

securityGUIDE

Software-gestütztes
Kompendium zur IT-Sicherheit

Teil - III
Abschnitt - 4
Sicherungssysteme

April 2004

Inhaltsverzeichnis Teil 3 – Abschnitt 4

1	Sicherungssysteme	5
1.1	Einführung in Datenback-UP-Systeme	5
2	Daten-Back-Up-Durchführung	7
2.1	Datensicherung-Check-Points	9
2.1.1	Check Betriebsэлеmente	9
2.1.2	Check Detail-Elemente	10
2.2	Ziele der Datensicherung	12
2.3	Verteiltes Sicherungskonzept	13
2.4	Bestandsaufnahme	14
2.5	Trägerische Sicherheit des Backup's	14
2.6	Sicherungsablauf	16
3	Sicherung Systemkomponenten	17
3.1	Hardware	17
3.2	Software	17
3.3	Erläuterung Bandgenerationen	17
3.4	Doppelte Datensicherung / Auslagerung	18
3.5	Aufbewahrungsort	18
3.6	Generationskonzept	18
3.7	Sicherungsläufe	19
3.8	HSM (Hierarchical Storage Management)	19
4	Firewall's	20
4.1	Schutz durch Einsatz einer Firewall	20
4.2	Übersicht Firewall-Funktionalitäten	22
4.2.1	Paketfilter	22
4.2.2	Virtual Private Network (VPN)	24
4.2.3	Application Level Firewall	25
4.2.4	Circuit Level Firewall	28
4.2.5	Stateful Inspection	28
4.2.6	Proxy	30
4.2.7	Socks	31
4.2.8	Firewallpolicy	32
4.3	IT-Sicherheitsgrundhaltung	32
4.3.1	Alles, außer...	32
4.3.2	Nichts, außer	33
4.4	Firewall Sicherheitsnotes	33
4.4.1	Firewall-Basisinformationen	33
4.4.2	Source Porting	34
4.4.3	Source-Routing	34

4.4.4	TCP-Sequence-Prediction	35
4.4.5	Direct RPC Scan.....	35
4.4.6	Stealth-Scanning	36
4.4.7	Denial-of-Service Attack	36
4.4.8	Default-Accounts	36
4.4.9	Intranet Scanner	37
4.4.10	Plazierung der Firewall	38
4.4.11	Bastion Host	38
4.4.12	Router mit Firewall-Funktionalitäten	39
4.4.13	Firewall-Rechner mit Routerfunktion	40
4.4.14	Firewall-Rechner hinter Router.....	40
4.4.15	Screened Subnet.....	41
4.4.16	NAT.....	41
4.4.17	Masquerading	42
4.5	Management einer Firewall	43
5	Internet-Angriffsmöglichkeiten	44
5.1	Angriffsmethoden.....	44
5.1.1	Einbrüche.....	44
5.1.2	Lahmlegen eines Dienstes	45
5.1.3	Einsatz von Spionagesoftware	45
5.1.4	Denial-of-Service-Attacks (DoS).....	45
5.1.5	Brute-Force-Attacks.....	48
5.2	Gefährliche Hintertüren.....	48
6	Gefährdete Internet-Dienste	50
6.1	email (SMTP).....	50
6.2	file-transfer (ftp)	51
6.3	usenet-news (NNTP)	52
6.4	terminal-Zugang (telnet)	52
6.5	World-Wide-Web (WWW).....	53
6.6	Domain-Name-Service (DNS)	54
6.7	Virtual Private Network (VPN)	55
7	Personal Firewall	56
8	Viren und andere "Schädlinge"	57
8.1	Virenbeschreibung.....	57
8.2	Anti-Virus	58
8.3	Viren in Emails: Fakten und Maßnahmen	60
8.4	Programm, Replikat, Trigger und Payload	60
8.5	Zahlreiche Virenvarianten.....	61
8.6	Schutzmaßnahmen gegen Viren	62
8.7	Was tun bei Virenbefall?	64
9	Filter.....	66

9.1	Spamfilter.....	66
9.2	Contentfilter	67
9.3	Fernzugriff VPN	67
9.4	Honey Pot	67
9.5	Rootkit.....	67
9.6	Servermonitoring/Logfileauswertung	67
10	Index.....	68

1 Sicherungssysteme

1.1 Einführung in Daten-Back-up

Das wichtigste einer Firma im IT Bereich ist nicht Hardware und Software, sondern die eigenen Daten.

