber völlig ungeschützt, während sich neue Viren oft binnen wenigen Stunden bereits weltweit verbreiten.

Wenn Sie hingegen von vorneherein die Kanäle abdichten, über die E-Mail-Viren eindringen können, erreichen Sie auch im E-Mail-Bereich eine 100%ige Sicherheit.

**Wie funktioniert ein Angriff über E-Mails?**

E-Mails können in Dateianlagen beliebige Inhalte transportieren, darunter natürlich auch Viren. Diese Programme "schlagen zu", wenn die Dateianlage z. B. durch einen Doppelklick geöffnet (und dadurch gestartet) wird.

Wie der Virus ILOVEYOU (alias VBS/Love Letter) gezeigt hat, hilft es wenig, den Anwendern einzuschärfen, unbekannte E-Mail-Anlagen nicht durch einen Doppelklick zu aktivieren: Der ILOVEYOU-Virus wurde auch durch Mailserver diverser Landesregierungen in angeblich völlig sichere Verwaltungsnetze verbreitet, und fast überall fand sich zumindest eine Person, die trotz aller oft gehörten Warnungen auf den merkwürdigen "Liebesbrief der übergeordneten Behörde" doppelklickte und den Virus damit aktivierte (und weiter verbreitete).

Hinzu kommt der Umstand, dass sich für einen Nichtfachmann unter Windows kaum erkennen lässt, ob eine Dateianlage potentiell gefährlich oder harmlos ist, da Windows bestimmte Dateierweiterungen *stets* verbirgt. Eine Dateianlage mit der angezeigten Erweiterung ".JPG" muss unter Windows noch lange keine harmlose JPG-Grafik sein, sondern kann ein Programm und somit einen Virus enthalten - wie dies beispielsweise beim Virus "BillGates.JPG.pif" der Fall war, dessen Erweiterung ".pif" nicht angezeigt wurde. Dies liegt daran, dass unter Windows über 20 Dateierweiterungen stets unsichtbar bleiben - auch dann, wenn die Explorer-Option "Dateinamenerweiterung bei bekannten Dateitypen ausblenden" explizit **aus**geschaltet wurde.

Bei den aktuellen Versionen der MS-Mailprogramme *Outlook* und *Outlook Express* kommt noch hinzu, dass diese Programme bestimmte Instruktionen in E-Mails automatisch ausführen, ohne dass dazu die E-Mail überhaupt geöffnet werden muss. Die früher gültige Regel "E-Mails können erst durch Doppelklick auf eine Dateianlage gefährlich werden" gilt daher für *Outlook* und *Outlook Express* nicht mehr. Bei einem Virus, der Techniken wie "BubbleBoy" einsetzt, reicht es schon aus, dass er mit *Outlook Express* **empfangen** wird, und er schlägt danach ohne jeden Mausclick des Empfängers zu.

Virenscanner bieten hier nur einen begrenzten Schutz, da sie - auch wenn sie stets aktuell gehalten werden - neue Viren erst verspätet erkennen. Während der ganzen Zeit vom Freisetzen eines neuen Virus im Internet bis zur Entdeckung als Virus, zur Berücksichtigung durch die Hersteller der Virenscanner und zur Installation eines entsprechenden Updates beim Anwender bleibt das Firmennetz ungeschützt. Diese Zeitspanne (in der Regel mehrere Tage) reicht aus, dass ein Großteil aller Firmennetze binnen weniger Stunden weltweit lahmgelegt werden kann - eine Gefahr, vor der unabhängige Experten und auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnen und das Ergreifen geeigneter Maßnahmen fordern.

**Welche Maßnahmen sind für eine lückenlose Sicherheit nötig?**

Eine lückenlose Sicherheit für E-Mails kann nur erreicht werden, wenn nicht einzelne Viren bekämpft, sondern gleich die technischen **Kanäle**, über die Viren hereinkommen können, abgedichtet werden. Da die bestehenden E-Mail-Programme dies nicht tun, lässt man eingehende E-Mails am besten durch ein vorgeschaltetes System analysieren und bei Bedarf aussortieren bzw. bereinigen, bevor sie an die E-Mail-Clients der Anwender geleitet werden.

**Wie sieht das in der Praxis aus?**

Eine Möglichkeit, das obige Sicherheitskonzept kostengünstig und in der Regel ohne wahrnehmbare Einschränkungen zu realisieren, ist das KT-Mail/Filter-Gateway. (Eine Einschränkung ist dort beispielsweise nur gegeben, wenn ein Anwender sich tatsächlich eine PIF- oder EXE-Datei oder ein Worddokument, das Makros benötigt, zuschicken lässt. In diesem Fall müsste er sich diese Datei vom Mail-Administrator abholen - siehe unten.)

