

Cisco Safe



Safe

Cisco Security Lösungen





Sicherheitsarchitektur für Unternehmen

| | |
|--|-----------|
| Einleitung | 5 |
| Viele Angriffsarten, ein Ziel: Ihre Daten | 6 |
| Die Cisco Secure-Sicherheitskomponenten | 17 |
| • Cisco Firewall | 17 |
| • Cisco IOS Firewall | 17 |
| • Cisco Router | 18 |
| • Cisco Secure PIX Firewall Serie | 20 |
| • Cisco Secure ACS Access Control Server | 21 |
| • Cisco Secure Intrusion Detection System | 22 |
| • Cisco Secure Policy Manager | 23 |
| • Cisco 3000 VPN Concectrator Serie | 23 |
| Safe – Sicherheitsarchitektur für Unternehmensnetzwerke | 26 |
| Sicheres Management und Reporting | 34 |
| Übersicht über die Safe-Architektur | 36 |
| Richtlinien zur Nutzung von Safe | 47 |
| Anhang – Architekturelemente | 48 |



Einleitung

Stellen Sie sich vor, Sie könnten eines Tages in Ihrem Unternehmen alle Telefongespräche kostenlos über das Internet führen. Oder stellen Sie sich vor, Sie könnten sich auf der Webseite einer Kindertagesstätte anmelden und sich erkundigen, wie es Ihrem Kind geht. Unsere Gesellschaft fängt gerade erst an zu entdecken, welche Möglichkeiten das Internet bietet.

Doch mit dem unvergleichlichen Wachstum des Internets geht auch eine noch nie da gewesene Gefährdung persönlicher Daten, kritischer Unternehmensressourcen, Staatsgeheimnisse usw. einher. Jeden Tag wächst die Bedrohung, die diese Daten und Ressourcen durch Hacker ausgesetzt sind und die immer neue Arten von Angriffen entwickeln. Diese Angriffe, die im folgenden näher erläutert werden, verbreiten sich immer mehr und können auch immer einfacher gestartet werden. Dafür gibt es im Wesentlichen zwei Gründe.

An erster Stelle steht die Allgegenwart des Internets. Bereits heute sind Millionen von Geräten in das Internet eingebunden und täglich werden es mehr. Damit haben Hacker auch immer leichteren Zugriff auf Schwachstellen im System. Die Allgegenwart des Internets hat außerdem dazu geführt, dass Hacker ihr Wissen weltweit austauschen können. Sucht man im Internet nach Begriffen wie „hack“, „crack“ oder „phreak“, findet man Tausende von Sites, die vielfach einen bösartigen Code oder gar Tools zur Verwendung dieses Codes enthalten.

An zweiter Stelle steht die Verbreitung benutzerfreundlicher Betriebssysteme und Entwicklungsumgebungen. Dadurch benötigen Hacker immer weniger echtes Fachwissen. Wirklich gute Hacker können einfach zu verwendende Applikationen entwickeln, die sie dann an die interessierte Masse weitergeben.

Für verschiedene Hackertools, die in der Public Domain zu finden sind, benötigt man lediglich eine IP-Adresse oder einen Hostnamen, und schon kann man mit einem Mausklick einen Angriff starten.

Welche Arten von Netzwerkangriffen gibt es?

Netzwerkangriffe sind ebenso vielfältig wie die Systeme, auf die sie angewendet werden. Manche sind unglaublich komplex, andere hingegen werden unabsichtlich durch den Bediener eines Geräts ausgelöst. Will man die verschiedenen Angriffsarten bewerten, muss man sich über einige dem TCP/IP-Protokoll eigene Beschränkungen im Klaren sein.

Zu Beginn seiner Entwicklung bestand das Internet lediglich aus einem Verbund verschiedener Regierungseinrichtungen und Universitäten, die den ausschließlichen Zweck verfolgten, das Lernen und die Forschung zu erleichtern. Seine Begründer konnten nicht ahnen, welche Ausmaße das Internet bis heute annehmen würde. Daher spielte zu Beginn der Entwicklung der Internet Protocol-Spezifikation das Thema Sicherheit noch keine Rolle. Und aus eben diesem Grunde sind die meisten IP-Implementierungen grundsätzlich unsicher.

Erst nach vielen Jahren und Tausenden von „Requests for Comments“ (RFCs) verfügen wir heute über die Hilfsmittel, um IP sicher einsetzen zu können. Da nicht von Anfang an spezifische Vorkehrungen zur Sicherung von IP getroffen wurden, ist es wichtig, IP-Implementierungen durch Methoden, Dienste und Produkte für die Netzwerksicherheit zu ergänzen, um so die dem Internet Protocol eigenen Risiken zu beschränken.

„Das Internet bietet fast unbegrenzte Möglichkeiten – allerdings auch des Missbrauchs.“

Viele Angriffsarten, ein Ziel: Ihre Daten



„Wird vom Benutzer nur ein einziges **Kennwort** für mehrere **Accounts** verwendet, haben **Hacker** leichtes Spiel.“

Schnüffler im Netz: Packet Sniffer

Bei einem Packet Sniffer handelt es sich um eine Softwareapplikation, die sich einer Netzwerkadapterkarte im Promiscuous-Mode bedient (also in einem Modus, in dem die Netzwerkadapterkarte alle über die physische Netzwerkleitung empfangenen Pakete zur Verarbeitung an eine Applikation sendet), um alle Netzwerkpakete, die über eine bestimmte Collision Domain gesendet werden, abzufangen.

Heutzutage werden Sniffer von Administratoren als Hilfsmittel bei der Fehlersuche und Datenverkehrsanalyse eingesetzt. Da jedoch verschiedene Netzwerkapplikationen Daten unverschlüsselt versenden (z. B. Telnet, FTP, SMTP, POP3 usw.), kann ein Packet Sniffer dem Benutzer wichtige und in vielen Fällen vertrauliche Informationen wie Benutzernamen und Kennwörter liefern.

Und darin besteht das Problem: Viele Benutzer verwenden in verschiedenen Applikationen und Systemen dieselben Anmeldenamen und Kennwörter. Das geht sogar so weit, dass Benutzer häufig nur ein einziges Kennwort zum Zugriff auf alle Konten und Applikationen verwenden. Wird nun eine Applikation im Client-Server-Modus ausgeführt und werden dabei Authentifizierungsinformationen unverschlüsselt durch das Netzwerk gesendet, ist es sehr wahrscheinlich, dass eben diese Authentifizierungsinformationen auch für den Zugriff auf andere Ressourcen innerhalb wie außerhalb des Unternehmens verwendet werden können.

Hacker kennen die menschlichen Schwächen der Benutzer (wie zum Beispiel die Wahl eines einzigen Kennworts für mehrere Accounts) und machen sich diese zunutze, um sich Zugang zu sensiblen Informationen zu beschaffen. Solche Angriffsmethoden werden kollektiv als „Social Engineering“-Angriffe bezeichnet. Im schlimmsten Fall kann ein Hacker sich Zugang zu einem Benutzerkonto auf Systemebene verschaffen und nutzt dieses dann dazu, ein neues Konto anzulegen, das er jederzeit für erneute Zugriffe auf das Netzwerk und dessen Ressourcen nutzen kann.

So wehrt man Packet Sniffer ab

Die erste Verteidigungsmethode gegen Packet Sniffer besteht in einer strengen Authentifizierung.

Der Begriff „strenge Authentifizierung“ bezeichnet im weitesten Sinne eine Methode zur Benutzerauthentifizierung, die nicht problemlos unterlaufen werden kann. Als ein Beispiel für häufig angewandte strenge Authentifizierung ist die Verwendung von Einmalkennwörtern (OTP) zu nennen. Bei OTP handelt es sich um eine Art von Zwei-Faktoren-Authentifizierung. Die Zwei-Faktoren-Authentifizierung umfasst die Kombination eines bekannten Elements mit einem anderen Element. Zum Beispiel kommt eine solche Zwei-Faktoren-Authentifizierung bei Geldautomaten zum Einsatz. Jeder Kunde benötigt zur Tätigung von Transaktionen sowohl seine Karte als auch seine PIN. Bei OTP benötigt der Benutzer eine PIN sowie seine Token Card, um sich gegenüber einem Gerät oder einer Softwareapplikation auszuweisen.

Bei einer Token Card handelt es sich um eine Hardware- oder Softwarekomponente, die in festgelegten Intervallen (in der Regel 60 Sekunden) scheinbar zufällige neue Kennwörter generiert. Dieses zufällige Kennwort kombiniert der Benutzer mit seiner PIN und erhält so ein eindeutiges Kennwort, das nur für eine einzige Authentifizierung gilt. Gelingt es einem Hacker, dieses Kennwort mittels eines Packet Sniffers auszuspionieren, ist diese Information nutzlos für ihn, denn das Kennwort ist zu diesem Zeitpunkt bereits nicht mehr gültig. Es ist allerdings zu beachten, dass diese Abwehrtechnik nur bei Sniffen von Nutzen ist, die auf das Ausspionieren von Kennwörtern ausgerichtet sind. Bei Sniffen, die darauf ausgelegt sind, sensible Informationen auszuspionieren (wie zum Beispiel E-Mail-Nachrichten), wirkt diese Methode hingegen nicht.

Als weitere Methode zur Abwehr von Packet Sniffen, bietet sich der Einsatz einer gewichteten Infrastruktur an.

Würde zum Beispiel ein Unternehmen vollständig mit gewichteten Ethernet arbeiten, könnte ein Hacker nur den Datenverkehrsfluss an dem einen Port, mit dem er verbunden ist, sehen. Natürlich lässt sich damit die Bedrohung durch Packet Sniffer nicht vollständig aus der Welt schaffen, ihre Effizienz kann jedoch erheblich eingeschränkt werden.

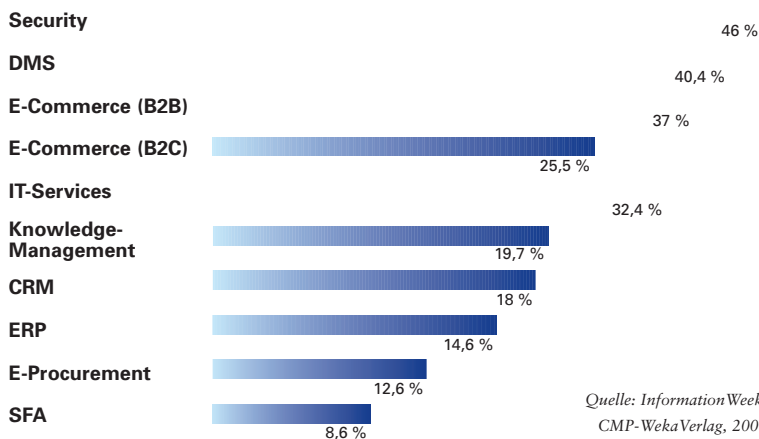
Die dritte Methode zur Abwehr von Sniffen besteht darin, spezielle Software und Hardware einzusetzen, die auf die Erkennung von Packet Sniffen in einem Netzwerk ausgelegt ist. Solche Software und Hardware ist zwar keineswegs dafür geeignet, die Bedrohung vollständig zu beseitigen, stellt jedoch wie viele andere Tools in der Netzwerksicherheit auch einen nützlichen Bestandteil des gesamten Systems dar. Diese so genannten „Anti-Sniffer“ erkennen Veränderungen in der Antwortzeit von Hosts und können so ermitteln, ob diese mehr als ihren eigenen Datenverkehr verarbeiten. Ein solches Tool bietet zum Beispiel L0pht unter dem Namen Antisniff an.

Weitere Information hierzu finden Sie unter: <http://www.l0pht.com/antisniff/>

Bei der letzten und effektivsten Methode werden Packet Sniffer nicht unterbunden oder erkannt, sondern einfach überflüssig gemacht. Ist ein Kommunikationskanal kryptografisch gesichert, sieht ein Packet Sniffer lediglich den verschlüsselten Text (also eine scheinbar willkürliche Bitfolge), nicht aber die Originalmitteilung. Die von Cisco angewandte Kryptografie auf Netzwerkebene basiert auf IPSec (IP Security). Bei IPSec handelt es sich um eine Standardmethode, anhand derer Netzwerkgeräte über das IP-Protokoll vertraulich kommunizieren können. Als weitere kryptografische Protokolle für das Netzwerkmanagement werden unter anderem Secure Shell (SSH) und Secure Sockets Layer (SSL) eingesetzt.

**„Die beste Methode:
Kommunikationskanäle
kryptografisch sichern.“**

In welche Bereiche werden Sie im kommenden Jahr mehr investieren als zuvor?



Mehr Budget für mehr Sicherheit

Die Sicherheit der Daten im Internet ist heute eines der wichtigsten Themen im IT-Bereich und inzwischen zur „Chefsache“ geworden. Spätestens seit jenen globalen Hacker-Attacken, bei denen das „I love you“-Virus zweifelhaft Berühmtheit erlangte, ist jedem klar geworden, wie wichtig ein wirksamer Schutz der Daten ist. So ist es nicht verwunderlich, dass die Investitionen von Unternehmen in Sicherheitsmaßnahmen ihrer Datennetze noch stärker steigen als beispielsweise die für die Entwicklung und den Einsatz von Web-Technologien und für E-Commerce. Fast die Hälfte der Unternehmen haben ihr Budget für den IT-Bereich in diesem Jahr um rund 30 Prozent erhöht, der Löwenanteil hiervon wird für Datensicherheit ausgegeben.

Maskenspiel: IP-Spoofing



„Werden **Routing-Tabellen** in bestimmter Weise **verändert**, erhält der **Hacker Zugriff** auf **vertrauliche Daten** des Benutzers.“

Beim IP-Spoofing-Angriff gibt sich ein Hacker innerhalb oder außerhalb eines Netzwerks als Computer aus, zu dem ein Vertrauensverhältnis besteht. Dabei hat er zwei Möglichkeiten: Entweder verwendet er eine IP-Adresse innerhalb des Bereichs vertrauenswürdiger IP-Adressen für ein Netzwerk oder eine externe IP-Adresse, die vertrauenswürdig ist und Zugriff auf bestimmte Ressourcen eines Netzwerks hat. IP-Spoofing-Angriffe sind häufig nur ein erster Schritt, um den Weg für weitere Angriffe vorzubereiten. Als klassisches Beispiel sind hierbei DoS-Angriffe zu nennen, in denen gespoofte Absenderadressen verwendet werden, um die Identität des Hackers nicht preiszugeben.

Normalerweise beschränkt sich ein Hacker bei einem IP-Spoofing-Angriff darauf, schädliche Daten oder Befehle in einen bestehenden Datenstrom zwischen einer Client- und einer Server-Applikation oder in eine Peer-to-peer-Netzwerkverbindung einzubringen. Damit eine bidirektionale Kommunikation möglich wird, muss der Hacker alle Routing-Tabellen so ändern, dass diese auf die gespoofte IP-Adresse verweisen. Vielleicht legt der Hacker aber auch gar keinen Wert darauf, Antworten von den Applikationen zu erhalten. Versucht der Hacker nämlich, ein System dazu zu veranlassen, ihm per E-Mail eine vertrauliche Datei zu senden, sind die Antworten von den Applikationen uninteressant.

Wenn es dem Hacker allerdings gelingt, die Routing-Tabellen so zu ändern, dass sie auf die gespoofte IP-Adresse verweisen, erhält er alle Netzwerkpakete, die an die gespoofte

Adresse gerichtet sind, und kann ebenso wie jeder vertrauenswürdige Benutzer antworten.

Mit Hilfe der nachfolgend genannten Maßnahmen kann die Bedrohung, die von IP-Spoofing-Angriffen ausgeht, zwar eingeschränkt, nicht jedoch völlig ausgeschaltet werden.

Was man gegen IP-Spoofing tun kann

Die am weitesten häufigsten verwendete Methode zur Abwehr von IP-Spoofing-Angriffen besteht darin, die Zugangskontrolle entsprechend zu konfigurieren.

IP-Spoofing-Angriffen kann etwas von ihrer Effektivität genommen werden. Dazu muss die Zugangskontrolle so konfiguriert werden, dass kein Datenverkehr aus dem externen Netzwerk zugelassen wird, wenn dessen Absenderadresse sich eigentlich im internen Netzwerk befinden sollte. Zu beachten ist jedoch, dass sich auf diese Weise Spoofing-Angriffe nur verhindern lassen, wenn ausschließlich die internen Adressen als vertrauenswürdige Adressen gelten. Sind hingegen auch einige externe Adressen vertrauenswürdig, greift diese Methode nicht.

Man sollte auch verhindern, dass Benutzer eines Netzwerks Spoofing-Angriffe auf andere Netzwerke fahren, indem man jeden abgehenden Datenverkehr, dessen Absenderadresse nicht innerhalb des IP-Bereichs des Unternehmens liegt, abfängt.

Diese Art der Filterung, die allgemein als Filterung nach RFC 2827 bezeichnet wird, kann auch durch den ISP implementiert werden.

Schwer zu unterbinden: Denial-of-Service

Durch diese Filterung wird Datenverkehr unterbunden, der nicht die an einer bestimmten Schnittstelle erwartete Absenderadresse aufweist. Wenn zum Beispiel ein ISP eine Verbindung zum Netz 15.1.1.0/24 bereitstellt, kann der ISP den Datenverkehr so filtern, dass von dieser Schnittstelle aus auch nur Datenverkehr mit dem Adressbereich 15.1.1.0/24 zum ISP-Router gelangen kann.

An dieser Stelle muss darauf hingewiesen werden, dass diese Filterung nur wirklich effektiv ist, wenn sie von allen ISPs implementiert wird. Zudem wird es immer schwieriger, eine differenzierte Filterung durchzuführen, je größer der Abstand zu den zu filternden Geräten ist. So wäre es beispielsweise für eine Filterung nach RFC 2827 am Access-Router zum Internet erforderlich, das gesamte Netzwerk (in diesem Fall das gesamte Klasse-A-Netzwerk, d. h. 10.0.0.0/8) den Access-Router passieren zu lassen. Wird die Filterung in der Verteilungsschicht vorgenommen, wie es in dieser Architektur der Fall ist, ist eine spezifische Filterung möglich (d. h. 10.1.5.0/24).

Die effektivste Methode zur Abwehr von IP-Spoofing-Angriffen ist genau die Methode, die auch zur Abwehr von Packet Sniffen die beste ist. Dabei geht es nicht darum, IP-Spoofing völlig zu unterbinden, sondern den Angriffen ihre Wirksamkeit zu nehmen. Das IP-Spoofing funktioniert nur dann richtig, wenn die Geräte mit einer Authentifizierungsmethode arbeiten, die auf IP-Adressen basiert. Kommen nun zusätzliche Authentifizierungsmethoden zum Einsatz, sind IP-Spoofing-Angriffe nutzlos. Die beste zusätzliche Authentifizierungsmethode besteht in der kryptografischen Authentifizierung. Ist diese jedoch nicht möglich, kann auch eine strenge Zwei-Faktoren-Authentifizierung durch die Verwendung von OTP sehr effektiv sein.

Die bekanntesten Angriffe: Denial-of-Service

Denial-of-Service-Angriffe (DoS) sind die bekannteste Angriffsform. Und sie sind auch am schwierigsten vollständig zu unterbinden. Selbst in Hackerkreisen gelten DoS-Angriffe als trivial und ungenügend, da ihre Ausführung mit so wenig Anstrengung verbunden ist.

Und doch sollte der Sicherheitsadministrator DoS-Angriffen besondere Aufmerksamkeit schenken, gerade weil sie so leicht auszuführen sind und dabei großen Schaden anrichten können.

Wer sich eingehender über DoS-Angriffe informieren möchten, sollte die Methoden kennen, die bei einigen der bekannteren Angriffsformen angewandt werden. Hierzu zählen:

- TCP SYN Flood
- Ping of Death
- Tribe Flood Network (TFN) und Tribe Flood Network 2000 (TFN2K)
- Trinoo
- Stacheldraht
- Trinity

Eine hilfreiche Informationsquelle zu allen Aspekten der Sicherheit ist das Computer Emergency Response Team (CERT). Dieses Team hat ein sehr informatives Dokument zur Reaktion auf DoS-Angriffe veröffentlicht.

Das Dokument ist zu finden unter: http://www.cert.org/tech_tips/denial_of_service.html



„Auch bei **Spoofing** gilt: Die beste **Abwehrmethode** besteht in einer **kryptografischen** oder einer **strengen Zwei-Faktoren-Authentifizierung**.“

„Zwingt jedes Netzwerk in die Knie: Angriffe durch Überflutung mit nutzlosen Netzwerkpaketen.“

DoS-Angriffe unterscheiden sich insofern von den meisten anderen Angriffsarten, als sie in der Regel nicht darauf abzielen, dem Hacker Zugang zum Netzwerk oder den darin enthaltenen Daten zu verschaffen. Vielmehr besteht ihr einziger Zweck darin, einen Dienst für den normalen Gebrauch unbenutzbar zu machen. Und dies geschieht in der Regel dadurch, dass eine begrenzte Ressource im Netzwerk oder innerhalb eines Betriebssystems oder einer Applikation erschöpft wird.

Sind bestimmte Netzwerkserverserverapplikationen betroffen, z. B. ein Webserver oder ein FTP-Server, können solche Angriffe darauf abzielen, alle durch den betreffenden Server unterstützten verfügbaren Verbindungen zu belegen und offen zu halten, wodurch dann die regulären Benutzer des Servers bzw. Dienstes nicht mehr zugreifen können.

DoS-Angriffe können auch mittels häufig verwendeter Internetprotokolle wie TCP und Internet Control Message Protocol (ICMP) ausgeführt werden. Bei den meisten DoS-Angriffen macht der Hacker sich eine Schwachstelle in der Gesamtarchitektur des betroffenen Systems, nicht jedoch einen

Softwarebug oder eine Sicherheitslücke zunutze. Manche Angriffe führen jedoch zu einer Reduzierung der Netzwerkleistung, indem das Netzwerk mit unerwünschten und in vielen Fällen nutzlosen Netzwerkpaketen überflutet wird und falsche Informationen über den Status der Netzwerkressourcen ausgegeben werden.

