CISCO SYSTEMS

CONSULTANT NEWS

Aktuelle Informationen für Beratungsunternehmen

Ausgabe Dezember 2000

Company News

Cisco übernimmt Radiata

Cisco Systems übernimmt Radiata, Inc. Das Unternehmen mit Sitz in San Jose, Kalifornien, und Sydney, Australien, ist ein führender Hersteller von Chips und Prozessoren für drahtlose Highspeed-Netze. Die Übernahme erfolgt im Rahmen der „New- World"-Strategie von Cisco. Mit den Produkten von Radiata können drahtlose Netzwerke für schnellere Datenraten entwickelt werden, die dem IEEE-Standard 802.11a entsprechen.

http://www.cisco.com/warp/public/3/de/4-presse/meld_2000/11_07_2000_pmeld.html

Unified-Messaging-Lösung mit Active Voice

Cisco Systems übernimmt die Active Voice Corporation. Das Unternehmen aus Seattle, Washington, ist ein führender Anbieter von IP-Lösungen (Internet Protocol) zum Unified Messaging. Mit diesen Lösungen können Unternehmen E-Mail-, Sprach- und Fax-Nachrichten in einer gemeinsamen Mailbox zusammenführen und diese jederzeit von jedem beliebigen Endgerät mit Internet-Zugang abrufen. Die Übernahme von Active Voice steht im Kontext der Cisco-Strategie für Unified Communications und Sprach-, Daten- und Videointegration in Ende-zu-Ende IP-Netzwerken von Unternehmen.

http://www.cisco.com/warp/public/3/de/4-presse/meld_2000/11_06_2000_pmeld.html

Babcock und Cisco unterzeichnen „Trusted Advisor Agreement"

Die Babcock Borsig AG, international operierender Technologie-Konzern für Energie und Schiffbau, und Cisco haben auf der Kölner Netzwerk-Messe Exponet mit der Unterzeichnung eines „Trusted Advisor Agreement" ihre strategische Partnerschaft bekräftigt. Cisco unterstützt Babcock als „Trusted Advisor" bei der Umsetzung von E-Business-Initiativen wie Customer Relationship Management und E-Commerce sowie bei der Optimierung der internen Geschäftsprozesse. Als weltweiter Technologie-Partner von Babcock stattet Cisco das Unternehmen mit der dafür erforderlichen IT-Infrastruktur aus.

http://www.cisco.com/warp/public/3/de/4-presse/meld_2000/11_09_2000_pmeld.html

Lufthansa wählt Cisco zum Partner für E-Business-Strategie

Cisco Systems und die Deutsche Lufthansa haben ein strategisches Abkommen unterzeichnet. Der weltweit führender Anbieter von Netzwerk-Lösungen für das Internet wird das Luftfahrt-Unternehmen mit technologischer Netzinfrastruktur ausstatten und bei der Planung und Entwicklung von Internet basierenden E-Business-Lösungen beraten.

http://www.cisco.com/warp/public/3/de/4-presse/meld_2000/11_05_2000_pmeld.html

Technologie News

Erweiterung des Sicherheitskonzepts CiscoSAFE

Mit der Cisco Secure PIX Firewall 535 und der Cisco Secure PIX Firewall VPN Accelerator Card stellt der Netzwerk-Gigant neue Erweiterungen für Firewalling und VPN-Netze vor. Durch die VPN Services Accelerator Cards erreichen die Router der Serien Cisco 7140 VPN und Cisco 7200 einen extrem hohen Durchsatz beim Aufbau von VPNs. Diese Neuerungen sind Bestandteil von CiscoSAFE, dem Cisco Sicherheitskonzept für zuverlässiges und skalierbares E-Business. Mit der kontinuierlichen Erweiterung der SAFE-Strategie reagiert Cisco auf die rasch anwachsende Nachfrage nach robusten und skalierbaren Sicherheitslösungen mit hoher Performance für Unternehmens- und Service-Provider-Netzwerke.
Zu CiscoSAFE finden Sie einen weiteren Artikel in dieser CN-Ausgabe.

http://www.cisco.com/warp/public/3/de/4-presse/meld_2000/12_02_2000_pmeld.html

GPRS-Roaming – Cisco macht das Internet mobil

Cisco Systems liefert die Ende-zu-Ende-IP-Infrastruktur für den weltweiten GRX Service (GPRS Roaming Exchange) von Equant und Sonera. Mit den Highspeed-Routern und Switches von Cisco lassen sich die Mobilfunknetze unterschiedlicher Betreiber verbinden. Es kommen vor allem die auf Standards basierenden Internet-Router der Reihe Cisco 12000 GSR zum Einsatz. Der GRX Service ermöglicht das Roaming zwischen GPRS-Netzen (General Packet Radio Standard) mehrerer Betreiber und den nahtlosen Zugriff auf mobile Internet-Anwendungen und Services auf der ganzen Welt.

