Grundprinzipien der Netzwerksicherheit - Teil 1: Eine Einführung

Sicherheitsvorfälle nehmen jedes Jahr mit alarmierender Geschwindigkeit zu. Je komplexer die Bedrohungen, desto komplexer werden auch die Sicherheitsmaßnahmen zum Schutz von Netzwerken. Die Mitarbeiter in Datencentern, Netzwerkadministratoren und andere Datencenterfachleute müssen die Grundlagen von Sicherheitsmaßnahmen kennen, um Netzwerke heute sicher einrichten und verwalten zu können. In dieser Fachartikelreihe werden die Grundlagen sicherer Netzwerksysteme sowie Firewalls, Netzwerktopologie und sichere Protokolle behandelt. Darüber hinaus werden empfohlene Vorgehensweisen erläutert, die den Lesern eine Einführung in die schwierigeren Aspekte der Sicherung von Netzwerken geben.

Einführung

Die Sicherung moderner Unternehmensnetze und IT-Infrastrukturen verlangt allumfassende Maßnahmen und eine sichere Kenntnis von Sicherheitslücken und entsprechenden Schutzmaßnahmen. Mit diesen Kenntnissen lassen sich zwar nicht alle Versuche vereiteln, in Netzwerke einzudringen und Systeme anzugreifen. Netzwerktechniker sind damit jedoch in der Lage, allgemeine Probleme zu beseitigen, potenzielle Beschädigungen deutlich zu reduzieren und Sicherheitslücken schnell zu entdecken. Angesichts der stetig zunehmenden Anzahl und Komplexität der Angriffe dürfen Sicherheitsfragen sowohl in großen als auch in kleinen Unternehmen keinesfalls vernachlässigt werden. Abbildung 1 zeigt den steilen jährlichen Anstieg von Sicherheitsereignissen, die dem CERT® Coordination Center (einem Zentrum für Internetsicherheit) gemeldet werden.

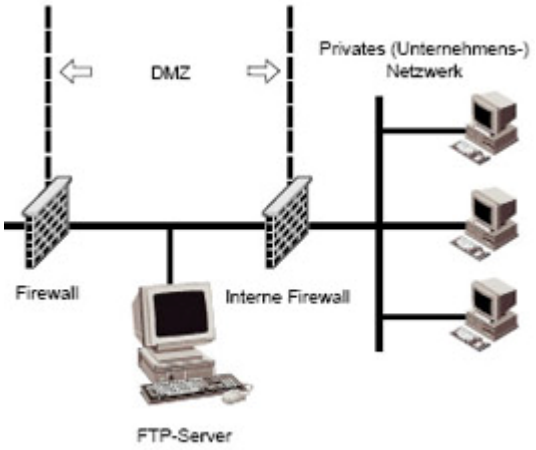
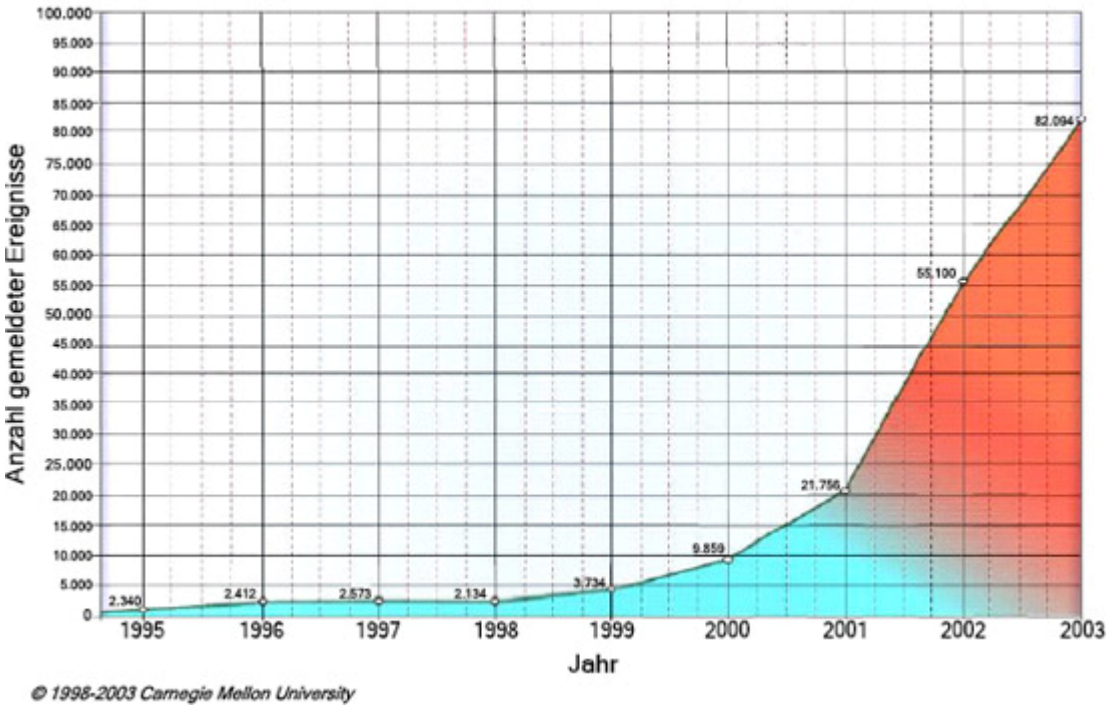