Angriffe dieser Art sind häufig besonders schwierig zu verhindern, da hierzu eine Zusammenarbeit mit dem vom Unternehmen aus nächsten Netzwerkanbieter in Richtung Internet erforderlich ist. Wenn nicht jeder Datenverkehr, der darauf abzielt, die gesamte verfügbare Bandbreite einzunehmen, hier bereits aufgehalten wird, ist es auch wenig effektiv, ihn am Zugangspunkt zu Ihrem Netzwerk abzufangen, denn zu diesem Zeitpunkt ist die verfügbare Bandbreite dann bereits aufgebraucht. Ein Angriff dieser Art, der von vielen verschiedenen Systemen gleichzeitig gestartet wird, wird häufig als Distributed-Denial-of-Service-Angriff (DDoS) bezeichnet.

Die Bedrohung durch Denial-of-Service-Angriffe kann mit folgenden Methoden abgeschwächt werden: An erster Stelle bei der Angriffsabwehr steht eine korrekte Konfiguration der Anti-Spoofing-Funktionen von Routern und Firewalls. Hierzu zählt mindestens die Filterung nach RFC 2827. Wenn nämlich ein Hacker seine Identität nicht geheim halten kann, sieht er möglicherweise von einem Angriff ab.

Zum zweiten kann eine korrekte Konfiguration der Anti-DoS-Funktionen von Routern und Firewalls dazu beitragen, Angriffen ihre Effektivität zu nehmen. Zu diesen Funktionen zählt in vielen Fällen eine Beschränkung der Anzahl halboffener Verbindungen, deren Öffnung ein System jeweils zulässt.

Weitergehenden Schutz kann eine integrierte Intrusion Detection Funktionalität auf Routern und Firewalls bieten. Cisco Systems bietet hier eine breite Implementation auf verschiedensten Komponenten und kann somit eine ausgefeilte Lösung für die Abwehr von DoS-Angriffen realisieren.

Und drittens kann ein Unternehmen in Zusammenarbeit mit dem jeweiligen ISP eine Ratenbegrenzung für den Datenverkehr implementieren. Durch diese Art der Filterung kann der Umfang von nicht wesentlichem Verkehr, der Netzwerksegmente passiert, auf eine bestimmte Rate begrenzt werden. Häufig wird in einem solchen Szenario der Umfang des in die Umgebung eingelassenen ICMP-Datenverkehrs begrenzt, da dieser ausschließlich zu Diagnosezwecken dient. ICMP-basierte (D)DoS-Angriffe sind an der Tagesordnung.

„Schutz vor DoS-Angriffen bietet eine in Routern und Firewalls integrierte Intrusion Detection.“

Mit der Brechstange: Kennwortangriffe

Kennwortangriffe variieren

Kennwortangriffe können mit den unterschiedlichsten Methoden ausgeführt werden. Hierzu zählen Brute-Force-Angriffe, Trojanische Pferde, IP-Spoofing und Packet Sniffer. Beim Einsatz von Packet Sniffern und IP-Spoofing können zwar Benutzerkonten und Kennwörter ausspioniert werden. Bei den eigentlichen Kennwortangriffen werden jedoch meist wiederholte Versuche unternommen, ein Benutzerkonto und/oder Kennwort auszuspionieren. Diese wiederholten Versuche werden als Brute-Force-Angriffe bezeichnet.

Häufig verwenden Hacker für Brute-Force-Angriffe ein Programm, das das Netzwerk durchläuft und versucht, sich an einer gemeinsam genutzten Ressource wie einem Server anzumelden. Gelingt es einem Hacker, sich Zugang zu einer Ressource zu verschaffen, hat er dieselben Rechte wie der Benutzer, dessen Account er ausspioniert hat, um auf die jeweilige Ressource zuzugreifen. Und wenn das betreffende Konto auch noch über ausreichende Berechtigungen verfügt, kann der Hacker sich ein Hintertürchen öffnen, durch das er jederzeit wieder eindringen kann, ohne sich über Status- und Kennwortänderungen des kompromittierten Benutzeraccounts Gedanken machen zu müssen.

Ein weiteres Problem liegt darin, dass Benutzer häufig dasselbe (möglicherweise strenge) Kennwort für jedes System verwenden, zu dem sie eine Verbindung herstellen. Bei diesen Systemen handelt es sich in vielen Fällen um per-

sönliche Systeme, unternehmenseigene Systeme und Systeme im Internet. Da jedes Kennwort nur so sicher ist wie der am schwächsten gesicherte Host, auf dem es abgelegt ist, eröffnen sich einem Hacker, der diesen Host kompromittiert, zahlreiche Möglichkeiten, dasselbe Kennwort auch an anderen Hosts auszuprobieren.

Kennwortangriffe lassen sich am einfachsten unterbinden, indem grundsätzlich keine Kennwörter verwendet werden, die nur aus Text bestehen. Durch die Verwendung von OTP und/oder kryptografischer Authentifizierung können Kennwortangriffe beinahe gänzlich verhindert werden.

Leider werden diese Authentifizierungsmethoden nicht von allen Applikationen, Hosts und Geräten unterstützt. Wenn Standardkennwörter verwendet werden müssen, muss auf alle Fälle darauf geachtet werden, dass das gewählte Kennwort schwierig zu erraten ist. Idealerweise sollten Kennwörter mindestens acht Zeichen lang sein und aus einer Kombination aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen (#%\$ usw.) bestehen. Optimale Kennwörter werden nach dem Zufallsprinzip erzeugt. In diesem Fall sind sie jedoch schwer zu behalten, wodurch Benutzer häufig dazu verleitet werden, ihr Kennwort irgendwo zu notieren.



**„Sicheres Mittel gegen
Passwortattacken:
Kryptografische
Authentifizierung.“**

Angriff über Mittelsmänner



„Auch **Mann-in-der-Mitte-Angriffe** lassen sich nur durch **kryptografische Sicherung abwehren.**“

Es wurden bereits diverse Anstrengungen unternommen, um sowohl Benutzern als auch Administratoren die Verwaltung von Kennwörtern zu erleichtern. So gibt es beispielsweise heutzutage Applikationen, mit denen eine Kennwortliste verschlüsselt und anschließend auf einem Handheld-computer gespeichert werden kann. Auf diese Weise muss sich der Benutzer nur noch ein kompliziertes Kennwort merken, während die übrigen Kennwörter sicher in der Applikation gespeichert sind.

Für Administratoren gibt es verschiedene Methoden, die Kennwörter der eigenen Benutzer im Brute-Force-Verfahren anzugreifen. Dazu gibt es beispielsweise ein auch in Hackerkreisen beliebtes Tool mit dem Namen „L0phtCrack“. L0phtCrack führt Brute-Force-Angriffe auf NT-Kennwörter aus und zeigt an, wenn ein Benutzer ein sehr leicht zu erratendes Kennwort gewählt hat.

Weitere Informationen hierzu erhalten Sie unter <http://www.l0pht.com/l0phtcrack/>.

„Mann-in-der-Mitte“-Angriffe („Man-in-the-Middle“)

Voraussetzung für einen „Mann-in-der-Mitte“-Angriff ist, dass der Hacker Zugriff auf Netzwerkpakete hat, die über ein Netzwerk versendet werden. Bei einem „Mann-in-der-Mitte“ kann es sich z. B. um einen Mitarbeiter eines ISP handeln, der Zugriff auf sämtliche zwischen dem Netzwerk seines Arbeitgebers und anderen Netzwerken versendeten Netzwerkpakete hat.

Solche Angriffe erfolgen oftmals unter Verwendung von Netzwerk-Packet Sniffern sowie Routing- und Transportprotokollen. Sinn und Zweck solcher Angriffe:

- Informationsdiebstahl
- Entführung laufender Sessions, um Zugriff auf private Netzwerkressourcen zu bekommen.
- Datenverkehrsanalysen, um Informationen über ein Netzwerk und dessen Benutzern zu erhalten.
- Verfälschung übermittelter Daten und Einbringen neuer Informationen in Netzwerksitzungen.

Das einzig wirksame Mittel gegen „Mann-in-der-Mitte“-Angriffe ist die Kryptografie. Wenn ein Hacker Daten aus einer kryptografisch gesicherten Sitzung entführt, kann er lediglich den verschlüsselten Text, nicht aber die Originalmitteilung lesen. Sind dem Hacker jedoch Informationen zu der kryptografischen Sitzung (wie z. B. der Sitzungsschlüssel) bekannt, kann er nach wie vor „Mann-in-der-Mitte“-Angriffe fahren.

Angriffe in der Anwendungsschicht

Angriffe in der Anwendungsschicht können auf unterschiedliche Art und Weise erfolgen. Am häufigsten werden die allgemein bekannten Schwachstellen von Software ausgenutzt, die auf Servern oftmals zum Einsatz kommt, so z. B. sendmail, HTTP und FTP. Durch Ausnutzung dieser Schwachstellen erhalten Hacker Zugriff auf einen Computer und zwar mit den Berechtigungen des Benutzers, der die Applikation ausführt. Dabei handelt es sich in der Regel um ein mit weit reichenden Berechtigungen ausgestattetes Konto der Systemebene.

Solche Angriffe in der Anwendungsschicht werden oft bekannt gemacht, damit Administratoren die Möglichkeit haben, dem Problem mittels eines Patches entgegenzuwirken. Allerdings abonnieren auch viele Hacker die entsprechenden Mailinglisten. So erfahren sie natürlich zur gleichen Zeit von dem Angriff (wenn er ihnen nicht ohnehin schon bekannt ist).

Das Hauptproblem bei Angriffen in der Anwendungsschicht besteht darin, dass bei den Angriffen oftmals Ports verwendet werden, die eine Firewall durchaus zulässt. Ein Hacker, der eine ihm bekannte Schwachstelle für einen Angriff auf einen Webserver ausnutzt, verwendet für seinen Angriff z. B. gemeinhin TCP-Port 80.

Und da der Webserver Benutzern Seiten zur Verfügung stellt, muss eine Firewall den Zugriff auf diesen Port zulassen. Aus Sicht der Firewall handelt es sich ja lediglich um ganz normalen Datenverkehr an Port 80.

Daher können Angriffe in der Anwendungsschicht niemals ganz ausgeschlossen werden. Es werden ständig neue Schwachstellen entdeckt und in der Internetgemeinde bekannt gemacht. Die Risiken lassen sich am besten durch eine effiziente Systemadministration verringern. Die folgenden Punkte sollten immer beachtet werden:

- Lesen Sie die Betriebssystem- und Netzwerkprotokolldateien und/oder lassen Sie diese von Applikationen zur Protokollanalyse untersuchen.
- Abonnieren Sie die Mailinglisten, in denen Schwachstellen bekannt gemacht werden, so z. B. Bugtraq (<http://www.securityfocus.com>) und CERT (<http://www.cert.org>).
- Halten Sie das Betriebssystem und die Applikationen immer mit den aktuellen Patches auf dem neuesten Stand.

Angriffe frühzeitig erkennen

„Vor **Netzwerk-
erkundungen** kann
man sich **nicht
völlig schützen.**“



Intrusion Detection System (IDS)

Neben einer effizienten Systemadministration kann auch die Verwendung von Intrusion Detection Systemen (IDS) sehr hilfreich sein.

Es gibt zwei sich ergänzende IDS-Technologien. Das netzwerkbasierte ID-System (NIDS) überwacht alle Pakete, die eine bestimmte Collision Domain durchlaufen. Sobald das NIDS ein Paket bzw. eine ganze Reihe von Paketen erkennt, die das Muster eines bekannten Angriffs aufweisen oder die Vermutung nahe legen, dass es sich um einen Angriff handelt, wird ein Alarm ausgegeben und/oder die Sitzung beendet.

Das Host-basierte ID-System (HIDS) platziert Agenten in dem zu schützenden Host. Diese Technologie greift erst dann, wenn ein Angriff gegen diesen einen Host erfolgt. ID-Systeme arbeiten unter Verwendung von Angriffssignaturen. Bei Angriffssignaturen handelt es sich um die für einen bestimmten Angriff oder eine bestimmte Art von Angriff typischen Muster. Diese Signaturen definieren bestimmte Bedingungen, die erfüllt sein müssen, bevor Datenverkehr als Angriff definiert wird. Ein ID-System kann gut mit einer Alarmanlage oder einer Überwachungskamera in der realen Welt verglichen werden. Doch auch ID-Systeme stoßen an ihre Grenzen. Das lässt sich an der Zahl der Fehlalarme, die ein bestimmtes System erzeugt, erkennen. Damit ein ID-System in einem Netzwerk keine Fehlalarme ausgibt, ist eine Feineinstellung des Systems unerlässlich.

Geht einem Angriff oft voraus: Netzwerkerkundung

Unter Netzwerkerkundung versteht man grundsätzlich das Sammeln von Informationen über ein Zielnetzwerk unter Verwendung allgemein erhältlicher Informationen und Applikationen. Unternimmt ein Hacker den Versuch, in ein bestimmtes Netzwerk einzudringen, muss er in der Regel zunächst alles Wissenswerte über dieses Netzwerk in Erfahrung bringen, bevor er seinen Angriff starten kann. Dies geschieht in der Regel in Form von DNS-Abfragen, Ping-Sweeps und Port-Scanning. Mittels DNS-Abfragen erhält der Hacker z. B. Informationen zu dem Eigentümer einer bestimmten Domäne und darüber, welche Adressen dieser Domäne zugewiesen wurden. Werden auf den durch die DNS-Abfrage ermittelten Adressen Ping-Sweeps durchgeführt, bietet sich dem Hacker ein Bild der aktiven Hosts in einer bestimmten Umgebung.

Nach der Erstellung einer solchen Liste können mit Hilfe von Port-Scanning-Tools alle bekannten Ports durchsucht werden. Das Ergebnis ist eine Liste sämtlicher Dienste, die auf den durch den Ping-Sweep gefundenen Hosts ausgeführt werden. Und dann kann der Hacker auch noch die Charakteristika der Applikationen, die auf den Hosts ausgeführt werden, untersuchen. Der Hacker erhält auf diese Weise spezielle Informationen, die hilfreich sein können, wenn er diesen Dienst ausnutzen will.

Vor Netzwerkerkundungen kann man sich nicht völlig schützen. Wenn auf Edge-Routern z. B. ICMP Echo und Echo Reply deaktiviert werden, können Ping-Sweeps zwar gestoppt werden, dies geht jedoch zu Lasten der Daten zur Netzwerkdiagnose. Außerdem können auch ohne vollständige Ping-Sweeps Port-Scanning-Angriffe gestartet werden. Deren Ausführung dauert dann lediglich etwas länger, da auch die IP-Adressen gescannt werden müssen, die nicht aktiv sind.

Netzwerk- und Host-basierte Intrusion Detection Systeme (IDS) setzen einen Administrator in der Regel darüber in Kenntnis, wenn ein Erkundungsangriff gestartet wurde. Dadurch hat der Administrator die Möglichkeit, sich besser auf den bevorstehenden Angriff vorzubereiten bzw. den ISP zu benachrichtigen, bei dem das System gehostet ist, von dem der Erkundungsangriff ausgeht.

Nicht zu verhindern: Vertrauensbruch

Hier kann man nicht von einem Angriff im eigentlichen Sinne sprechen, da der Vertrauensbruch ein Angriff ist, bei dem eine Einzelperson ein Vertrauensverhältnis innerhalb eines Netzwerks ausnutzt. Als klassisches Beispiel dient die Peripherienetzwerkverbindung eines Unternehmens.

Innerhalb dieser Netzwerksegmente befinden sich oftmals DNS-, SMTP- und HTTP-Server. Da diese sich alle in demselben Segment befinden, kann

die Kompromittierung eines dieser Systeme zur Kompromittierung anderer Systeme führen, da möglicherweise eine Vertrauensbeziehung zu anderen in dieses Netzwerk eingebundenen Systemen besteht.

Ein weiteres Beispiel ist ein System außerhalb einer Firewall, das jedoch in einer Vertrauensbeziehung zu einem System innerhalb der Firewall steht. Wird dann das System außerhalb der Firewall kompromittiert, kann das Vertrauensverhältnis für einen Angriff auf das Netzwerk innerhalb der Firewall ausgenutzt werden.

Angriffe, denen ein Vertrauensbruch zugrunde liegt, können durch strenge Beschränkungen der Vertrauensbeziehungen innerhalb eines Netzwerks reduziert werden. Zwischen Systemen außerhalb und innerhalb einer Firewall sollte niemals ein uneingeschränktes Vertrauensverhältnis bestehen. Vertrauensverhältnisse sollten auf bestimmte Protokolle beschränkt werden und wenn möglich immer anhand eines anderen Elements als der IP-Adresse authentifiziert werden.

Erst Vertrauensbruch, dann Portumleitung

Bei der Portumleitung handelt es sich um einen Angriff, dem ein Vertrauensbruch zugrunde liegt. Dabei wird ein kompromittierter Host verwendet, um Daten durch eine Firewall zu transportieren, die sonst zurückgewiesen würden.

Stellen Sie sich eine Firewall mit drei Schnittstellen und einem Host an jeder dieser Schnittstellen vor. Der Host außerhalb der Firewall kann zwar eine Verbindung zu dem Host in dem Segment für öffentliche Services (gemeinhin als demilitarisierte Zone (DMZ) bezeichnet) herstellen, nicht aber zu dem Host innerhalb der Firewall. Der Host in dem Segment für öffentliche Services kann sowohl eine Verbindung zu dem Host außerhalb als auch innerhalb der Firewall aufbauen.

Wenn ein Hacker nun in der Lage ist, den Host in dem Segment für öffentliche Services zu kompromittieren, könnte Software installiert werden, um den Datenverkehr von dem Host außerhalb direkt an den Host innerhalb der Firewall umzuleiten. Obwohl dadurch keine der in der Firewall implementierten Regeln verletzt werden, hat der Host auf der Außenseite nun durch den Prozess der Portumleitung auf dem Host in dem Segment für öffentliche Services eine Verbindung zu dem Host auf der Innenseite aufgenommen. Ein Beispiel für eine Applikation, die diese Art von Zugriff ermöglicht, ist netcat.

Weitere Informationen hierzu erhalten Sie unter: <http://www.avian.org>



„Methoden zur Abwehr nicht autorisierter Zugriffe lassen sich recht einfach umsetzen.“

Angriffe mittels Portumleitung lassen sich – wie bereits erwähnt – in erster Linie durch die Verwendung geeigneter Vertrauensmodelle abwehren.

Auf einem System, auf das ein Angriff ausgeführt wird, kann mittels eines Host-basierten ID-Systems dieser Angriff erkannt und der Hacker davon abgehalten werden, solche Programme auf einem Host zu installieren.

Unberechtigter Zugriff

Ein unberechtigter Zugriff ist keine spezielle Angriffsart. Damit jemand sich mittels des Brute-Force-Verfahrens für eine Telnet-Sitzung anmelden kann, muss zunächst die Telnet-Eingabeaufforderung angezeigt werden. Sobald die Verbindung zu dem Telnet-Port besteht, wird ggf. eine Meldung angezeigt, die besagt, dass für die Verwendung dieser Ressource eine Autorisierung erforderlich ist. Versucht der Hacker nun weiterhin, sich Zugriff zu verschaffen, so sind diese Versuche als „nicht autorisiert“ zu bezeichnen. Diese Art von Angriff kann sowohl von außerhalb als auch von innerhalb eines Netzwerkes erfolgen.

Methoden zur Abwehr derartiger nicht autorisierter Zugriffe lassen sich recht einfach umsetzen. Dazu gehört, dass die Möglichkeiten eines Hackers, sich mittels eines nicht autorisierten Protokolls Zugriff auf ein System zu verschaffen, eingeschränkt bzw. völlig beseitigt werden. So sollten Hacker z. B. nicht die Möglichkeit zum Zugriff auf den Telnet-Port auf einem Server haben, der Webdienste nach außen bereitstellt. Wenn ein Hacker keinen Zugriff auf diesen Port hat, ist die Gefahr eines Angriffs relativ gering.

Die Hauptfunktion einer Firewall in einem Netzwerk besteht in der Abwehr von Angriffen in Form von einfachem, nicht autorisiertem Zugriff.

Die größte Gefahr: Viren und Trojanische Pferde

Angriffe in Form von Viren und Trojanischen Pferden stellen für die Workstations von Endbenutzern die größte Gefahr dar. Bei Viren handelt es sich um eine schädliche Software, die an ein anderes Programm angehängt ist und auf der Workstation des Benutzers eine bestimmte Funktion ausführt. Als Beispiel für einen Virus kann ein an die Datei `command.com` (der wichtigste Interpreter für Windows-Systeme) angehängtes Programm genannt werden. Dieser Virus löscht bestimmte Dateien und infiziert jegliche anderen Versionen der `command.com`, die er finden kann.

Der Unterschied zwischen einem Virus und einem Trojanischen Pferd besteht lediglich darin, dass die gesamte Applikation so geschrieben wurde, dass sie nicht nach einem Angriffstool, sondern nach etwas ganz anderem aussieht.

Als Beispiel für ein Trojanisches Pferd ist eine Softwareapplikation zu nennen, die auf der Workstation des Benutzers ein einfaches Spiel ausführt. Während der Benutzer das Spiel ausprobiert, verschickt das Trojanische Pferd Kopien von sich selbst an jeden Benutzer im Adressbuch des Benutzers. Auf diese Weise erhalten auch andere Benutzer das Spiel und probieren es aus. Und so verbreitet sich das Trojanische Pferd.

Vor dieser von solchen Applikationen ausgehenden Gefahr kann man sich durch den gezielten Einsatz von Antivirenprogrammen auf Benutzer- und

Sicherheitskomponenten von Cisco

eventuell auf Netzwerkebene effizient schützen. Antivirenprogramme sind in der Lage, die meisten Viren und viele Trojanische Pferde zu erkennen, so dass sie nicht weiter über das Netzwerk verbreitet werden können. Dabei ist ein wirklich effektiver Schutz nur gewährleistet, wenn die Virenprogramme stets mit den neuen Virendefinitionen aktualisiert werden. Unternehmen sollten also immer mit der aktuellen Version eines Antivirenprogramms ausgerüstet sein, da täglich neue Viren oder Trojanische Pferde in Umlauf kommen.

Cisco bietet je nach Unternehmensgröße und individuellen Anforderungen eine Reihe von Produkten, um Netzwerke zu schützen und Daten sicher zu übertragen. Darüber hinaus gibt es die Möglichkeit, das Netz und alle angeschlossenen Geräte aktiv zu

überwachen. Die hier beschriebenen Komponenten finden in verschiedenen Bereichen der Safe-Architektur Verwendung. Hier werden grundlegende Eigenschaften der Sicherheitsprodukte von Cisco Systems erläutert. Für die spezielle Anwendung der Komponenten stellt Safe eine Richtlinie dar, die gleichzeitig alle Schritte der Planung, des Aufbaus und der Konfiguration der einzelnen Geräte beschreibt.