http://www.cisco.com/warp/public/3/de/4-presse/meld_2000/12_01_2000_pmeld.html

Cisco erweitert QoS Policy Manager
Ab sofort ist der Quality of Service (QoS) Policy Manager in der neuen Version 2.0 (QPM 2.0) erhältlich. Mit erweiterten Funktionalitäten wurde der QPM auf die zunehmend komplexere Administration der QoS-Policies großer Unternehmen zugeschnitten. Dadurch lassen sich auch große Installationen auf Service-Ebene einfacher und zuverlässiger verwalten. Die QoS-Steuerung der Ressourcen in Netzwerken ermöglicht eine zuverlässige Übertragung kritischer Informationen. Neben der verbesserten QoS-Administration konvergenter Netze für Sprache, Daten und Video unterstützt der QPM 2.0 auch eine Reihe neuer Geräte und Software.
http://www.cisco.com/warp/public/3/de/4-presse/meld_2000/11_08_2000_pmeld.html

Unabhängige IP-basierende Voice-Messaging-Lösung
Netzwerk-Gigant Cisco Systems und CarryVoice, ein Anbieter eines offenen auf IP-basierenden Voicemail-Systems, realisieren gemeinsam eine Unified-Communication-Lösung. Sprache und Daten werden dabei Carrier-unabhängig auf einem Server zentralisiert. Das System gleicht einem Informationsspeicher, in dem Sprache, Anrufe, E-Mails und Faxverkehr für jeden einzelnen Benutzer hinterlegt werden. Der Anwender kann im Einzelfall entscheiden, wie er die Information weiter verarbeiten möchte. Er kann sich seine Nachrichten vorlesen lassen, sie ablegen oder kommentiert weiterleiten. Unified Communication ist über Telefon oder das Internet möglich.
http://www.cisco.com/warp/public/3/de/4-presse/meld_2000/12_03_2000_pmeld.html

Highspeed-Fernzugriff auf Unternehmensnetze
Cisco Systems und iPass, ein Anbieter von Remote Access auf das Internet, bieten mit „Global Broadband Roaming" den ersten Breitband-Roaming-Service, mit dem Geschäftsreisende einen einfachen und sicheren Highspeed-Fernzugriff auf ihr Unternehmensnetzwerk erhalten. Die beiden Unternehmen arbeiten an einem weltweiten Breitbandnetz, mit dem Service Provider auch Dienste außerhalb ihres Einzugsgebietes sowie eine einfache, integrierte Gebührenabrechnung anbieten können. Mobile Mitarbeiter können den Service zu Hause, im Büro oder unterwegs in Anspruch nehmen.
http://www.cisco.com/warp/public/3/de/4-presse/meld_2000/12_05_2000_pmeld.html

Cisco mit neuem Breitband-Router
Cisco uBR10012 heißt der neue Breitband-Router des Netzwerk-Giganten. Das hoch skalierbare CMTS (Cable Modem Termination System) wurde für die Zusammenfassung des Datenverkehrs am Edge von Kabelnetzen optimiert und basiert auf dem Universal Broadband Router von Cisco. Der uBR10012 wurde als Aggregations-Plattform mit hoher Kapazität entwickelt, die eine neue Ebene der Intelligenz an die Kante des Netzwerkes verlagert, sodass Anbieter von Kabeldiensten ihre Umsätze durch die Übertragung anspruchsvollerer Services an ihre Teilnehmer maximieren können. Durch seine Flexibilität und Skalierbarkeit eignet sich der uBR10012 als Mittelpunkt von IP-Breitbandnetzen.
http://www.cisco.com/warp/public/3/de/4-presse/meld_2000/12_04_2000_pmeld.html

Cisco erweitert Sprach-/Daten-Integration für Mittelstand
Eine Erweiterung seiner konvergenten Ende-zu-Ende-Lösungen bietet Cisco Systems mit dem neuen Integrated Communications System (ICS) 7750. Einfache Verwaltung, Web- und Sprach/Daten-Anwendungen stehen im Vordergrund. Niederlassungen von Großunternehmen sowie mittelständische Betriebe können so den Schritt zum dynamischen und reaktionsschnellen E-Business-Unternehmen tätigen. Der ICS 7750 bietet Investitionssicherheit für die zukünftige Integration leistungsfähiger „New-World"-Applikationen wie Unified Messaging, integrierte Web-basierte Call-Center, interaktive Websites mit Daten-, Sprach- und Video-Kommunikation.
http://www.cisco.com/warp/public/3/de/4-presse/meld_2000/12_07_2000_pmeld.html

DSL-Anschluss für den professionellen Einsatz
Mit dem neuen ADSL-Router (Asynchronous Digital Subscriber Line) Cisco 826 erweitert Cisco Systems die Router der Reihe 800. Das Gerät unterstützt ADSL über ISDN-Anschlüsse und bietet mit der Software Cisco IOS eine Funktionalität für den Einsatz in Unternehmen und für Telearbeiter. Mit dem neuen Cisco 826 können Service Provider ihren Teilnehmern DSL-Mehrwertdienste anbieten und damit ihre Betriebskosten senken sowie die Kundenbasis ausbauen.
http://www.cisco.com/warp/public/3/de/4-presse/meld_2000/12_06_2000_pmeld.html