- © Kundendaten,
- © Betriebsdaten,
- © Daten aus dem Rechnungswesen

Ein einfacher Festplattendefekt kann ohne Datensicherung einen immensen Schaden anrichten. Es können aber bei jeder - auch qualitativen hohen - Hardware Fehler auftreten.

Jeder Verantwortliche, Geschäftsführer, Datenschutzbeauftragter oder IT-Verantwortlicher sollte sich bewußt sein, welche qualitative und quantitative Bedeutung ein Ausfall der IT für das Unternehmen bedeutet.

TIPP!

Ermitteln Sie folgende Kennzahlen:

1. *Welche Kosten entstehen durch Ausfall für eine Stunde, einen Tag, eine Woche für den Betrieb?*
2. *Wie lange kann das Unternehmen ohne Daten seine unternehmerische Tätigkeiten aufrechterhalten?*

Ferner ist zu checken, welche Daten vorliegen und in welcher Anzahl.

Mit diesen Eckwerten lässt sich die Wiederanlaufzeit der Server, d.h. der Zeitraum bis die volle Produktivität wieder erreicht ist, ermitteln.

Datensicherungen werden in der Regel auf tauschbare Medien vorgenommen, so dass ein physischer Wechsel in der Lokation mit dem Datenträger vorgenommen werden kann. In der Regel werden Magnet-Bänder und CDs eingesetzt.

TIPP!

Eine gespiegelte Festplatte oder ein FestplattenRAID System ersetzt aufgrund der hohen Lesbarkeit / Verfüg-

barkeit keine Datensicherung auf Bänder.

Die Systemwiederherstellung ist reine Installationszeit eines Windows NT/W2k- oder Linux-Betriebssystems. Je nach Hardware sind zwischen zwei bis vier Stunden zu kalkulieren.

Anschließend ist der Back-up-Client zu installieren. Nach Installation ist der "eigentliche" Restore zu starten. Dazu werden die Daten vom Datensicherungsträger (Band/Bänder) zurückgespielt.

Die Datenwiederherstellung dauert in der Regel nach Installation des Betriebssystems genauso lange, wie die Sicherung des Servers gedauert hat.

Sind es 3, 15 oder 30 Stunden?

2 Firewall's

2.1 Schutz durch Einsatz einer Firewall

Das Internet bietet einem Unternehmen diverse Möglichkeiten der Kommunikation des Informations- und Datenaustausches zwischen verschiedenen Firmenstandorten, Teleworkern, externen Dienstleistern und sonstigen Quellen wie WWW oder FTP. Angestellte können von zu Hause aus im Firmennetz arbeiten und benutzen dazu einen sogenannten VPN Tunnel.

Außenstellen haben die Möglichkeit auf interne Datenbanken zurück zu greifen, Server unter externer Wartung sind online ohne der Anreise eines Technikers konfigurierbar, aktuelle Programme und Treiber liegen auf öffentlichen FTP-Servern bereit.

Die Verteilung der Information kostet nur noch den Bruchteil der früheren Ausgaben, die Nutzung dieser Dienste und Informationen ist im Gegensatz zu den oft angefallenen "anteiligen Transportgebühren" verschwindend gering.

Achtung!

In all der Euphorie werden schnell die entstehenden Gefahren vergessen, dass das eigene Netzwerk dem Internet offen gegenüberliegt!

Diese Offenheit erfordert aber eine genaue geplante und gut implementierte Sicherheit. Ein Teil eines Sicherheitskonzeptes besteht in der Implementation einer Firewall. Diese Hard- oder Softwarekomponente wird als Schutzwall zwischen das eigene LAN und das Internet gestellt.