***Abbildung 1** – Sicherheitsereignisse nach Jahr – CERT.ORG*



© 1998-2003 Carnegie Mellon University

In diesem Fachartikel werden Sicherheitsgrundlagen sowie einige empfohlene Vorgehensweisen für das Netzwerk, die Computerhosts und Elemente der Netzwerkinfrastruktur dargestellt. Da es für die Sicherheit kein „Allheilmittel“ gibt, muss der Leser / Umsetzer geeignete Maßnahmen selbst auswählen und abwägen.

Quelle: www.voltimum.de

Das menschliche Problem
Der menschliche Faktor ist in jedem Sicherheitsschema sicherlich das schwächste Glied. Die meisten Benutzer gehen mit Informationen wie Kennwörtern und Zugriffscodes, auf denen die meisten sicheren Systeme beruhen, sehr sorglos um. In allen Sicherheitssystemen gibt es eine Reihe von Maßnahmen zur Steuerung des Zugriffs, zur Überprüfung der Identität und zur Verhinderung der Offenlegung sensibler Informationen. Zu diesen Maßnahmen gehören in der Regel verschiedene „Geheimnisse“. Wenn ein Geheimnis aufgedeckt oder gestohlen wird, können die damit geschützten Systeme gefährdet werden. Der Hinweis mag banal erscheinen, aber die meisten Systeme werden durch sehr einfache Dinge gefährdet. Es mag dumm sein, einen Zettel mit dem Systemkennwort am Bildschirm anzubringen, viele Benutzer tun dies jedoch. Kaum weniger gedankenlos ist die Tendenz, werkseitig vorgegebene Kennwörter für bestimmte Netzwerkgeräte nicht zu ändern. Ein solches Gerät könnte z. B. eine Netzwerkverwaltungsschnittstelle für eine USV sein. USV-Systeme gleichgültig welcher Kapazität werden in einem Sicherheitsschema häufig übersehen. Wenn auf solchen Geräten der vorgegebene Benutzername und das Standardkennwort erhalten bleiben, ist es eventuell nur eine Frage der Zeit, bis ein Angreifer, der lediglich den Gerätetyp und die dokumentierten Standardanmeldeinformationen kennt, Zugriff auf das Gerät erlangt. Stellen Sie sich eine Serverbank mit absolut zuverlässigen Sicherheitsprotokollen auf jedem Web- und E-Mail-Server vor, die aufgrund eines einfachen Ein-Ausschaltvorgangs einer ungeschützten USV abstürzt!

Sicherheit – das Gesamtbild
Wirksame Sicherheitsmaßnahmen in großen wie kleinen Unternehmen müssen umfassend sein. Die meisten Organisationen haben allerdings keine entsprechenden Richtlinien und Verfahren. Dafür gibt es einige gute Gründe: Sicherheit verursacht natürlich auch Kosten. Diese Kosten lassen sich nicht nur in Geld, sondern auch in Komplexität, Zeit und Effizienz messen. Um Sicherheit zu gewährleisten, ist es notwendig, Geld auszugeben, weitere Maßnahmen durchzuführen und zu warten, bis diese Maßnahmen abgeschlossen sind (eventuell müssen auch Dritte einbezogen werden).

