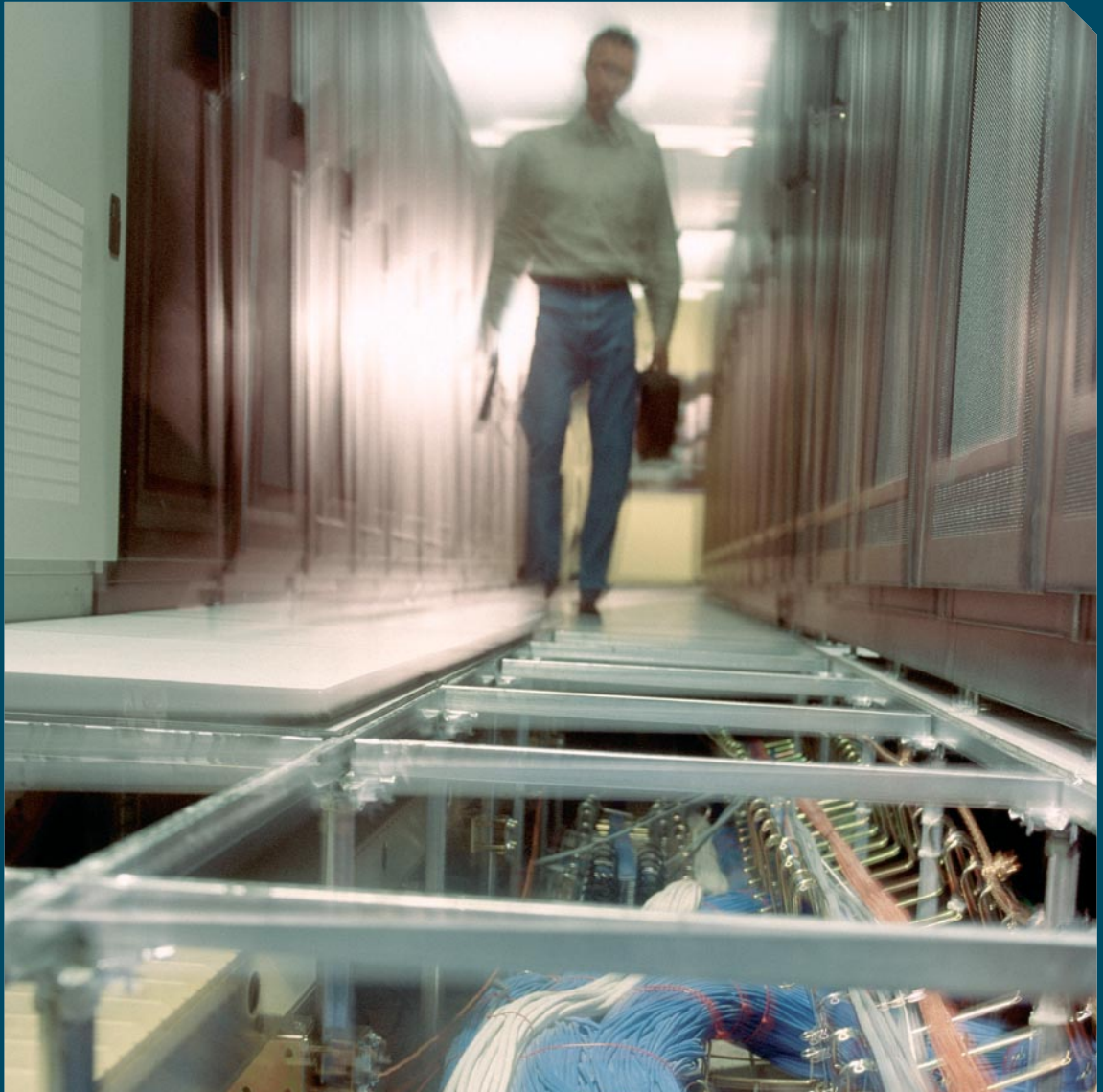


CISCO INTEGRATED NETWORK SECURITY



Der Weg zum Self-Defending Network



INHALT

Die Bedrohungen sind überall	3
Der Weg zum Self-Defending Network	4
Drei Säulen für mehr Sicherheit	5
– Das Intelligent Information Network	7
Intelligente Security-Lösungen von Cisco	8
– Sicherheitslösung für Endgeräte	9
– Cisco Remote Access VPN-Lösungen	9
– Cisco VPN-Client-Lösungen	10
– Cisco Content-Management-Lösung	10
– Cisco Trust und Identity-Management-Lösung	10
– Cisco Security-Management-Lösungen	10
Cisco Service und Support	13
– Cisco Outsourcing Services	14
– Zusammenfassung – Self-Defending Network	15

DIE BEDROHUNGEN SIND ÜBERALL

Immer mehr Unternehmen nutzen Internet-basierte Lösungen, um ihren Geschäftserfolg zu verbessern. Sie optimieren Geschäftsabläufe, um Wettbewerbsvorteile zu erlangen. Sie erschließen über das Internet neue Vertriebswege und erweitern so ihre Kundenbasis. Sie implementieren neue Kommunikationslösungen, wie Wireless-Anwendungen oder IP-Telefonie, um die Produktivität der Mitarbeiter zu verbessern.

Doch hier lauern auch Gefahren: die Nutzung öffentlicher Netze, wie dem Internet, lässt auch unbefugten Zugriff auf Informationen zu.

Übertragene Informationen können mitgehört werden, Unbefugte, sowohl intern als auch extern, können sich den unerlaubten Zugriff auf wichtige Daten erschleichen. Trojaner, die über E-Mails eingeschleppt werden, spionieren Passwörter aus und senden sie weiter. Und dann gibt es noch die Freaks, die ohne eigenen Nutzen davon zu haben, Viren und Würmer programmieren, die in Minuten Netzwerke weltweit lahmlegen.

IT-Betreiber sind deshalb gezwungen Anti-Virus- oder Betriebssystemupdates in immer kürzeren Abständen an die Anwender zu verteilen und dort zu installieren. Dazu kommen zahlreiche „Feuerwehreinätze“ im Unternehmen, die durch Viren/Würmer ausgelöst werden sowie zum Teil umfangreiche und teure Wiederherstellungsmaßnahmen oder sogar die präventive Abschaltung der IT.

Dies bindet viele Ressourcen im Unternehmen und verursacht hohe Kosten.

Deshalb muss auf solche Gefahren, auf die Administratoren kaum noch reagieren können, weil sie sich so rasend schnell verbreiten, das Netzwerk selbst reagieren, am besten sich selbst verteidigen können – das ist Ciscos Vision vom Self-Defending Network.

„Netzwerke haben sich von geschlossenen Systemen in offene, hoch entwickelte Systeme gewandelt. Deshalb sind leider auch die Sicherheitsbedrohungen exponentiell gewachsen – sowohl von außen als auch von innen. Cisco hat darauf mit einer Strategie reagiert, Security-Dienste in die Netzwerkinfrastruktur zu integrieren. Dies liefert einen flexiblen, kostengünstigen und umfassenden Ansatz, komplexe Netzwerke von heute zu sichern.“

Zeus Kerravala
Vice President, Enterprise Computing and
Networking Application Infrastructure and
Software Platforms, The Yankee Group

In einigen Industriebereichen ist Datenschutz gesetzlich vorgeschrieben. In den Vereinigten Staaten müssen Unternehmen der Gesundheitsindustrie dem Health Insurance Portability and Accountability Act (HIPAA) folgen, US-Finanzunternehmen dem Gramm-Leach-Bliley Act. In Großbritannien wird Datenschutz für alle Unternehmen durch den Turnbull Report on Internal Control for public companies und den Data Protection Act von 1995 geregelt und für Deutschland gilt das Bundesdatenschutzgesetz, das Strafgesetzbuch, Basel-II, KontraG oder das GmbH-Gesetz. Sobald sensitive, sprich personenbezogene Daten verarbeitet werden, müssen Unternehmen Maßnahmen zur Sicherung des Datenschutzes und der Risikokontrolle einführen, die garantieren, dass die Information vor Manipulationen und Missbrauch, gemäß den geltenden gesetzlichen Bedingungen, geschützt werden.