Firewalls

Firewalls verhindern den unbefugten Zugriff auf Daten über das Internet – aber auch von intern. Man kann Firewalls mittels Hardware- und Softwarelösungen einrichten. Deshalb bietet Cisco zwei Produktfamilien für die Sicherheit von Daten.

Cisco IOS Firewall

Die Cisco IOS Firewall setzt auf dem IOS (Internet Operating System) von Cisco auf und bietet Schutzfunktionen für alle Schnittstellen nach außen, die ein Netzwerk benötigt. Sie ergänzt das IOS um Sicherheitsfunktionen wie z. B. das Erstellen von Zugangslisten pro Anwender und dazugehörige Applikationen, das Abblocken von unbekanntem Java-Applets sowie dynamische Authentifizierung und Autorisierung – ebenfalls pro Benutzer. Sogenannte Denial-of-Services Angriffe, bei denen in kurzer Zeit Router oder andere Netzwerksysteme lahmgelegt werden können, werden erkannt und verhindert. Attackieren Angreifer die Firewall, wird ein Echtzeitalarm ausgelöst und der Administrator benachrichtigt. Zusammen mit IPsec kann eine komplette VPN-Lösung realisiert werden.



Wichtig: Skalierbarkeit und Flexibilität



Cisco 800er Router



Cisco 1700er Router

Die Skalierbarkeit der Cisco IOS Firewall erlaubt die Kombination mit nahezu jedem Router von Cisco Systems. Je nach Anforderung findet jeder auf den folgenden Seiten die richtige Sicherheitslösung.

Informationen zum Thema IOS-Firewall finden Sie unter:

<http://www.cisco.com/warp/public/cc/pd/iosw/ioft/iowfwt/>

- Für kleine Firmen und Home Offices: Router der Serien 800 und 1700

Cisco 800

Der kleinste und kostengünstigste Cisco IOS-basierte-Router. Innerhalb dieser einfach und schnell zu konfigurierenden Serie gibt es für den Einsatz im SOHO-Bereich und für Telecomputer größerer Unternehmen folgende Modelle:

Den Cisco 801 mit einer Ethernet- und einer ISDN-Schnittstelle, den 803 mit einem eingebauten 4-Port-10BaseT-Mini-Hub, zwei a/b-Analog-Ports sowie einer ISDN-Schnittstelle, den 805 mit einem Ethernet und einem seriellen Interface sowie den 806 mit zwei eingebauten 10BaseT-Ethernet-Schnittstellen (inkl. PPPoE-Unterstützung für den Anschluss an ADSL-Modems). Alle Geräte verfügen über einen sehr schnellen RISC-Prozessor, so dass die möglichen Firewall- und Verschlüsselungs-Features genügend Systemleistung zur Verfügung haben.

Weiterführende Informationen unter:
<http://www.cisco.com/go/800>

Cisco 1700

Die modularen Router der Cisco 1700 Serie verfügen alle über eine 10/100 Ethernet LAN-Schnittstelle sowie einen internen Steckplatz zur Hardware-Beschleunigung der Daten-Verschlüsselung. Ein leistungsfähiger RISC-Prozessor sorgt schon in der Grundversion für viel Leistung für Firewall-, Verschlüsselungs- und Intrusion-Detection-Funktionen, die über spezielle IOS-Software ermöglicht werden. Das Modell 1720 verfügt über zwei Schächte für Daten-Module, sogenannte WAN-Interface-Cards (kurz WIC genannt), beispielsweise für ISDN, ein- oder zweifach seriell (synchron und asynchron), ADSL und 10BaseT-Ethernet. Das Modell 1751 hat drei Schächte für Sprach- und Datenmodule. Ein Slot ist dediziert für Sprachmodule – kurz VIC oder Voice Interface Card – ein weiterer dediziert für WIC-Module, und ein dritter kann WIC- oder VIC-Module aufnehmen. Beide Modelle unterstützen analoge VICs (FXS, FXO, E&M), der 1751 zusätzlich ein ISDN-VIC. Damit eignen sich die Cisco-Router der 1700er Serie hervorragend für kleine Außenstellen oder die Zentralen kleinerer Unternehmen – auch hinsichtlich der benötigten Sicherheitsfunktionen. Das Modell 1751 ermöglicht über die Unterstützung der Sprach-/ Datenintegration Gateway-Funktionen für VoIP (Voice-over-IP) und IP Telephonie.

Weiterführende Informationen unter:
<http://www.cisco.com/go/1700>

Für Niederlassungen und Firmenzentralen: Router der Serien Cisco 2600 und 3600

Cisco 2600/ 2600 XM

Diesen universell einsetzbaren modularen Router gibt es mittlerweile in 8(!) Basiskonfigurationen: Modelle mit einem oder zwei 10BaseT-Ethernet-Interfaces (2610, 2611), einem oder zwei 10/100-Ethernet-Schnittstellen (2620/21, 2650/51 – leistungsgesteigert) oder mit eingebautem TokenRing-Interface (2613) sowie ein Modell mit integrierter TokenRing- und 10BaseT-Ethernet-Schnittstelle (2612). Alle Systeme lassen sich über drei Modul-Einschub-Schächte erweitern.

Ein Schacht ist für sogenannten Netzwerk-Module, zwei für die aus der 1700er Serie bekannten WIC-Module. Weiterhin können die Router der 2600er Serie über einen internen Steckplatz um ein sogenanntes AIM (Advance Integration Module) erweitert werden. Es gibt AIMS für Datenkompression und eines für die Datenverschlüsselung. Mit diesen Modulen kann man die bereits in IOS integrierten Kompressions- und Verschlüsselungs-Funktionen per Hardware beschleunigen. Aus der großen Vielfalt der Netzwerk-Module seien hier nur einige genannt: Voice-Module für die Integration von zwei bis sechzig Sprachkanälen, Module für den Anschluss von bis zu zwei Daten-Primärmultiplex-Anschlüssen (bis zu 60 ISDN-B-Kanäle bzw. zwei S2M-Leitungen pro Modul), Ethernet-Module, Module mit asynchron und synchron-seriellen Anschlüssen, Modem-Module und vieles mehr. Über IOS lassen sich Firewall-, Verschlüsselungs- und Intrusion-Detection-Funktionen realisieren. Einzigartig ist auch die SRST-Funktion (Survivable Remote Site Telephony), die Außenstellen, die per Standleitung auf einen zentralen

Call-Manager verbunden sind, bei einem Ausfall der Standleitung den unterbrechungsfreien Betrieb der IP Telephonie ermöglicht.

Weiterführende Informationen:

<http://www.cisco.com/go/2600>

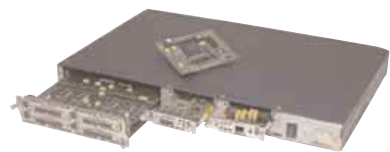
Cisco 3600/ 3700

Die Modularität und Vielfalt verfügbarer Erweiterungen ermöglichen eine breite Anwendungspalette (mehrere 1000 verschiedene Kombinationen sind möglich) innerhalb des Router-Angebots. Es gibt Modelle mit zwei (3620), vier (3640) und sechs (3660) Modulschächten. Die Modulschächte nehmen die bereits aus der 2600er Serie bekannten Netzwerkmodule auf. Sogenannte mixed WAN/LAN-Module kombinieren LAN-Schnittstellen wie Ethernet oder Fast Ethernet bzw. TokenRing mit WAN-Einschüben für WICs in einem Modul. Die 3600er Serie – ein wahrer Verwandlungskünstler – erfüllt nahezu alle Kundenwünsche. Über digitale Modem-Module und ISDN bzw. Primärmultiplex-Module lassen sich 3600er Router in einen Access-Server verwandeln, die Kompressions- und Verschlüsselungsmodule beschleunigen Software-Funktionen von IOS erheblich. Weiterhin gibt es für den 3600er Software-Features mit Firewall-, Verschlüsselungs- sowie Intrusion-Detection, SRST und Gatekeeper-Funktionalität. Damit ist die Cisco 3600er Router-Serie hervorragend für Unternehmenszentralen oder größere Außenstellen geeignet. Die Cisco 3700 Serie mit den Modellen 3725 und 3745 nutzt die gleichen Module aus der 3600 Serie, aber besticht durch höhere Leistung und zusätzliche Module wie 32 Port 10/100 –Inline Power Switching.

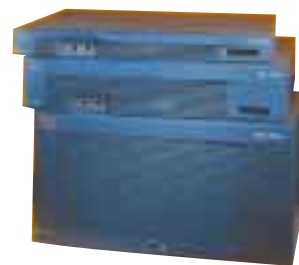
Weiterführende Informationen unter:

<http://www.cisco.com/go/3600>

<http://www.cisco.com/go/3700>



Cisco 2600er Router



Cisco 3600er Router



Cisco Firewall PIX 501



Cisco Firewall PIX 506E

Cisco Secure PIX Firewall Serie

Wird besonderer Wert auf ein dediziertes Firewall-System gelegt oder sind Netze mit Durchsatzraten von mehreren Mbps (Megabit pro Sekunde, z. B. eine Anbindung an ein SDSL- oder Fibre-to-the-Curb-Netz) bis hin zu einem Gbps (Gigabit pro Sekunde) abzusichern, so kommt die Cisco Secure PIX Firewall Produktlinie ins Spiel.

Diese vorinstallierten Systeme besitzen einen äußerst schlanken Betriebssystem-Kern, der höchste Performance bei maximaler Sicherheit ermöglicht. Sie bietet erheblich mehr Leistung und Sicherheit als Software-Lösungen, die auf Standard-Betriebssysteme aufsetzen. So können bis zu 500.000 Verbindungen gleichzeitig, mehr als 6.500 Verbindungen pro Sekunde auf- und abgebaut und bis zu 1.000 Mbps Durchsatzrate erreicht werden. Damit zählt die Secure PIX Firewall zu den leistungsfähigsten Systemen auf dem Markt. Derzeit gibt es fünf verschiedene Systeme, die PIX 501 mit einem integrierten 4-Port 10/100

Switch und einem Durchsatz von etwa 11 Mbit/s, die PIX 506 mit zwei 10BaseT-Ethernet-Interfaces und einem Durchsatz von bis zu 25 Mbit/s, die PIX 515E mit zwei bis sechs 10/100-Ethernet-Interfaces und einem Durchsatz von etwa 190 Mbit/s, die PIX525 mit 10/100 sowie Gigabit-Interfaces und einem Durchsatz von bis zu 370 Mbit/s. Das Spitzenmodell ist die PIX 535 mit bis zu zehn 10/100- bzw. Gigabit-Ethernet-Schnittstellen und einem Durchsatz von bis zu 1,7 Gbit/s.

Weitere Vorteile der Secure PIX Firewall

- Die integrierten Sicherheitsmechanismen, die von Cisco speziell für die Secure PIX Firewall entwickelt wurden, basieren auf keinem allgemein verfügbaren Betriebssystem, haben nur einen geringen Code-Umfang und können auf diese Weise auch nicht mit üblichen Hackertools angegriffen werden.
- Dynamische Filterung von IP-Adressen und dynamisches Öffnen/Schließen von UDP/TCP-Ports



- Filterung von SMTP-Kommandos
- Aufzeichnung von URL-Adressen
- Java-Applet Filter
- Cut-through-Proxy für die Authentifizierung auf Applikationsebene
- Integrierte IPsec-Funktionen (Hardware-Beschleuniger erhältlich für PIX 515, PIX 525 und PIX 535), L2TP-Support für Layer 2 Tunneling Protokoll
- Netzwerk Adress Translation (NAT) und Port Adress Translation (PAT) sowie PAT Port Redirection
- PPPoE Unterstützung für Anschluss an DSL-Ethernet Modems
- Sicheres Failover über das LAN
- Easy VPN Features für schnellen und reibungslosen Anschluss an IPSEC Infrastrukturen
- Unterstützung für Multimediaprotokolle wie H323, Skinny, Netmeeting und multicast Routing
- Integration von Ethernet-, Fast Ethernet- und GigabitEthernet
- Multimedia-Unterstützung für Streaming Audio und Video
- Voice-Protokoll-Support für SCCP (Skinny Client Control Protocol) und SIP
- System-Monitoring (z. B. PIX-CPU-Last)
- Shunning-Support für den Cisco Secure IDS-Sensor (dynamisches Blockieren von Angriffen)
- Integriertes grafisch-interaktives Management mit dem Pix Device Manager PDM, Management per Command Line Interface (CLI)
- Unterstützung des Cisco VPN Clients für Windows 95, 98, ME, NT 4.0 und 2000

Mehr dazu finden Sie unter:
<http://www.cisco.com/go/pix>

Cisco Secure ACS Access Control Server

Der Cisco Secure Access Control Server für Windows NT erlaubt die zentrale Authentifizierung, Autorisierung und das Accounting (man spricht auch gerne von Triple-A-Security) von Access-Servern, VPNs und Firewalls, Voice-over-IP-Lösungen. Neu sind die vom Standard IEEE 802.1x abgeleiteten Erweiterungen für die Schlüsselverwaltung und Zugriffskontrolle für drahtlose Netzwerke der Cisco AIRONET-Serie sowie das Management von Benutzerauthentifizierungen an Cisco LAN-Switchen.

Mit dem ACS beispielsweise können folgende Vorgänge gesteuert und überwacht werden:

- Wer kann sich in das Netzwerk einloggen?
- Welches Recht hat der Benutzer im Netzwerk?
- Welche Informationen werden für die Rechnungslegung oder für Sicherheits-Audits gespeichert?
- Welche Rechte hat jeder einzelne Administrator beim Verwaltungszugriff auf Cisco IOS-Router, Catalyst-Switches oder jegliches Device, welches TACACS+?

Der Cisco Secure Access Control Server bietet Funktionen wie einfaches Management per Web-Interface, kann existierende Windows-NT- oder Active Directory Datenbanken sowie LDAP-Directory-Informationen für Authentisierungszwecke nutzen und ermöglicht die Integration von Token-Card-Servern für die Unterstützung von Einmal-Passwörtern, z. B. von RSA, Secure Computing und CryptoCard. Zudem ist die Zugriffskontrolle auf Basis von



Cisco Firewall PIX 515E

Tageszeiten, Wochentagen, Netzwerk-Nutzung, Anzahl der Sessions möglich.

Weitere Features und Informationen finden Sie unter folgender URL:
<http://www.cisco.com/go/acs>

Cisco Secure Intrusion Detection System

Das Cisco Secure Intrusion Detection System ist ein netzwerkbasierendes Expertensystem zur Aufdeckung und Abwehr von Einbruchversuchen.

Es erfasst und beendet unautorisierte Aktivitäten in einem Netzwerk und ist damit ein wichtiger Bestandteil der Cisco Secure Produktlinie.

Das System umfasst zwei wichtige Komponenten:

- Cisco Secure IDS Sensor – Der Sensor ist Appliance, d. h. eine vorinstallierte Hard- und Software-Kombination, die in der Lage ist, über ein Sniffing-Interface den Datenverkehr in exponierten und sicherheitsrelevanten Netzwerkbereichen auf Anomalien hin zu untersuchen. Beim Aufdecken derartiger Anomalien, wie Denial-of-Service-Attacken, kann ein Alarm ausgelöst und der Angreifer über einen Cisco Router oder eine PIX Firewall dynamisch ausgesperrt werden.

Auch kann über einen TCP Reset z. B. eine Telnet-Session bei der Eingabe vorab festgelegter verbotener Befehle zurückgesetzt und unschädlich gemacht werden.

Die Alarme und Reaktionen auf Angriffe können individuell angepasst bzw. eingestellt werden. Über integrierte Funktionen auf IOS Routern mit IDS Feature Set und PIX Firewalls lassen sich diese Systeme auch als Sensoren nutzen, wobei der

Umfang der Signaturen auf PIX-Firewall und Router mit IDS-IOS geringer als auf den IDS-Sensoren ist. Die Sensoren gibt es in Ausführungen mit einer Analysekapazität von 45 Mbit/s (IDS 4210 Sensor), 200 Mbit/s (IDS 4235 Sensor) sowie bis zu 1 Gbit/s (IDS 4250 Sensor). Konfiguration und Management erfolgt bequem über ein mit SSL gesichertes Webinterface. Zur Anzeige der Alarme wird der IDS Event Viewer kostenfrei mitgeliefert. Weiterhin gibt es IDS Module für die Switches der Catalyst 6500 Serie mit einer Kapazität von 170 Mbit/s und 1 Gbit/s (fabric enabled).

- VMS 2.1 – VPN und Security Management Solutions für IDS. Diese Software für Windows 2000/ Solaris Plattformen verwaltet und konfiguriert IDS Sensoren, empfängt IDS Meldungen des Catalyst 6500 IDS Blades, der PIX Firewall, der Cisco IOS Router sowie des Cisco Host IDS Systems. Damit existiert ein einheitliches, übersichtliches Management für Cisco IDS

Systeme. Das IDS Management Center kann bis zu 500 Alarme pro Sekunde empfangen und kann bei Bedarf über Mail oder Pager rechtzeitig den Administrator alarmieren.

Mehr dazu finden Sie unter:
<http://www.cisco.com/go/ids>



Cisco Secure Policy Manager (CSPM)

Der Cisco Secure Policy Manager (CSPM) für Windows NT ist eine skalierbare und umfangreiche Software-Lösung für das Management von Security Policies auf Cisco Firewalls, VPN Gateways und IDS Sensoren. Mit dem CSPM können Anwender netzwerkweite Sicherheitsrichtlinien definieren, verteilen, umsetzen und überwachen. Sicherheitsfunktionen wie Zugangskontrolle, NAT (Network Address Translation), IDS und IPSec-basierende VPNs werden einer zentralen Management-Instanz zusammengefasst.

Die Definition der Security Policies für mehrere Firewalls und VPN-Gateways erfolgt über die graphische Benutzerschnittstelle des CSPM. Danach werden diese Informationen automatisch auf die Zielsysteme verteilt, ohne dass die Geräte eines nach dem anderen händisch mit Befehlen versorgt werden müssen.

Integrierte System-Überwachungsfunktionen – inklusive Monitoring, Benachrichtigung bei Vorfällen und webbasierte Berichtsfunktionen – vervollständigen den Funktionsumfang der Software.

Mehr dazu finden Sie unter:

<http://www.cisco.com/warp/public/cc/pd/sqsw/sqppmn/>

Cisco 3000 VPN Concentrator-Serie

Virtuelle Private Netzwerke, kurz VPNs genannt, sind Netzwerke, die über öffentliche Netzwerkinfrastrukturen – wie beispielsweise das Internet oder einen Service-Provider-Backbone – aufgebaut werden. In punkto Sicherheit, Management und Dienstgüte (Quality-of-Service – QoS) werden die gleichen Ansprüche wie in privaten Netzwerken gestellt. Die Vorteile eines VPNs sind zum einen in Kosteneinsparungen begründet (Standleitungen werden i. d. R. entfernungs- und bandbreitenabhängig abgerechnet, eine Verbindung zum lokalen Provider ist um einiges günstiger als z. B. eine Verbindung zum 400 km entfernten Standort), zum anderen gewinnt man neue Verbindungsmöglichkeiten hinzu, z. B. die Anbindung von Telearbeitern, mobilen Benutzern und Außenstellen über das Internet. Weiterhin lassen sich neue Bereiche wie Kunden, Zulieferer und Partner einfach und schnell an das eigene Netzwerk anbinden. Man unterscheidet zwischen Site-to-Site- und Remote-Access-VPNs. Site-to-Site-VPNs werden zur permanenten Anbindung von weiteren Standorten oder Partnern genutzt – diese lassen sich mit Cisco Routern und PIX-Firewalls über die IPSec-Funktionalität einfach realisieren. Möchte man viele mobile Benutzer, die sich über analog- oder ISDN-Dial-In über einen lokalen Service-Provider einwählen, über das Internet an eine Unternehmenszentrale anbinden, so spricht man in diesem Fall von einem Remote-Access-VPN.

Eine ideale Produktserie zur Realisierung derartiger VPNs ist die Cisco VPN 3000 Concentrator Serie. Für die mobilen Benutzer steht eine Client-Software – der Cisco VPN Client – zur Verfügung. Der Client stellt das IPSec-Framework auf den PCs der Benutzer zur Verfügung und sorgt somit für die sichere Kommunikation mit dem Zielnetzwerk. Neben der Software-Lösung gibt es noch einen Hardware Client – den Cisco VPN 3002 Hardware Client – mit dem man Rechnersysteme anschließen kann, die derzeit nicht von der Software-Lösung unterstützt werden. Selbstverständlich ist auch die Verwendung von Cisco IOS-Routern als Client System möglich. Für die Zielnetzwerke gibt es eine umfangreiche Palette an Konzentratoren, die je nach Ausführung 100 bis zu 10.000 Benutzer gleichzeitig unterstützen. Weiterhin gibt es Möglichkeiten der Systemredundanz und Skalierbarkeit, d. h. einige Modelle können redundant ausgelegt werden sowie bei steigenden Anforderungen erweitert werden. Letztere Funktionalität wird durch die Scalable-Encryption-Processing-(SEP)-

Module sichergestellt. Der Cisco-VPN-Software-Client liegt allen Systemen kostenlos bei. Bemerkenswert ist auch die Möglichkeit für mobile User, verschlüsselte Verbindungen aufzubauen, die von Netzen ausgehen, die z. B. beim Internetzugriff PAT oder NAT (Port Address Translation oder Network Address Translation) verwenden. Dies ist oft der Fall, wenn sich mehrere Benutzer eine Einwahlverbindung über einen Router teilen.