In der Praxis sind echte Sicherheitsprogramme schwierig umzusetzen. Normalerweise muss ein Schema ausgewählt werden, das gewisse „Kosten“ verursacht und eine überschaubare Sicherheitsgarantie bietet. (Ein solches Konzept ist kaum als „umfassend“ zu bezeichnen.) Wichtig ist, zu jedem Aspekt eines Gesamtsystems sachlich begründete Entscheidungen zu treffen und mehr oder weniger Mittel bewusst und kalkuliert einzusetzen. Wenn man die weniger geschützten Bereiche kennt, können diese Bereiche wenigstens überwacht werden, um Probleme oder Sicherheitslücken zu entdecken.

Kenntnis des Netzwerks
Es ist nicht möglich, etwas zu schützen, wenn man nicht genau weiß, WAS geschützt werden soll. Organisationen jeder Größe müssen ihre Ressourcen und Systeme dokumentieren. Allen Elementen muss ein relativer Wert zugewiesen werden, aus dem die Bedeutung der Elemente für die Organisation hervorgeht. Die gilt z. B. für Server, Workstations, Speichersysteme, Router, Switches, Hubs, Netzwerk- und Telekommunikationsverbindungen und weitere Netzwerkelemente wie Drucker, USV-Systeme und HVAC (Heating, Ventialtion and Airconditioning)-Systeme. Wichtig ist zudem die Dokumentierung des Gerätestandorts sowie Hinweise auf Abhängigkeiten. Die meisten Computer sind z. B. auf eine Notstromversorgung (USV) angewiesen, die wiederum Teil des Netzwerks sein kann, wenn sie verwaltet wird. Klimageräte wie HVAC-Geräte und Luftreiniger gehören eventuell ebenfalls hierzu.

Kenntnis unterschiedlicher Bedrohungen
Im nächsten Schritt werden, wie in Tabelle 1 dargestellt, die potenziellen „Bedrohungen“ all dieser Elemente ermittelt. Die Bedrohungen können sowohl aus internen als auch aus externen Quellen stammen. Es kann sich um menschliches Versagen, automatische Ereignisse oder nicht beabsichtigte natürliche Ereignisse handeln. Letztere könnten eigentlich eher unter die Kategorie Bedrohung der Systemintegrität als unter Sicherheitsbedrohung subsumiert werden, jedoch kann ein Problem ein anderes nach sich ziehen. Ein Beispiel dafür ist ein Stromausfall infolge eines Einbrecheralarms. Der Stromausfall könnte willentlich oder durch ein natürliches Ereignis wie einen Blitzschlag herbeigeführt worden sein. In beiden Fällen ist die Sicherheit beeinträchtigt.

Bedrohung	Intern \ Extern	Konsequenzen der Bedrohung
E-Mail mit Virus	Externe Herkunft, interne Verwendung	Kann System infizieren, auf dem die E-Mail gelesen wird, und sich danach in der ganzen Organisation ausbreiten.

Quelle: www.voltimum.de

Netzwerkvirus	Extern	Kann über ungeschützte Anschlüsse eindringen und das gesamte Netzwerk gefährden.
Webbasierter Virus	Interner Aufruf einer externen Website im Browser	Kann Systemsicherheit während des Browsens gefährden und danach andere interne Systeme beeinträchtigen.
Webserverangriff	Außerhalb von Webservern	Wenn die Sicherheit des Webservers beeinträchtigt ist, können Hacker Zugriff auf andere interne Systeme des Netzwerks erlangen.
Dienstverweigerungs-angriff	Extern	Externe Dienste wie Web, E-Mail und FTP können unter Umständen nicht mehr verwendet werden. Wird ein Router angegriffen, kann das gesamte Netzwerk ausfallen.
Angriff durch Netzwerkbenutzer (interner Mitarbeiter)	Generell intern	Herkömmliche Firewalls an der Netzwerkgrenze sind bei solchen Angriffen wirkungslos. Interne Segmentierungsfirewalls können Schaden eindämmen.