DER WEG ZUM SELF-DEFENDING NETWORK

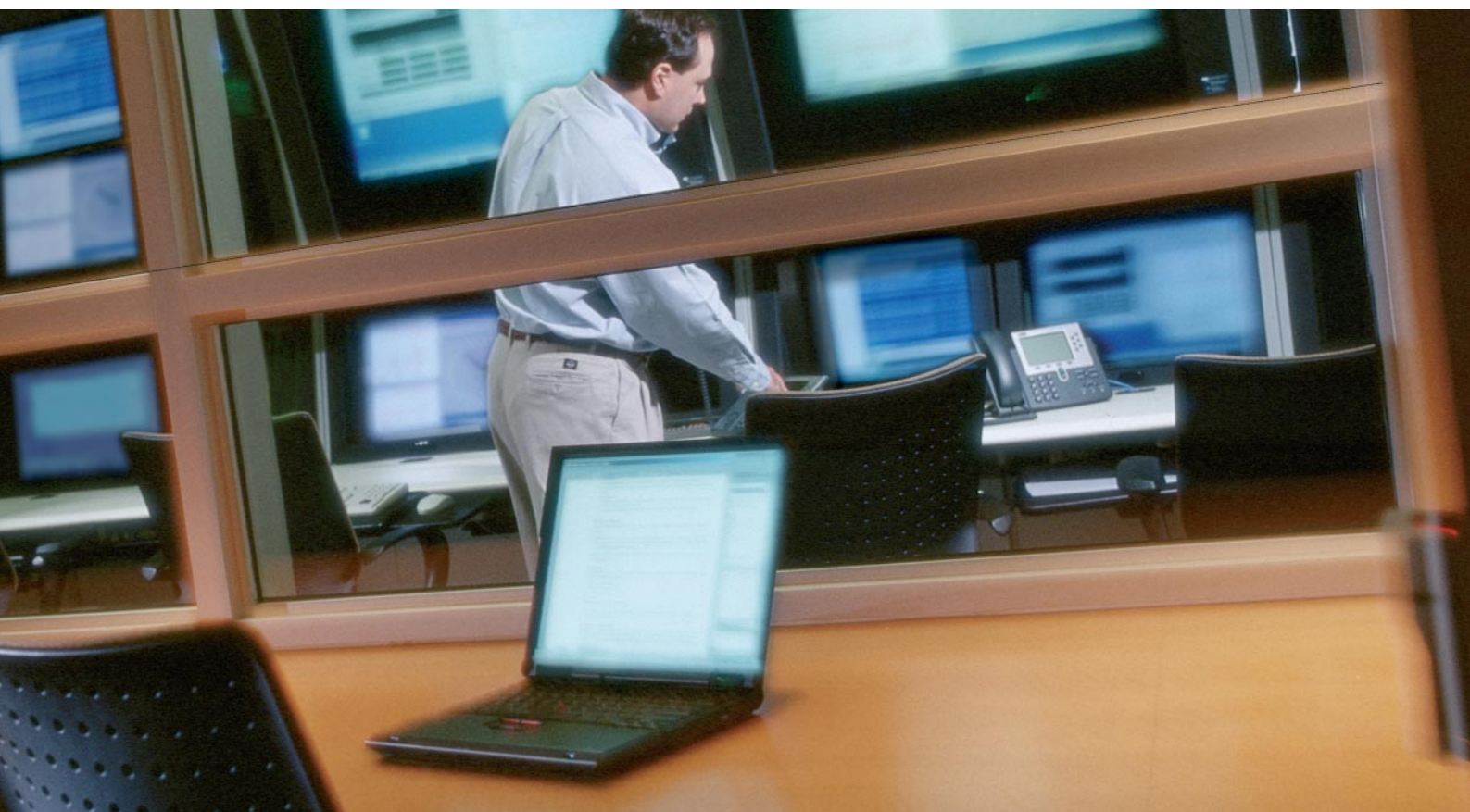
Die Cisco Self-Defending Network-Strategie beschreibt Ciscos Vision von zukünftigen IT-Sicherheitssystemen und bereits heute verfügbaren Lösungen. Da sich Bedrohungen für Unternehmen ständig verändern und weiterentwickeln, muss dies auch für die Verteidigung des Unternehmens gelten. In der Vergangenheit war die Bedrohungslage relativ stabil und veränderte sich nur langsam, so dass es einfach war, sich zu schützen. Heute verbreiten sich Internetwürmer und Malware in Minuten um den ganzen Globus, deshalb müssen Sicherheitssysteme – und das Netzwerk selbst – blitzschnell reagieren.

Die Grundlage eines selbst-schützenden Netzwerkes ist integrierte Sicherheit – Sicherheit, die allen Aspekten einer Organisation gerecht wird. Jedes Gerät der IT-Infrastruktur – angefangen von den Endgeräten wie Desktop PCs und Server über die Netzwerkkomponenten vom LAN bis hin zum WAN – müssen im Sinne einer umfassenden, verteilten Verteidigung zur Sicherheit der Infrastruktur beitragen. Solche Systeme sichern die Vertraulichkeit von Informationen während der Übertragung, schützen vor internen und externen Bedrohungen und geben dem Unternehmen die volle Kontrolle über den Zugang zu den verschiedenen Unternehmensressourcen.

Anders als andere Hersteller verfolgt Cisco einen integrierten, systemweiten Sicherheitsansatz. Die kontinuierliche Weiterentwicklung unserer Vision schließt die Integration von Sicherheitstechniken anderer mit ein. Cisco arbeitet beispielsweise mit Antivirus-, Patchmanagement-, Softwareverteilungs- und Endgerätsicherheits-Herstellern in der Cisco Network Admission Control Initiative (NAC) zusammen, mit dem Ziel, infizierte Geräte erst gar nicht in das Netzwerk hinein zu lassen. Solche selbst-schützenden Netzwerke identifizieren Bedrohungen, reagieren je nach Schweregrad der Bedrohung, isolieren Server und Desktops, die nicht den aktuellen Sicherheitsrichtlinien entsprechen und passen die Netzwerkressourcen an, um adäquat reagieren zu können.

„Die Industrie steht am Scheideweg – sie kann so weitermachen wie bisher und spezialisierte Einzelprodukte für die IT-Sicherheit entwickeln, oder sie kann die essentiell wichtigen Funktionen in die Netzwerke integrieren und so Plattformen schaffen, die Unternehmen dabei helfen ihre Produktivität zu steigern, Kosten zu senken und deshalb wettbewerbsfähig zu sein. Wir von Cisco Systems glauben, dass Letzteres der richtige Weg ist.“

Jayschree Ullal,
Senior Vice President
Security Technology Group
Cisco Systems



Ciscos Vision eines Self-Defending Networks ist ein Systemansatz, der Secure Connectivity, Threat Defense Systems sowie Systeme zum Trust und Identity Management in einer Lösung vereint. Ein Cisco Self-Defending Network umfasst diese drei Komponenten, die Cisco für absolut notwendig zur Umsetzung von Netzwerksicherheitslösungen hält:

THREAT DEFENSE SYSTEM

Heutige Bedrohungen sind immer zerstörerischer, treten immer häufiger auf und breiten sich wesentlich schneller aus als in der Vergangenheit. Interne und externe Bedrohungen wie Würmer, Denial-of-Service-Angriffe (DoS), Man-in-the-middle-Angriffe oder Trojaner können die Profitabilität eines Unternehmens stark beeinträchtigen. Das Cisco Threat Defense System bietet deshalb starke Verteidigungsmaßnahmen gegen bekannte und auch gegen bisher unbekannte Angriffsformen.

