Datenschutzkonforme Netzwerksicherheit

Firewalls durchschauen!

Werden personenbezogene Daten auf vernetzten Rechnern verarbeitet, so muss das Netz über eine Firewall geschützt werden. Der Datenschutzbeauftragte muss dann auch die Firewall als Bestandteil des Sicherheitskonzepts nach der Anlage zu § 9 BDSG prüfen. Beim Einsatz von Firewalls gibt es viele Lösungsmöglichkeiten, die sicher und sinnvoll sein können. Je direkter man sich an Standardkonzepten orientiert, desto leichter fällt die sicherheitstechnische Überprüfung.

Um Firewalls von der Funktion und den Abläufen her zu verstehen, muss ein Datenschutzbeauftragter über Basiswissen zum Thema TCP/IP-Protokolle verfügen. Begriffe wie IP-Adressen, Port-Nummern und IP-Protokolle (z.B. TCP, UDP, ICMP, IPsec) sollten bekannt sein, da sie bei der Regelerstellung für eine Firewall unverzichtbar sind.

Kenntnis der Netzwerkstrukturen und -dienste notwendig

Die erste Grundlage für eine Firewall-Prüfung ist eine genaue Kenntnis der Netzwerkstrukturen und -dienste, also welche Adressen sind für welche Rechner in Benutzung, und welche Dienste werden von welchem Rechner angeboten bzw. benötigt. Hieraus kann abgeleitet werden, welche Dienste dann in der Firewall freigeschaltet werden müssen. Außerdem ergibt sich aus diesem Konzept die Topologie, die auch relevant für die Konfiguration der Firewall ist. Gibt es eine Neutrale Zone (DMZ) oder nur ein internes Netz mit einigen von außen erreichbaren Rechnern (sog. exposed Hosts)? In Abbildung 1 sehen wir einige typische Firewall-Topologien. Eine einfache Firewall, die internes und externes Netz trennt (a), ist nur sinnvoll, wenn man keinen öffentlichen Server im internen Netz betreibt. Öffentliche Server stehen typisch in der DMZ. Eine DMZ kann zwischen zwei Firewall-Systemen (b) oder an einem dritten Netzwerkinterface des Firewall-Systems (c) realisiert werden.

In der Abbildung sind die Netze vereinfacht als Wolken dargestellt. Reale Netzwerkpläne zeigen die detaillierte Netzwerkstruktur mit allen aktiven Komponenten und Rechnern sowie den verwendeten Netzwerkadressen.

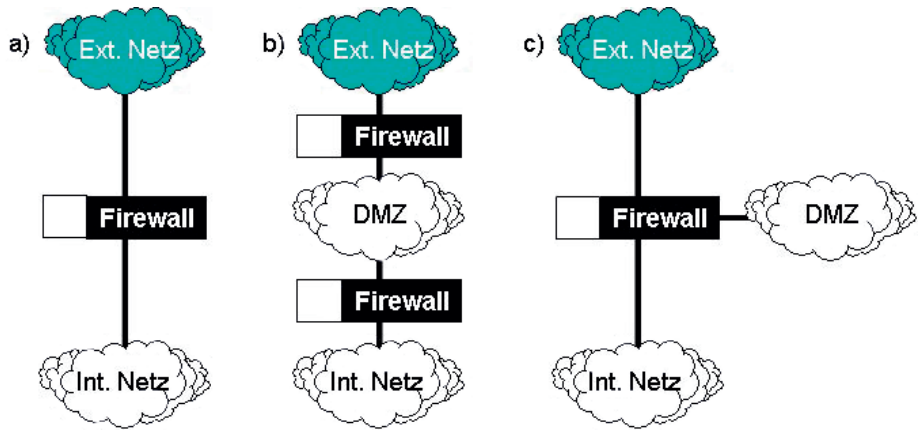

Abbildung 1: Drei typische Beispiele für Netztopologien mit Firewall-Systemen.