Weitere Informationen zum Thema gibt es unter:

<http://www.cisco.com/warp/public/cc/pd/hb/vp3000>

Weiterführende Lösungen

Die Cisco Secure und Cisco VPN Produktserien decken nahezu das gesamte Spektrum an Maßnahmen für den Aufbau einer optimalen Sicherheitsarchitektur im Unternehmensnetz ab. Für zusätzliche flankierende Maßnahmen in den Bereichen Identität, Integrität, Perimeter- und Content-Security, Application Security, Management und Überwachung gibt es Applikationen von Cisco Partnerunternehmen, den Cisco Security Associates. Die einzelnen Bereiche umfassen derzeit folgende Applikationen:

- **Identität:** Applikationen, die die Identifizierung von Benutzern unterstützen, z. B. Zertifikatsautoritäten von Baltimore, Entrust, RSA Security Smart-Trust und VeriSign oder Einmal-Passwort-Systeme von CryptoCard, RSA Security und Secure Computing.
- **Integrität:** Weitere VPN-Clients von Certicom (für Handhelds), F-Secure und iPass.
- **Perimeter- und Content-Security:** Systeme, die z. B. zusammen mit einer Cisco Secure PIX Firewall E-Mails oder aktive Web-Applets auf böswillige Inhalte überprüfen – Lösungen von Baltimore, F-Secure, Finjan, N2H2, Sygate, TrendMICRO. Weiterhin ist die Blockierung bestimmter Websites über Software von SurfControl und WEBSENSE in Zusammenarbeit mit der PIX Firewall möglich.
- **Application Security:** Applikationen, die netzwerkbasierende IDS-Maßnahmen unterstützen (Host-basiertes IDS) – Produkte von entercept, SANCTUM und ZONE LABS.
- **Management und Überwachung:** Tools zum Überwachen der Security-Policies, z. B. zum Auslesen von Syslog-Dateien etc. Produkte von eSecurity, F-Secure, netforensics.com, OpenSystems, PENTASAFE, Telemate.Net, WEBTRENDS.

Weitere Informationen zum Thema sowie Links zu den genannten Partnern gibt es unter folgender URL:
<http://www.cisco.com/warp/public/779/largeent/partner/esap/secvpn.html>

Was heißt schon sicher?

Letzten Endes ist es eine Frage von Aufwand und Nutzen. Wie im richtigen Leben – wenn Sie geeignete Sicherheitsmaßnahmen ergreifen, ist Ihr Netzwerk zu 99% sicher. Ganz gleich, ob Sie mit einem Netzwerk arbeiten oder ob Sie mit einem Netz verbunden sind – Sie sollten vorzeigbare Sicherheitsmaßnahmen haben.

Es ist sicherlich nicht einfach, ein Handbuch über die Netzwerk-Sicherheit zur Verfügung zu stellen, ohne Aufregung und lange Diskussionen auszulösen.

Aber es lohnt sich, den Tatsachen ins Auge zu sehen: Computer-Networking bringt selbst dem kleinsten Unternehmen enorme Vorteile. Wenn sich zum Beispiel Kunden zu jeder Tages- und Nachtzeit einloggen und bestellen können.

Oder wenn Bestandslisten just-in-time im Bruchteil einer Sekunde verwaltet werden – dann zahlt sich dies schnell in barer Münze aus.

Aber auch Organisationen, die nicht gewinn- oder umsatzorientiert arbeiten, können enorme Vorteile aus den Möglichkeiten der allgemeinen Vernetzung ziehen. So könnte beispielsweise die Realisierung von behördlichen Funktionen durch Internet-Technologien zu schlankeren Behördenapparaten und schnelleren, weil einfacheren Prozeduren führen.

Das wachsende Interesse, das Internet zu einem sicheren Handelsplatz zu machen – so wie Banken, Kreditkarten-Unternehmen und Computerfirmen – forcieren Technologien wie „Public Key Interface (PKI)“ und „Secure Electronic Transaction-System (SET)“. Und den Gebrauch von Digital IDs, um E-Commerce sicherer zu machen. Das wird das Vertrauen stärken und

die intensivere Nutzung des Internets durch Unternehmen und ihre Kunden fördern.

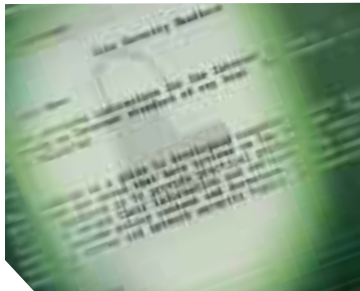
Die Frage der Sicherheit ist einfach ein zentraler Aspekt der Internet-Technologie im Unternehmen. Es gibt gute Lösungen für jede Bedrohung und die Vorteile überwiegen die Risiken bei weitem. Alles was man braucht, ist ein bisschen Vorsicht und gesundes Misstrauen – und eine Digital ID.

Mit dem Sicherheitsframework für Unternehmensnetzwerke (Safe) verfolgt Cisco in erster Linie das Ziel, Interessenten mit Informationen zur optimalen Vorgehensweise bei der Konzeption und Implementierung sicherer Netzwerke zu versorgen. Safe stellt ein Handbuch für Netzwerkdesigner dar, in dem die Sicherheitsanforderungen eines Cisco-Netzwerks berücksichtigt werden. Der hierbei gewählte Ansatz zeichnet sich durch sehr tief greifende Abwehrmechanismen aus. Bei dieser Art der Konzeption richtet sich das Augenmerk primär auf die erwarteten Bedrohungen und Methoden zu deren Abwendung. Es ist nämlich nicht damit getan, einfach hier eine Firewall und dort ein Intrusion Detection System (IDS) einzusetzen. Daraus ergibt sich ein mehrschichtiger Sicherheitsansatz, bei dem auch der Ausfall eines Sicherheitssystems aller Wahrscheinlichkeit nach keine Sicherheitsverletzungen an Netzwerkressourcen nach sich zieht. Safe basiert auf den Produkten von Cisco und dessen Partnern.



„Brief und Siegel
für **absolute**
Sicherheit kann
niemand geben.“

„Safe“ – die Sicherheitsarchit



„Eine gute
Sicherheitspolicy
ist in jedem Fall
erforderlich.“

Im folgenden wollen wir eine Übersicht über die Struktur von Safe geben. In drei Abschnitten werden die wichtigsten Module an Hand einfacher Abbildungen des Datenverkehrsflusses, der Hauptgeräte und der erwarteten Bedrohungen beschrieben.

Zentrales Thema im Rahmen dieses Dokuments sind die Bedrohungen, denen Netzwerk-Umgebungen in Unternehmen ausgesetzt sind. Netzwerkdesigner, die diese Bedrohungen kennen, können gezielt entscheiden, wo und auf welche Weise sie Abwehrmechanismen einsetzen. Wo dieses Wissen fehlt, besteht die Gefahr, dass Abwehrmechanismen falsch konfiguriert oder zu stark auf die Sicherheitsgeräte konzentriert werden oder dass nicht flexibel genug auf Bedrohungen reagiert werden kann.

Grundvoraussetzung für die Umsetzung von Safe ist immer eine bestehende Sicherheitspolicy, d.h.

Sicherheitstechnologien sollten nie ohne ein entsprechendes Konzept eingesetzt werden.

Die hier diskutierte Sicherheitsarchitektur ist auf die Anforderungen von Großunternehmen abgestimmt. Dennoch treffen die meisten dieser Prinzipien auch auf kleine und mittlere Unternehmen, ja sogar auf Heimbüros zu – wenn auch in anderem Umfang. Es werden Alternativen und Optionen vorgestellt, die eine Kostenersparnis bzw. stufenweise Implementierung der Architektur ermöglicht.

Allerdings: Auch bei Einhaltung der in Safe dargelegten Richtlinien kann eine hundertprozentige Sicherheit nicht garantiert werden. Absolute Sicherheit ließe sich nur erzielen, wenn man das betreffende System vom Netzwerk trennt, in Beton gießt und im Keller von Fort Knox einlagert. Nur: Dann wären zwar die Daten absolut sicher, aber auch nicht mehr erreichbar.

Was versteht man unter Sicherheitspolicy?

Bei einer Sicherheitspolicy kann es sich einerseits um eine einfache Vorschrift in Bezug auf Netzwerkressourcen und andererseits um eine mehrere hundert Seiten lange Ausführung handeln, in der jedes einzelne Element der Konnektivität und entsprechende Policies behandelt werden. RFC 2196 ist zwar nicht sehr umfangreich, liefert aber eine gute Definition des Begriffs Sicherheitspolicy:

Eine Sicherheitspolicy ist eine formale Darlegung der Richtlinien, an die sich die Personen halten müssen, die Zugang zu den Technologie- und Informationsbeständen einer Organisation erhalten. Im vorliegenden Dokument wird die Entwicklung einer Sicherheitspolicy nicht vertieft. RFC 2196 enthält einige wertvolle Informationen zu diesem Thema, und im Internet finden sich zahlreiche Beispiele zum Thema Sicherheitspolicy und Richtlinien. Die folgenden Webseiten enthalten interessante Informationen:

- RFC 2196 „Site Security Handbook“
<http://www.ietf.org/rfc/rfc2196.txt>
- Die Sicherheitspolicy der University of Illinois als Beispiel
www.aits.uillinois.edu/security/securestandards.html
- Design und Implementierung der Sicherheitspolicy für Unternehmen
<http://www.knowcisco.com/cotent/1578700434/ch06.shtml>

Architektur für Unternehmensnetzwerke

Virtuelle Private Netzwerke (VPNs) sind in dieser Architektur zwar berücksichtigt, werden jedoch nicht ausführlich besprochen. Auch bestimmte Themen in Bezug auf VPNs oder Identifizierungsstrategien (beispielsweise Skalierungsinformationen oder Strategien für die Netzwerkzuverlässigkeit, Zertifizierungsstellen [CAs] usw.) können hier nicht erschöpfend besprochen werden. Eine umfassende Abhandlung dieser Themen würde den Rahmen dieses Dokuments sprengen.

Außerdem ist hierbei zu beachten, dass die meisten Unternehmensnetzwerke noch nicht mit voll funktionsfähigen CA-Umgebungen arbeiten und daher den Erläuterungen zur Sicherung von Netzwerken ohne diese CA-Umgebungen eine umso höhere Bedeutung zukommt. Schließlich wurden auch bestimmte hoch entwickelte Netzwerkanwendungen und -technologien (wie beispielsweise Contentnetzwerke, Caching und Serverlastverteilung) in diesem Dokument nicht berücksichtigt. Es ist zwar zu erwarten, dass auch diese in Safe integriert werden, derzeit wird jedoch keine Zeit auf die besonderen Sicherheitsanforderungen dieser Applikationen verwandt.

Obwohl Safe unter Verwendung von Produkten von Cisco und dessen Partnern konzipiert wurde, werden die betreffenden Produkte in diesem Dokument nicht explizit genannt. Das heißt, die einzelnen Komponenten werden nicht anhand ihrer Modellnummer, sondern anhand ihrer Funktion identifiziert.

Während der Validierungsphase von Safe wurden in exakt der in diesem Dokument beschriebenen Netzwerkimplementierung echte Produkte konfiguriert. Informationen zum Prüflabor und den Ergebnissen mitsamt spezifischer Konfigurationssnapshots aus dem Labor sind Bestandteil der Architektur und sind verfügbar.

Router sind Angriffsziele ...

Router steuern den Zugriff von einem Netzwerk auf ein anderes. Sie werben für Netzwerke und filtern zulässige Benutzer – und sind bei Hackern besonders beliebt. Daher stellen sie ein kritisches Element in jeder Sicherheitsstrategie dar. Router haben grundsätzlich die Aufgabe, Zugriffe zu ermöglichen, und eben deshalb müssen sie gegen direkte Kompromittierung gesichert werden. Zu diesem Aspekt der Sicherheit wurden bereits diverse Dokumente verfasst, die ebenfalls beachtet werden sollten, da sie nähere Erläuterungen zu den folgenden Themen enthalten:

- Sperren des Telnet-Zugriffs auf einen Router
- Sperren des SNMP-Zugriffs auf einen Router
- Steuern des Zugriffs auf einen Router unter Verwendung von TACACS+
- Deaktivieren nicht benötigter Dienste
- Protokollieren auf entsprechenden Ebenen
- Authentifizierung von Routing-Updates

Das neueste Dokument zu diesem Thema finden Sie unter:

<http://www.cisco.com/warp/public/707/21.html>

Warum ist eine Sicherheitspolicy sinnvoll?

Wenn es um Netzwerksicherheit geht, sollte man sich darüber im Klaren sein, dass man dabei niemals einen Zielpunkt erreicht. Es existiert kein Produkt, das allein ein Unternehmen „sicher“ machen kann. Wirkliche Netzwerksicherheit entsteht erst durch eine Kombination von Produkten und Diensten zusammen mit einer umfassenden Sicherheitspolicy und deren Einhaltung sowohl auf der Managementebene als auch auf den untergeordneten Ebenen in einem Unternehmen. Die Praxis hat erwiesen, dass eine korrekt implementierte Sicherheitspolicy ohne dedizierte Sicherheitsgeräte viel effizienter für eine Abwehr von Angriffen sorgen kann als die umfassende Implementierung eines Sicherheitsprodukts ohne entsprechende Policy.

Die Grundsätze von Safe

Switches sind Angriffsziele ...

Ebenso wie Router sind auch Switches (sowohl L2 als auch L3) besonderen Sicherheitsrisiken ausgesetzt. In diesem Fall sind jedoch weniger Informationen zu Sicherheitsrisiken und möglichen Abwehrmaßnahmen öffentlich zugänglich als bei Routern. Die meisten im vorangegangenen Abschnitt über Router genannten Sicherheitstechniken sind auch auf Switches anwendbar. Zusätzlich sind die folgenden Maßnahmen zu empfehlen:

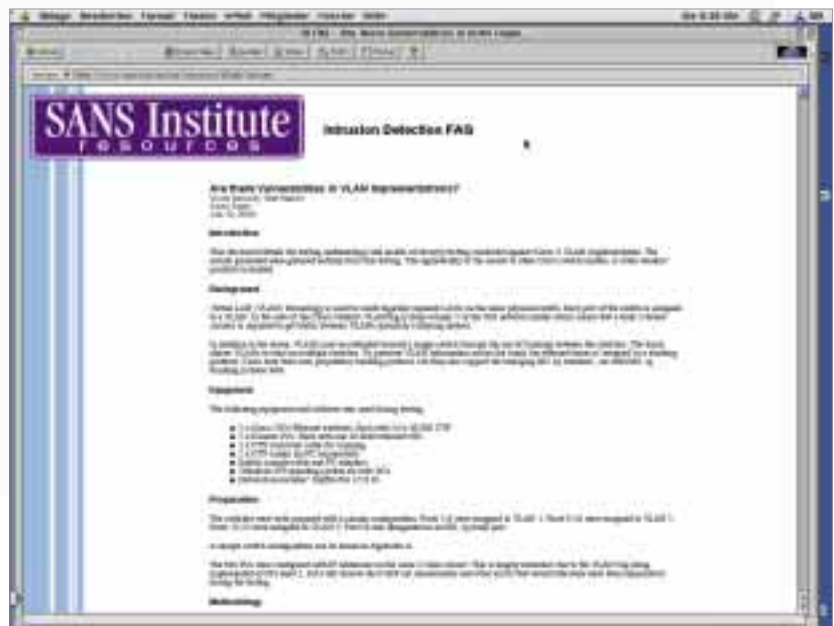
- Für Ports, für die keine Trunk-Funktionalität erforderlich ist, sollten alle Trunk-Einstellungen deaktiviert werden (also nicht auf Auto gesetzt sein). Auf diese Weise lässt sich verhindern, dass ein Host zu einem Trunk-Port wird und allen Datenverkehr empfängt, der normalerweise zu einem Trunk-Port gelangt.
- Trunk-Ports sollte eine innerhalb des Switches eindeutige VLAN-Nummer zugewiesen werden. Auf diese Weise lässt sich vermeiden,

dass Pakete, die mit demselben VLAN markiert sind wie der Trunk-Port, ein anderes VLAN erreichen, ohne ein L3-Gerät passieren zu müssen.

Weitere Informationen hierzu finden Sie unter:

<http://www.sans.org/newlook/resources/IDFAQ/vlan.htm>

- Alle ungenutzten Ports eines Switches sollen auf ein VLAN ohne L3-Konnektivität eingestellt werden. Noch besser ist es, jeden nicht verwendeten bzw. benötigten Port zu deaktivieren. Auf diese Weise kann vermieden werden, dass ein Hacker eine Verbindung zu einem ungenutzten Port herstellen und so mit dem Rest des Netzwerks kommunizieren kann.
- Es ist allerdings nicht zu empfehlen, sich zur Sicherung des Zugriffs zwischen zwei Subnetzen allein auf VLANs zu verlassen. Angesichts der Tatsache, dass hier ein großes Fehlerpotenzial im Hinblick auf menschliches Versagen besteht und außer-



dem bei der Konzeption von VLANs und VLAN-Taggingprotokollen Sicherheitsfragen nicht in Betracht gezogen wurden, ist die Verwendung von VLANs in sensiblen Umgebungen nicht zu empfehlen. Ist allerdings der Einsatz von VLANs in Sicherheitsstrategien nicht zu umgehen, sollten Sie genau die weiter oben angeführten Konfigurationshinweise und Richtlinien befolgen.

Innerhalb eines bestehenden VLANs bieten private VLANs in gewissem Maße zusätzliche Sicherheit für bestimmte Netzwerkanwendungen. Ihre Funktionsweise besteht darin, dass sie nur eine Kommunikation zwischen bestimmten Ports innerhalb eines VLANs und anderen Ports innerhalb desselben VLANs zulassen. Isolierte Ports innerhalb eines VLANs können nur mit Ports im Promiscuous-Mode kommunizieren. Community-Ports können nur mit anderen Mitgliedern derselben Community sowie mit Ports im Promiscuous-Mode kommunizieren. Ports im Promiscuous-Mode können mit jedem beliebigen Port kommunizieren. Auf diese Weise kann ein einzelner kompromittierter Host keinen großen Schaden anrichten.

Stellen Sie sich ein durchschnittliches Segment für öffentliche Services mit einem Webserver, einem FTP-Server und einem DNS-Server vor. Ist die Sicherheit des DNS-Servers nicht mehr gewährleistet, kann ein Hacker die beiden anderen Hosts angreifen, ohne die Firewall erneut passieren zu müssen. Bei Verwendung privater VLANs könnte ein kompromittiertes System nicht mehr mit den anderen Systemen kommunizieren. In diesem Fall könnte der Hacker nur die Hosts auf der anderen Seite der Firewall angreifen.

Hosts sind Angriffsziele ...

Hosts stellen das beliebteste Angriffsziel dar und sind gleichzeitig am schwierigsten zu schützen.

Es gibt zahlreiche Hardwareplattformen, Betriebssysteme und Applikationen, für die jeweils zu unterschiedlichen Zeiten Updates, Patches und Fehlerkorrekturen erhältlich sind. Da Hosts anderen Hosts die von diesen angeforderten Applikationsdienste zur Verfügung stellen, sind sie innerhalb des Netzwerks sehr exponiert. So wurden zum Beispiel unter der Adresse *www.whitehouse.gov* (dies ist ein Host) zahlreiche Besucher verzeichnet, wohingegen nur wenige versucht haben, auf *s2-0.whitehouse.bbnplanet.net* (einen Router) zuzugreifen.

Aufgrund dieser Sichtbarkeit werden Hosts bei unbefugten Zugriffsversuchen weitaus häufiger angegriffen als andere Netzwerkgeräte. Es kann zum Beispiel vorkommen, dass auf einem bestimmten Webserver die Hardwareplattform eines Herstellers, die Netzwerkkarte eines anderen Herstellers, das Betriebssystem eines dritten Herstellers und eine Webserversoftware – entweder als Open Source-Produkt oder als Produkt eines weiteren Herstellers – verwendet werden.

Und damit nicht genug. Nun könnten auf demselben Webserver auch noch Applikationen ausgeführt werden, die frei über das Internet verteilt werden. Der Webserver könnte schließlich zusätzlich mit einem Datenbankserver kommunizieren, der aus nicht weniger unterschiedlichen Komponenten zusammengesetzt ist.



„Es ist nicht von der Hand zu weisen, dass mit **zunehmender Komplexität** eines Systems auch die **Wahrscheinlichkeit** eines Ausfalls oder **Fehlers zunimmt.**“



„In der Regel zielen die **Urheber** eines solchen **Angriffs** nicht darauf ab, einen bestimmten **Host** zum **Absturz** zu bringen, sondern das **gesamte Netzwerk lahm zu legen.**“

Natürlich heißt das nicht, dass Schwachstellen in Sicherheitsfragen besonders von der Verwendung unterschiedlichster Herstellerprodukte herühren. Es ist jedoch nicht von der Hand zu weisen, dass mit zunehmender Komplexität eines Systems auch die Wahrscheinlichkeit eines Ausfalls oder Fehlers zunimmt.

Zur Sicherung von Hosts müssen alle einzelnen Komponenten der Systeme mit besonderer Sorgfalt ausgewählt werden. Für all die oben genannten Systeme müssen stets die neuesten Patches, Fehlerkorrekturen usw. installiert sein. Dabei darf aber auch die spezielle Wirkung dieser Patches auf die Funktion der anderen Komponenten im System nicht außer Acht gelassen werden. Aus diesem Grund empfiehlt es sich, alle Updates vor der Implementierung in einer Produktionsumgebung auf Testsystemen zu prüfen und auszuwerten. Wird diese Prüfung nicht durchgeführt, kann der Patch selbst einen Denial-of-Service verursachen.

Netzwerke sind Angriffsziele ...

Die schlimmsten Angriffe sind die, die unaufhaltsam ihren Lauf nehmen. Und genau solch ein Angriff ist ein richtig ausgeführter DDoS (Distributed Denial of Service). Wie schon erwähnt, werden durch einen DDoS Dutzende oder gar Hunderte von Computern veranlasst, gleichzeitig falsche Daten an eine IP-Adresse zu senden.

In der Regel zielen die Urheber eines solchen Angriffs nicht darauf ab, einen bestimmten Host zum Absturz zu bringen, sondern das gesamte Netzwerk lahm zu legen. Stellen Sie sich zum Beispiel ein Unternehmen vor,

das über eine DS3-Verbindung (also eine Verbindung mit einer Geschwindigkeit von 45 Mbit/s) zum Internet verfügt und Benutzern auf seiner Webseite E-Commerce-Dienste anbietet. Eine solche Site ist sehr sicherheitsbewusst angelegt und mit Angriffserkennung, Firewalls, Protokollierfunktion und aktivem Monitoring ausgestattet. Nur leider nutzen diese ganzen Sicherheitsvorkehrungen bei einem erfolgreichen DDoS-Angriff gar nichts.

Stellen Sie sich nun 100 Geräte in aller Welt mit einer DS1-Verbindung (also einer Verbindung mit 1,5 Mbit/s) zum Internet vor. Wenn diese Systeme von einem Remotestandort die Anweisung erhalten, die serielle Schnittstelle des Internetrouters des Unternehmens mit Daten zu überschütten, kann dabei problemlos die DS3-Verbindung mit falschen Daten überflutet werden.