SAFE – Ein Security-Framework für Unternehmensnetze

Cisco wird von Kunden häufig nach einem Sicherheitskonzept für ihr Unternehmen gefragt. Es ist immer schwierig, eine zufriedenstellende Antwort auf diese Frage zu geben, denn es gibt kein Standard-Sicherheitskonzept. Sicherheit ist ein Prozess, der individuell an die Anforderungen im Unternehmen angepasst werden muss. Der Wert der verwendeten Informationen und die Bedrohungen, denen diese Informationen ausgesetzt sind, entscheiden, welche Maßnahmen getroffen und wie tief diese implementiert werden. An der Lösung dieser komplexen Aufgabe sind viele Unternehmensbereiche beteiligt. Grundsätzlich aber ist Sicherheit vor allem Chef-Sache. Nur so kann eine nahtlose, ganzheitliche Umsetzung der Firmen-Sicherheitspolitik erreicht werden.

Um den Kunden die Orientierung zu erleichtern, hat Cisco ein Security-Framework für Unternehmensnetze (SAFE) entwickelt. SAFE stellt ein Handbuch für Netzwerkdesigner dar. Sein Ziel ist es, Informationen zur optimalen Vorgehensweise bei der Konzeption und Implementierung sicherer Netze zur Verfügung zu stellen. Der zur Gewährleistung der Netzwerksicherheit gewählte Ansatz zeichnet sich durch tief greifende Abwehrmechanismen aus. Das Augenmerk richtet sich primär auf die zu erwartenden Bedrohungen und die Methoden ihrer Abwendung. Es ist nicht damit getan, einfach hier eine Firewall und dort ein Intrusion Detection System (IDS) einzusetzen.

Für die SAFE-Architektur wurde ein modularer Aufbau gewählt. Unternehmensnetze setzen sich in der Regel aus folgenden Blöcken zusammen:

- Enterprise-Campus-Netzwerk
- Enterprise Edge
- Service Provider Edge

Diese Blöcke lassen sich weiter verfeinern. Für jeden Block werden Anforderungen bestimmt und Sicherheitsmechanismen definiert, um diese Anforderungen zu erfüllen. So kann im Rahmen der Architektur die sicherheitstechnische Beziehung zwischen den einzelnen Funktionsblöcken des Netzwerks beschrieben werden. Daraus ergibt sich ein mehrschichtiger Ansatz, bei dem auch der Ausfall eines Systems aller Wahrscheinlichkeit nach keine Sicherheitsverletzungen anderer Netzwerkressourcen nach sich zieht. SAFE basiert auf den Produkten von Cisco und der Cisco-EcoSystem-Partner.

SAFE beschreibt eine allgemeine Sicherheitsarchitektur und ersetzt in keinem Fall eine Firmen-Sicherheitspolitik. Diese wird vielmehr vorausgesetzt. Virtuelle private Netzwerke (VPNs) sind in dieser Architektur zwar berücksichtigt, werden jedoch nicht ausführlich besprochen.

Übersicht über die Architektur

Designgrundlagen

SAFE wurde während der Entwicklungsphase so weit wie möglich auf die funktionellen Anforderungen heutiger Unternehmensnetze abgestimmt. Der Architektur liegen eine Reihe gemeinsamer Designziele zugrunde:

- 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 Netzwerkapplikationen

Ein weiteres Designkriterium ist, dass Sicherheit die Anwender und die Anwendungen nicht behindert und sich transparent in die Infrastruktur integriert. SAFE eröffnet keine revolutionären Wege im Netzwerkdesign, sondern zeigt lediglich auf, wie Netzwerke gesichert und zuverlässig, gut skalierbar und redundant implementiert werden können.

Integrierte Funktion oder zusätzliche Hardware?

Es stellt sich immer wieder die Frage, ob Sicherheitsfunktionen in einen Netzwerkknoten integriert oder ob eine spezialisierte Hardware eingesetzt werden soll. In vielen Fällen scheint die integrierte Funktionalität die bessere Wahl zu sein. Sie spart Kosten und hält die Komplexität des Designs in Grenzen. Spezialisierte Hardware wird beispielsweise dann verwendet, wenn sehr weit reichende Funktionen erforderlich sind oder wenn ihr Einsatz aufgrund der Leistungsanforderungen unumgänglich ist. So kann in bestimmten Fällen anstelle eines integrierten Cisco-IOS-Routers mit IOS-Firewall-Software auch eine Kombination aus IOS-Router und PIX-Firewall zum Einsatz kommen, wenn die Leistungsanforderungen vom integrierten Gerät nicht mehr erfüllt werden können.