Physische Sicherheit, interner Schutz
Die meisten Experten würden zustimmen, dass Sicherheit stets mit der physischen Sicherheit beginnt. Die Steuerung des physischen Zugriffs auf Rechner und Netzwerkknotenpunkte ist vermutlich wichtiger als alle anderen Sicherheitsaspekte. Durch jede Art physischen Zugriffs auf einen internen Standort wird dieser einem größeren Risiko ausgesetzt. Wenn der physische Zugriff möglich ist, können in der Regel auch sichere Daten, Kennwörter, Zertifikate und alle anderen Daten abgerufen werden. Glücklicherweise gibt es alle möglichen Arten von Zugriffssteuerungsgeräten und sicheren Schränken, mit denen sich dieses Problem lösen lässt. Weitere Informationen über die physische Sicherheit von Datencentern und Netzwerkräumen finden Sie im APC White paper Nr. 82, „Physische Sicherheit in betriebskritischen Gebäuden“.

Partitionieren des Netzwerks und Schützen der Netzwerkgrenzen durch Firewalls
Neben der grundlegenden physischen Sicherheit eines Standorts ist die Kontrolle des digitalen Zugriffs auf das Netzwerk der Organisation und aus dem Netzwerk heraus der nächste wichtige Aspekt. In den meisten Fällen müssen dazu die Verbindungen mit der externen Welt, also im Regelfall mit dem Internet überwacht werden. Fast jedes mittlere und große Unternehmen verfügt über einen Internetauftritt, mit dem das Netzwerk der Organisation verbunden ist. Auch kleinere Unternehmen und private Anwender besitzen in zunehmendem Maß eine permanente Internetanbindung. Die Abtrennung des externen Internets und des internen Intranets ist ein entscheidendes Element des Sicherheitskonzepts. Gelegentlich wird die interne Seite als „vertrauenswürdig“ und das externe Internet als „nicht vertrauenswürdig“ bezeichnet. Das ist zwar grundsätzlich richtig, allerdings noch nicht genau genug, wie im Folgenden zu zeigen sein wird.

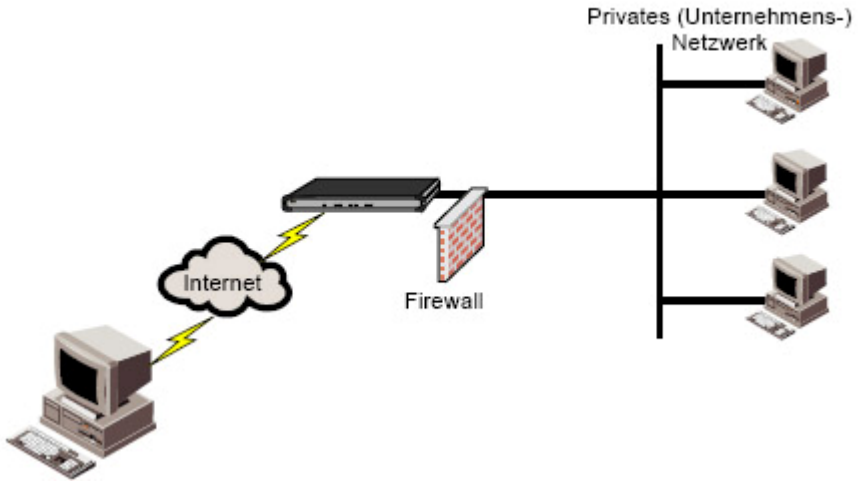
Eine Firewall ist eine überwachte Barriere, mit welcher der Netzwerkverkehr in das Intranet UND aus dem Intranet einer Organisation gesteuert wird. Firewalls sind im Wesentlichen anwendungsspezifische Router. Es kann sich dabei um spezielle eingebundene Systeme, z. B. Internetgeräte, oder um Softwareprogramme handeln, die auf einer allgemeinen Serverplattform ausgeführt werden. Normalerweise haben diese Systeme zwei Netzwerkschnittstellen, eine für das externe Netzwerk – das Internet – und eine für das interne Intranet. Mit einer Firewall lässt sich genau kontrollieren, welche Daten von einer Seite zur anderen übertragen werden dürfen. Firewalls können sehr einfach oder sehr komplex sein. Wie bei den meisten Sicherheitsaspekten richtet sich die Festlegung des zu verwendenden Firewalltyps nach Faktoren wie Datenverkehrsvolumen, schutzbedürftige Dienste und die Komplexität der erforderlichen Regeln. Je größer die Anzahl der Dienste, die die Firewall passieren müssen, desto komplexer werden die Anforderungen. Die Unterscheidung zwischen legitimem und illegitimem Datenverkehr ist bei Firewalls nicht ganz einfach.