Selbst wenn jeder Host nur Datenverkehr mit 1 Mbit/s erzeugen kann (und Tests haben bewiesen, dass eine handelsübliche Unix-Arbeitsstation mit einem beliebigen DDoS-Tool ohne Weiteres 50 Mbit/s erzielen kann), ist diese Datenmenge immer noch mehr als doppelt so groß wie die, die die E-Commerce-Site verarbeiten könnte. Das führt dazu, dass legitime Webanforderungen verloren gehen und die Site für die meisten Benutzer ausgefallen zu sein scheint. Zwar würde die lokale Firewall alle falschen Daten zurückweisen, aber zu diesem Zeitpunkt wäre der Schaden schon eingetreten. Die Daten hätten die WAN-Verbindung bereits passiert und die Verbindung blockiert.

Unser fiktives E-Commerce-Unternehmen hat daher nur in Zusam-

menarbeit mit seinem ISP eine Chance, derartige Angriffe zu vereiteln. Der ISP kann für die Ausgangsschnittstelle der Unternehmensseite eine Ratenbegrenzung konfigurieren. Mit Hilfe dieser Ratenbegrenzung kann der größte Teil des unerwünschten Datenverkehrs zurückgewiesen werden, sobald dieser mehr als einen festgelegten Teil der verfügbaren Bandbreite einnimmt. Das Wichtigste hierbei ist, Daten korrekt als unerwünscht zu kennzeichnen.

Häufig verwendete Formen von DDoS-Tools arbeiten mit ICMP-, TCP SYN- oder UDP-Flooding. In einer E-Commerce-Umgebung ist diese Art von Datenverkehr recht einfach zu kategorisieren. Die einzige Gefahr besteht darin, dass der Administrator durch die Begrenzung von TCP SYN-Angriffen auf Port 80 (http) während eines Angriffs Zugriffe durch legitime Benutzer unterdrückt. Und selbst dann ist es besser, neue legitime Benutzer vorübergehend zu sperren und dafür die Routing- und Managementverbindungen zu erhalten, als einen Angriff auf den Router zuzulassen und dadurch jegliche Konnektivität einzubüßen.

Bei ausgeklügelteren Angriffen wird Datenverkehr an Port 80 mit gesetztem ACK-Bit verwendet, so dass dieser wie legitimer Webverkehr aussieht. Dass ein Administrator einen solchen Angriff richtig kategorisieren könnte, ist sehr unwahrscheinlich, denn schließlich lässt jeder gerade TCP-Kommunikationen mit Bestätigung gerne in sein Netzwerk.

Es gibt dennoch Möglichkeiten, solche Angriffe abzuwehren. Dazu bietet

sich zum Beispiel die Befolgung der Filterrichtlinien für Netzwerke an, die in RFC 1918 und RFC 2827 niedergelegt sind. Dabei werden in RFC 1918 die Netzwerke benannt, die der privaten Verwendung vorbehalten sind und im öffentlichen Internet niemals sichtbar werden sollten.

Die Filterung gemäß RFC 2827 wird unter dem Eintrag zu IP-Spoofing in der Fibel zur Netzwerksicherheit in diesem Dokument erläutert. Die Filterung nach RFC 1918 und 2827 sollte beispielsweise in Form von Eingangsfiltern an mit dem Internet verbundenen Routern eingesetzt werden, um zu verhindern, dass unerlaubter Datenverkehr das Unternehmensnetzwerk erreicht. Bei Implementierung auf Seite des ISP lässt sich mit Hilfe der Filterung verhindern, dass DDoS-Angriffspakete, die diese Adressen als Absender verwenden, die WAN-Verbindung passieren, wodurch gegebenenfalls während des Angriffs Bandbreite eingespart werden kann.

Würden alle ISPs auf der ganzen Welt die in RFC 2827 niedergelegten Richtlinien umsetzen, ließe sich das Absenderadressen-Spoofing erheblich reduzieren. Damit wäre es zwar noch immer nicht möglich, DDoS-Angriffe von vornherein zu unterbinden, jedoch könnte die Absenderadresse eines solchen Angriffs nicht mehr getarnt werden, und eine Rückverfolgung zu den angreifenden Netzwerken würde erheblich einfacher.

„Die **Angriffserkennung** funktioniert nicht anders als eine **Alarmanlage** in der realen Welt.“

„Als umfassendes **Angriffserkennungssystem** empfiehlt sich eine **Kombination** beider Systeme, d. h. **HIDS*** auf kritischen Hosts und **NIDS**** für das gesamte Netzwerk.“

... und Applikationen sind Angriffsziele!

Applikationscodes werden zum überwiegenden Teil von Menschen geschrieben und sind daher fehleranfällig. Solche Fehler können gutartig sein, z. B. wenn sie dazu führen, dass ein Dokument im Druck merkwürdig aussieht. Sie können aber auch schwerwiegenderer Natur sein, so zum Beispiel, wenn durch einen Fehler die Kreditkartennummern auf dem Datenbankserver per Anonymous FTP abgerufen werden können.

Diese Probleme sowie eine ganze Reihe anderer, allgemeinerer Sicherheitsprobleme können mit Hilfe von Angriffserkennungssystemen (Intrusion Detection Systeme, ID-Systeme, Abk. IDS) aufgedeckt werden. Die Angriffserkennung funktioniert dabei nicht anders als eine Alarmanlage in der realen Welt: Sobald das IDS etwas erkennt, das es als Angriff wertet, kann es entweder selbstständig entsprechende Maßnahmen ergreifen oder eine Mitteilung an ein Managementsystem senden, damit der Administrator entsprechende Schritte einleiten kann.

Manche Systeme sind mehr oder weniger in der Lage, auf solche Angriffe zu reagieren und diese zu vereiteln. Die Host-basierte Angriffserkennung kann Betriebssystem- und Applikationsaufrufe auf einzelnen Hosts abfangen. Alternativ kann ein solches ID-System auch nachträglich lokale Protokolldateien analysieren. Im ersten Fall können Angriffe effektiver vereitelt werden, während im zweiten Fall die Reaktion auf einen Angriff eher passiv ausfällt.

Aufgrund ihrer besonderen Rolle sind Host-basierte ID-Systeme (HIDS) im Vergleich zu Netzwerk-IDS (NIDS) häufig besser geeignet, bestimmte Angriffe zu vereiteln als einfach nur bei Erkennen eines Angriffs eine Warnung auszugeben. Durch diese Eigenschaft geht jedoch die Perspektive für das Netzwerk als Ganzes verloren. In diesem Bereich glänzt wiederum das NIDS. Daher empfiehlt sich als umfassendes Angriffserkennungssystem eine Kombination der beiden Systeme, d. h. HIDS auf kritischen Hosts und NIDS für das gesamte Netzwerk. Nach der ersten Einrichtung muss jede IDS-Implementierung fein abgestimmt werden, um ihre Effektivität zu steigern und Fehlalarme zu vermeiden. Bei Fehlalarmen handelt es sich um Alarme, die fälschlicherweise durch legitimen Datenverkehr bzw. legitime Aktivitäten ausgelöst werden. Als Fehlzulassung hingegen werden Angriffe bezeichnet, die das ID-System nicht erkennt. Nach einer Feinabstimmung des IDS kann dieses gezielter für seine Aufgabe zur Abwehr von Bedrohungen konfiguriert werden.

Wie bereits erwähnt, sollte das HIDS so konfiguriert werden, dass die

meisten wirklichen Bedrohungen auf Hostebene abgefangen werden können, denn dieses System bietet die besten Voraussetzungen, um eine bestimmte Aktivität als tatsächliche Bedrohung zu erkennen.

Bei jeder Entscheidung in Bezug auf die Aufgaben von NIDS in der Sicherheit gibt es im Wesentlichen zwei Möglichkeiten. Die erste, die bei falscher Verwendung potenziell den größten Schaden anrichten kann, besteht darin, Datenverkehr „auszugrenzen“, indem Router mit Zugriffskontrollfiltern ausgestattet werden. Wenn ein NIDS einen Angriff von einem bestimmten Host über ein bestimmtes Protokoll erkennt, kann es den betreffenden Host für einen zuvor festgelegten Zeitraum daran hindern, auf das Netzwerk zuzugreifen.

Auf den ersten Blick mag diese Methode als hilfreiches Instrument für den Sicherheitsadministrator erscheinen. Tatsächlich jedoch muss dieser bei der Implementierung größte Vorsicht walten lassen, wenn er nicht sogar ganz von einer Implementierung absieht.

Das erste Problem, das hierbei auftritt, ist das Adressenspoofing. Erkennt das NIDS Daten, die es als Angriff wertet, so dass durch den entsprechenden Alarm eine Ausgrenzungssituation ausgelöst wird, kommt die Access-Liste für das Gerät zum Einsatz. Wenn nun aber bei dem Angriff, der den Alarm ausgelöst hat, eine gespoofte Adresse verwendet wurde, hat das NIDS eine Adresse gesperrt, von der niemals ein Angriff ausgegangen ist. Und handelt es sich bei der von dem Hacker

verwendeten IP-Adresse zufällig um die IP-Adresse des für den abgehenden Datenverkehr zuständigen HTTP-Proxyserver eines großen ISP, kann es sogar passieren, dass unzählige Benutzer gesperrt werden. Das allein könnte für kreative Hacker schon als Anreiz für einen DoS-Angriff ausreichen.

Um die Risiken des Ausgrenzungsverfahrens möglichst gering zu halten, sollte diese Methode grundsätzlich nur bei TCP-Datenverkehr angewandt werden, denn dabei ist erfolgreiches Spoofing sehr viel schwieriger als bei UDP. Zudem ist der Einsatz dieser Methode nur in Fällen einer realen Bedrohung zu empfehlen, wenn also die Gefahr, dass es sich bei einem erkannten Angriff eigentlich um einen Fehlalarm handelt, gering ist.

Innerhalb eines Netzwerks gibt es jedoch noch zahlreiche weitere Möglichkeiten. So lässt sich beispielsweise durch den effektiven Einsatz der Filterung nach RFC 2827 das Spoofing weitgehend unterbinden. Zudem können auch Angriffe aus dem internen Netzwerk strenger vermieden werden, da sich Kunden in der Regel nicht im internen Netzwerk befinden. Dabei fällt auch ins Gewicht, dass interne Netzwerke häufig nicht über so statusbetonte Filtermechanismen verfügen wie Edgeverbindungen. Aus diesem Grund kommt hier dem IDS eine wesentlich wichtigere Rolle zu als in der externen Umgebung.

Die zweite Möglichkeit zur Abwehr von Bedrohungen mittels NIDS stellt die Verwendung von TCP-Resets dar. Diese TCP-Resets funktionieren, wie der Name schon sagt, nur bei TCP-

Datenverkehr. Dabei werden aktive Angriffe beendet, indem TCP-Resetmeldungen sowohl an den angreifenden als auch an den angegriffenen Host gesendet werden. Da sich bei TCP-Datenverkehr das Spoofing schwieriger gestaltet, ist die Verwendung von TCP-Resets in vielen Fällen eher zu empfehlen als das Ausgrenzungsverfahren.

Unter dem Gesichtspunkt der Leistung muss berücksichtigt werden, dass ein NIDS Pakete bei der Übertragung überwacht. Werden nämlich Pakete schneller gesendet, als das NIDS sie verarbeiten kann, hat das keinen negativen Einfluss auf die Netzwerkleistung, denn das NIDS befindet sich nicht unmittelbar im Datenfluss. Allerdings kann das NIDS dann nicht mehr so effektiv arbeiten, und es können Pakete übersehen werden, wodurch es sowohl zu Fehlalarmen wie auch zu nicht erkannten Angriffen kommen kann. Besonders ist darauf zu achten, dass die Kapazität des IDS ausreichend hoch ist, damit alle Vorteile voll ausgenutzt werden können.

Unter dem Gesichtspunkt des Routing ist zu beachten, dass ID-Systeme ebenso wie viele statusorientierte Engines in Umgebungen mit asymmetrischem Routing nicht einwandfrei arbeiten. Wenn Pakete über eine Gruppe von Routern und Switches nach außen gesendet werden, jedoch über eine andere Gruppe von Routern und Switches zurückkommen, hat dies zur Folge, dass die ID-Systeme nur die Hälfte des Datenverkehrs sehen und daher Fehlalarme ausgeben oder echte Angriffe nicht erkennen.



* HIDS = Hostbasiertes Intrusion Detection System

** NIDS = Netzwerkbasiertes Intrusion Detection System

Sicheres Management und Reporting



„Was man **protokolliert**, sollte man auch lesen.“

Was man protokolliert, sollte man auch lesen!“ Leicht gesagt! In der Praxis ist es aber in der Regel ziemlich schwierig, Daten von über 100 Geräten zu protokollieren und sie dann auch noch zu lesen. Welche Protokolle sind die wichtigsten? Wie kann man wichtige Meldungen von einfachen Benachrichtigungen unterscheiden? Wie kann man sicherstellen, dass die Protokolle zwischenzeitlich nicht manipuliert werden? Wie kann man gewährleisten, dass alle Zeitstempel übereinstimmen, wenn mehrere Geräte denselben Alarm melden? Welche Informationen sind von Bedeutung, falls die Daten des Event-Protokolls für polizeiliche Ermittlungen benötigt werden? Wie kann man die Unmengen von Meldungen handhaben, die in einem großen Netzwerk erzeugt werden können? All diese Fragen müssen bedacht werden, wenn ein effektives Management von Protokolldateien angestrebt wird.

Im Hinblick auf das Management stellen sich ganz andere Fragen: Wie lässt sich ein Gerät sicher managen? Wie können Inhalte im Push-Verfahren an öffentliche Server gesendet und dabei sichergestellt werden, dass die Daten während der Übertragung nicht manipuliert werden? Wie lassen sich zum Zweck der Fehlersuche nach Angriffen oder Netzwerkausfällen Änderungen an Geräten zurückverfolgen? Unter dem Gesichtspunkt der Architektur betrachtet, sollte optimalerweise als erster Schritt einer jeden Management- und Reportingstrategie Out-of-band-Management für Netzwerksysteme implementiert werden. Der Begriff Out-of-band (OOB) bezieht sich auf ein Netzwerk, in dem kein Produktionsdatenverkehr stattfindet.

Sofern dies möglich ist, sollten Geräte über eine direkte lokale Verbindung zu einem solchen Netzwerk verfügen.

Ist eine OOB-Implementierung (aufgrund von geografischen Gegebenheiten oder Problemen im System) nicht möglich, sollte die Verbindung über einen privaten, verschlüsselten Tunnel innerhalb des Produktionsnetzwerks hergestellt werden. Ein solcher Tunnel sollte zuvor so konfiguriert werden, dass eine Kommunikation ausschließlich über die Ports möglich ist, die für die Management- und Reportingfunktionen erforderlich sind. Darüber hinaus ist es ratsam, den Tunnel zu filtern, so dass nur Hosts mit entsprechender Berechtigung Tunnels initiieren und beenden können. Besonders ist darauf zu achten, dass das Out-of-band-Netzwerk nicht selbst eine Schwachstelle im Hinblick auf die Sicherheit darstellt.

Nach der Implementierung eines OOB-Managementnetzwerks gestaltet sich die Handhabung der Protokollierung und des Reporting etwas unkomplizierter. Die meisten Netzwerkgeräte sind in der Lage, Syslog-Daten zu senden, die wiederum bei der Fehlersuche aufgrund von Netzwerkproblemen oder Sicherheitsrisiken mitunter von unschätzbarem Wert sind. Solche Daten sollten an einen oder mehrere für die Syslog-Analyse zuständige Hosts im Managementnetzwerk gesendet werden. Je nach Art des betreffenden Geräts stehen verschiedene Protokollierungsebenen zur Auswahl, wodurch gewährleistet werden kann, dass weder zu viele noch zu wenige Daten an die Protokollierungsgeräte gesendet werden.

Des Weiteren sollten die Protokolldaten der Geräte innerhalb der Analysesoftware mit Flags gekennzeichnet werden, um so eine Differenzierung bei Anzeige und Reporting zu ermöglichen. So sind unter Umständen während eines Angriffs die von Layer-2-Switches gesendeten Protokolldaten von geringerem Interesse als die Daten, die das ID-System bereitstellt. Spezialisierte Applikationen wie zum Beispiel IDS verwenden häufig eigene Protokollierungsprotokolle zur Übertragung von Alarminformationen. Diese Daten sollten grundsätzlich an separate Managementhosts übermittelt werden, die für die Verarbeitung von Angriffsalarmzuständen besser ausgestattet sind.

Eine Kombination der Alarmdaten aus vielen unterschiedlichen Quellen ermöglicht unter Umständen einen Einblick in den Gesamtzustand des Netzwerks.

Um zu gewährleisten, dass Protokollmeldungen einander zeitlich entsprechen, müssen die Systemuhren der Hosts wie der Netzwerkgeräte aufeinander abgestimmt werden. Für Geräte, die NTP (Network Time Protocol) unterstützen, bietet dies eine effektive Möglichkeit zur Einstellung und Synchronisierung der genauen Uhrzeit auf allen Geräten. Im Falle eines Angriffs zählt jede Sekunde, denn es ist von großer Bedeutung, die genaue Reihenfolge der Schritte zu ermitteln, in denen der betreffende Angriff stattfand.

Im Hinblick auf das Management, zu dem wir hier alle auf einem Gerät oder durch einen Administrator ausgeführten Funktionen zählen, bei denen es sich nicht um Protokol-

lierung und Reporting handelt, stellen sich weitere Probleme und bieten sich weitere Lösungen an. Wie bei der Protokollierung und dem Reporting ermöglicht das OOB-Netzwerk auch in diesem Fall die Übertragung von Informationen in eine kontrollierte Umgebung, in der Manipulationen ausgeschlossen sind.

Dennoch sollte einer sicheren Konfiguration wie beispielsweise unter Verwendung von Secure Socket Layer (SSL) oder Secure Shell (SSH) der Vorzug gegeben werden, sofern dies möglich ist. SNMP ist mit größter Vorsicht zu genießen, da das zugrunde liegende Protokoll eine Reihe eigener Schwachstellen in Bezug auf die Sicherheit aufweist. Ziehen Sie in Erwägung, ob es nicht sinnvoll ist, über SNMP nur Lesezugriff auf die Geräte zuzulassen und den SNMP-Community-String mit derselben Sorgfalt zu schützen, die Sie auch bei einem root-Kennwort auf einem kritischen Unix-Host walten lassen würden.

Im Rahmen des sicheren Managements stellt das Management von Konfigurationsänderungen ein weiteres Problem dar. Wird ein Netzwerk angegriffen, sind Informationen über den Zustand kritischer Netzwerkgeräte sowie den Zeitpunkt der letzten bekannten Änderungen von größter Bedeutung. Daher sollte im Rahmen jeder umfassenden Sicherheitspolicy ein entsprechender Plan erarbeitet werden, zumindest jedoch sollten alle Änderungen unter Verwendung von Authentifizierungssystemen auf den Geräten sowie über FTP/TFTP archivierten Konfigurationen aufgezeichnet werden.

„Eine Kombination der **Alarmdaten** aus vielen **unterschiedlichen Quellen** ermöglicht unter Umständen einen **Einblick** in den **Gesamtzustand** des Netzwerks.“

Safe wurde während der Entwicklungsphase so weit wie möglich auf die funktionellen Anforderungen heutiger Unternehmensnetzwerke abgestimmt. Natürlich variierten die einzelnen Entscheidungen bezüglich der Implementierung je nach angestrebter Netzwerkfunktionalität, aber jeder Entscheidungsfindung lag eine Reihe gemeinsamer Designziele zugrunde. Diese werden nachfolgend nach Priorität geordnet aufgelistet:

- Policybasierte Sicherheit und Angriffsabwehr
- Sicherheitsimplementierung unter Verwendung der Infrastruktur (nicht einfach mit speziellen Sicherheitsgeräten)
- Sicheres Management und Reporting
- Authentifizierung und Autorisierung von Benutzern und Administratoren für kritische Netzwerkressourcen
- Angriffserkennung für kritische Ressourcen und Subnetze
- Unterstützung für neue Netzwerkanwendungen

Übersicht über die Safe-Architektur



Als Sicherheitsarchitektur muss Safe so weit als möglich verhindern, dass Angriffe auf wertvolle Netzwerkressourcen Erfolg haben. Neben der erforderlichen Sicherheit muss das Netzwerk aber auch weiterhin die wichtigen Dienste bieten, die die Benutzer erwarten. Eine solide Netzwerksicherheit in Kombination mit guter Netzwerkfunktionalität ist möglich.

Alle Angriffe, die die erste Verteidigungslinie überwinden (oder sogar aus dem Innern des Netzwerks kommen), müssen zuverlässig erkannt und rasch unter Kontrolle gebracht werden, um die negativen Auswirkungen auf das übrige Netzwerk so gering wie möglich zu halten. Zudem ist Safe vom Ansatz her zuverlässig und skalierbar.

Netzwerkzuverlässigkeit wird durch physische Redundanz gewährleistet, die Schutz bei einem Geräteausfall bietet, und zwar unabhängig davon, ob dieser nun durch Konfigurationsfehler, eine Störung oder einen Angriff auf das Netzwerk ausgelöst wurde. Es sind zwar einfachere Designs möglich, besonders, wenn keine hohen Leistungsanforderungen an das Netzwerk gestellt werden, hier wurde jedoch ein komplexes Design gewählt, da in komplexen Umgebungen die Entwicklung eines Sicherheitskonzepts komplizierter ist als in einfacheren Umgebungen. Innerhalb des Dokuments werden aber immer wieder Vorschläge gemacht, anhand derer sich das Design vereinfachen lässt.

Im Netzwerkdesign stellt sich immer wieder die Frage, ob besser integrierte Funktionalität in einem Netzwerkgerät oder ein Dienstgerät mit einer speziellen Funktion eingesetzt werden soll.

In vielen Fällen scheint die integrierte Funktionalität sicherlich die bessere Wahl zu sein, da sie in vorhandenen Geräten implementiert werden kann oder die Funktionen mit dem Gerät im Übrigen interagieren können.