Innerhalb von SAFE kommen beide Arten von Systemen zum Einsatz. Viele kritische Sicherheitsfunktionen wurden inzwischen aufgrund der Leistungsanforderungen in großen Unternehmensnetzwerken auf speziell dafür vorgesehene Dienstgeräte verlagert.

Modulares Konzept

Für die SAFE-Architektur wurde ein modularer Aufbau gewählt. Dieser bietet zwei wichtige Vorteile: Zum einen kann im Rahmen der Architektur auf diese Weise die sicherheitstechnische Beziehung zwischen den einzelnen Funktionsblöcken des Netzwerks berücksichtigt werden. Zum anderen bietet dieser Aufbau Designern die Möglichkeit, Sicherheitsmechanismen Modul für Modul zu bewerten und zu implementieren, ohne die gesamte Architektur in nur einem Schritt bewältigen zu müssen.

Die nachfolgende Abbildung zeigt die erste Modulschicht in SAFE. Hierbei stellt jeder Block einen Funktionsbereich dar. Das ISP-Modul wird nicht durch das Unternehmen selbst implementiert. Einige Sicherheitsfunktionen müssen jedoch von jedem Internet Service Provider (ISP) gefordert werden, um Angriffe abzuwehren.

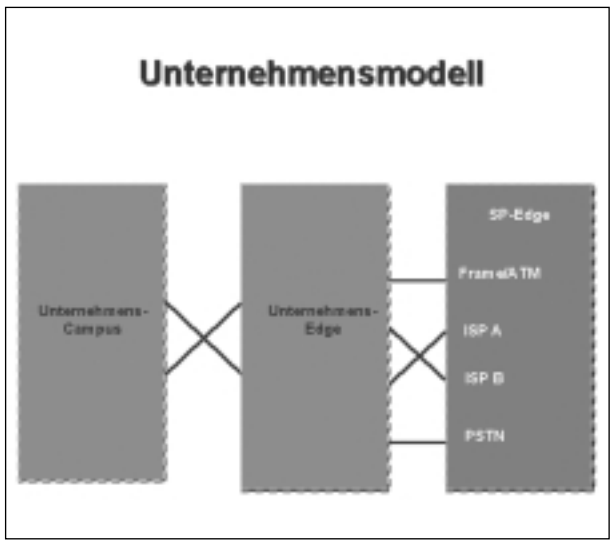

Abbildung 1: Unternehmensmodell

Abbildung 2 stellt die Unterteilung der Module in die Funktionsbereiche dar. Diese Module erfüllen innerhalb des Netzwerks bestimmte Aufgaben. Darüber hinaus gelten jeweils spezielle Sicherheitsanforderungen. Die Größe, in der die einzelnen Module dargestellt sind, ist jedoch nicht als Hinweis auf den tatsächlichen Anteil dieser Module am eigentlichen Netzwerk zu werten. So kann beispielsweise das Gebäudemodul, in dem die Endbenutzergeräte zusammengefasst sind, 80 Prozent der Netzwerkgeräte umfassen.

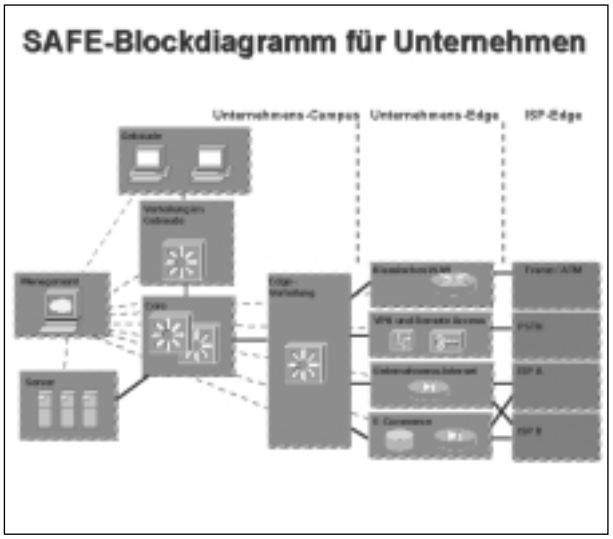

Abbildung 2: SAFE-Blockdiagramm für Unternehmen

Die Grundsätze von SAFE

Router sind Angriffsziele

Router haben grundsätzlich die Aufgabe, den Zugang zum Netz zu kontrollieren. Deshalb müssen sie gegen direkte Kompromittierung gesichert werden.
Die Sicherungsmaßnahmen sollten folgende Punkte umfassen:

- 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

Weitere Informationen zu diesem Thema finden sich auf der Website von Cisco Systems (siehe Literatur).