Wovor schützen Firewalls, und welchen Schutz bieten sie nicht? Für Firewalls gilt, was auch für viele andere Dinge gilt: Wenn sie richtig konfiguriert sind, können sie ein sinnvoller Schutz vor externen Bedrohungen einschließlich bestimmter Dienstverweigerungsangriffe sein. Sind sie fehlerhaft konfiguriert, stellen sie in einer Organisation unter Umständen größere Sicherheitslücken dar. Der grundlegendste Schutz, den eine Firewall bietet, ist die Blockierung von Netzwerkverkehr zu bestimmten Zielen. Dies gilt sowohl für IP-Adressen als auch für spezielle Netzwerkdienstanschlüsse.

Quelle: www.voltimum.de

Soll für eine Site der externe Zugriff auf einen Webserver möglich sein, kann der gesamte Datenverkehr auf Anschluss 80 beschränkt werden (den standardmäßigen HTTP-Anschluss). In der Regel wird diese Einschränkung nur auf Datenverkehr nicht vertrauenswürdiger Herkunft angewandt. Datenverkehr vertrauenswürdiger Herkunft wird nicht eingeschränkt. Der gesamte übrige Datenverkehr wie E-Mails, FTP, SNMP usw. wird von der Firewall nicht ins Intranet durchgelassen. Ein Beispiel für eine einfache Firewall sehen Sie in Abbildung 2.

***Abbildung 2** – Einfache Firewall für ein Netzwerk*



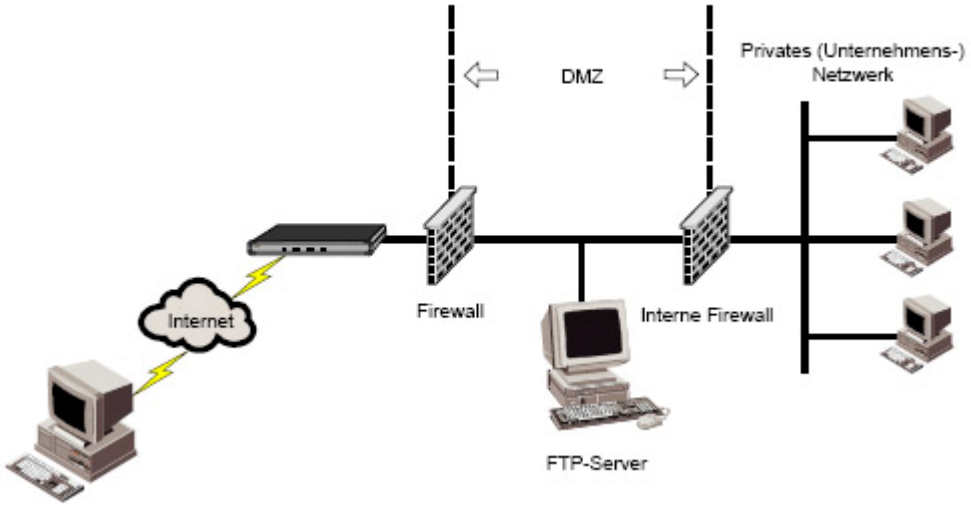
Noch einfacher sind Firewalls, die häufig von Benutzern in Heimbüros oder kleinen Unternehmen mit Kabel- oder DSL-Routern verwendet werden. Diese Firewalls sind normalerweise so eingerichtet, dass der GESAMTE externe Zugriff eingeschränkt ist und nur Dienste des internen Systems zugelassen sind. Ein aufmerksamer Leser hat vielleicht bemerkt, dass eine Firewall in keinem dieser Fälle tatsächlich den gesamten Verkehr von außen abblockt. Wäre das wirklich der Fall, wie wäre es dann möglich, im Web zu surfen und Websites aufzurufen? Was die Firewall tatsächlich bewirkt, ist die Einschränkung von Verbindungsanforderungen, die von außen kommen. Im ersten Fall werden alle Verbindungsanforderungen aus dem internen Netz sowie die gesamte folgende Datenübertragung über diese Verbindung an das externe Netz weitergeleitet. Von außen wird nur eine Verbindungsanforderung für den Webserver zugelassen, um Daten zu vervollständigen und weiterzugeben, alle übrigen Anforderungen werden abgeblockt. Im zweiten Fall ist die Vorgehensweise rigoroser, da Verbindungen nur von innen nach außen aufgebaut werden können.

