Sonderdruck aus
InformationWeek

SICHERHEITSSCHLEUSE MIT MEHREREN STUFEN

VON THOMAS NEUMANN | juergen.hoefling@informationweek.de

Paketfilter reichen als Sicherheitsschleuse schon lange nicht mehr aus. Beispiel »Aktive Inhalte«: Um diese sicher beherrschen zu können, empfiehlt das BSI eine dreistufige Firewall-Konstruktion.

Das Emissionshaus Dr. Peters in Dortmund betreut das Vermögen von über 34 500 Anlegern, insgesamt 1,75 Milliarden Euro bei einem Investitionsvolumen von rund 3,6 Milliarden Euro. Investiert wird das Geld fast ausschließlich in Schiffe. Heute fahren 32 Tanker und 33 große Handelsschiffe für die Fondsgesellschaft über die Weltmeere – damit unterhält das Unternehmen aus Westfalen die größte deutsche Schiffsflotte.

Neben den Einlagen ist das Vertrauen der Kunden das größte Kapital der Fonds-Gesellschaft. »Die Anleger müssen sich absolut darauf verlassen können, dass ihre Ersparnisse seriös investiert und verwaltet werden. Wir arbeiten mit einer Menge äußerst sensibler Daten, die vor Manipulation, Verlust und unberechtigten Zugriffen unbedingt geschützt werden müssen. Deshalb hat IT-Sicherheit für unser Geschäft höchste Priorität«, sagt Jürgen Salamon, geschäftsführender Gesellschafter bei Dr. Peters.

GEFÄHRDUNGSPOTENZIAL DURCH »AKTIVE INHALTE«

Regelmäßige Überprüfungen der IT-Sicherheit sind deshalb bei der Dr. Peters Gruppe selbstverständlich: Im Zuge einer Risiko-Analyse Anfang 2004 durch das auf Netzwerk- und Internet-Lösungen spezialisierte Unternehmen Dr. Bülow & Masiak GmbH ergab sich die Notwendigkeit, die Firewall-Lösung zu erweitern. Der Grund: eine Gefährdung durch aktive Inhalte, also Webseiten, die lokal auszuführende Programmteile enthalten, war nicht auszuschließen. Der Datenaustausch zwischen Unternehmensnetz (LAN) und Internet ist zwar bei Dr. Peters sehr restriktiv organisiert – lediglich E-Mail-Verkehr und eine WWW-Anbindung für die Mitarbeiter sowie eine FTP-Verbindung zum externen Webserver sind erlaubt –, die existierende Firewall-Lösung gab indes nicht die Gewähr, dass aktive Inhalte zuverlässig erkannt werden können. Der Übergang vom LAN zum Internet wurde nämlich allein durch einen Paketfilter gesichert. Dieser Firewall-Typ ist auf dem Auge »aktive Inhalte« blind. Paketfilter sind technisch gesehen Netzwerk-Router mit erweiterten Regelsätzen. Eingehende Datenpakete können ausschließlich anhand der Informationen im IP-Header geprüft werden. Geprüft werden also Absender- und Empfänger-Adresse, der verwendete Protokolltyp und die angesteuerte Port-Nummer. Welche IP-Pakete durchgelassen werden, definiert der Firewall-Administrator in den Filterregeln. Paketfilter ermöglichen somit lediglich eine formale Kontrolle des Datenverkehrs, sie können jedoch nicht in die Datenströme hineinschauen, um aktive Inhalte zu erkennen.

Bei der Firewall-Box GeNUGate sind das Application Level Gateway und der Paketfilter in einem Gehäuse untergebracht, laufen jedoch auf getrennten Rechnern.

Foto: Dr. Peters Gruppe

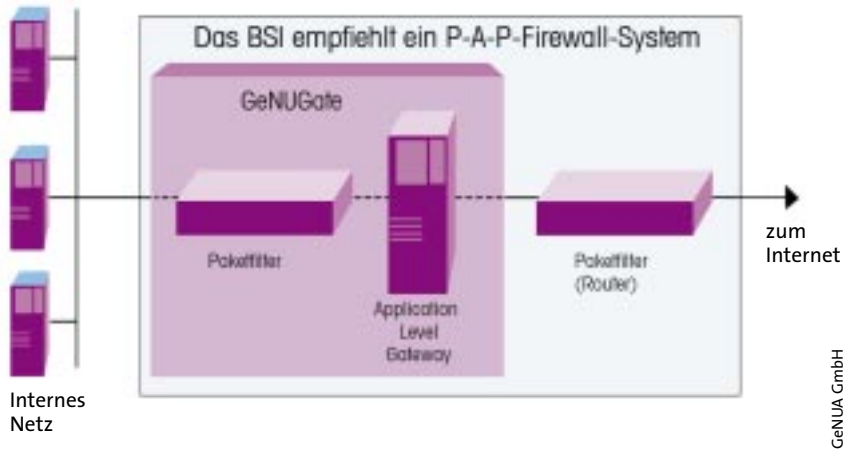
Das Emissionshaus Dr. Peters in Dortmund investiert das Geld seiner Anleger fast ausschließlich in Schiffe.