Hierzu braucht man die passende Sicherheitstechnologie, gepaart mit Intelligenz im Netzwerk. Zur wirkungsvollen Umsetzung sollte Sicherheit im gesamten Netzwerk implementiert werden und nicht nur an wenigen Einzelpunkten, denn ein Angriff kann an jedem Punkt des Netzwerks starten und sich in kurzer Zeit über die gesamte Infrastruktur ausbreiten. Das Cisco Threat Defense System erhöht deshalb die Sicherheit innerhalb der existierenden Netzwerkinfrastruktur durch Integration von Sicherheit in jedes Gerät und erweitert diese um umfassende Schutzfunktionen für die Endgeräte – Server und Desktops. Mit diesem gesamtheitlichen (holistischen) Ansatz werden Ihr Geschäft, Anwendungen, Benutzer und die gesamte Infrastruktur vor Geschäftsunterbrechungen, Umsatzverlusten und damit Ansehens-/Vertrauensverlust geschützt.

Das Cisco Threat Defense System umfasst alle notwendigen Technologien und Funktionen mit denen Sicherheit integriert im Router, Switch oder einer Appliance ermöglicht wird: Anwendungssicherheit durch Deep Packet Inspection Firewalls, Netzwerk-basierte Intrusion Prevention Sensoren und Verkehrstrennungstechniken. Der Schutz der Endgeräte erfolgt durch den Cisco Security Agent.

SECURE CONNECTIVITY SYSTEM

Mit zunehmender Vernetzung der Systeme steigt das Bedrohungsrisiko. Wenn Unternehmen anfangen, das Internet für Filialanbindungen, Extranet oder die Anbindung von Telearbeitern über „always-on“ Breitbandverbindungen zu nutzen, sind Sicherheitsmaßnahmen zur Erhaltung von Vertraulichkeit und Integrität der Daten auf diesen Verbindungen von größter Bedeutung.

LAN-Anschlüsse – aus der Historie heraus als sicher und verlässlich betrachtet – erfordern heute ebenfalls ein höheres Sicherheitsniveau. Tatsächlich verursachen innere Bedrohungen zehnmals höhere finanzielle Schäden als externe. „Bedrohung von innen“ ist nicht zu verwechseln mit „eigenen Mitarbeitern“ – es geht dabei um die missbräuchliche Nutzung von LAN-Ports durch Personen, die Zugang zu den Gebäuden haben. Die Erhaltung von Vertraulichkeit und Integrität von Daten und Anwendungen, die auf drahtlosen oder kabelgebundenen LANs betrieben werden, ist deshalb geschäftskritisch.

Das Cisco Secure Connectivity System (Sichere Transport Systeme) stellt Verschlüsselungs- und Authentisierungsmechanismen bereit und ermöglicht damit den sicheren Datenaustausch über unsichere Netzwerke. Um Daten-, Sprach- und Videoanwendungen über drahtlose oder kabelgebundene Medien zu schützen bietet Cisco ver-

Anti-X Defenses

Bei Anti-X Defenses geht es um die Reaktion auf Bedrohungen für das Netzwerk durch eine Kombination innovativer verkehrs- und inhaltsorientierter Sicherheitsservices – und deren Abwehr. Dazu gehören Firewall, Intrusion-Prevention-Systeme (IPS), Anomaly Detection und Entschärfung von Distributed-Denial-of-Service-Angriffen (DDoS), gekoppelt mit Anwendungsinspektion wie Netzwerk-Anti-Virus, Anti-Spyware und URL-Filterung. Dies bringt die Kontrolle des Datenverkehrs an die zentralen Punkte zur Durchsetzung der Netzwerksicherheit, sodass bösartiger Verkehr gestoppt wird, bevor er sich im Netzwerk ausbreiten kann.

Zu den Neuerungen in diesem Bereich gehören:

- **Cisco Intrusion-Prevention-System (IPS) Version 5.0.** Die Lösung bietet hochgenaue und intelligente Inline-IPS-Funktionen, die durch Anti-Virus-, Anti-Spyware- und Wurm-Entschärfungsfunktionen, insbesondere durch Peer-to-Peer- oder Instant-Messaging-Traffic, ergänzt wurden. Daraus resultiert eine verbesserte Bedrohungsabwehr für viele Form-Faktoren wie Appliances, integrierte Switch-/Router-Module und Cisco IOS Software-basierte Lösungen, mit einer Performance von bis zu sieben Gigabit pro Sekunde.
- **Cisco Anomaly Guard Module und Cisco Traffic Anomaly Detector Module** für die Cisco Catalyst Switches der 6500er und 7600er Serien Version 4.0 dieser Verhaltensbasierten Lösung zur Eindämmung von Distributed-Denial-of-Services-Angriffen bietet Multi-Gigabit-Schutz kritischer Netzwerkressourcen gegen Day-Zero-DDoS-Attacken als integriertes Switch-Modul.
- **Cisco Security Agent (CSA) Version 4.5.** Die Software bietet verhaltensbasierten Schutz vor Malware und Spyware, umfassendes Tracking des Sicherheitsstatus von Objekten und ortsabhängige Durchsetzung von Sicherheitsrichtlinien. Der neue Client ist für alle internationalen Windows-Versionen, Solaris sowie für Redhat Linux verfügbar und bietet jetzt die vollständige NAC-Unterstützung.

Anwendungssicherheit

Diese Technologien schützen Geschäftsanwendungen durch den Einsatz von Zugangskontrolle auf der Anwendungsebene und die Durchsetzung von Richtlinien für die Anwendungsnutzung sowie die Kontrolle von Webanwendungen und Transaktionsschutz.

Zu den Neuerungen in diesem Bereich gehören:

- **Secure-Socket-Layer-/Virtual-Private-Network-Services (SSL-VPN) in der Cisco VPN Concentrator Version 4.7** Diese Lösung bietet erweiterten Zugang zu nahezu jeder Anwendung mit zusätzlichem Endgeräte- und Malware-Schutz inklusive Funktionen zur Anwendungsoptimierung mit dem neuen Cisco Security-Desktop. Neu ist ebenfalls die Unterstützung von Citrix-Umgebungen ohne zusätzlichen SSL-Client.
- **Cisco PIX Security Appliance Software Version 7.0.** Die neue Version ist die umfangreichste Funktionsergänzung seit der Einführung der PIX Firewall-Lösung. Sie ermöglicht Inspektion und Kontrolle einer Vielzahl von HTTP-, Sprach- und IP-basierten Anwendungen. Darüber hinaus wird mit der neuen Version ein sehr flexibles Framework für Sicherheitsrichtlinien vorgestellt, das eine genaue Kontrolle individueller User-to-Application-Flows bietet.

Cisco IPS Version 5.0 und Cisco IOS Software Release

12.3(14)T Die beiden Lösungen bieten Funktionen gegen neue Klassen von Bedrohungen wie Spyware oder Malware im Instant-Messaging und in Voice-over-IP-Umgebungen. Sie verbessern so die Möglichkeit Schäden durch Viren-/Wurm-Angriffe zu reduzieren oder ganz auszuschließen. Durch benutzerdefinierbare Custom-Signatures lässt sich das neue IPS leicht an neue Bedrohungen anpassen und bietet so umfassenden Schutz.