Hier werden alle gefährlichen oder ungewollten Datenpakete verworfen, so dass sie nicht in das interne Firmennetz eindringen können.

Firewalls sind Schutzvorrichtungen, um den Anschluss an das Internet mit einem kalkulierbaren Risiko zu ermöglichen. Dabei sind folgende Punkte zu beachten:

- Daten sind besonders in den Bereichen Vertraulichkeit, Geheimhaltung vor Dritten zu schützen.
- Daten sind durch Dritte nicht zu verändern.

- Verfügbarkeit zur eigenen Bearbeitung ist zu gewährleisten.
- Rechner mit vertraulichen Daten sind zu schützen.
- Prestige - der gute Ruf der Firma ist zu beachten.

Häufig wird die eigentliche Gefahrenquelle falsch eingeschätzt!

Potentielle Täter zielen darauf ab, sich fremde Rechnerressourcen zugänglich zu machen. Damit ist es möglich, durch eine fremde IP-Adresse mehrere hundert oder tausend Rechner für einen Angriff gegen einen anderen Internetrechner zu benutzen.

Eine Firewall filtert daher den gesamten Datenstrom, der aus und in das betriebsinterne LAN geht, aus. Ein Höchstmaß an Leistungsfähigkeit dieser Lösung ist daher gefordert. Der Datentransfer darf nicht behindert werden, d.h. die Geräte müssen extrem schnell sein und der Datenfluss muss permanent zur Verfügung stehen.

Ein Fehler im System kann die Kommunikation im gesamten Netzwerk in Mitleidenschaft ziehen. Hier ist auf erhöhte Ausfallsicherheit absolut hohen Wert zu legen.

Achtung: Die Fehlerfreiheit kann nur temporär erkauf werden!

Wichtiger Hinweis!

Solange eine Sicherheitslücke nicht bekannt ist, kann eine Filterregel nicht dafür definiert werden. Firewalls sollten daher immer wieder erneut überprüft und die Konfiguration angepasst werden.

Es existieren verschiedene Typen von Firewalls. Jeder Typ hat spezielle Eigenschaften und damit auch Vor und Nachteile für bestimmte Anwendungen.

Sollte ein Typ einer bestimmten Firewall nicht den innerbetrieblichen Anforderungen genügen, ist die am nächsten kommende Firewall auszuwählen.

In größeren Netzen sollten zwei oder mehrere Typen von Firewalls miteinander kombiniert werden.

Die Konfiguration und Wartung der Soft- und Hardwarelösung setzt sehr genaue Kenntnisse des benutzten Protokolls (in der Regel TCP/IP) voraus. Ein Firewalladministrator, Spezialist in Funktionalitäten für Pakete, Ports, Fragmente, DDOS, UTP, ICMP, sollte beim Aufbau einer Firewall hinzugezogen werden.

2.2 Übersicht Firewall-Funktionalitäten

2.2.1 Paketfilter

Paketfilter sind Router oder Rechner mit spezieller Firewallsoftware, welche die in den Schichten drei und vier der TCP/IP-Protokollfamilie vorhandenen Informationen (Quell- und Zieladresse, Portnummern) zum Filtern der Pakete benutzen.

Hierzu werden Access- bzw. Deny-Listen benutzt. Paketfilter sind ein relativ einfacher Mechanismus, da jeder Router die Möglichkeiten besitzt, Paketfilterung durchzuführen. Im allgemeinen ist es jedoch schwierig, die Access- und Deny-Listen zu erstellen und erfordert sehr gute Kenntnisse in der Programmierung des jeweiligen Routers.

Auch können sich - insbesondere bei komplexen Filterregeln - Fehler einschleichen, welche die Konsistenz des Regelsystems gefährden. Paketfilter allein bieten keinen ausreichenden Schutz vor Angriffen. IP-Spoofing ist beispielsweise eine Möglichkeit, einen Paketfilter zu überwinden.