APPLICATION LEVEL GATEWAY PRÜFT DATENINHALT

»Bei hohen Anforderungen an die IT-Sicherheit stoßen Paketfilter an ihre

Grenzen. Hier sollte zusätzlich eine hochwertige Firewall vom Typ ´Application Level Gateway' eingesetzt werden, das die Daten aus dem Internet sorgfältig durchleuchtet«, erläutert Gerhard Bülow, Geschäftsführer der Dr. Bülow & Masiak GmbH. Ein Application Level Gateway überprüft den Inhalt eines Datenstroms. Dazu werden die ankommenden Pakete zunächst gestoppt, das Application Level Gateway lässt also niemals eine durchgehende Verbindung zwischen Internet und LAN zu. Dann werden die einzelnen IP-Pakete wie bei einem Puzzle zusammengefügt, da nur anhand kompletter Datensätze eine inhaltliche Prüfung möglich ist. Jetzt analysiert das System den Content. Die aktiven Inhalte Java, JavaScript, VB-Script und ActiveX werden identifiziert und gemäß der individuellen Konfiguration gefiltert. So können beispielsweise automatisch aufgehende Fenster zugelassen werden, während das Nachladen von Daten untersagt ist. Darüber hinaus können die Daten nach MIME-Types, Extensions und URLs gefiltert sowie Cookies entfernt werden. So können bereits an der Firewall schädliche Daten wie aktiver Content, Viren und auch Spam blockiert werden. Erst nach dieser sorgfältigen Kontrolle auf der inhaltlichen Ebene leitet das Application Level Gateway die Daten über eine neue Verbindung weiter ins LAN.

Doppeldeckung



Quelle: GeNUA GmbH

Für die Nahtstelle LAN-Internet empfiehlt das BSI die Kombination von zwei Paketfiltern mit einem Application Level Gateway als Kernstück.

Auch das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt, an der kritischen Nahtstelle LAN-Internet nicht auf eine einzelne Firewall zu vertrauen. Vielmehr sollten zwei Paketfilter und ein Application Level Gateway miteinander kombiniert werden, wobei die hochwertige Firewall als Kernstück in der Mitte platziert wird (PAP-Konstruktion). So ist das Application Level Gateway gegen direkte Angriffe auf beiden Seiten geschützt und auch beim Ausfall eines Firewall-Systems weiterhin ein hohes Sicherheitsniveau garantiert.

ZWEI FIREWALL-SYSTEME IN EINER KISTE

Bei der Dr. Peters Gruppe wurde die vom BSI befürwortete PAP-Konstruktion durch die Kopplung des existierenden Paketsfilters mit einer Firewall-Box der Firma GeNUA in Kirchheim bei München umgesetzt. Bei der Firewall-Box »GeNUGate« befinden sich das Application Level Gateway und der Paketfilter in einem einzigen Gehäuse, laufen jedoch auf getrennten Rechnern. »Die Kontrollmechanismen der beiden in der Box integrierten Firewalls sind exakt aufeinander abgestimmt und ergänzen sich auf unterschiedlichen Ebenen zu einem effizienten Schutzschild«, erklärt Gerhard Bülow. Administriert wird das Gesamtsystem über eine einheitliche Oberfläche im Browser, wobei die Verbindung mit SSL verschlüsselt wird.

Damit hat das Dortmunder Emissionshaus nun ein Firewall-System, das »die für das EDV-System benötigten extrem hohen Sicherheitsmaßnahmen durch die installierten Sicherheitslevels der Firewall gewährleistet«, so das Fazit von Prof. Dr. Rolf Lauser, Experte für Wirtschaftsinformatik/Datenschutz und Datensicherheit an der FH München, nach einer Begutachtung des Systems. ■

TECHNISCHE GRUNDLAGEN

Zentrale Behandlung von Aktiven Inhalten

Aktive Inhalte reisen per Huckepack mit E-Mail- oder www-Daten und können beliebige Aktionen auf dem Ziel-Rechner ausführen, beispielsweise eine animierte Webseite aufbauen oder die Festplatte löschen. Die Anzahl von Anwendungen mit aktiven Inhalten im Datenverkehr, seien sie nun harmlos oder schädlich, nimmt ständig zu. In Browsern und E-Mail-Programmen kann dieser Content zwar mit wenigen Mausklicks »ausgeschaltet« werden. Diese Unterdrückung auf jedem einzelnen Client ist jedoch genauso undifferenziert wie unsicher. Zum einen werden dadurch auch viele erwünschte und unschädliche Inhalte blockiert, weil keine Filterung vorgenommen wird, zum anderen ist das Zonenmodell von Microsoft zur Absicherung der Clients unzureichend und kann mit Tricks umgangen werden. So gelten beispielsweise alle Applikationen, die bereits auf dem Client vorhanden sind, pauschal als sicher. Wenn aber das Ablage-System eines bestimmten Clients bekannt ist, können diesem Applikationen per E-Mail untergeschoben und dann in der vermeintlich sicheren Zone auch ausgeführt werden. Darüber hinaus kann der sicherheitsbewusste Umgang mit aktiven Inhalten in einem Unternehmen nicht über einzelne Einstellungen an allen Clients, sondern nur durch eine zentrale Administration gewährleistet werden. Diese einheitliche Steuerung sollte dort erfolgen, wo die Daten aus dem Internet angenommen werden, nämlich an der Firewall.