Switches sind Angriffsziele

Ebenso wie Router sind auch Switches (sowohl Layer 2 als auch Layer 3) besonderen Sicherheitsrisiken ausgesetzt. Die meisten im vorangegangenen Abschnitt über Router genannten Sicherheitstechniken sind auch auf Switches anwendbar. Folgende Maßnahmen sind zu empfehlen:

- Trunk-Funktionalität für alle Non-Trunking-Ports deaktivieren
- VLANs sollten nicht zu sehr ausgedehnt, vielmehr durch L3-Funktionalität verbunden werden.
- Ungenutzte Ports deaktivieren
- VLANs sind als einziges Mittel zur Verkehrstrennung nicht sicher genug, da ein zu großes Fehlerpotenzial im Hinblick auf menschliches Versagen besteht. Bei der Konzeption von VLANs und VLAN-Taggingprotokollen wurden Sicherheitsfragen nicht in Betracht gezogen, deshalb ist die alleinige Verwendung von VLANs zur sicheren Verkehrstrennung in sensiblen Umgebungen nicht zu empfehlen.

Auch zu diesem Thema finden sich weitere Informationen im Internet (siehe Literatur).

Private VLANs

Innerhalb einer VLAN-Architektur bieten private VLANs in bestimmtem Maße zusätzliche Sicherheit. 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 von einem einzelnen kompromittierten Host kein weiterer Angriff auf andere Resourcen im selben VLAN erfolgen.

Hosts sind Angriffsziele

Hosts stellen das beliebteste Angriffsziel im Netzwerk 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 Applikationsdienste zur Verfügung stellen, sind sie innerhalb des Netzwerks sehr exponiert. Zur Sicherung von Hosts müssen alle einzelnen Komponenten des Hostsystems mit Sorgfalt ausgewählt werden. Es müssen stets die neuesten Patches, Fehlerkorrekturen und Updates installiert werden. Dabei darf aber auch die spezielle Wirkung dieser Patches auf die Funktion der anderen Komponenten im System nicht außer Acht gelassen werden, da diese möglicherweise zu unerwünschtem Verhalten des Systems führt. 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

Lassen sich einzelne Komponenten eines Unternehmensnetzwerkes nicht kompromittieren, so kann dennoch ein Angriff gegen das gesamte Netzwerk gestartet werden. dDoS (distributed Denial of Service)-Angriffe stellen eine Attacke gegen die Verfügbarkeit von Unternehmensnetzen dar. Durch Manipulation einer Vielzahl von ungenügend geschützten Rechnern im Internet lassen sich hohe Verkehrsvolumina mit gefälschten IP-Adressen (IP-Spoofing) produzieren. Werden diese gezielt auf ein Firmennetz gerichtet, können sie das gesamte Netzwerk lahm legen. Häufig verwendete Formen von dDoS-Tools arbeiten mit ICMP-, TCP-SYN- oder UDP-Flooding. Im Februar 2000 wurde die Mächtigkeit dieser Angriffe sehr eindrucksvoll bei den Angriffen auf CNN.com, ebay.com oder Amazon.com deutlich.

Netzwerke sollten generell mit Angriffserkennung, Firewalls, Logging und aktivem Monitoring ausgestattet sein, um Angriffe rechtzeitig zu erkennen. Leider nutzen diese Sicherheitsvorkehrungen bei einem dDoS-Angriff nichts.

Es gibt dennoch Möglichkeiten, die Mächtigkeit solcher Angriffe zu reduzieren. Quality-of-Service (QoS)-Maßnahmen im Netzwerk erlauben es, die verfügbare Bandbreite individuell den Diensten zuzuteilen. So läßt sich Traffic-Policing dazu verwen-

den, nicht gewünschten Verkehr (ICMP, TCP-SYN oder UDP Echo) gezielt zu verwerfen. Dieser Verkehr erreicht das Unternehmensnetz nicht mehr und kann nicht zu dDoS-Zwecken missbraucht werden. Filterungen gemäß RFC 2827 und RFC 1918 schränken die Möglichkeiten für IP-Spoofing ein und reduzieren so das Risiko.

Applikationen sind Angriffsziele
Applikationen sind fehleranfällig. Solche Fehler können gutartig sein, wenn sie zum Beispiel dazu führen, dass ein Dokument im Druck merkwürdig aussieht. Sie können aber auch schwerwiegender Natur sein, wenn beispielsweise aufgrund eines Fehlers die Kreditkartennummern auf dem Datenbankserver per Anonymus FTP abgerufen werden können.

Eine Vielzahl dieser Probleme kann mit Hilfe von Intrusion-Detection-Systemen (IDS) erkannt werden. IDS können Angriffe entweder basierend auf einer Signatur oder mit Hilfe von Heuristiken oder Künstlicher Intelligenz aufspüren. Außerdem unterscheidet man zwischen Host- und Netzwerk-basierten IDS. Das Cisco IDS ist netzwerkbasiert und verwendet eine Signatur-Datenbank mit mehr als 300 bekannten Angriffsmustern.