DIE DREI SÄULEN DES SELF-DEFENDING NETWORKS

Secure Connectivity

Vertraulichkeit

Die Sicherheit, dass nicht berechtigte Dritte keinerlei Zugriff auf Firmen- oder Kundeninformationen, Daten und die Kommunikation erlangen.

Threat Defense

Verfügbarkeit

Schutz von Netzwerk-Ressourcen, um für Anwender eine maximale Verfügbarkeit zu gewährleisten, selbst bei ersten Sicherheitsbedrohungen

Trust/Identity Management

Integrität

Überprüfung der Identität von Benutzern und deren Computern sowie die Kontrolle über den Zugriff auf deren Daten und Ressourcen

schiedene VPN-Technologien: IP Security (IPsec), Secure Socket Layer (SSL), Secure Shell (SSH) und Multiprotocol Label Switching (MPLS). Darüber hinaus stehen umfassende Sicherheitsfunktionen in den Cisco Wireless- und IP-Telefonie-Lösungen zur Verfügung, um so die Vertraulichkeit jeglicher IP-Kommunikation zu garantieren.

Cisco Lösungen bieten verlässliche Konnektivität durch die Integration von dynamischem Routing, Multiprotokollunterstützung und einer breiten Palette an Anschlussmöglichkeiten und lässt sich so perfekt auf die individuellen Anforderungen abstimmen.

TRUST AND IDENTITY MANAGEMENT SYSTEM

Vertrauens- und Identitätsmanagementsysteme sind der Unterbau für jedes sichere Netzwerk und deshalb zwingend notwendig, wenn man Geschäftsprozesse darüber abwickeln möchte. Sie regeln den Zugang zu Geschäftsanwendungen und anderen Netzwerkressourcen je nachdem, welche Rechte dem Benutzer eingeräumt werden.

Das Cisco Trust and Identity Management System stützt sich auf Netzwerk-basierte Zugangskontrolle – Network Based Admission Control. Nach der Identitätsüberprüfung eines Benutzers oder Gerätes und der Überprüfung, ob das Endgerät die unternehmensweiten Sicherheitsrichtlinien einhält, wird erst der Zugang zu genau festgelegten Ressourcen oder Teilen des Netzwerks freigegeben. Das Netzwerk ist zuständig für die Authentifizierung und Autorisierung – also der Durchsetzung (Enforcement) der Sicherheitsrichtlinien. Um dies zu realisieren, integriert die Cisco Trust and Identity Lösung den Cisco Secure Access Control Server (ACS) und AAA-Funktionen (Authentication, Authorization and Accounting) der Cisco Switches, Router, Wireless Access Points und Sicherheits-Appliances, wie z.B. das 802.1x Authentisierungsprotokoll oder auch NAC. So kann eine sehr granular einstellbare Netzzugangskontrolle implementiert werden, mit der Endgeräte, die nicht den geltenden Sicherheitsrichtlinien entsprechen, entweder nur in eine Quarantänezone verbannt werden oder der Netzwerkzugang wird gänzlich verweigert. Mit dieser effektiven Kontrolle lässt sich das Ausbreiten von Schädlingen verhindern und infizierte Geräte können im Netzwerk leicht identifiziert und isoliert werden.

Das Intelligent Information Network

Cisco Self-Defending Network ist Teil einer übergreifenden Vision von Cisco, wie Netzwerke in Zukunft aussehen sollen: Alle Netzwerkkomponenten müssen von Grund auf so entwickelt werden, dass sie nahtlos zusammenarbeiten, wichtige Dienste (zu denen auch Security gehört) bereits integriert sind, intelligent auf Service-Anforderungen oder Gefahren reagieren, gemeinsam und einheitlich verwaltet werden können und dabei auch noch herausragende Leistung bringen.

Während andere Hersteller sich darauf konzentrieren, für einzelne Problemfelder einzelne Produkte zu entwickeln, behält Cisco bei der Produktentwicklung das gesamte Netzwerk und die Geschäftsprozesse im Blick. Denn die Einbindung einzelner Produkte verschiedener Hersteller erhöhen Kosten und Zeitaufwand bei Implementierung, Bedienung und Wartung.

Sicherheit ist von grundlegender Bedeutung für Cisco und hat deshalb höchste Priorität bei der Produktentwicklung. Cisco ist deshalb in der Lage integrierte Netzwerksicherheit zu liefern – Sicherheit in jedem Netzwerkgerät, Sicherheit sowohl im Netzwerk als auch auf dem Endgerät – die für den Schutz von geschäftskritischen Prozessen in Unternehmensnetzwerken unerlässlich ist.

INTEGRIERTE SECURITY LÖSUNGEN VON CISCO

Die Highlights der Cisco PIX Software

Fortschrittliche Firewall-Dienste

- Deep Packet Inspection Firewall für http, FTP, ESMTP u.a.
- Abschottung von Instant Messaging-, Peer-to-Peer- und Tunneling-Anwendungen
- Modulare, ablaufbasierte Sicherheitsrichtlinien
- Virtuelle Firewall-Dienste
- Layer-2-transparente Firewall
- 3G Mobile Wireless Security Services

Robuste IPsec VPN-Dienste

- VPN Client Security Überprüfung und Durchsetzung
- Automatische Aktualisierung von VPN-Client-Software
- OSPF dynamisches Routing über VPN-Tunnel

Hochverfügbarkeits-Dienste

- Aktiv/Aktiv Ausfallsicherung mit asymmetrischer Routing-Unterstützung
- Stateful Failover-Funktion für Remote Access- und Site-to-Site-VPN
- Durchführung von Software-Upgrades ohne Ausfallzeiten

Intelligente Netzwerk-Dienste

- PIM Multicast Routing
- Quality of Service
- Ipv6-Verbindungen

Flexible Management-Lösungen

- SSHv2 und SNMPv2
- Rückverfolgung von Konfigurationsänderungen
- Verbesserte Benutzerfreundlichkeit



Cisco PIX 525



Cisco PIX 535

Integrierte Firewall, VPN und Intrusion Protection

Cisco PIX 500 Serie Security Appliance

Die Cisco PIX® 500 Security Appliance gehört zu den führenden Firewallprodukten am Markt. Sie zeichnet sich durch umfassende Sicherheitsfunktionen, sehr hohe Zuverlässigkeit, Skalierbarkeit und ein innovatives, leicht bedienbares Management aus. Egal in welcher Bauform, ob als spezialisierte Sicherheits-Appliance oder als Sicherheitsmodul für die Catalyst® Switches (FWSM), liefert die PIX zuverlässige Sicherheit mit Deep-Packet-Inspection- und Layer-2-transparent Firewalling, Intrusion Prevention und IPsec VPN-Funktionen. Die Cisco PIX Security Appliance bietet diese Sicherheit gepaart mit großer Leistung, denn sie unterstützt mehr parallele Verbindungen als jede andere Firewall am Markt und ist unübertroffen in der Geschwindigkeit. Durch Firewall-Virtualisierung lassen sich komplexe Umgebungen problemlos und kosteneffizient schützen.

Cisco Security Routers und Cisco Catalyst Switches

Cisco integriert Sicherheit direkt in die Netzwerkinfrastruktur durch die umfangreichen, integrierten Sicherheitsfunktionen der Cisco Router und Cisco Catalyst Switches. Dies bietet Ihnen große Flexibilität und enorme Kostenreduzierung bei der Umsetzung Ihrer Sicherheitsprojekte. Unternehmen sind so in der Lage, ihre unternehmensweiten Sicherheitsrichtlinien auch wirklich gezielt im Netzwerk durchzusetzen.