Die drei Firewalltypen

Da Firewalls keine „physischen" Produkte sind, gibt es in der Praxis viele mögliche Realisierungen. Drei grundlegende Klassifizierungen bringen etwas Ordnung in den Dschungel:

- Paketfilter
- Stateful Inspection Firewall
- Anwendungsfilter (Application Level Gateways)

Typ 1: Paketfilter

Ein Paketfilter kontrolliert den Datenstrom auf Basis von Quell- und Ziel-IP-Adresse sowie Quell- und Ziel-Portnummer. Da ein einfacher Paketfilter ein- und ausgehende Datenpakete nicht korrelieren kann, muss er relativ offen konfiguriert werden. So gibt es immer zwei Regeln, eine für die Anfrage (z.B. ausgehende Verbindung) und eine für die Antwort (entsprechende eingehende Verbindung). Für einen Zugriff auf beliebige externe Webserver erlaubt die eine Regel alle Zugriffe von einem Port größer 1023 aus dem internen Netz auf Port 80 auf externe Server, und die zugehörige zweite Regel erlaubt eingehend jede Verbindung von Port 80 auf einen Port größer als 1023.

Typ 2: Stateful Inspection Firewall

Eine Stateful Inspection Firewall speichert den Zustand einer Verbindung und benötigt deshalb jeweils nur eine Regel für das erste Datenpaket einer Verbindung sowie eine globale Regel, die alle Pakete einer bereits bestehenden Verbindung (established oder related) durchlässt. Damit sieht das Regelwerk übersichtlicher aus.

Einige weit verbreitete Firewalls (z.B. Access-Listen in Cisco-Routern und IP-Tables unter Linux) werden über relativ kryptische Konfigurationsdateien verwaltet. Während die Konzeption die gleiche ist, ist die Syntax gewöhnungsbedürftig. Abbildung 2 zeigt einen Ausschnitt aus einer Datei zur Konfiguration der Access-Listen eines Cisco-Routers. Nach dem Verb „permit" ist angegeben: Protokoll (hier

tcp bzw. udp), Quell-IP-Adresse (hier any), Ziel-IP-Adresse (hier any bzw. host mit IP-Adresse) und dann in der ersten Regel das Schlüsselwort „established“, danach „eq“ mit der entsprechenden Port-Nummer.

Typ 3: Anwendungsfilter

Weder ein Paketfilter noch eine Statefull Inspection Firewall kann feststellen, ob auch die „richtige“ Anwendung einen Port benutzt. So kann auf dem erlaubten Port 80 nicht nur das vorgesehene http-Protokoll, sondern z.B. auch die Chat-Anwendung ICQ Datenverbindungen aufbauen. Insbesondere ICQ kann jeden (!) Port benutzen. Ein Anwendungsfilter kann hier helfen, da dieser Firewalltyp prüft, ob die Daten auch zum erwarteten Protokoll passen.

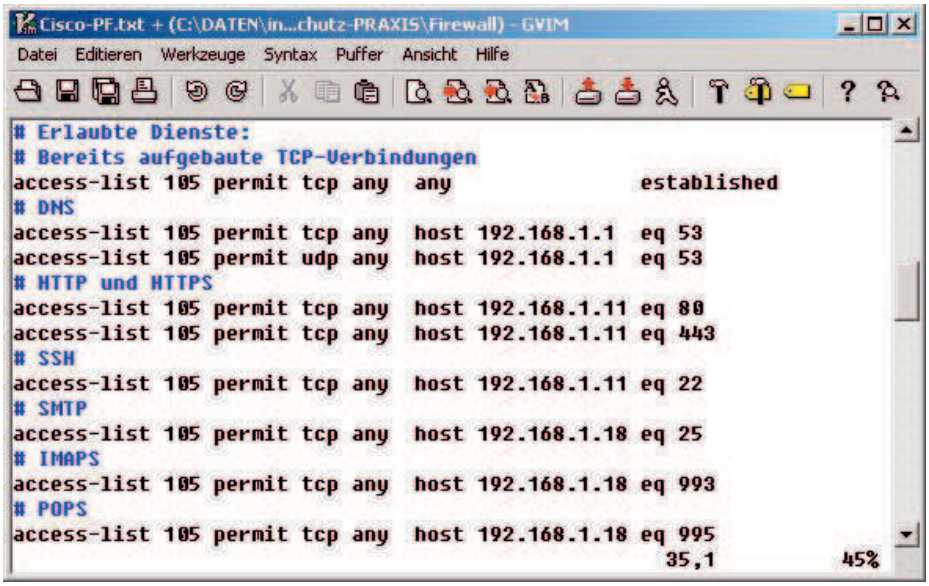

Abbildung 2: Das bekommen Sie von einer Firewall normalerweise zu sehen - protokollierte Einträge und Daten.