Neben der reinen Erkennung und dem Alarmieren bei Angriffen oder Unregelmäßigkeiten kann ein IDS auch aktiv reagieren.Im einfachsten Fall wird die verdächtige Verbindung mittels TCP-Reset beendet. Eine weitere Methode, um Angreifer auszusperren, ist Shunning. Hierbei wird vom IDS eine temporäre Access-Control-Liste (ACL) auf dem Edge-Device generiert, die den Verkehr von verdächtigen Quellen für einen bestimmten Zeitraum blockiert.

Sicheres Management und Reporting
In der Praxis werden teilweise Daten von über 100 Geräten protokolliert und analysiert. 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 beantwortet werden, wenn ein effektives Management von sicheren Netzen 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?

Die Funktionsbereiche der SAFE-Architektur
Ein Unternehmensnetzwerk setzt sich aus zwei Funktionsbereichen zusammen, nämlich dem Campus- und dem Edgebereich. Diese sind wiederum in Untermodule aufgeteilt, die den unterschiedlichen Funktionen des jeweiligen Bereichs im Einzelnen entsprechen.

SAFE-Module des Unternehmens-Campus-Bereiches
Im Hinblick auf Bedrohungen unterscheiden sich Unternehmensnetzwerke nicht von den meisten anderen Netzen, die mit dem Internet verbunden sind. Es gibt interne Benutzer, die Zugriff auf Ressourcen außerhalb des Netzwerks benötigen, und externe Benutzer, die auf die Ressourcen des internen Netzwerks zugreifen müssen. Zudem gibt es eine Reihe allgemeiner Bedrohungen, die zu der Art von anfänglicher Kompromittierung führen, die ein Hacker sich zunutze machen kann, um tiefer in das Netzwerk einzudringen und dort Schaden anzurichten.

Unternehmensmodul
Das Unternehmensmodul setzt sich aus folgenden Untermodulen zusammen:
- Edgeverteilungsmodul
- Kernmodul
- Servermodul
- Gebäudeverteilungsmodul
- Gebäudemodul (Benutzer)
- Managementmodul

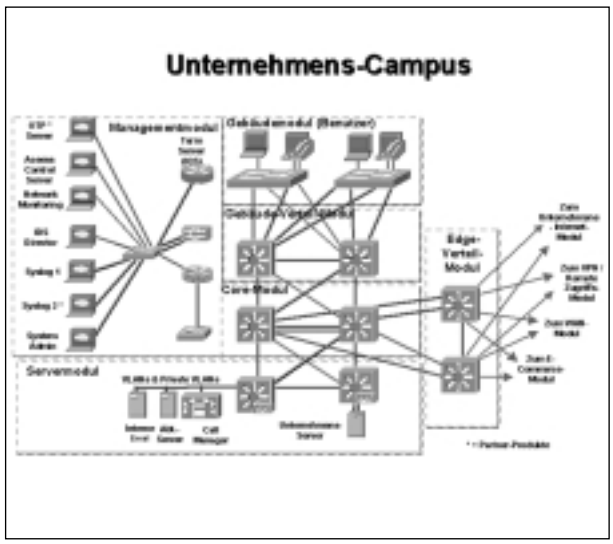

Abbildung 3: Der Unternehmens-Campus

Die SAFE-Architektur beschreibt detailliert jedes Modul auf der Hardware-Ebene, listet mögliche Bedrohungen auf und gibt Hinweise, wie diese abgewendet werden können. Im Abschnitt Entwicklungsrichtlinien werden die Designüberlegungen hergeleitet. Am Beispiel des Managementmoduls wird die Vorgehensweise verdeutlicht. Die vollständige Erläuterung der SAFE-Architektur findet sich im SAFE-Whitepaper (siehe Literatur).

Managementmodul
Das Managementmodul (Abbildung 4) implementiert das sichere Management aller Geräte und Hosts innerhalb der SAFE-Architektur. Protokoll- und Reportinginformationen werden von den Geräten an die Managementhosts gesendet, während Inhalte, Konfigurationen sowie neue Software umgekehrt von den Managementhosts an die Geräte gesendet werden.

Hauptgeräte

- SNMP-Managementhost
  – bietet SNMP-Management für Geräte
- NIDS-Host
  – sammelt Alarme für alle NIDS-Geräte (Network Intrusion Detection Systems) im Netzwerk
- Syslog-Hosts
  – sammeln Protokollinformationen für PIX- und NIDS-Hosts
- Zugangskontrollserver
  – stellt einmalige Zwei-Wege-Authentisierungsdienste für die Netzwerkgeräte zur Verfügung
- OTP-Server
  – autorisiert die vom Zugangskontrollserver übertragenen Einmalkennwörter (OTP – One-Time Password)
- Systemadministrationshost
  – ist zuständig für Konfigurations-, Software- und Inhaltsänderungen an Geräten
- Cisco IOS Firewall
  – ermöglicht die differenzierte Kontrolle des Verkehrsflusses zwischen den Managementhosts und den verwalteten Geräten
- Cisco Catalyst-Switches
  – gewährleisten, dass die Daten von den verwalteten Geräten nur direkt an die IOS Firewall übermittelt werden können