Beispielsweise unterstützen Cisco Router und Cisco Catalyst Switches für die kostengünstige und sichere Anbindung von Zweigstellen und Niederlassungen MPLS- und IPsec-VPN nach den geltenden, internationalen Standards. Zusätzliche Sicherheit bieten die Cisco Router und Cisco Catalyst Switches durch eine robuste Deep-Packet-Inspection-Firewall sowie Intrusion-Prevention-Funktionen. Sollte die gegebene Leistung nicht ausreichen, können die meisten Geräte mit Security-Hardware-Beschleunigermodulen problemlos aufgerüstet werden.

Router und Switches sind die primären Zugangsgeräte im Netzwerk. Ihnen kommt damit eine besondere Bedeutung im Bereich Zugangskontrolle zu. Cisco hat hierfür das NAC-Programm (Network Admission Control) initiiert, das in Zusammenarbeit mit anderen Security-Herstellern dazu dient, Zugriffsberechtigungen im Netzwerk aufgrund von Sicherheitsinformationen der Endgeräte durchzusetzen.

Ein wichtiger Bestandteil des NAC-Programms ist der Cisco Trust Agent (CTA), Software, die auf Desktop-Rechnern und Servern installiert wird und dort Informationen zum Sicherheitsstatus sammelt. Der CTA fragt diese Informationen bei den Produkten der teilnehmenden Hersteller ab, wie z.B. Antivirus- oder Softwareverteilungs-Programmen, und leitet sie an einen zentralen Richtlinienserver (Cisco Secure ACS), der entscheidet, ob der Netzwerkzugriff zulässig ist oder nicht. Der CTA arbeitet ebenfalls mit dem Cisco Security Agent (CSA) zusammen, einer Sicherheitslösung für Endgeräte, die vor bekannten und unbekanntem (Day-Zero) Angriffen schützt.

Mit Cisco Network Admission Control ist es möglich, eine Überprüfung und Durchsetzung von Sicherheitsrichtlinien für Endgeräte auch in großen Netzwerken automatisch vorzunehmen.



Cisco IDS 4250



Cisco IPS 4255

Cisco Intrusion Prevention (IPS)

Das Cisco IPS ermöglicht durch den In-Line-Ansatz mit seiner intelligenten und hochgenauen Bedrohungserkennung in Echtzeit umfassenden Schutz, der jetzt auch Anti-Virus-, Anti-Spyware und Mechanismen zur Reduzierung des Risikos durch Wurmangriffe enthält – und das für Bandbreiten bis zu 7 Gigabit/Sekunde.

Hoch performante Netzwerksensoren analysieren jedes einzelne Paket und erkennen verdächtige Aktivitäten, wie beispielsweise unberechtigten Zugriff auf Netzwerkressourcen oder Versuche, Produkt- oder Protokoll-Schwachstellen auszunutzen. Dies gilt seit kurzem auch für Voice-over-IP- und Protokoll-Anwendungen. Das IDS alarmiert den Systemadministrator und kann auch aktiv Angreifer aus dem Netzwerk entfernen.

Sicherheitslösung für Endgeräte

Cisco Security Agent

Der Cisco Security Agent (CSA) ist eine Sicherheitslösung für Endgeräte wie beispielsweise Server oder Personal Computer. Sie geht viel weiter als bisherige Lösungen, weil der CSA böses Verhalten identifizieren und verhindern kann, bevor Schaden angerichtet wird.

Der Cisco Security Agent arbeitet mit vorgegebenen Richtlinien, die sich auf spezifische Benutzererfordernisse anpassen lassen. Die eingebauten Richtlinien erkennen potenziell gefährliche Aktionen („Day-Zero“) schon beim ersten Versuch – und das für ein enorm breites Spektrum von Applikationen und Betriebssystemversionen.

Dabei hat der Cisco Security Agent den Vorteil, dass nur ein verhältnismäßig kleiner Bestand von Richtlinien zu verwalten ist, der nicht wie bei bisherigen Ansätzen permanent aktualisiert und an die Endgeräte verteilt werden muss. Durch dieses sogenannte „Zero-Update“-Konzept lassen sich Endgeräte besser und vor allen Dingen preiswerter schützen.

Cisco Remote Access VPN-Lösungen

Cisco VPN 3000 Series Concentrator

Die Cisco VPN 3000 Concentrator-Serie ist eine universelle Remote-Access VPN-Plattform, die Hochverfügbarkeit, hohen Durchsatz und sehr gute Skalierbarkeit mit den besten heute verfügbaren Verschlüsselungs- und Authentisierungsmechanismen verbindet. Mit Hilfe von Remote-Access VPNs lassen sich Kommunikationskosten durch die Nutzung des Internets dramatisch reduzieren. Die Cisco VPN 3000 Concentrator-Serie wächst mit dem Bedarf und kann vom Benutzer einfach erweitert werden. Mit Hilfe der Scalable Encryption Processing (SEP) Module kann man Kapazität und Durchsatz schnell und einfach ausbauen. Die Remote-Access VPN-Lösungen unterstützen sowohl IPsec- als auch SSL/WebVPN Tunnel Terminierung, wodurch die Flexibilität erhöht und gleichzeitig die Betriebskosten (TCO) gesenkt werden. Der Vorteil einer SSL/WebVPN-Lösung besteht darin, eine sichere Remote Access VPN-Verbindung aufzubauen, ohne die Notwendigkeit von Client-Software auf dem zugreifenden PC. Der integrierte Cisco Security Desktop sorgt dafür, dass auch von öffentlichen PCs sicher auf Firmendaten zugegriffen werden kann, ohne dass Spuren oder gar Dokumente aus der Verbindung auf dem PC zurückbleiben.

Cisco VPN 3000 Serie Concentrators





Cisco VPN-Client-Lösungen

Cisco VPN Client

Für eine Remote-Access-Lösung braucht man neben dem zentralen VPN-Gateway noch Endgeräte-Software. Der Cisco VPN-Client bietet sichere Konnektivität für eCommerce-Anwendungen, mobile Benutzer und Telearbeitsanwendungen. Er ist kompatibel mit Windows-, Linux-, Solaris- und Macintosh-Betriebssystemen und bietet eine vollständige Implementierung des IPsec-Standards, einschließlich Verschlüsselung nach Data Encryption Standard (DES und 3DES) und des Advance Encryption Standards (AES) mit Schlüssellängen bis zu 256 Bit, starke Authentisierung mit Hilfe von digitalen Zertifikaten, One-Time-Passworts (OTP) oder Pre-Shared Keys für die Authentifizierung gegenüber RADIUS Servern, NT Domänen oder Active Directories, Kerberos oder LDAP-Verzeichnisdiensten. Der VPN-Client wird von allen Cisco Gateway-Plattformen unterstützt – Cisco VPN 3000 Concentrator-Serie, Cisco PIX Security Appliance und allen Cisco VPN-Routern.

Cisco Content-Management-Lösung

Cisco SSL Acceleration

Cisco bietet eine leistungsfähige und umfassende Lösung für SSL-basierte Intranet-, Extranet- und Internet-Anwendungen. Die Cisco-Lösung beschleunigt die Verarbeitung von SSL-Transaktionen und entlastet so gleichzeitig den eigentlichen Server. Dies steigert die Leistungsfähigkeit der Website, erhöht die Zuverlässigkeit und Verfügbarkeit des Transaktionsservers und vereinfacht stark das Benutzer-Zertifikate-Management, wodurch sich insgesamt die Kapital- und Betriebskosten senken lassen.