Dienstgeräte hingegen werden häufig verwendet, wenn sehr weit reichende Funktionen erforderlich sind und/oder aufgrund der Leistungsanforderungen der Einsatz spezieller Hardware unumgänglich ist. So muss von Fall zu Fall unter Berücksichtigung der Kapazität und Funktionalität des Dienstgeräts gegenüber dem Integrationsvorteil des Netzwerkgeräts eine Entscheidung getroffen werden. So kann beispielsweise anstelle eines kleineren IOS-Routers mit separater Firewall ein integrierter IOS-Router mit höherer Kapazität und IOS-Firewallsoftware gewählt werden. Innerhalb der Safe-Architektur kommen beide Lösungsansätze zum Einsatz.

Struktur eines kleineren Netzwerkes

Für ein kleines Netzwerk-Design benötigt man zwei Module: Das Corporate Internet Modul und das Campus Modul.

Mit dem Corporate Internet Modul wird die Anbindung ans Internet hergestellt. Es terminiert VPN-Verbindungen sowie den Datenverkehr für öffentlich verfügbare Netzwerkdienste wie DNS, HTTP, FTP und SMTP. Das Campus Modul stellt als Basis Layer 2 Switching Funktionen zur Verfügung. Hier erfolgt die Anbindung sämtlicher User bzw. Arbeitsplätze, des Netzwerkmanagements sowie der Intranet Server für das Unternehmen. Dieses Design wird bei den Unternehmen als Head-End eingesetzt. Änderungen des Designs bei der Nutzung in Teilbereichen bzw. Filialen sind möglich.

Das Corporate Internet Modul stellt den internen Usern den Zugriff auf das Internet zur Verfügung. Externen Internet-Nutzern wird der Zugriff auf die öffentlichen Server bereitgestellt. Ein VPN-Zugang zur Anbindung von Außenstellen/Niederlassungen und Heim-Arbeitsplätzen wird ebenfalls zur Verfügung gestellt.

Schlüsselemente

- Der SMTP-Server holt die E-Mails vom Mail-Server des Service Providers ab und stellt diese den lokalen Clients zu Verfügung. Hier können die E-Mails bereits auf bösartige Inhalte hin untersucht werden.
- Der interne DNS Server beantwortet DNS-Anfragen, die Intranet-Systeme betreffen, Anfragen für externe Adressen werden ins Internet weitergereicht.

- FTP und HTTP Server stellen öffentliche Informationen über das Unternehmen und beispielsweise Preislisten und Updates für eigene Produkte zur Verfügung.
- Die Firewall bzw. der Firewall Router schützt das Unternehmensnetzwerk vor unautorisierten Zugriffen, filtert den Verkehr und terminiert VPN-Verbindungen von mobilen Benutzern und Außenstellen.
- Layer 2 Switches (mit Unterstützung privater VLANs) garantieren, dass die Daten kritischer Systeme immer über die Firewall laufen.

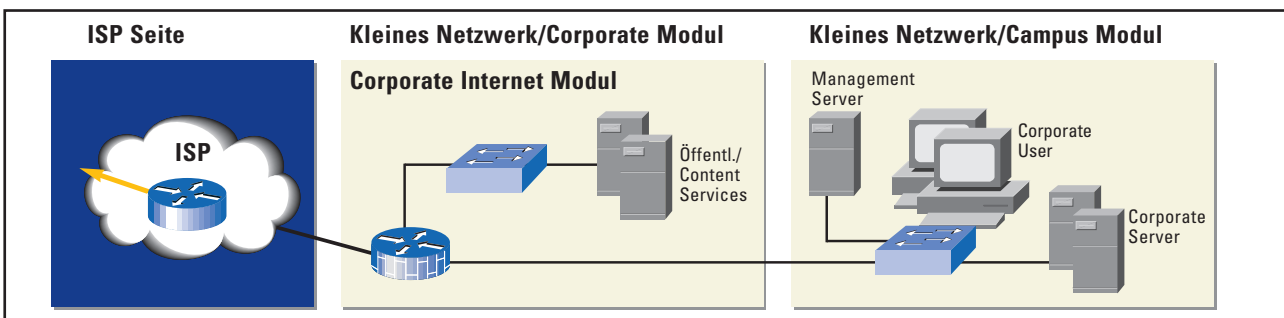


Abbildung 1: Detailliertes Modell eines kleineren Netzwerkes

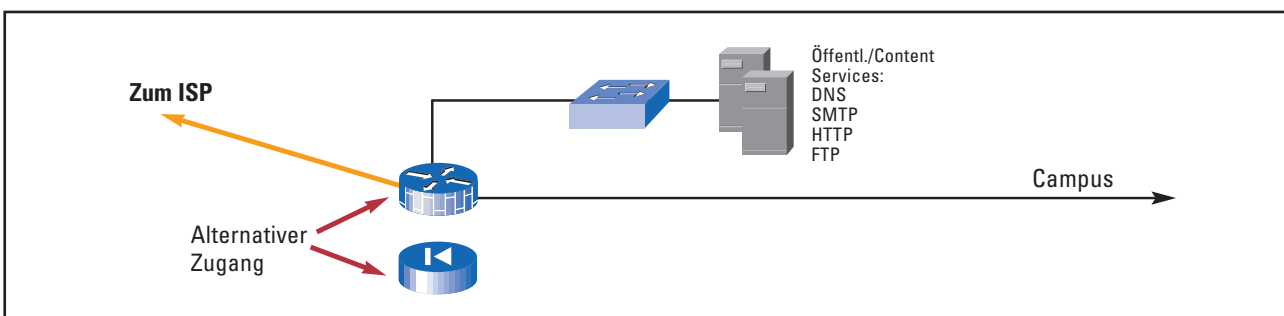


Abbildung 2: Detailliertes Modell des Internet-Moduls

Abwehr von Angriffen

Die öffentlich verfügbaren Server eines Unternehmens sind üblicherweise der Bereich, in dem am häufigsten Angriffe zu erwarten sind. Das Corporate Internet Modul bietet dem Unternehmensnetzwerk wirksamen Schutz bei folgenden Bedrohungen:

- Unautorisierte Zugriffe werden durch die Firewall verhindert.
 - Intrusion-Detection-Systeme (IDS) schützen öffentliche Server vor Application Layer Attacks.
 - Virenangriffe und das Einschleusen von Trojanischen Pferden werden durch Viren-Scanner auf Host- oder Server-Basis vermieden.
 - Passwort-Angriffe können vom Betriebssystem und den Intrusion Detection Systemen erkannt werden.
 - Garantierte Zugangsraten (CAR) auf der ISP-Seite und TCP-Intercept auf Router und Firewall beschränken die Angriffsmöglichkeiten beim Denial of Service (DoS).
- IP Spoofing wird durch Filterung nach RFC 2827 und 1918 ISP-seitig oder auf der lokalen Firewall verhindert.
 - Eine geschwächte Infrastruktur sowie der Einsatz von Host- und Netzwerk-basierten Intrusion Detection Systemen limitieren die Einsatzmöglichkeiten von Packet Sniffern.
 - Ein Ausspionieren der Netzwerke wird durch IDS erkannt. Geeignete Protokoll-Filter flankieren diese Maßnahme.
 - Trust Exploitation wird durch ein restriktives Trust-Modell sowie den Einsatz von privaten VLANs vermieden.
 - Eine Umleitung von Ports (Port Redirection) wird durch strenges Filtern und den Einsatz von Intrusion Detection Systemen verhindert.

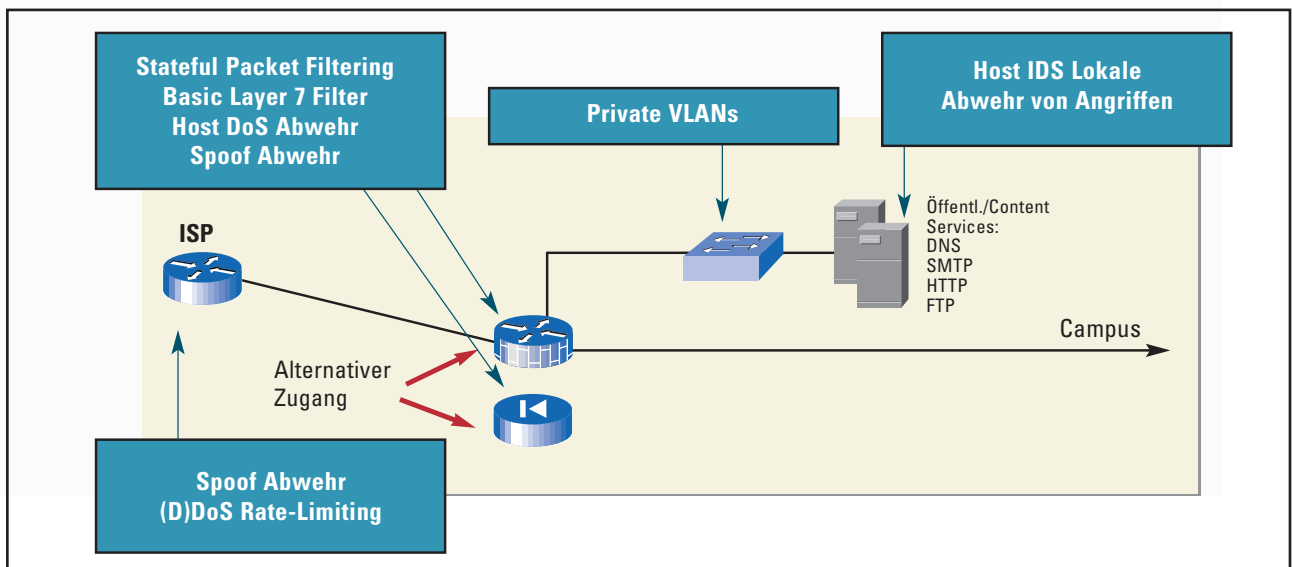


Abbildung 3: Abwehr von Angriffen im Corporate Internet Modul

Das Campus Modul

Das Campus Modul beinhaltet die Arbeitsstationen, die unternehmenseigenen Intranet Server, die Netzwerkmanagement-Server sowie die dazugehörige Layer 2 Infrastruktur. Üblicherweise können in kleinen Netzwerken sämtliche Layer 2 Funktionalitäten in einem einzigen Switch oder einem Stack zusammengefasst werden.

Schlüsselemente

- Über Layer-2-Switches werden allen Arbeitsstationen und Servern Infrastruktur-Dienste zur Verfügung gestellt.
- Der unternehmenseigene Intranet Server bietet Dienste wie File-Sharing, Print-sharing, DNS sowie die Bereitstellung von E-Mail-Diensten (SMTP, IMAP und POP3).
- Die berechtigten Arbeitsstationen erhalten Zugriff zu Datendiensten im Netz.

- Management-Systeme bieten Dienste wie IDS, Syslog, TACACS+/ RADIUS-Authentisierung, Autorisierung und Accounting sowie allgemeines Konfigurationsmanagement.

Abwehr von Angriffen

- Durch die geschichtete Architektur werden Packet Sniffer Attacks ineffizient.
- Host-basierte Virens Scanner schützen vor Viren und Trojanischen Pferden.
- Durch den Einsatz von Host-basierenden Intrusion-Detection-Systemen und Zugangskontrollen bei den Applikationen werden unautorisierte Zugriffe abgewehrt.
- Application Layer Attacks auf Betriebssystem und Anwendungen werden über Host-basierte IDS und immer aktuell gehaltene Virens Scanner vermieden.

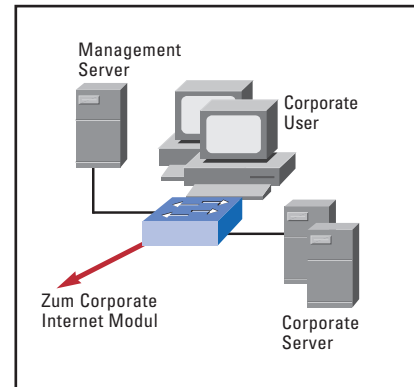


Abbildung 4: Campus Modul detailliert

- Trust exploitation – Private VLANs ermöglichen die kontrollierte Kommunikation zwischen Hosts auf einem Subnetz.
- Host-basierte IDS schützen vor der Installation von Port Redirection Agents.

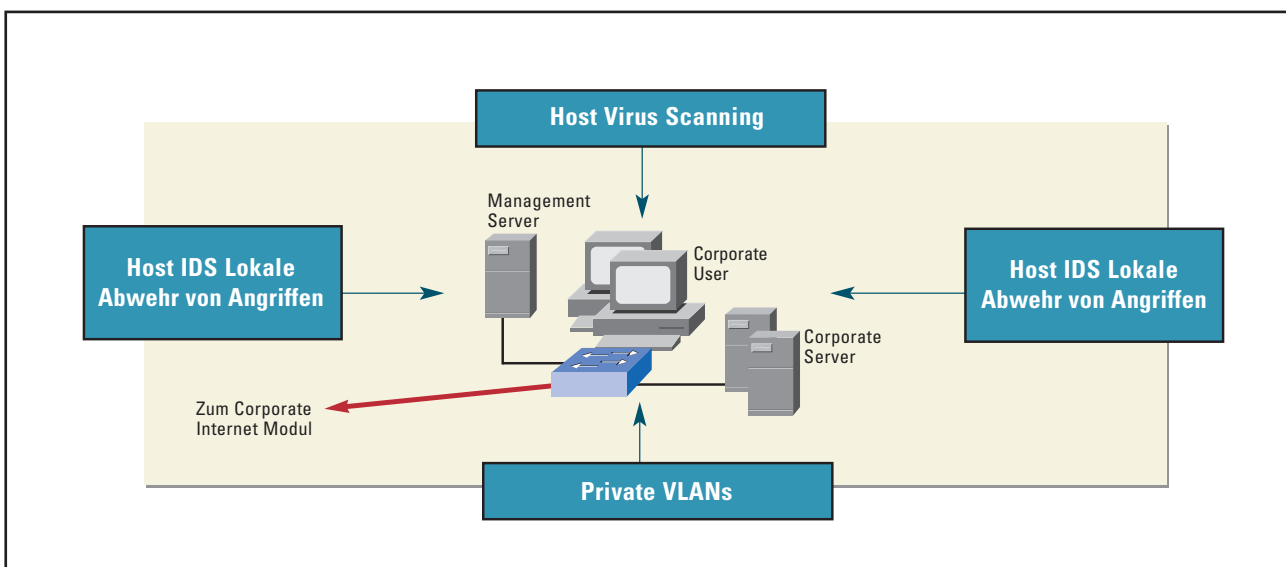


Abbildung 5: Abwehr von Angriffen im Campus Modul

Design eines mittelgroßen Netzwerkes

Ein Safe-konformes Netzwerk mittlerer Größe besteht aus drei Modulen: Dem Corporate Internet Modul, dem Campus Modul und dem WAN Modul. Wie beim Design für kleinere Netzwerke stellt das Corporate Internet Modul die Verbindung ins Internet her und terminiert VPN-Verbindungen sowie den Datenverkehr zu öffentlich verfügbaren Netzwerkdiensten. Nutzer oder Außenstellen, die sich per Einwahl verbinden wollen, werden ebenfalls im Corporate Internet Modul angeschlossen.

Das Campus Modul beinhaltet neben der Layer 2 auch die Layer 3-Infrastruktur. Hier erfolgt die Anbindung aller Benutzer, des Netzwerkmanagements sowie der Intranet-Server des Unternehmens. Für die Anbindung der Remote-User gibt es zwei Möglichkeiten: Entweder eine direkte Anbindung per Stand- oder Wählleitung an das WAN-Modul oder via IPSec VPN-Verbindung an das Corporate Internet Modul. Änderungen des Designs bei der Nutzung für Filiale und Außenstellen sind möglich.

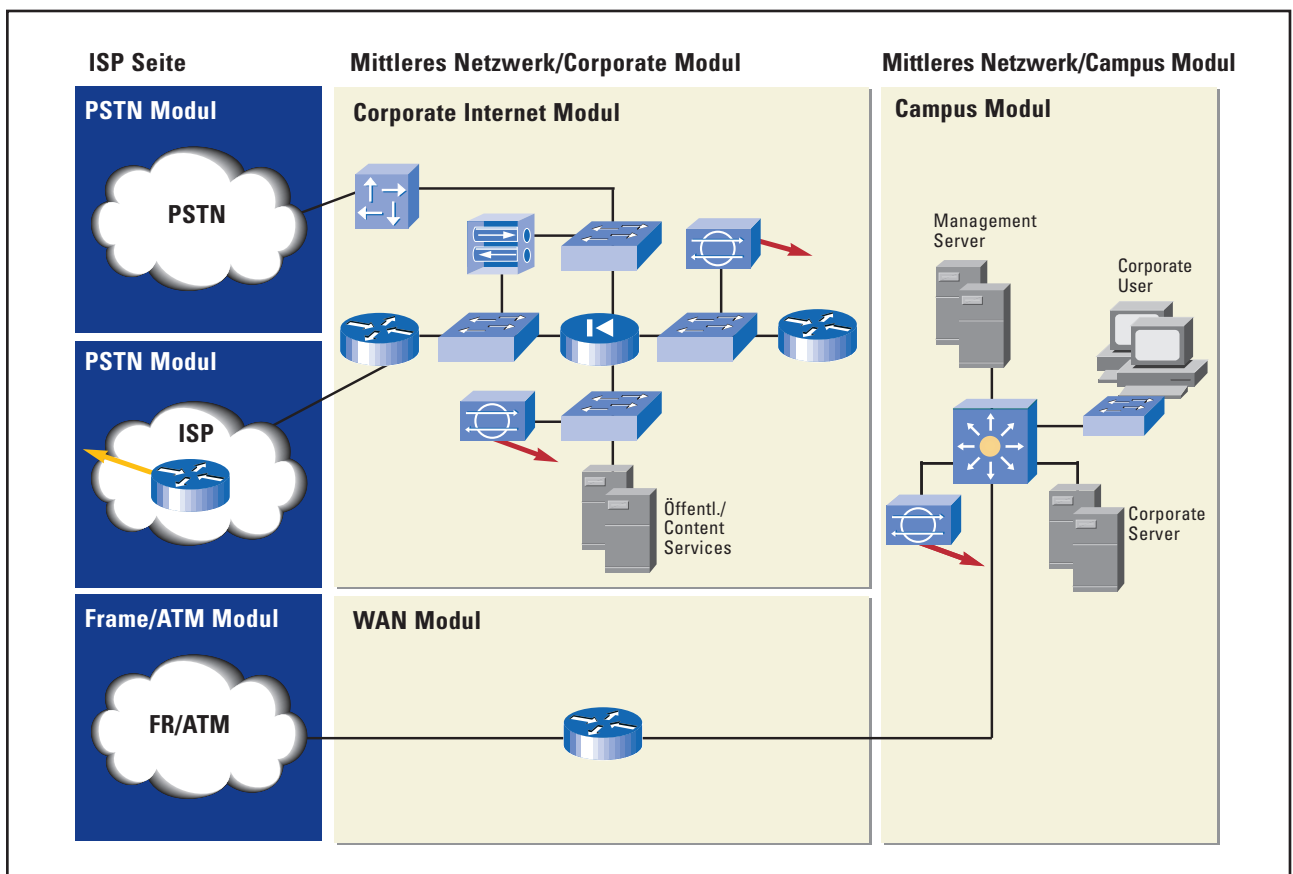


Abbildung 6: Design eines mittelgroßen Netzwerkes

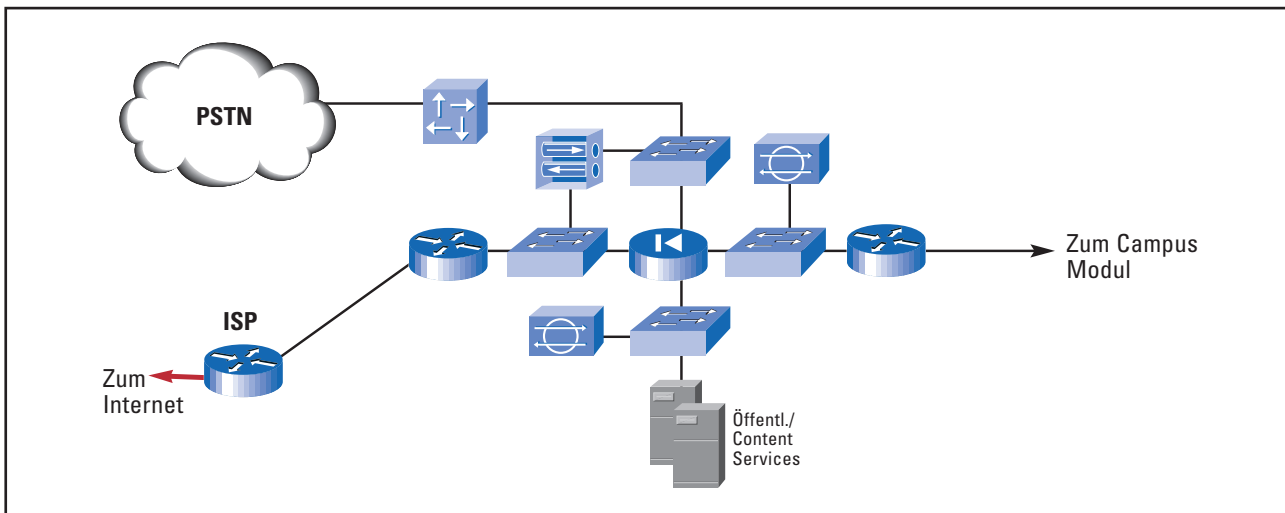


Abbildung 7: Corporate Internet Modul im mittelgroßen Netzwerk

Corporate Internet Modul

Das Corporate Internet Modul stellt den internen Usern über die öffentlichen Server (HTTP, FTP, SMTP und DNS) den Zugang zu den Internet Diensten bereit. Das Modul terminiert VPN-Tunnel aus Niederlassungen und von mobilen Benutzern sowie den Datenverkehr, der von Einwahl-Leitungen verursacht wird.

Schlüsselemente

- Der Dial-in Server authentifiziert mobile Benutzer und terminiert deren analoge oder ISDN-Wählverbindungen.
- Der interne DNS Server beantwortet DNS-Anfragen, die Intranet-Systeme betreffen, Anfragen für externe Adressen werden ins Internet weitergereicht.
- FTP und HTTP Server stellen öffentliche Informationen über das Unternehmen und beispielsweise Preislisten und Updates für eigene Produkte zur Verfügung.
- Die Firewall sorgt für einen Schutz der Ressourcen auf Netzwerkebene,

beispielsweise mit stateful-Filtering-Funktionen. Über unterschiedliche Sicherheitszonen stellt diese differenzierte Sicherheitslösungen für mobile Benutzer und andere zur Verfügung. Berechtigte externe Netze, z. B. Außenstellen- oder Partner-Netze, werden authentifiziert, IPSec-Tunnel für VPNs können auf der Firewall terminiert werden.