Für Dritte ist es einfach, Schwachstellen wie Buffer Overflow oder WinNuke auszunutzen. Für die Protokollierung stehen nur eingeschränkte Möglichkeiten zur Verfügung.

Eine Content-Filterung, z.B. über Active-X, Cookies, FTP-PUT, ist nicht möglich.

Paketfilterung auf einfachen Routern hat einen weiteren Nachteil:

Ein Router bietet kaum Möglichkeiten, eine Protokollierung des TCP/IP-Verkehrs vorzunehmen, damit gehen wertvolle Protokollinformationen verloren. Es wird schwierig, einen Angriff zu erkennen oder gar zu verfolgen, da ein Teil der "böartigen" Pakete bereits von den Paketfilter-Modulen des Routers verworfen oder abgewiesen werden.

Neuere Firewallprodukte bieten inzwischen die Möglichkeit, Paketfilterung in Verbindung mit einer vollständigen Protokollierung des TCP/IP- Verkehrs auf einem Dual Homed Host durchzuführen.

Die dort implementierten Filtermodule prüfen die erstellten Filterregeln auch auf Widerspruchsfreiheit.

Vorteile:

- gute Performance, aufgrund der vergleichsweise geringen Funktionalität
- einfache Konfigurierbarkeit bei wenig komplexen Problemstellungen

Nachteile:

- Missbrauch von Protokollen nicht erkennbar (z.B. Fragmentation-Attack, bei der der TCP-Header auf das erste und zweite Paket aufgeteilt wird),
- Ausnutzung von Schwachstellen (Buffer Overflow, WinNuke),
- nur eingeschränkte Möglichkeiten zur Protokollierung,
- keine Content-Filterung (z.B. Active-X, Cookies, FTP-PUT)
- unübersichtlich bei großer Anzahl von Filterregeln (Fehlerquelle!)

Beim IP-Filtering wird der Datenverkehr aufgrund der Informationen in den einzelnen IP-Packet-Headern geregelt. Dabei werden Quell- und Zieladresse als Hauptkriterium für die Filterung verwendet.

So werden z.B. Pakete vom äußeren Netz kommend mit einer Quelladresse aus dem inneren Netz abgelehnt, um Angriffe abzuwehren. Auch die angesprochenen Ports (Source und Destination) werden blockiert um einzelne Dienste zu verbieten oder zuzulassen.

Es stehen zwei Arten der Filterung zur Verfügung:

1. Statische Filterung

Filterung aufgrund genau festgelegter Regeln bezüglich der IP-Header.

2. Stateful Inspection

Filterung erfolgt abhängig von älteren Paketen, die mit dem aktuellen Paket in Verbindung stehen. Hiermit werden Antwortpakete bei verschiedenen Diensten akzeptiert, welche bei statischer Filterung nicht zugelassen sind.

Trifft auf ein eintreffendes Paket eine Filterregel zu, so wird es entweder fallengelassen oder dem Absender signalisiert, dass es abgelehnt wurde.

Die Reaktion kann bei jeder Filterregel angegeben werden. Abgelehnte Pakete werden nach der ausgelösten Filterregel sortiert und aufgezeichnet, um später eventuelle Angriffe zu analysieren.

2.2.2 Virtual Private Network (VPN)

Mehrere lokale Netzwerke können mit Hilfe des Internets verbunden werden. Diese Verbindung liegt jedoch offen und ist für jeden abhörbar.

Mit einem sogenannten IP-Tunnel zwischen zwei LANs kann die Verbindung nach außen geschützt werden.

Zuerst wird eine IP-Verbindung erstellt, bei der sich die Endstellen (Firewall oder Router) authentifizieren und einen session key für die Übertragung festlegen. Alle Datenpakete, die die

beiden Netzwerke danach austauschen, werden mit dem "session key" verschlüsselt und auf dieser Verbindung übertragen.