Content Access Management und Content Filtering

Cisco bietet Lösungen für die Verwaltung des Zugriffs auf Inhalte im Netzwerk. Damit können Unternehmen und Schulen anstößige Webseiten und unerwünschte URLs blockieren. Der Vorteil: umfassendere Verwaltung von Webzugriffen und ein geringeres Risiko durch Haftungsansprüche.

Cisco Trust und Identity-Management-Lösung

Cisco Secure Access Control Server

Cisco Secure ACS ist die zentrale Instanz für die Aufstellung von Richtlinien und liefert die Intelligenz und die Kontrollmöglichkeiten, die eine Organisation für seine Sicherheitsrichtlinien benötigt.

Der Cisco Secure ACS ist eine hoch skalierbare und sehr leistungsfähige Serverlösung mit der sich zentralisierte RADIUS oder TACACS+ Zugangskontrollsysteme implementieren lassen. So lassen sich Authentisierung, Authorisierung und Accounting (AAA) der Benutzer beim Zugang zu Unternehmensressourcen über das Netzwerk kontrollieren. Mit Hilfe des ACS lässt sich die Verwaltung der Benutzer und ihrer Zugriffsrechte stark vereinfachen. Benutzerindividuell oder je Benutzergruppe lässt sich der Zugang zu verschiedenen Teilen des Netzwerks oder auch nur auf bestimmte Netzdienste einschränken. Accounting-Records geben Aufschluss darüber, welche

Dienste die Benutzer wirklich genutzt haben und können so individuell abgerechnet werden. Gleichzeitig kann dieses AAA-Framework unternehmensweit für die Verwaltung der Administrationsrechte per TACACS+ verwendet werden. Pro Administrator/Gruppe kann individuell festgelegt werden, welche Geräte sie verwalten dürfen und wenn gewünscht, kann sogar der Zugriff auf einzelne Baugruppen des Gerätes beschränkt werden. So können beispielsweise Sicherheitsadministratoren die Firewall- und VPN-Konfiguration eines Routers ändern, doch nur den Netzwerkadministratoren ist der Zugriff auf die QoS- und Routing-Konfiguration des gleichen Gerätes erlaubt.

Cisco Security-Management-Lösungen

Integriertes Management via Cisco Works VPN/Security Management Solution (VMS)

CiscoWorks VMS ist eine innovative Lösung für das unternehmensweite Infrastrukturmanagement. Der integrierte Workflow vereinfacht das Management von Firewalls durch eine starke Automation des Prozesses. So ermöglicht VMS eine schnellere Bereitstellung oder ein Upgrade von Firewalls, VPN-Geräten und IDS-/IDP-Sensoren durch ein einfach zu bedienendes Web-Interface. Geschäftsprozesse und Sicherheitsrichtlinien lassen sich so einfacher und ohne Unterbrechung umsetzen und einhalten. In Summe führt dies zu höherer Produktivität und niedrigeren Betriebskosten.

CiscoWorks VMS ist sehr gut skalierbar und jetzt von einer Basisversion für maximal fünf Geräte bis hin zur High-End-Version für mehr als 1.000 Cisco IOS-Sicherheitsgeräte verfügbar. VMS bietet höhere Produktivität und Investitionsschutz durch seine vollständige Integration in die CiscoWorks Management-Produktfamilie.

Single and Multiple Device Management

Jede Cisco Plattform verfügt über ein eigene, intelligente, grafische Bedienoberfläche für die individuelle Verwaltung eines Gerätes – den Cisco Device Manager. Durch das einfach zu bedienende Web-basierte Interface lassen sich Änderungen schnell durch-

Cisco Router and Security Device Manager v2.1
Seit kurzem ist die neue Version des Cisco Router and Security Device Manager (SDM) Version 2.1 verfügbar. Sie ermöglicht die komfortable Verwaltung von Routing- und Security-Diensten, umfasst intelligente Assistenten und ermöglicht eine detaillierte Fehlersuche und -behebung. Die neue Version unterstützt weitere Cisco Geräte und Interface Karten und ist in sechs Sprachen, darunter auch deutsch, erhältlich.

Zum kostenlosen Download der neuesten Cisco SDM Version besuchen Sie <http://www.cisco.com/cgi-bin/tablebuild.pl/sdm>

Action	Source	Destination	Service	Log	Option	Description
Permit	171.71.221.30	any	ip	Log		
Permit	171.71.221.30	any	dest: irc/tcp	Log		
Permit	171.71.221.30	any	dest: echo/tcp			
Deny	171.71.222.50		telnet			

führen und so Produktivität steigern bei gleichzeitig niedrigen Betriebskosten (TCO). Für die Netzwerk-übergreifende Verwaltung von vielen Geräten kann CiscoWorks VMS eingesetzt werden.

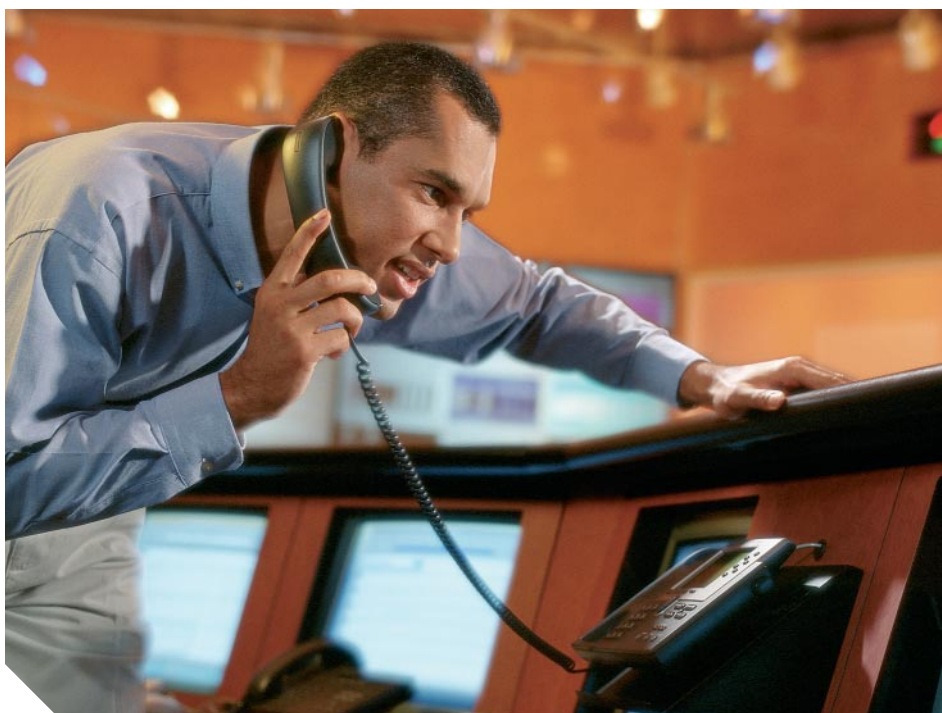
CiscoWorks Security Information Management Solutions (SIMS)

Speziell für den Einsatz in großen Unternehmensnetzwerken gedacht, sammelt und analysiert CiscoWorks SIMS Nachrichten von Intrusion Detection Systemen, Firewalls, Routern und Switchen, Betriebssystemen und Sicherheitsanwendungen wie beispielsweise Antivirus-Software. Diese Sicherheitsinformationen werden statistisch korreliert und nach vorgegebenen Regeln ausgewertet und in Echtzeit dem Administrator in einem dynamischen, verlinkten Format präsentiert, so dass es auf Ereignisse schnell und flexibel reagieren kann. CiscoWorks SIMS ist für die Verwaltung heterogener Infrastrukturen mit Geräten verschiedener Hersteller ausgelegt und basiert auf der mehrfach ausgezeichneten Technik von netForensics.