Technisch führt das KT-Mail/Filter-Gateway im Hintergrund folgende Prüfungen an E-Mails durch, bevor diese an das E-Mail-System und damit in die Postfächer der Anwender verteilt werden:

- Es prüft alle Bestandteile jeder E-Mail und lässt unbedenkliche Formate wie ASCII-Texte (außer BAT-, CMD-, VBS-, PIF-Dateien usw.), echte Grafiken (GIF, JPG, BMP, PCX usw.) sowie andere häufige Binärformate, die als harmlos verifiziert werden können, unverändert durch.
- Entdeckt es in einer E-Mail ein Dateiformat, das potentiell Viren enthalten kann, so versucht es, diese Komponente von dem Programm-/Makrocode zu säubern. Bei DOC-Dateien geschieht dies z. B. durch Entfernen von Makros, dynamischen OLE-Inhalten und sog. "remote Template-Links", bei HTML-Dateien durch das Entfernen "aktiver Inhalte" (Java,

Java-Script, Active-X usw.). Anschließend leitet es die bereinigte E-Mail an den Anwender weiter. Das Original bleibt noch eine Zeitlang in einem speziellen Verzeichnis gespeichert, um bei Bedarf zur Verfügung zu stehen.

- Potentiell gefährliche E-Mail-Bestandteile, die nicht zuverlässig gesäubert werden können, wie z. B. EXE- oder PIF-Dateien, werden aus der E-Mail herausgeschnitten und zur Prüfung an den Mail-Administrator geleitet. Statt der Dateianlage erhält der Empfänger nur eine Meldung, welche Anlage hier ursprünglich enthalten war und wo er die geprüfte Datei bei Bedarf abholen kann. Der Mail-Administrator braucht bei dieser Lösung nur auf Anfragen zu reagieren und kann die restlichen (i. d. R. unaufgefordert zugeschickten) E-Mail-Anlagen nach einer Frist von ca. 1-2 Wochen ungeprüft löschen.

Durch diese Maßnahmen werden alle Gefahren ausgeschlossen, die durch Unkenntnis der Empfänger (Doppelklick auf gefährliche Dateianlagen) oder durch Sicherheitsmängel in E-Mail-Programmen (automatisches Reagieren auf "aktive Inhalte") entstehen können. Die obige Vorgehensweise hätte jeden einzelnen aller Virenvorfälle vermieden, die je in der Presse Schlagzeilen gemacht haben.

**Was sind die Voraussetzungen für das KT-Mail/Filter-Gateway?**

Das KT-Mail/Filter-Gateway kann einem bestehenden E-Mail-System hinzugefügt werden, das gegenüber dem Internet das SMTP-Protokoll verwendet. Diese Voraussetzung sollte bei jedem E-Mail-System mit eigenem Mailserver erfüllt sein. Konkrete Installationen existieren derzeit für MS-Exchange-Server, Lotus Notes, Novell Groupwise, David/Tobit u. a.

An Betriebssystemen werden Windows (9x/ME/NT/2000/XP) und Linux unterstützt. (Die automatische Konversion von DOC-Dateien ins RTF-Format erfordert derzeit noch ein Windows-System. Alle anderen Funktionen sind auch für Linux verfügbar.)

An den Arbeitsplatz-PCs oder der dort installierten Software erfordert das KT-Mail/Filter-Gateway keinerlei Änderungen. Es arbeitet ausschließlich zwischen dem Mailserver und der Firewall (bzw. dem Internet-Service-Provider) und bleibt für jegliche Software im PC-Netz praktisch unsichtbar.

**Was kostet das KT-Mail/Filter-Gateway?**

Das KT-Mail/Filter-Gateway besteht aus einem SMTP-Basis-Gateway, dem Filter-Gateway-Konversionsmodul und dem Filter-Gateway-Routingmodul. Jedes dieser Module kostet je 495 EUR, so dass sich für die obige Lösung ein Gesamtpreis von 1485 Euro zzgl. MWSt ergibt.

Für die Installation empfehlen wir einen eigenen Pentium-PC. Bei kleinerem Mail-Aufkommen kann die Installation auch als Zusatz auf dem bestehenden Mailserver erfolgen.

Die durchschnittliche Installations- und Einweisungszeit für ein Filter-Gateway durch uns bzw. unsere Systempartner beträgt ca. 3-4 Stunden vor Ort.

Laufende Wartungskosten für das Gateway fallen keine an. Erweiterungen im Gateway-Bereich werden von uns preisgünstig angeboten und sind nur erforderlich, wenn z. B. durch neue Techniken/Formate neue Kanäle geschaffen werden, über die Viren in Systeme eindringen können. In Anspruch genommene Leistungen unseres technischen Supports berechnen wir mit 1,50 EUR/Minute (= 90 Euro/Std) + MWSt.