Diese Technik hat mehrere Vorteile:

- die verschlüsselte Verbindung sorgt für vertraulichen Datentransfer,
- Authentifizierung stellt sicher, dass nur der entsprechende Partner die Verbindung aufbauen kann,
- beide Netzwerke werden völlig transparent kombiniert,
- es sind keine WAN-Direktverbindungen nötig, da die Verbindung mit jeweils einem (meist Ortsnetz-) Zugang ins Internet funktioniert.

Nachteilig wirkt sich der erhöhte Administrationsaufwand, z.B. in der Schlüsselverwaltung aus und die unsichere Übertragungskapazität des Internets.

2.2.3 Application Level Firewall

Application Level Gateways untersuchen den Verkehr auf der Applikationsebene (Schicht 7 des OSI- Modells).

Für jede weitergeleitete Anwendung wird ein spezieller Code verwendet, ein sogenannter Proxy-Server. Der Proxy-Server fungiert praktisch als Client und Server gleichzeitig. Der Client im internen Netz spricht den Server-Teil des Proxy-Servers an.

Über diesen wird der gesamte Datenverkehr geleitet, der in das Internet gesendet wird. Der Server im externen Netz kommuniziert mit dem Client-Teil des Proxy's.

Der Proxy-Server übernimmt die Vermittlung, führt also eine store- and- forward-Funktion aus. Es muss sichergestellt sein, dass alle Daten zwischen dem Client und dem Server vom Proxy-Server weitergeleitet werden.

Nur so hat die Proxy Firewall die vollständige Kontrolle über den stattfindenden Datenverkehr und kann eine detaillierte Protokollierung vornehmen. Neuere Proxy-Server verlangen außer der Eingabe ihrer Adresse oder ihres Namens keine Anpassung der verwendeten Clientsoftware (Internetbrowser).

Für jeden Dienst, den das Application Level Gateway anbietet, muss ein eigenes Programm, eben der Proxy-Server, geschrieben werden.

Deshalb bieten die meisten Firewallprodukte mit Application Level Filterung nur für die gängigen Internetdienste Gateways an. Bei einigen Produkten gibt es zusätzlich noch Module (sogenannte generische Proxies), die für ungewöhnliche Dienste konfiguriert werden können.

Da in Firewall-Rechnern standardmäßig die TCP/IP- Weiterleitung (IP-Forwarding) abgeschaltet wird, kann **keine Verbindung** aufgebaut werden, wenn für den Dienst kein passender Proxy-Server vorhanden ist.

Damit entspricht ein Application Level Gateway der Philosophie: was nicht ausdrücklich erlaubt ist, ist verboten.

Vorteile des Einsatzes eines Proxy:

- ein Proxy arbeitet systembedingt richtungsabhängig,
- eine Fehlfunktion des Proxy stellt weitestgehend keine Sicherheitslücke dar, sondern unterbindet im Zweifelsfall die Kommunikation.

Nachteile des Einsatzes eines Proxy

- aufgrund der Bearbeitung auf OSI-Layer 7 geringere Performance,
- es stehen nicht für alle Firewalls und Applikationen Proxies zur Verfügung (Abhilfe ggf. "Generic Proxy").

Risiko	Gefahrenabwendung
SOCKs ist eine für Proxy-Application Firewalls entwickelte Programm-bibliothek, um bestimmte Services durchzulassen und Eindringlinge abzuweisen. Das grundlegende Problem mit	Ein Firewall Scanner versucht, mit wichtigen Services über den SOCKs-Port Verbindung aufzunehmen, um zu sehen, ob die Filterregeln korrekt konfiguriert worden sind. Die Proxy-Checks sollen eben-

<p>SOCKs ist dasselbe wie bei vielen anderen Tools: SOCKs ist häufig falsch konfiguriert. Oft entwickelt der Verwalter Regeln, um bestimmte Services durch die Firewall hindurchzulassen; aber die Regeln, die notwendig sind, um Eindringlingen den Zugang zu verweigern, werden nicht implementiert.</p> <p>Folglich arbeiten Services anscheinend problemlos mit der Firewall.</p> <p>Dass diese nicht in der Lage sind, Eindringlinge abzuwehren, wird erst bemerkt, wenn bereits eingebrochen worden ist.</p>	<p>falls versuchen, über die Proxies eine Verbindung innerhalb der Firewall aufzubauen. Es wird festgestellt, welche Services freigeschaltet sind. Services die freigeschaltet sind, aber bekannte Schwachstellen haben, werden als mögliche Angriffspunkte aufgelistet.</p>
--	--

2.2.4 Circuit Level Firewall

Circuit Level Firewalls arbeiten auf der Verbindungsschicht. Sie vermitteln TCP-Verbindungen.