Cisco MARS Appliance und Cisco Security Auditor

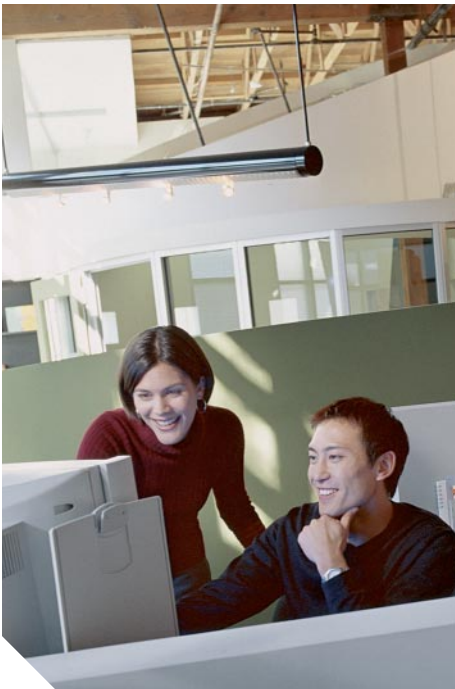
Cisco Security Monitoring, Analysis and Response System (CS-MARS) und der Security Auditor bieten gemeinsam die netzwerkweite Aufzeichnung und intelligente Korrelation von sicherheitsrelevanten Events und können so die Einhaltung der Sicherheitsrichtlinie überprüfen und bei Verstößen, wie beispielsweise unerlaubtem Netz-zugriff automatisch eingreifen. CS-MARS ist Hardware-basiert und kombiniert die Möglichkeiten des traditionellen Eventmonitorings mit Netzwerkitelligenz, Kontext-basierter Korrelationstechnik, Vektoranalyse, Anomalie-Erkennung und Hotspot-Identifizierung, um Angriffe präzise und schnell erkennen und bekämpfen zu können.

Mit Hilfe des Cisco Security Auditors können Sie Web-basiert Ihre Infrastruktur überprüfen. Durch die Möglichkeit, den Sicherheitsstatus eines dynamischen Netzwerkes zu messen, reporten und mit einem Soll-Ist-Abgleich jederzeit das Restrisiko zu bewerten, lässt sich das IT-Risikomanagement im Unternehmen stark vereinfachen.



Cisco Guard / Detectors

Diese Module für die Catalyst 6500 Familie und die Cisco 7600 Router Familie ermöglichen die Entdeckung und Abwehr von DDoS-Angriffen (Distributed Denial of Service). Sie bieten dieselben Funktionen und Leistungswerte wie herkömmliche Geräte-basierte Lösungen für die Abwehr von DDoS-Angriffen



Das Cisco Service- und Support-Modell basiert darauf, dass die Nutzung der Internets für die Lösung von Problemen sehr vorteilhaft ist: Netzwerkprobleme lassen sich schneller beheben, weil Kunden auf kritische Informationen schneller und zeitlich unabhängig zugreifen können, umfangreiche Hintergrundinformationen für ein besseres Verständnis und für Aus- und Weiterbildung zur Verfügung stehen und somit nicht nur reaktiv, sondern vorbeugend Netzwerke optimiert werden können.

Cisco.com ist die Basis hierfür, mit einer ganzen Reihe von interaktiven Netzwerk-anwendungen, die direkten Zugriff auf Cisco Informationen, Ressourcen und Systeme bietet. Über Cisco.com können Kunden und Partner direkt auf zahlreiche Anwendungen wie beispielsweise den Cisco Internet Technical Support (ITS), der online umfassende technische Unterstützung bietet, zugreifen. Das Cisco Technical Assistance Center (TAC) bietet Hilfe rund um die Uhr, um ihnen bei der Aufrechterhaltung der maximalen Netzwerkverfügbarkeit zu helfen. Weitere Informationen finden Sie unter: <http://www.cisco.com/tac>.

Cisco Advanced Services for Network Security

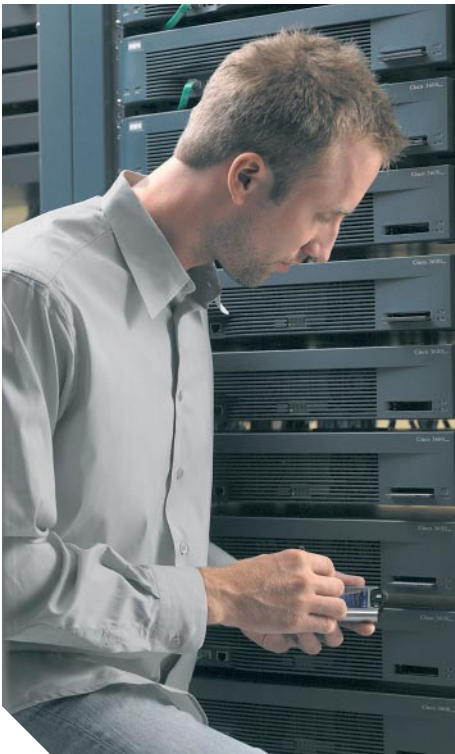
Berater des Cisco Advanced Service Teams sind Experten mit CCIE- und CISSP-Zertifizierung, die langjährige Erfahrung im Bereich Planung, Implementierung und Optimierung von großen Netzwerken und Sicherheitsinfrastrukturen für Unternehmen und staatliche Einrichtungen haben.

Planung und Beurteilung: Cisco bietet Ihnen umfangreiche Dienste im Bereich der Netzwerksicherheitsanalyse an. Erfahrene Sicherheitsexperten unterziehen das Netzwerk einem Cisco Security Posture Assessment (SPA), eine detaillierte Bestandsaufnahme des Sicherheitszustands eines Netzwerks, das alle Netzwerkgeräte, Server, Desktops und Datenbanken auf Schwachstellen und Verwundbarkeiten untersucht. Unsere Experten analysieren die Sicherheit der Infrastruktur und legen dabei gängige Industriestandards und führende Lösungen als Maßstab an. Basierend auf dieser detaillierten Analyse werden Empfehlungen und priorisierte Aufgabenlisten erarbeitet, mit der die Gesamtsicherheit der Infrastruktur verbessert werden kann.

Cisco bietet Ihnen die folgenden Netzwerk Security Services:

- Cisco Security Agent Implementierungsservice
- IP-Telefonie Sicherheitsüberprüfung
- Netzwerk Security Design Entwicklung
- Netzwerk Security Design Überprüfung
- Netzwerk Security Implementierungstechnik
- Netzwerk Security Implementierung/Planüberprüfung
- Netzwerk Security Optimierung
- Abschätzung der Sicherheitslage

Entwurf: Cisco unterstützt Sie beim Entwurf eines leistungsfähigen, sich selbst schützenden Netzwerks. Basierend auf dem Ansatz „defense in-depth“ – Verteidigung in der Tiefe – entwickeln Cisco-Experten eine mehrstufige Sicherheitsarchitektur, die vor Hackern, Viren und Würmern schützt. Cisco erarbeitet auf Wunsch auch



Empfehlungen zur Verbesserung eines bereits existierenden Sicherheitskonzeptes oder einer -infrastruktur. Unter Berücksichtigung aller Aspekte der Netzwerksicherheit und Skalierbarkeit, Performance und Verwaltbarkeit, empfiehlt Cisco geeignete Protokolle, Richtlinien und Funktionen, um sich besser gegen Angreifer zu schützen.