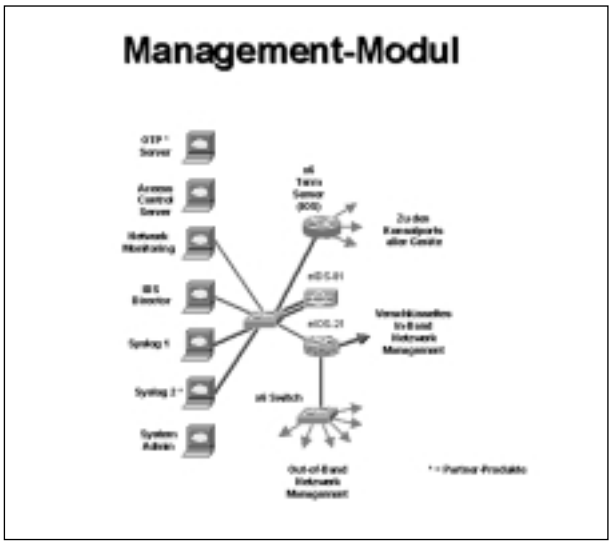

Abbildung 4: Das Managementmodul im einzelnen

Abgewendete Bedrohungen (Abbildung 5)

- Unberechtigter Zugriff
  – durch die Filterung an der IOS Firewall wird unberechtigter Datenverkehr in beide Richtungen in den meisten Fällen abgefangen
- „Mann-in-der-Mitte"-Angriffe (man-in-the-middle)
  – Managementdaten passieren ein privates Netzwerk, wodurch „Mann-in-der-Mitte"-Angriffe erschwert werden
- Kennwortangriffe
  – der Zugangskontrollserver ermöglicht eine strenge Zwei-Faktoren-Authentifizierung an jedem Gerät
- IP-Spoofing
  – gespoofter Datenverkehr in beide Richtungen wird an der IOS Firewall abgefangen
- Packet Sniffer
  – der Einsatz von Paket-Sniffern ist in einer geswitchten Infrastruktur nur begrenzt effektiv
- Vertrauensbruch
  – private VLANs verhindern, dass ein kompromittiertes Gerät sich als Managementhost ausgibt

Abbildung 5: Angriffsabwehr im Managementmodul

SAFE-Module des Unternehmens-Edge-Bereiches

Das Edge-Modul setzt sich ebenfalls aus Untermodulen zusammen. SAFE unterscheidet folgende Module:

- ISP-Module: A und B
- E-Commerce-Modul
- Unternehmens-Internet-Modul

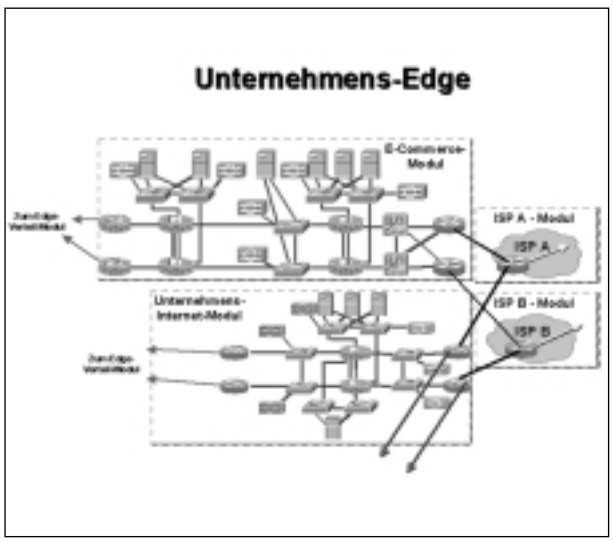

Abbildung 6: Das Unternehmens-Edge

Unternehmens-Internet-Modul
Das Unternehmens-Internet-Modul bietet internen Benutzern die Verbindung zu Internetdiensten und Internetbenutzern Zugriff auf Daten, die auf öffentlich zugänglichen Servern abgelegt sind. Von diesem Modul aus fließen Daten auch zum VPN- und Remotezugriffsmodul, wo die VPN-Terminierung stattfindet.

E-Commerce-Modul
Da es in diesem Modul in erster Linie um E-Commerce geht, müssen die beiden Komponenten Zugang und Sicherheit sorgfältig gegeneinander abgewogen werden. Durch die Aufteilung einer E-Commerce-Transaktion in drei verschiedene Komponenten können im Rahmen dieser Architektur verschiedene Sicherheitsstufen bereitgestellt werden, ohne dass dadurch der Zugang erschwert wird.