- Über Layer-2-Switches werden allen Arbeitsstationen und Servern Infrastruktur-Dienste zur Verfügung gestellt.
- Mit Hilfe netzwerkbasierter IDS Appliances werden die Netzwerk-Segmente auf Layer 4 bis Layer 7 innerhalb des Moduls überwacht.
- Der SMTP-Server holt die E-Mails vom Mail-Server des Service Providers ab und stellt diese den lokalen Clients zu Verfügung. Hier können die E-Mails bereits auf bösartige Inhalte hin untersucht werden.
- Auf dem VPN-Concentrator werden die VPN-Verbindungen mobiler Benutzer aus dem Internet terminiert.

Abwehr von Angriffen

Die öffentlich zugänglichen Server des beschriebenen Moduls sind möglichen Angriffen aus dem Internet ausgesetzt. Diese können folgendermaßen vereitelt werden:

- Unautorisierte Zugriffe werden durch Filter auf der ISP-Seite und dem Zugangsrouten sowie mittels der Firewall verhindert.
- Der Schutz vor Application Layer-Attacken erfolgt durch den Einsatz von Netzwerk- und Host-basierten Intrusion Detection Systemen.
- Content filtering, d. h. die Filterung aktiver oder ungewünschter Inhalte von E-Mails oder Websites, sowie IDS wehren Virenattacken und das Einschleusen von Trojanischen Pferden ab.
- Passwort-Angriffe können vom Betriebssystem und den Intrusion Detection Systemen erkannt werden.

- Garantierte Zugangsraten (CAR) auf der ISP-Seite und TCP-Intercept auf Router und Firewall beschränken die Angriffsmöglichkeiten beim Denial of Service (DoS).
- IP Spoofing wird durch Filterung nach RFC 2827 und 1918 ISP-seitig oder auf der lokalen Firewall verhindert.
- Eine geschichtete Infrastruktur sowie der Einsatz von Host- und Netzwerk-basierten Intrusion Detection Systemen limitieren die Einsatzmöglichkeiten von Packet Sniffern.
- Ein Ausspionieren der Netzwerke wird durch IDS erkannt. Geeignete Protokoll-Filter flankieren diese Maßnahme.
- Trust Exploitation wird durch ein restriktives Trust-Modell sowie dem Einsatz von privaten VLANs vermieden.
- Eine Umleitung von Ports (Port Redirection) wird durch strenges Filtern und den Einsatz von Intrusion Detection Systemen verhindert.
- Die Verwendung von Einmal-Passwörtern (OTP – One Time Passwords) verhindert sogenannten Brute-Force-Attacken.
- Durch den Einsatz von Firewall Diensten nach der Packet-Entschlüsselung wird der Zugriff auf unerlaubte Ports verhindert.
- „Man-in-the-middle“-Attacken können durch verschlüsselten Datenverkehr mit Außenstellen abgewehrt werden.
- Eine geschichtete Infrastruktur sowie der Einsatz von Host- und Netzwerk-basierten Intrusion Detection Systemen limitieren die Einsatzmöglichkeiten von Packet Sniffern.

Die RAS- und Site-to-Site-VPN-Dienste innerhalb des Moduls können ebenfalls Ziel von Angriffen werden:

- Network Topology Discovery – Filterlisten (Access Control Lists – ACL) auf dem Internet-Router beschränken den Zugriff auf den VPN Concentrator und die Firewall für Verschlüsselungszwecke.

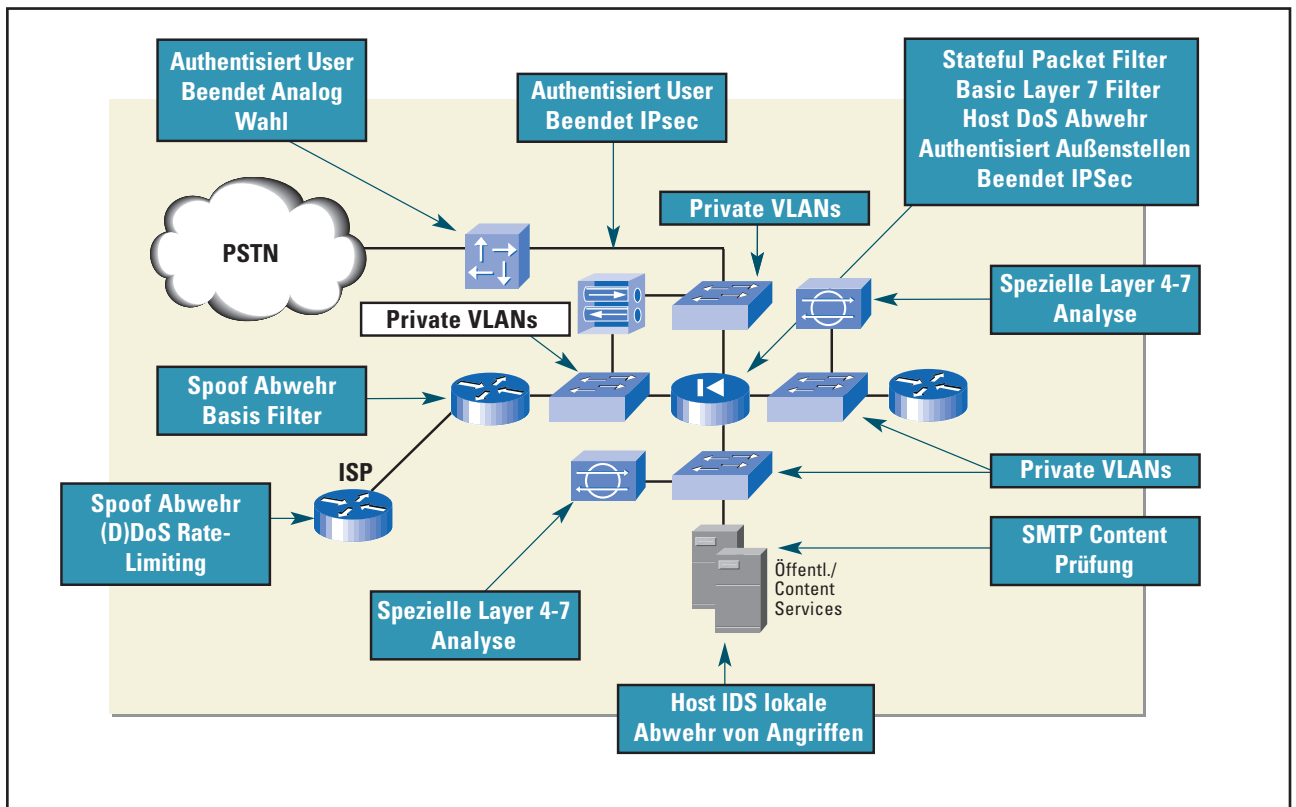


Abbildung 8: Abwehr von Angriffen im Corporate Internet Modul

Campus Modul

Das Campus Modul beinhaltet die Arbeitsstationen, die unternehmenseigenen Intranet Server, die Netzwerk-Management Server sowie die dazugehörige Layer 2 und Layer 3 Infrastruktur. Wie auch das Corporate Internet Modul für mittlere Netzwerke ist das Campus Modul frei von Redundanzen.

Schlüsselemente

- Layer 3 Switches sind für das Routing und Switching des Nutz- und Management-Datenverkehrs innerhalb des Campus-Moduls zuständig. Hier werden auch die Etagen-Switches angeschlossen sowie Filter-Regeln umgesetzt.
- Über Layer-2-Switches werden allen Arbeitsstationen Infrastruktur-Dienste zur Verfügung gestellt.
- Der unternehmenseigene Intranet Server bietet Dienste wie File-Sharing, Print-Sharing, DNS sowie die Bereitstellung von E-Mail-Diensten (SMTP, IMAP und POP3)
- Die Arbeitsstationen erhalten Zugriff zu den ihnen zur Verfügung stehenden Daten im Netzwerk.
- Der SNMP Management Host stellt Management-Dienste für SNMP-fähige Geräte zur Verfügung.
- Der IDS Management Host stellt allen Netzwerk-basierten IDS-Einheiten ein zentrales Management und eine zentrale Darstellung der Alarme zur Verfügung.
- Der Syslog Host sammelt und wertet die Syslog-Meldungen der Router, Firewalls und IDS-Systeme aus.
- Der Access Control Server liefert den Netzwerksystemen und Benutzern Dienste zur Authentifizierung, Autorisierung und zum Accounting.
- Der One-Time-Password (OTP) Server autorisiert die One-Time-Password Informationen, die vom Access Control Server angefragt werden.
- Der Ressource Manager liefert Informationen über Konfiguration, Systemsoftware und Hardware-Ausstattung der Netzwerksysteme.
- Mit Hilfe Netzwerk-basierter IDS Appliances werden die Netzwerk-Segmente auf Layer 4 bis Layer 7 innerhalb des Moduls überwacht.

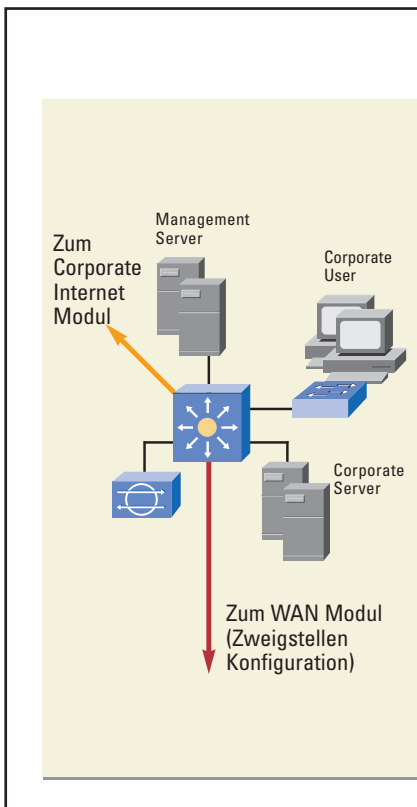


Abbildung 9: Detaillierte Ansicht des Campus Moduls

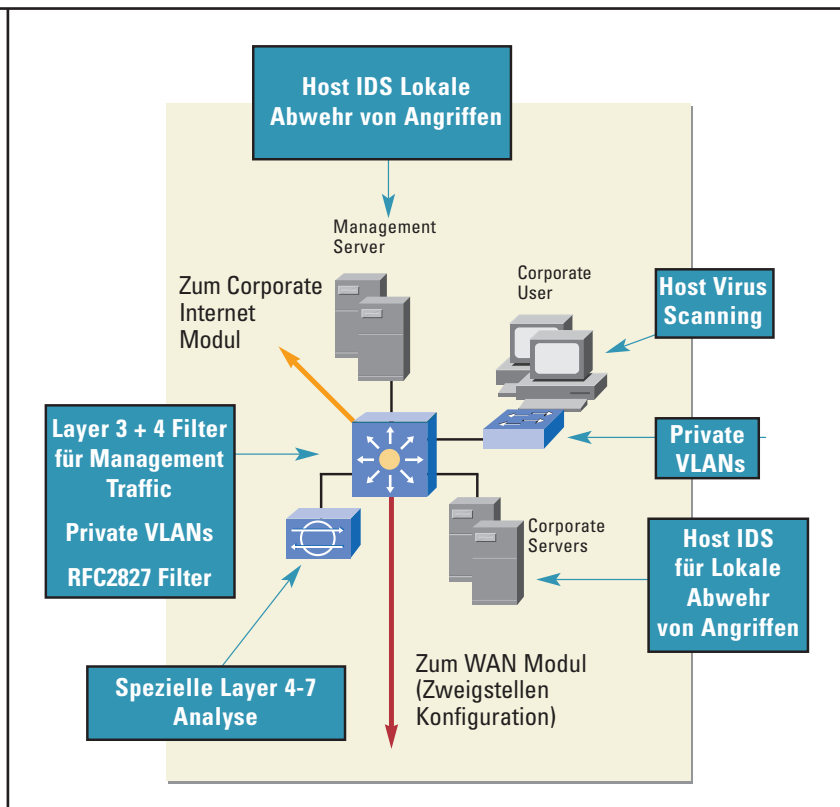


Abbildung 10: Abwehr von Angriffen im Campus Modul

Folgender Schutz wird geboten

- Eine geschwächte Infrastruktur limitiert die Einsatzmöglichkeiten von Packet Sniffern.
- Host-basierte Virens Scanner schützen vor Viren und Trojanischen Pferden.
- Application Layer Attacken auf Betriebssystem und Anwendungen werden über Host-basierte IDS, immer aktuell gehaltene Virens Scanner und Zugangs-Filter vermieden.
- Trust Exploitation wird durch ein restriktives Trust-Modell sowie dem Einsatz von privaten VLANs vermieden.
- IP Spoofing wird durch Filterung nach RFC 2827 und 1918 ISP-seitig oder auf der lokalen Firewall verhindert.
- Kritische Systeme werden durch eine Authentifizierung über den Access Control Server vor Password-Angriffen geschützt.
- Betriebssystem, Einheiten und Applikationen werden stets mit den neuesten Virenprofilen versorgt und schützen so, gemeinsam mit HIDS-Erkennung, vor Application Layer-Attacken.
- Eine Umleitung von Ports (Port Redirection) wird durch strenges

Filtern und den Einsatz von Intrusion Detection Systemen verhindert.

Das WAN Modul

Das WAN Modul wird nur dann erforderlich, wenn die Verbindung zu den Niederlassungen über ein privates Netzwerk – also über Stand- und Wählleitungen – erfolgen soll.

Schlüsselemente

- IOS-Router – Routing, Zugriffskontrolle und QoS-Mechanismen werden genutzt.

Remote User Design

Im folgenden werden insgesamt vier Safe-konforme Möglichkeiten vorgestellt, mobile Benutzer über das Internet an das Unternehmensnetz anzubinden.

- Software Zugang: Die Station des mobilen Benutzers wird mit dem Cisco VPN-Software-Client und einer Personal Firewall ausgerüstet.
- Zugang über eine externe Firewall: Die Arbeitsstation wird durch eine dedizierte Firewall geschützt und mit einem IPSec-Tunnel per VPN an das Unter-

nehmen angebunden. Die WAN Verbindung wird über einen Breitbandzugang (beispielsweise Kabel- oder xDSL) hergestellt.

- Zugang über einen Hardware VPN Client: Die Arbeitsstation nutzt einen Hardware VPN Client, der die IPSec-VPN-Verbindung zum Unternehmen über das Internet herstellt. Die WAN Verbindung wird über einen Breitbandzugang (beispielsweise Kabel- oder xDSL) hergestellt.

Folgender Schutz wird geboten

- Durch Filterung auf Layer 3 werden IP Spoofing-Attacken abgewehrt.
- Über einfache Access Control Listen auf dem Router kann der Zugriff auf Netzwerkressourcen beschränkt und kontrolliert werden.
- Zugang über einen Router: Die mobile Station nutzt einen Router, der eine IPSec-VPN-Verbindung zum Unternehmen herstellt. Der Router kann entweder einen direkten Zugang zum Breitbandnetz herstellen oder an ein Breitbandmodem angeschlossen werden. Weiterhin kann der Router mit einer IOS-Firewall-Software ausgestattet werden.

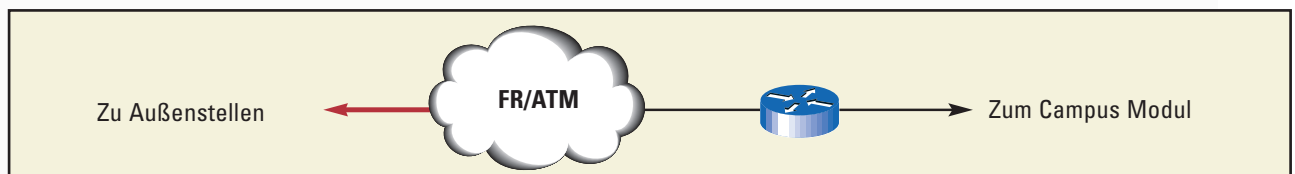


Abbildung 11: Darstellung WAN Modul

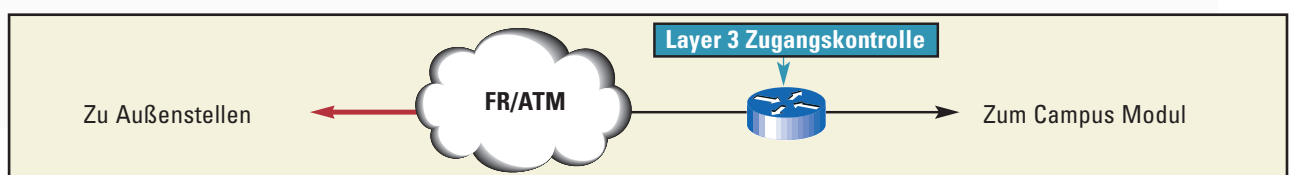


Abbildung 12: Zugriffskontrolle im WAN Modul

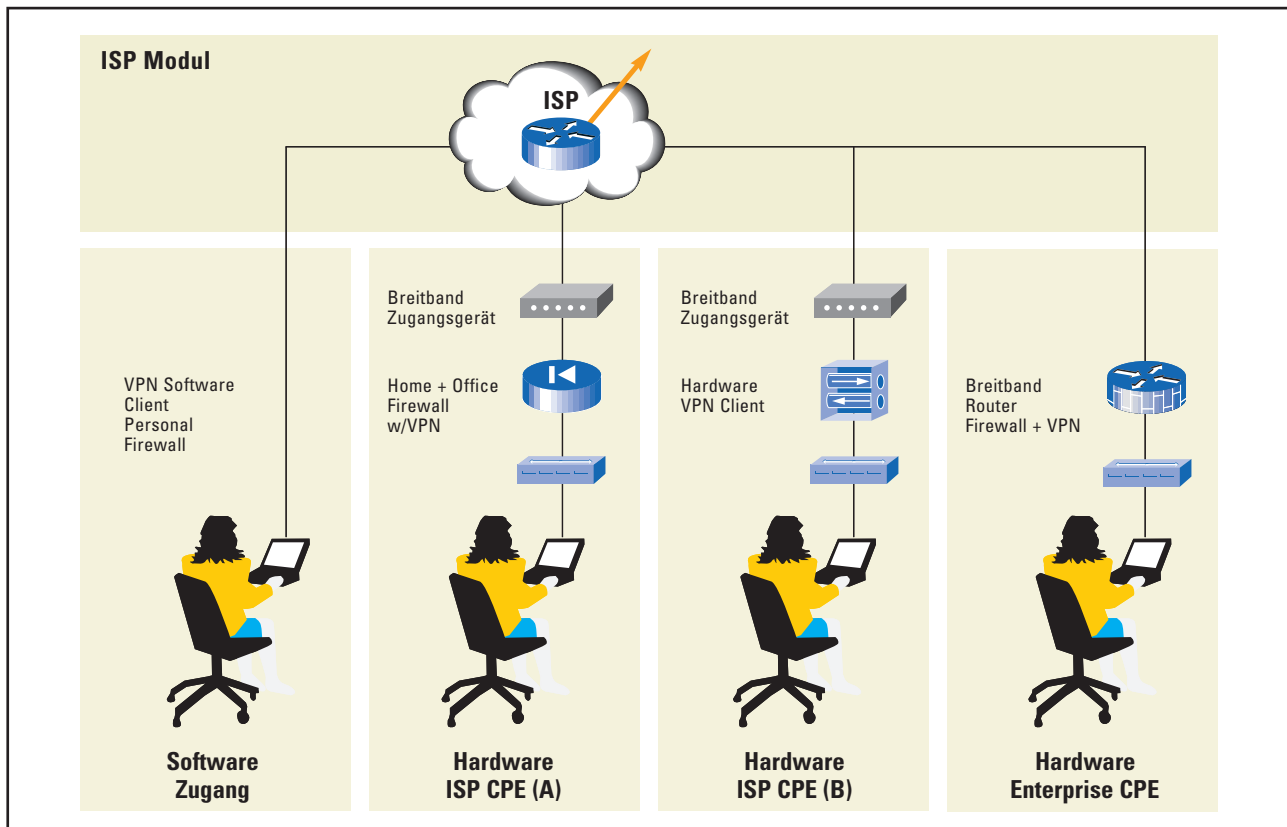


Abbildung 13: Detaillierte Ansicht der Konfiguration für mobile User

Bei allen dargestellten Verbindungen wird davon ausgegangen, dass die Verbindung via Internet hergestellt wird. Wenn private WAN Verbindungen (analoge oder ISDN-Wählleitung, Standleitung) genutzt werden, ist eine Verschlüsselung des Verkehrs nicht unbedingt notwendig.

Schlüsseltechnologien

- Ein Breitbandmodem stellt die Internet-Verbindung des mobilen Nutzers her.
- Eine dedizierte Firewall mit VPN-Unterstützung stellt sichere verschlüsselte Ende-zu-Ende Tunnel zwischen der Arbeitsstation und dem Headend des Unternehmens-
- netzwerkes her. Das Firewallsystem schützt den PC des mobilen Benutzers auf Netzwerk- und Transportebene durch die stateful-Inspection und die integrierte IDS-Funktion.
- Ein Hub- oder Layer-2-Switch verbindet die Systeme auf der Seite des mobilen Benutzers.
- Die Arbeitsstation des mobilen Benutzers wird über eine Personal Firewall zusätzlich geschützt.
- Der Router mit Firewall- und VPN-Funktion stellt sichere verschlüsselte Ende-zu-Ende Tunnel zwischen der Arbeitsstation und dem Headend des Unternehmensnetzwerkes her. Das Router-Firewallsystem schützt
- den PC des mobilen Benutzers auf Netzwerk- und Transportebene durch die stateful-Inspection Funktion und die integrierte IDS-Funktion. Der Router kann zusätzlich höherwertige Dienste wie QoS (Quality-of-Service) sicherstellen.
- Der VPN Software Client stellt sichere verschlüsselte Ende-zu-Ende Tunnel zwischen den individuellen PCs und dem Headend des Unternehmensnetzwerkes her.
- Der VPN Hardware Client stellt sichere Ende-zu-Ende verschlüsselte Tunnels zwischen der Arbeitsstation und dem Headend des Unternehmensnetzwerkes her.