Umsetzung: Ein „self-defending“ Netzwerk muss nicht nur strategisch geplant, sondern auch sorgfältig installiert, konfiguriert und nahtlos in die bestehende Infrastruktur eingefügt werden. Nachdem das Sicherheitsdesign feststeht, können Cisco-Ingenieure Sie bei der Umsetzung der neuen Lösung innerhalb der Produktionsumgebung unterstützen. So werden kostspielige Ausfälle der Infrastruktur reduziert und ihr Team in die Lage versetzt, enge zeitliche Vorgaben einzuhalten.

Optimierung: Nach der erfolgreichen Inbetriebnahme der Sicherheitslösung ist die Infrastruktur bereit für die wachsenden Anforderungen, die aus Geschäftsdynamik und -wachstum, resultieren. Wenn sich die Anforderungen an das Netzwerk ändern, unterstützen Cisco-Ingenieure Sie bei der Optimierung der Infrastruktur und stellen gleichzeitig sicher, dass die gegebenen Sicherheitsrichtlinien eingehalten werden.

Cisco Outsourcing Services

Cisco Managed Security Services Solutions

Damit Service Provider den stark wachsenden Markt für Managed Security Services (MSS), speziell Managed VPN Services effektiv adressieren können, bietet Cisco eine breite Palette an Diensten und Funktionen für die schnelle und kosteneffiziente Einführung von Sicherheitsdiensten für Kunden. Managed VPN Services, die auf IPsec, MPLS oder beidem basieren, erlauben Service Providern existierende Angebote um Dienste wie Remote-Access- oder Site-to-Site-VPNs zu erweitern und darüber höherwertige Dienste wie IP Telephony, E-Commerce, Supply-Chain-Management oder Content-Delivery anzubieten. Auch Managed Security Services, beispielsweise Managed Firewall und Managed Intrusion Detection, sind höherwertige Dienste, mit denen der wachsende Securitybedarf gerade im Mittelstand bedient werden kann. Egal welchen der Managed Services Sie realisieren möchten, in jedem Fall können Sie die Erweiterungsmöglichkeiten der bereits existierenden Cisco Router und Cisco Catalyst Switches für die Realisierung Ihres Vorhabens ausschöpfen. Durch die Nutzung des existierenden Investments sinken die Kosten für Implementierung und Betrieb und wachsen die Chancen auf neue Ertragsquellen.

Cisco Channel Partners

Mit dem Cisco Security Spezialisierungsprogramm würdigt Cisco Channelpartner, die in Trainings- und Fortbildungsmaßnahmen im Bereich Sicherheit investiert haben und jetzt in der Lage sind Cisco-Netzwerksicherheitslösungen zu designen, installieren und Kundenunterstützung zu bieten. Geschäftliche Lösungen über das Internet werden immer häufiger verlangt – die Cisco VPN und Security Specialized Partner helfen diese Lösungen rasch und kompetent umzusetzen.

Cisco Training Services – Cisco Security Certifications

Cisco Security Certifications bieten für den Spezialisten und Unternehmen einen Maßstab zur Überprüfung der Fähigkeiten und Kompetenzen von Sicherheitsspezialisten. Das CCSP und die drei dazugehörigen Zertifizierungen – Cisco VPN Spezialist, Cisco

Firewall Spezialist und Cisco IDS/IPS Spezialist – erfüllen die Forderungen der Industrie nach einem soliden Ausbildungsprogramm, einschließlich Zertifizierungspfad, für den IT-Sicherheitsmarkt. Das CCSP stellt sicher, dass Ihre Mitarbeiter erfolgreich umfassende und durchgängige Sicherheitslösungen implementieren.

Authorized Cisco Learning Partners mit Spezialisierung auf Security

Viele autorisierte Cisco Learning Partner weltweit fokussieren auf Cisco Sicherheits-trainings. Sie bieten Kurse, Remote Labs und Materialien für ein Selbststudium über die neuesten Sicherheitstechnologien. Dazu gehören Advanced Cisco PIX Firewalls, Cisco Secure Intrusion Prevention Systeme, Cisco SAFE Design Implementierung und Managing Cisco Network Security. Eine Übersicht aller Kurse und Prüfungstermine und eine ausführliche Liste von Partnern, die auf Security spezialisiert sind finden Sie unter: <http://www.cisco.com/go/training>

Cisco Security Ecosystem

Die Security-Produkte, Technologien und Services von Cisco bilden die grundlegenden Bestandteile einer erfolgreichen Netzwerksicherheitslösung. Ein umfassender Ansatz für Netzwerksicherheit muss jedoch auch andere Bereiche abdecken – gleichsam wie in einem Security-Ökosystem, das alle Vorzüge der Cisco-Produkte komplett ausschöpft. Solch ein Ökosystem umfasst mehrere wichtige Teile, wie kompatible Produkte anderer Hersteller, Dienstleistung zur Implementierung, Kundenunterstützung und ergänzende Dienstleistungsangebote.

Das Cisco AVVID Security Partner Programm ist ein Testprogramm mit Co-Marketing-Angeboten, das die Interoperabilität ergänzender Sicherheitslösungen anderer Hersteller mit den Produkten von Cisco sicherstellt. Dieses Programm verwandelt unabhängige Produkte in schlagkräftige Sicherheitslösungen und bietet so Cisco-Kunden getestete, zuverlässige Security-Implementierungen.

Zusammenfassung – das Self-Defending Network von Cisco

Die Cisco-Vision für mehr Sicherheit ermöglicht es Cisco-Kunden, ihre Produktivität zu steigern. Heute liefert Cisco integrierte Sicherheitslösungen, die eine sichere Vernetzung erlauben, durch die Einbindung einer Vielzahl an Sicherheitsfunktionen in die Cisco-Infrastruktur und durch das Angebot von zahlreichen speziellen Security-Appliances, Software und Beratungsdienstleistungen.

Ciscos Sicherheitslösungen ermöglichen es Ihrem Unternehmen kosteneffizient von den Vorteilen der Internet-Economy zu profitieren und die neuen Möglichkeiten zu erforschen, die riesige Wachstumschancen in sich bergen.

Weitere Informationen über Ciscos integrierte Sicherheit und den Aufbau eines Self-Defending Networks finden Sie unter:

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

<http://www.cisco.com/selfdefend>

<http://www.cisco.com/securitynow>





Cisco Systems GmbH
Kurfürstendamm 22
10719 Berlin
Fax: 030/9 78 92-110

Cisco Systems GmbH
Neuer Wall 77
20354 Hamburg
Fax: 040/376 74-444

Cisco Systems GmbH
Hansaallee 249
40545 Düsseldorf
Fax: 02 11/52029-10

Cisco Systems GmbH
GS Bonn
Friedrich-Ebert-Allee 67
53113 Bonn
Fax: 02 28/32 95-10

Cisco Systems Austria
Millennium Tower
Handelskai 94-96
A-1200 Wien
Tel.: +43/1/2 40 30-0
Fax: +43/1/2 40 30-63 00
Hotline: 00 8 00/99 99 05 22
www.cisco.at

Cisco Systems GmbH
Industriestraße 3
65760 Eschborn
Fax: 061 96/7 73 97-00

Cisco Systems GmbH
Herold Center
Am Wilhelmsplatz 11
70182 Stuttgart
Fax: 07 11/239 11 11

Cisco (Switzerland) GmbH
Glatt-Com
8301 Glattzentrum
Schweiz
Tel.: +41/1/8 78 92 00
Fax: +41/1/8 78 92 92
www.cisco.ch

Cisco Systems GmbH
Am Söldnermoos 17
85399 Hallbergmoos
Fax: 08 11/55 43-10

Tel.: 00800-9999-0522
info-center@cisco.com
Internet: www.cisco.de