Zusammenfassung
Die SAFE-Architektur bietet Kunden eine Orientierungshilfe bei der Konzeption und Implementierung sicherer Netzwerke. SAFE stellt ein Handbuch für Netzwerkdesigner dar, in dem die Sicherheitsanforderungen an ein Cisco-Netzwerk berücksichtigt werden. Der zur Gewährleistung der Netzwerksicherheit gewählte Ansatz zeichnet sich durch tief greifende Abwehrmechanismen und die Modularisierung aus. So können die einzelnen Untermodule sicherheitstechnisch bewertet werden und zueinander in Beziehung gesetzt werden. So werden auch komplexe Systeme handhabbar.

Literatur
Whitepaper und Design-Guide zu SAFE:
http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm

Das SAFE-Whitepaper beleuchtet ausführlich die zu erwartenden Bedrohungen und wie diese abgewehrt werden können. Zusätzlich werden Designansätze für die Skalierungs- und Verfügbarkeitsproblematik diskutiert.

Security-Produkte von Cisco:
http://www.cisco.com/warp/public/44/jump/secure.shtml

Weitere Informationen zur Sicherung von Routern:
http://www.cisco.com/warp/public/707/21.html

Weitere Informationen zur Sicherung von Switches:
http://www.sans.org/newlook/resources/IDFAQ/vlan.htm.

Events

Cisco-Endkundenseminar im Januar und Februar 2001

Seminar-Code Storage Networks	S1040
Seminar-Code Mobile Enterprise Communication	S1041

Termine und Orte

29. Januar 2001	Düsseldorf Hilton Hotel
30. Januar 2001	Hamburg Steigenberger Hotel
31. Januar 2001	Berlin Dorint Schweizer Hof
6. Februar 2001	München City Hilton
7. Februar 2001	Stuttgart Steigenberger Zeppelin
8. Februar 2001	Frankfurt Hilton Hotel

Agenda

9.00 – 9.30 Uhr	Anmeldung
9.30 – 11.00 Uhr	Storage Networks Überblick, Einführung in WDM (Wavelength Division Multiplexing)
11.00 – 11.30 Uhr	Kaffeepause
11.30 – 12.30 Uhr	Cisco Metro 1500, iSCI
12.30 – 13.30 Uhr	Lunchbuffet
13.30 – 15.00 Uhr	802.11 versus UMTS – Ausblick in die Zukunft
15.00 – 15.30 Uhr	Kaffeepause
15.30 – 16.30 Uhr	Gastvortrag der IBM Deutschland Informationssysteme GmbH: Applikationen im mobilen Office
16.30 – 17.15 Uhr	Realität und Einsatzbereiche im mobilen Office
17.15 Uhr	Seminar-Ende

Anmelden können Sie sich per E-mail bei Cisco@ecco-events.de.
Telefonisch erreichen Sie die Seminar-Hotline unter (089) 30 61 06 15.

Access to Information

Weitere Informationen zu Cisco, seinen Produkten oder Dienstleistungen erhalten Sie über:

- das kostenlose Abonnement der Kundenzeitung CISCOnnect und CISCOnnect online
- den Zugriff auf die Web-Seiten von Cisco Systems (http://www.cisco.de)
- oder persönlich bei Heinz Deininger, Tel.: 0711-23911-303 Fax: 0711-23911-11, E-Mail: hdeining@cisco.com

---

CISCO SYSTEMS

Wir über uns
Cisco Systems Inc. mit Hauptsitz in San Jose, Kalifornien, ist mit 18,93 Milliarden US-Dollar Umsatz Marktführer bei Networking-Lösungen für das Internet. Die Router, LAN- und ATM-Switches sowie Dial-up-Access-Server-Produkte – versehen mit dem Internetwork Operating System (IOS) von Cisco – werden eingesetzt, um unternehmensweite Netze mit einer unbeschränkten Anzahl von geographisch verteilten LANs, WANs und IBM-Netzwerken aufzubauen. Mehr als 80 Prozent der Basistechnologie des Internet stammen von Cisco. Die deutsche Niederlassung Cisco Systems GmbH hat ihren Sitz in Hallbergmoos bei München.

Cisco-Geschäftsstellen:

München/Hallbergmoos
Tel.: 0180 - 3 67 10 01
Fax: 0811 - 55 43 - 10
Stuttgart
Tel.: 0180 - 3 67 10 01
Fax: 0711 - 23 91 1-11
Frankfurt/Eschborn
Tel.: 0180 - 3 67 10 01
Fax: 06196 - 479-777
Düsseldorf
Tel.: 0180 - 3 67 10 01
Fax: 0211 - 9547-10
Berlin
Tel.: 0180 - 3 67 10 01
Fax: 030 - 2934 27-10
Hamburg:
Tel.: 0180 - 3 67 10 01
Fax: 040 - 3 50 85 80

Cisco Systems GmbH
Heinz Deininger
Herold Center
Wilhelmsplatz 11
D-70182 Stuttgart
Tel.: 07 11-23 91 1-303
Fax: 07 11-23 91 1-11
Email: hdeining@cisco.com