Bei komplexeren Firewallregeln werden so genannte „statusbehaftete Prüfverfahren“ eingesetzt. Dabei wird die einfache Anschlussblockierung um die Prüfung von Verhaltensweisen und Sequenzen im Datenverkehr erweitert, um Angriffe mit vorgetäuschter Identität und Dienstverweigerungsangriffe zu erkennen. Je komplexer die Regeln, desto größer ist die erforderliche Rechenleistung der Firewall.

Ein Problem für die meisten Organisationen ist es, legitime Zugriffe auf „öffentliche“ Dienste wie Web, FTP und E-Mail zuzulassen und gleichzeitig die Integrität des Intranets zu sichern. In der Regel wird dazu eine so genannte demilitarisierte Zone (DMZ) erstellt; dieser aus dem kalten Krieg stammende Euphemismus wurde auf Netzwerke angewandt. In dieser Architektur gibt es zwei Firewalls: eine zwischen dem externen Netzwerk und der DMZ sowie eine weitere zwischen der DMZ und dem internen Netzwerk. Alle öffentlichen Server befinden sich in der DMZ. Bei einer solchen Konfiguration können Firewallregeln festgelegt werden, die den öffentlichen Zugriff auf die öffentlichen Server gestatten, während die innere Firewall alle eingehenden Verbindungen beschränkt. Durch die DMZ sind die öffentlichen Server dennoch besser geschützt, als wenn sie sich außerhalb einer Site mit einfacher Firewall befänden. Abbildung 3 zeigt die Verwendung einer DMZ.

Quelle: www.voltimum.de

Abbildung 3 – *Doppelte Firewalls mit DMZ*



Durch die Verwendung interner Firewalls an verschiedenen Intranetgrenzen lassen sich außerdem Schädigungen durch interne Bedrohungen und Objekte wie Würmer eindämmen, denen es gelang, die äußeren Firewalls zu überwinden. Interne Firewalls können auch im Bereitschaftsmodus ausgeführt werden. Der normale Datenverkehr wird auf diese Weise nicht blockiert, bei Auftreten eines Problems werden jedoch strenge Regeln aktiviert.

Workstation-Firewalls

Es gibt einen wichtigen Faktor für die Netzwerksicherheit, der den meisten Benutzern erst jetzt bewusst wird: die Tatsache, dass ALLE Knoten oder Workstations in einem Netzwerk potenzielle Sicherheitslücken darstellen. In der Vergangenheit wurden hauptsachlich Firewalls und Server beachtet. Mit dem Aufkommen ÆÉ2005 American Power Conversion. Alle Rechte vorbehalten. Kein Teil dieser Publikation darf ohne schriftliche Erlaubnis des Copyright- Eigentümers verwendet, reproduziert, fotokopiert, übertragen oder in irgendeinem System zum Abrufen von Daten gespeichert werden. www.apc.com Version 2005-0 9 des Webs und dem Entstehen immer neuer Klassen von Knoten wie z. B. Internetgeraten sind beim Schutz des Netzwerks einige zusätzliche Aspekte zu beachten. Zahlreiche Wurmprogramme erobern Computer und benutzen sie, sowohl um sich selbst zu verbreiten als auch um gelegentlich Systeme zu schädigen. Viele dieser Würmer konnten gestoppt oder stark behindert werden, wenn die internen Systeme der Organisationen besser gesichert waren. Firewalls für Workstations konnen sämtliche Zugriffe auf einzelne Hosts und aus einzelnen Hosts heraus blockieren, die nicht der normalen Funktion der einzelnen Hosts entsprechen. Zusätzlich können Firewallregeln auf der INTERNEN Seite, die verdächtige ausgehende Verbindungen aus der Organisation blockieren, verhindern, dass sich die Würmer wieder aus einer Organisation heraus verbreiten. Die interne und externe Replikation auf beiden Seiten kann reduziert werden. Grundsätzlich sollten alle Systeme in der Lage sein, alle Anschlüsse zu blockieren, die nicht benotigt werden.

Quelle: www.voltimum.de