Protokolle und Aufbewahrungsfristen

Eine Firewall wird immer auch protokollieren, denn nur so lassen sich eventuelle Angriffsversuche oder Missbrauch nachweisen. Umfang und Aufbewahrungsdauer der Protokolle gehören auch zum Prüfprogramm eines Datenschutzbeauftragten. Da eine Firewall eine Telekommunikationsanlage (§ 3 Nr. 17 TKG) ist, muss die Verarbeitung und Nutzung der Protokolle im Rahmen der Erlaubnisnormen der §§ 85 und 89 TKG erfolgen.

Der DSB sollte sich alle Logs und Auswertungen beispielhaft anschauen, um die Rechtmäßigkeit beurteilen zu können. Insbesondere sollte er nach den ältesten Log-Dateien bzw. Log-Einträgen schauen: Daraus ergibt sich die Aufbewahrungsfrist.

Maximale Aufbewahrungsfristen sind häufig in Betriebs- oder Dienstvereinbarungen geregelt. Auch die Einhaltung dieser betrieblichen bzw. behördlichen Rechtsgrundlagen muss der DSB prüfen. Hierzu gehört an erster Stelle eine Überprüfung der personenbeziehbaren Auswertungen. Die Zuordnung der Log-Einträge zu den Beschäftigten erfolgt meist über die IP-Adresse des Arbeitsplatzrechners.

Sicherheit der Netzwerkverbindungen

Network Address Translation (NAT) ist ein im Zusammenhang mit Firewalls häufig eingesetztes Feature. Es sorgt dafür, dass die Rechner in der Firma beim Zugriff auf das Internet nur mit einer IP-Adresse oder mit wenigen IP-Adressen in Erscheinung treten. Dazu legt die NAT-Firewall bei jedem erlaubten Verbindungsaufbau von innen nach außen einen Tabelleneintrag an, aufgrund dessen die Antwort zugestellt werden kann. Verbindungsaufbauten von außen nach innen sind ohne besondere Konfiguration nicht möglich, da dafür die entsprechenden Tabelleneinträge fehlen.

Ein besonderes Augenmerk ist auf die impliziten Regeln – auch Policy genannt – zu richten. Diese impliziten Regeln kümmern sich z.B. um DNS-Anfragen, ICMP-Pakete oder RIP-(Routing Information Protocol-)Pakete. Werksseitige Voreinstellungen sind meist recht offen, um die Inbetriebnahme der Firewall zu erleichtern. Die Gefahr ist, dass man diese Pakete für gesperrt hält, sie aber aufgrund impliziter Regeln durchgelassen werden.

Vollständige Dokumentation nötig

Für jede Regel in der Firewall muss es eine Dokumentation geben, die besagt, warum und von wem diese Regel eingerichtet wurde. Wichtiger Bestandteil der Prüfung ist der Abgleich der in der Firewall existierenden Regeln mit der Dokumentation. Da eine Firewall ein wichtiger Bestandteil der Sicherheitsinfrastruktur eines Unternehmens ist, muss die Dokumentation vollständig sein.

Leider sind viele Firewalls in der Administration noch nicht so auf Revisionsfestigkeit angelegt, dass das Anlegen von Regeln protokolliert wird und ausgewertet werden kann.

Nicht akzeptabel ist die Aussage mancher Firewall-Administratoren, dass die Firewall sich selbst dokumentiert, da man ja jederzeit das Regelwerk ausdrucken könne. Bei diesem Verfahren kann dann nicht mehr nachvollzogen werden, welche Fachabteilung für welche Anwendung eine Regel einrichten ließ und wer sie genehmigt hat.

Autor: Rainer W. Gerling

Zum Autor: Rainer W. Gerling ist Datenschutzbeauftragter der Max-Planck-Gesellschaft und Honorarprofessor für IT-Sicherheit an der FH München.