Folgender Schutz wird geboten

- Unautorisierte Zugriffe werden über die stateful-Inspection Funktionen von Firewall oder Router-Firewall bzw. durch die Zugangskontrollen der Personal Firewalls auf den User-PCs verhindert.
- Protokoll-Filterung auf den Access-Devices der mobilen User verhindert, dass deren Netzwerke ausspioniert werden können.
- Wirksamer Virenschutz verhindert Virenangriffe und das Einschleusen von Trojanischen Pferden.
- IP Spoofing wird durch Filterung

nach RFC 2827 und 1918 auf Host-Level verhindert.

- Man-in-the-middle Attacken können durch verschlüsselten Verkehr mit Außenstellen verhindert werden.

Die zweite Möglichkeit besteht darin, die Funktion des VPN- und Remote-zugriffsmodus und die des Unternehmensinternetmoduls miteinander zu kombinieren.

Eine weitere Möglichkeit besteht darin, einige der IDS-Dienstgeräte wegzulassen. Je nach angewandter Strategie der Abwehr von Bedrohungen sind möglicher-

weise weniger NIDS-Dienstgeräte erforderlich. Grundsätzlich wird die Anzahl der erforderlichen IDS-Sensoren durch die Anzahl der kritischen Netzwerksegmente bestimmt. Dieser Punkt wird gegebenenfalls an entsprechender Stelle in den einzelnen Modulen erläutert.

Wie den meisten Lesern nicht unbekannt sein dürfte, handelt es sich beim Netzwerkdesign nicht um eine exakte Wissenschaft. Der Designer muss immer je nach gestellten Anforderungen individuelle Entscheidungen treffen.

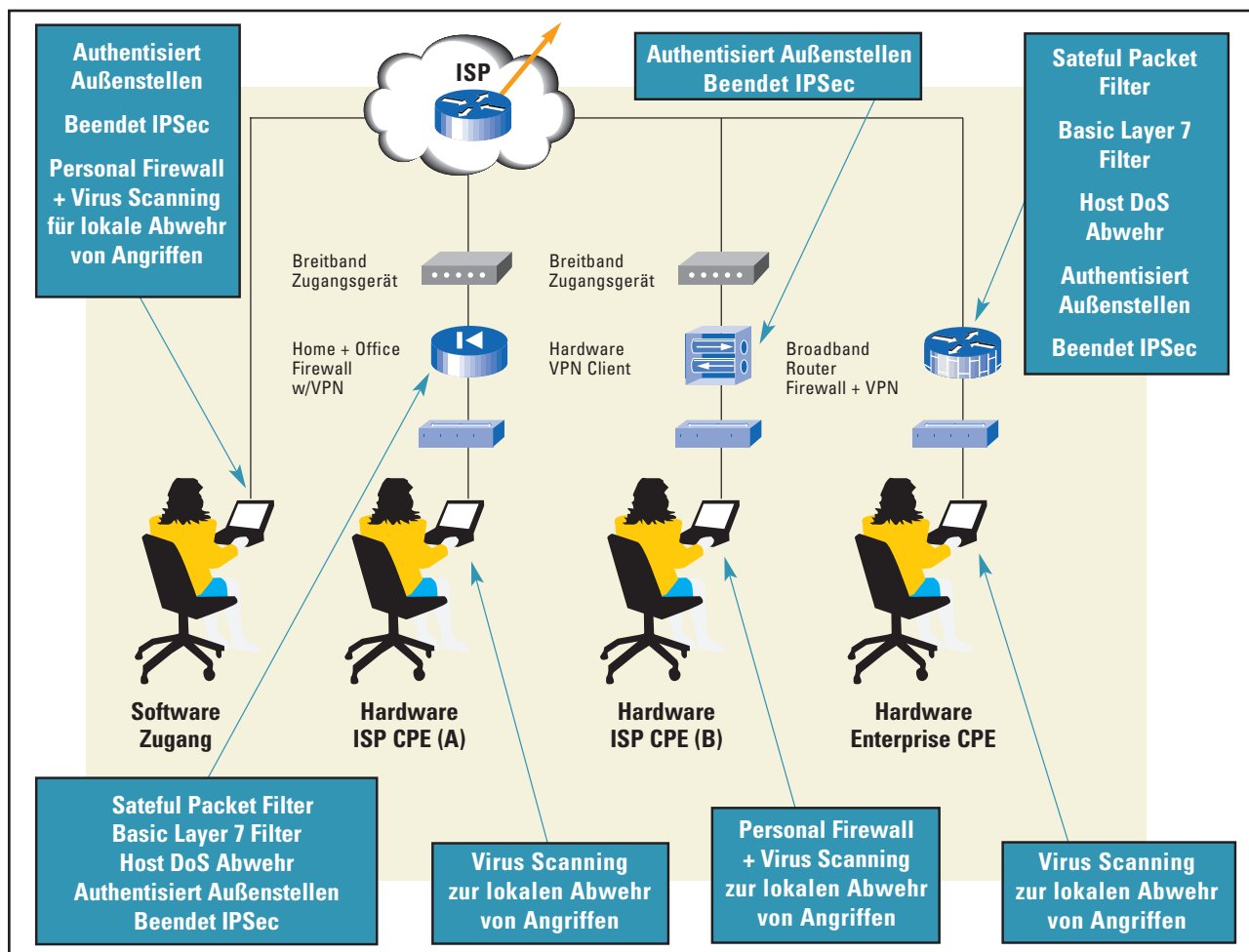


Abbildung 14: Remote-User-Design – Abwehr von Angriffen

Richtlinien zur Nutzung von Safe

Migrationstrategien

Safe bietet Hilfestellung für die Implementierung von Sicherheitslösungen in einem Netzwerk-System. Mit Hilfe von Safe können Systemarchitekten ihr Unternehmensnetzwerk unter den geforderten Sicherheitsaspekten flexibel gestalten.

Dabei sollte die Definition einer Security Policy die erste Aktivität bei der Migration eines Netzwerkes in eine sichere Infrastruktur darstellen.

Aufgrund der flexiblen Architektur kann Safe an die meisten Netzwerke angepasst werden. Safe erlaubt es, die Sicherheitsanforderungen einzelner Netzwerk-Funktion fast komplett unabhängig von anderen zu definieren. Jedes Modul ist eigenständig und mit der Prämisse aufgebaut, dass jedes Verbindungsmodul lediglich über ein niedriges Sicherheitslevel verfügt. Das Unternehmensnetzwerk kann in mehreren Phasen gesichert werden. Kritische Netzwerk-Funktionen können schnell abgesichert werden, ohne dass dabei das gesamte Netzwerk neu gestaltet werden muss.

„**Safe** ermöglicht es dem **Designer**, die **Sicherheitsanforderungen** einer jeden **Netzwerkfunktion** beinahe **unabhängig** von den anderen **Funktionen** zu erfüllen.“

Anhang: Architekturelemente

**Adapter:**

(auch: Netzwerkadapter) – siehe „Netzwerkkarte“

Applikationsserver:

Stellt Endbenutzern im Unternehmen direkt oder indirekt Applikationsdienste zur Verfügung. Die Dienste umfassen u. a. Workflow, allgemeine Bürotätigkeiten und Sicherheitsapplikationen.

Arbeitsgruppe:

(engl. „Workgroup“) Arbeitsgruppen (auch Segmente genannt) fungieren als Untereinheiten im Netz und werden meist durch gemeinsame Aufgaben definiert, z. B. Entwicklung, Fertigung, Vertrieb, Verwaltung etc. und können auch über weiträumig verteilte Standorte zusammenarbeiten. Im Netzwerk werden sie als eine Gruppe von PC-Arbeitsplätzen definiert, zu der auch Server und anderweitige Geräte im Netz gehören können und sind dadurch gekennzeichnet, dass sie meist gemeinsam bestimmte Anwendungen oder sonstige EDV-Ressourcen im Netz nutzen.

ATM:

Asynchronous Transfer Mode: Eine schnelle Datenübertragungstechnik für EDV-Netze, mit der sich ganz unterschiedliche Arten von Informationen übermitteln lassen, nämlich sowohl herkömmliche Computerdaten als auch Ton und Video. Die Daten werden in Form von Zellen befördert. ATM wird häufig im Backbone eingesetzt.

Backbone:

Jener Teil des EDV-Netzes, das als Hauptverkehrsader für den Datentransport dient – sozusagen das Rückgrat eines solchen Systems. Ein

Backbone ist eine Verbindung mit großer Bandbreite zwischen zwei Segmenten. Er verbindet lokale Netzwerke miteinander, entweder innerhalb eines Gebäudes oder auch zwischen räumlich getrennten Standorten (also zwischen Gebäuden, Städten, Ländern, Kontinenten).

Bandbreite:

Größtmögliche Datenmenge, gemessen in Bits pro Sekunde (bps), die von einer Netzwerkleitung übertragen werden kann.

Bridge:

Eine Netzwerkkomponente, die Datenpakete zwischen zwei Segmenten übermitteln, welche mit demselben Kommunikationsprotokoll arbeiten.

BRI:

Basic Rate Interface – ISDN-Anschluss mit zwei ISDN B-Kanälen.

Browser:

Ein Programm, mit dem man im Internet Informationen suchen und betrachten kann. Mit Hilfe des Browsers lassen sich auch Daten auf den eigenen PC übertragen (Download). Die am weitesten verbreiteten Browser sind von Netscape und Microsoft.

Client:

Ein Netzwerkteilnehmer – auch Knoten (engl. „Node“) genannt – wie beispielsweise ein Anwender-PC, der vom Server bereitgestellte EDV-Ressourcen nutzt.

Ethernet:

LAN Spezifikation, erfunden von der Xerox Corporation und gemeinsam von Xerox, Intel und Digital Equipment entwickelt. Ethernet-Netze nut-

zen verschiedene Kabeltypen: 1Base5, 10Base2, 10Base5, 10BaseF, 10BaseT.

Fast Ethernet:

Ethernet-Leitung mit 100 Mbps (siehe „Ethernet“)

Firewall (stateful packet inspection):

Gerät zur verbindungsorientierten Paketfilterung, welches Zustandstabellen für IP-basierte Protokolle verwaltet. Datenverkehr kann nur dann die Firewall passieren, wenn er den definierten Zugriffskontrollfiltern entspricht oder es sich dabei um einen Teil einer bereits initiierten Sitzung in der Zustandstabelle handelt.

Frame:

Ein Datenpaket mit variabler Länge, das per Frame-Relay-Technik durch EDV-Netze übertragen wird.

Frame Relay:

Ein Satz von Regeln für die Datenkommunikation, um kleinere Datenpakete über's Netzwerk zu versenden. Frame Relay verwendet Pakete mit variabler Länge und wird oft für WANs verwendet. Das ermöglicht eine schnelle und effizientere Datenübertragung, als dies mit Punkt-zu-Punkt-Verbindungen möglich wäre.

Homepage:

Die Leitseite einer Website und somit die erste Seite, die man beim Surfen im Internet zu sehen bekommt, sobald man im Browser eine entsprechende Internet-Adresse bzw. URL eingibt. Auf der Homepage befinden sich meist Verknüpfungen (sog. Hyperlinks) zu anderen Internetseiten innerhalb der betreffenden Site oder zu Seiten anderer Sites.

Host-basiertes ID-System:

Bei einem Host-basierten Intrusion Detection System handelt es sich um eine Softwareapplikation zur Überwachung der Aktivität auf einem einzelnen Host. Zu den Überwachungstechniken zählen u. a. die Validierung von Betriebssystem- und Applikationsaufrufen, die Überprüfung von Protokolldateien, Dateisysteminformationen und Netzwerkverbindungen.

HTML:

HyperText Markup Language – jene Programmiersprache, mit der die meisten Internet-Seiten erstellt werden.

Hub:

Sternverteiler für eine Gruppe von Knoten; wichtig für die zentrale Netzverwaltung, da Hubs für die LAN-Einbindung der Knoten nötig sind und die Reichweite der Netzwerkverbindungen vergrößern.

Hyperlinks:

Programmierte Verknüpfungen, die in Web-Seiten eingebaut werden können und von denen man beim Anklicken auf andere Seiten springen kann, egal wo diese im Internet liegen. Auch Hot-Spots genannt – sehr praktisch, um beispielsweise auf detaillierte Erläuterungen von Fachbegriffen zu verweisen.

IOS Firewall:

Optionale Erweiterung der Routersoftware Cisco Internetwork Operating System IOS um eine integrierte Firewall zur verbindungsorientierten Paketfilterung (stateful packet inspection).

IOS-Router:

Ein breites Spektrum an flexiblen Netzwerkgeräten, die zahlreiche

Routing- und Sicherheitsdienste für alle Leistungsanforderungen bieten. Die meisten Geräte sind modular und mit verschiedenen physikalischen LAN- und WAN-Schnittstellen ausgestattet.

IP:

Internet Protocol. Ein Satz von Regeln (TCP/IP = Transmission Control Protocol/Internet Protocol) für die Datenkommunikation im Internet. Es umfasst die Adressierung einzelner Rechner (Hosts) und Netzwerkkomponenten im World Wide Web sowie die Strukturierung einzelner Rechnerverbunde in logische Netzwerksegmente unter Berücksichtigung der entsprechenden Sicherheitsaspekte.

ISDN:

Integrated Services Digital Network – ein besonders leistungsfähiger Telekommunikationsdienst zum Übertragen von digitalisiertem Ton (Sprache und/oder Musik) sowie von Video und Computerdaten über öffentliche Telefonleitungen.

Knoten:

(engl. „Node“) – Verbindungspunkt von Segmenten (Leitungen) z. B. Hub, Router, Switch etc.

LAN:

Local Area Network – siehe „Lokales Netz“

Layer-2-Switch:

Bietet Bandbreite und VLAN-Dienste für Netzwerksegmente auf Ethernet-Ebene. In der Regel bieten diese Geräte individuelle geschaltete 10/100-Ports, Gigabit Ethernet-Uplinks, VLAN-Trunking und Funktionen zur L2-Filterung.

Layer-3-Switch:

Bietet ähnlich hohe Übertragungsraten wie der Layer-2-Switch mit zusätzlichen Routing-, QoS (Quality of Service)- und Sicherheitsfunktionen. Oftmals ist der modulare Switch mit Prozessoren für spezielle Funktionen ausgestattet.

Lokal:

Geräte, die unmittelbar am Standort des Netzwerkteilnehmers mit dem betreffenden PC verbunden sind (z. B. lokale Festplatte, lokaler Drucker) – im Gegensatz zu entlegenen Geräten, auf die der Zugriff über einen Server erfolgt (Remote Access).

Local Area Network:

LAN – siehe „Lokales Netz“

Lokales Netz:

(engl. „Local Area Network = LAN“) – ein EDV-Netz, in dem PC-Arbeitsplätze, Server und anderweitige Geräte (Drucker, Faxmaschinen, Scanner etc.) an einem Standort anhand einer bestimmten Technik miteinander verbunden sind.

Managementserver:

Bietet Betreibern von Unternehmensnetzwerken Dienste für das Netzwerkmanagement. Diese Dienste umfassen u. a. allgemeines Konfigurationsmanagement, Monitoring von Geräten für die Netzwerksicherheit und Ausführung von Sicherheitsfunktionen.

Netzwerk-basiertes ID-System:

Netzwerk-basiertes Intrusion Detection System. Dieses System überwacht stetig den Datenverkehr in einem LAN-Segment und versucht, den Echtzeitdatenverkehr mit bekannten Angriffssignaturen zu vergleichen.

Diese Signaturen reichen von unteilbaren Signaturen (einzelnes Paket in nur einer Richtung) bis zu zusammengesetzten Signaturen (mehrere Pakete), für die Zustandstabellen und Layer-7-Applikationsüberwachung erforderlich sind.

Netzkerbetriebssystem (NOS = Network Operating System)

Systemsoftware, mit der sich die Ressourcen eines EDV-Netzes verwalten lassen (z. B. Netware, Unix, Windows NT). Zu den typischen NOS-Leistungsmerkmalen gehört die gemeinsame Nutzung von Dateien (File Sharing), E-Mail, Druckerdiensten und Vorkehrungen zur Sicherung der Daten sowie deren Schutz vor unbefugtem Zugriff.

Netzwerkkarte:

(engl. Network Interface Card = NIC) – meist in Form einer Steckkarte im PC, Drucker, Scanner oder anderweitigen Geräten eingebaut, sorgt der Netzwerkkarte für die Verbindung zum EDV-Netz und steuert in Zusammenarbeit mit den anderen Netzwerkkomponenten den Datenaustausch.

NIC:

Network Interface Card = Netzwerkschnittstellenkarte, siehe „Netzwerkkarte“

POTS:

Plain Old Telephone Service – Anschlussbezeichnung für konventionelles, analoges Telefon, Faxgerät, Modem.

PRI:

Primary Rate Interface – PRI-Ports nutzen einen Primärmultiplexanschluss der Telekom und können bis zu 30

ISDN B-Kanäle für Ein- und Auswahl gleichzeitig verwalten.

Print Server:

Ein Computer, der die gemeinsame Nutzung von Druckern in größeren Netzen ermöglicht – darauf spezialisiert, im EDV-Netz die Druckaufträge mehrerer Netzwerkteilnehmer an die gewünschten Drucker zu übermitteln und zu koordinieren.

Protokoll:

Formale Beschreibung einer Reihe von Regeln und Übereinkünften, in denen festgelegt ist, wie der Datenaustausch zwischen Geräten im Netzwerk erfolgt.

Router:

Eine spezielle Netzwerkkomponente, die die Verbindung zwischen EDV-Netzen oder Netzwerksegmenten herstellt und die Zustellung der Daten über bestimmte Routen an die vorgesehenen Adressdaten im Netz erledigt. Router verwenden eine oder mehrere Messgrößen, um den optimalen Pfad zu ermitteln, auf dem Netzwerkverkehr weitergeleitet werden soll. Sie arbeiten ähnlich wie Bridges, beherrschen jedoch zusätzliche Funktionen (z. B. Zugriffskontrolle, Protokollumsetzungen, usw.) und arbeiten auf OSI-Ebene 3.

Segment:

Gruppe von Netzwerkteilnehmern, die mit einem Hub verbunden sind – siehe „Arbeitsgruppe“

Server:

Ein Netzknoten, der den Client-Rechnern im EDV-Netz alle möglichen Dienste bereitstellt, vom Datei-zugriff über Druckermanagement bis hin zur Ausführung von Programmen

(remote Execution), die nicht auf dem Client liegen, aber von diesem genutzt werden können.

SMTP-Inhaltsfilterungsserver:

Eine Applikation, die in der Regel auf einem externen SMTP-Server ausgeführt wird, den Inhalt ein- und abgehender E-Mails (einschließlich Anhänge) überwacht und darüber entscheidet, ob eine E-Mail unverändert weitergeleitet, verändert und weitergeleitet oder zurückgewiesen wird.

Splitter:

Ein Gerät für ADSL-Anschlüsse, das den Anschluss von konventionellem Telefon und Fax erlaubt.

Switch:

Eine Netzwerkkomponente, die die Datenpakete der Netzwerkteilnehmer empfängt, zwischenspeichert und nur an den bzw. die anhand der physikalischen Zieladresse definierten Empfänger weiterleitet – ähnlich wie eine Fernmeldezentrale Telefongespräche vermittelt.

URL:

Uniform Resource Locator – vereinheitlichte Benennung von Netzwerkressourcen im Internet, sei es eine Web-Adresse z. B. <http://www.cisco.com/> oder eine bestimmte Information (E-Mail, Dokumentation etc.) im World Wide Web.

URL-Filterungsserver:

Eine Applikation, die in der Regel auf einem Stand-alone-Server ausgeführt wird und URL-Anforderungen überwacht, die von einem Netzwerkgerät an diesen Server weitergeleitet wurden. Das Netzwerkgerät wird darüber in Kenntnis gesetzt, ob die Anforderung

in das Internet weitergeleitet wird. Ein Unternehmen hat so die Möglichkeit, eine Sicherheitspolicy zu implementieren, durch die bestimmt wird, auf welche Internetsites kein Zugriff erlaubt wird.

VPN-Terminierungsgerät:

Terminiert IPSec-Tunnel entweder für Site-to-Site- oder Remotezugriffs-VPN-Verbindungen. Dieses Gerät sollte zusätzliche Dienste bieten, damit dieselbe Netzwerkfunktionalität wie in einer klassischen WAN- oder DFÜ-Verbindung gewährleistet werden kann.

WAN:

siehe „Wide Area Network“

Wide Area Network (= WAN):

Ein Netz, das auf räumlich getrennte Standorte verteilt ist und das zwei oder mehrere LANs miteinander verbindet. Normalerweise erfolgt der Datenaustausch über ISDN, serielle (Stand-)Leitungen oder auch über Richtfunkstrecken bzw. via Satellit.

Workgroup:

siehe „Arbeitsgruppe“

Workstation:

PC-Arbeitsplatz im EDV-Netz – in dieser Broschüre meist Clients genannt.

Workstation oder Benutzerterminal:

Jedes Gerät im Netzwerk, das direkt von einem Endbenutzer verwendet wird. Dazu zählen u. a. PCs, IP-Telefone und drahtlose Geräte.

Abbildungslegende



Router



Router mit Firewall Funktionalität



Firewall



Network Intrusion Detection System Sensor



Layer 3 Switch



Access Server



VPN Concentrator



Layer Switch



Workstation



Management Server



Modem



VPN Hardware Client



Deutschland

Cisco Systems GmbH
Kurfürstendamm 22
D-10719 Berlin

Cisco Systems GmbH
Neuer Wall 77
20354 Hamburg

Cisco Systems GmbH
Hansaallee 249
40549 Düsseldorf

Cisco Systems GmbH
Friedrich-Ebert-Allee 67
53113 Bonn

Cisco Systems GmbH
Industriestraße 3
65760 Eschborn

Cisco Systems GmbH
Am Wilhelmsplatz 11
70182 Stuttgart
(Herold Center)

Cisco Systems GmbH
Lilienthalstraße 9
85399 Hallbergmoos

Tel.: 0180-3 67 10 01

www.cisco.de

Österreich/ Schweiz

Cisco Systems Austria GmbH
Milleniumtower
Handelskai 91-96
A-1200 Wien
Tel.: +43/1 240 30 60 00
Hotline: 0 0800/9 99 90 522
www.cisco.at

Cisco Systems Switzerland GmbH
Glatt-Com
CH-8301 Glattzentrum
Tel.: +41/1/878 9200

www.cisco.ch