Eine externe Verbindung geht auf einem TCP-Port des Gateway ein; dieses kontaktiert dann ein internes Ziel. Während die Verbindung besteht, kopiert das Gateway die Daten zwischen den Schnittstellen. Die Relaisdienste kontrollieren im allgemeinen den durchfließenden Datenstrom nicht.

Ein Circuit Level Gateway wird so konfiguriert, dass die Verbindung automatisch hergestellt wird oder dass das gewünschte Ziel mitgeteilt werden muss.

Für abgehende Verbindungen sind Transportschicht-Gateways unbedenklich. Eingehende Verbindungen stellen allerdings ein Sicherheitsrisiko dar, wenn die Verbindungen allgemein zur Verfügung stehen müssen.

Achtung!

Interne Benutzer könnten die Ziele des Gateways umgehen, indem sie für eingehende Verbindungen auf ihrem Rechner ungeschützte Dienste anbieten.

Eingehende Verbindungen auf festgelegten Portnummern und zu bestimmten Rechnern können eher kontrolliert werden, stellen aber auch ein höheres Risiko dar.

Auch für Circuit Level Gateways müssen in der Regel die Clients angepasst werden.

2.2.5 Stateful Inspection

Die von Checkpoint eingeführte Filtertechnik ist in der Lage, aktuelle Status- und Kontextinformationen sich zu merken und bei der Filterung zu berücksichtigen.

Auf diese Weise kann z.B. die Fragmentierungs-Attacke abgewendet oder ein manipulierter Verbindungsaufbau erkannt werden. Firewalls stellen daher eine Doppelfunktion zwischen Filtern und Application Level Firewalls dar.

Risiko	Gefahrenabwendung
<p>Allen Systemen ist gemein, dass sie Vorteile aber auch spezifische Nachteile haben. Sie müssen als Unternehmer festlegen, wie hoch der Schutz des Datenweges sein soll und welcher Aufwand für die Errichtung dieses Schutzes betrieben werden soll.</p>	<p>Es besteht durchaus die Möglichkeit, mehrere verschiedene Firewallsysteme hintereinander zu schalten. Als Erstes z.B. ein Paketfilter, weil der sehr schnell arbeitet und „schon mal das Grobe“ aus dem Datenverkehr herausfiltern kann. Was da durch kommt, soll auch noch inhaltlich mittels ApplicationlevelFW untersucht werden. In dieser Appliance wird dann auch gleich noch ein Virencheck vorgenommen.</p> <p>Wenn Sie es sehr weit treiben möchten, können auch noch alle Anhänge, die in Mails geliefert werden überprüft werden. Diejenigen, die Sie nicht in Ihrem Unternehmen haben möchten, z.B. VBS, EXE, COM werden gleich hier am Gateway gelöscht und zusätzlich erhalten Sender und Empfänger der Mail eine entsprechende Nachricht.</p>

Risiko	Gefahrenabwendung
<p>Falls ein in der beschriebenen Weise abgesicherter Zugang eingesetzt ist, werden findige User bald einen Weg finden, hier das eine oder andere Mail mit unerwünschten Inhalten einzuschleusen.</p> <p>Es gibt keine Möglichkeit, eine EXE Datei,</p>	<p>Checken der Nachricht ist die einzige Gewähr, ungewünschte Dateien zu verhindern.</p>

<p>also ausführbaren Code, die in TXT umbenannt und zudem noch in ein ZIP Archive verpackt wurde zu erkennen. Die angehängten Files kommen durch!</p>	
---	--