

NEUE TECHNOLOGIEN VON CISCO HELFEN KUNDEN BEI DER EINHALTUNG RECHTLICHER VORGABEN

Kurze Zusammenfassung/Lernziel

Unternehmen können es sich heute nicht mehr leisten, regulatorische Vorgaben zu ignorieren. Technologisch nicht im Rahmen rechtlicher Vorschriften zu sein kann Imageschäden, hohe Strafen für Firma und Management sowie Umsatzeinbußen bedeuten. Doch das Erlangen von Compliance hat auch Vorteile. Durch den Prozess der Vorbereitung haben Unternehmen die Chance, ihr Netzwerk stabiler und sicherer zu machen. Das Ergebnis sind gesteigerte Produktivität und höhere Verfügbarkeit. Die Vorschriften verlangen oft IT-Funktionalitäten in den Bereichen Vertraulichkeit, Integrität, Verfügbarkeit und Auditierbarkeit (CIAA), die älteres Netzwerk-Equipment noch nicht bieten kann. Das aktuelle Produktportfolio von Cisco Routern und Switches ist darauf ausgelegt, diese Anforderungen zu erfüllen, und bietet zudem Vorteile hinsichtlich Leistung, Management und Verfügbarkeit.

Regulatorische Compliance: Die Herausforderung

Auf der ganzen Welt verlangen Regierungen, große Unternehmen und die Öffentlichkeit, dass Organisationen alle notwendigen Schritte unternehmen, um sicherzustellen, dass sowohl firmen- als auch private Daten korrekt genutzt und geschützt werden. Als Folge davon verabschieden Industriegremien und Regierungsstellen immer neue Vorschriften – seit 1981 mehr als 114.000, wie eine Studie der Burton Group ergab.

Tabelle 1 zeigt einige Beispiele für solche Vorschriften, die Informationen, die damit geschützt werden sollen sowie das Jahr, in dem die Vorschrift in Kraft trat.

Tabelle 1 Diverse bekannte Compliance-Standards

Vorschrift	Geschützte Information	Gültig seit
Health Insurance Portability and Accountability Act (HIPAA)	Gesundheitsdaten von Patienten	1996
Gramm-Leach-Bliley Act (GLBA)	Finanzdaten von Verbrauchern	1999
Sarbanes-Oxley Act von 2002	Buchhaltungs- und Finanzdaten von Firmen	2002
Federal Information Security Management Act	Informationen der US-Bundesbehörden	2003
Payment Card Industry (PCI) Data Security Standard	Kreditkartendaten	2005
Federal Financial Institution Examination Council (FFIEC)	Finanzdaten von Firmen und Privatpersonen	2006
Basel II	Buchhaltungs- und Finanzdaten von Firmen	2008

Als Ergebnis dieses Drucks entwickelt sich IT-Governance zu einem wachsenden Problem in Unternehmen. Firmen versuchen ihre IT-Systeme und Netzwerke mit den Unternehmenszielen in Einklang zu bringen und gleichzeitig die neuen Informationsrisiken in den Griff zu bekommen, die die Vertraulichkeit, Integrität und Verfügbarkeit von Prozessen und Daten gefährden.

Die Compliance mit Vorschriften sicherzustellen ist eine Aufgabe für alle Abteilungen im Unternehmen, doch sie stellt für IT-Manager die größte Herausforderung dar. Die meisten Vorschriften formulieren nicht eindeutig, welche Anforderungen sie im Hinblick auf die IT stellen, und oft sind mehrere unterschiedliche Vorschriften gültig. Das macht es für IT-Manager schwierig, zu beurteilen, wie die Compliance-Vorgaben einzuhalten sind. Weil die Konsequenzen für das Nichteinhalten der Vorgaben durchaus drastisch ausfallen können – sie reichen von hohen Geld- bis hin zu Gefängnisstrafen bei besonders schweren Verstößen – sind viele IT-Manager in Bezug auf dieses Thema verständlicherweise sensibel.

Auch wenn es große Unterschiede zwischen den Vorschriften gibt, so haben sie doch in wichtigen Bereichen einiges gemeinsam: sie betreffen fundamentale Bereiche der IT-Sicherheit und des Datenschutzes. Darum gibt es für die IT einen durchaus optimalen Ansatz, um mit Compliance-Vorgaben umzugehen. Zunächst muss klar sein, welchen Bedrohungen und Schwachstellen sich Daten und Netzwerk gegenübersehen – dann kann eine sichere und effiziente Lösung auf Basis einer durchdachten technologischen Infrastruktur entwickelt und umgesetzt werden. Dieser Ansatz erleichtert es Firmen, mit neuen gesetzlichen Vorgaben umzugehen. Auch wenn viele Unternehmen heute bereits über solide Netzwerkinfrastrukturen verfügen, sind unter Umständen Upgrades oder eine Auffrischung der Technologie dennoch notwendig, um eine umfassende Lösung zu schaffen, die mit allen regulatorischen Vorgaben konform ist.

Einige Beispiele für die Kosten des Nichteinhaltens von Vorschriften

- Ein Großhändler wurde von Kreditkartenunternehmen auf 16 Millionen US Dollar verklagt, weil durch ihn Kreditkartendaten kompromittiert wurden
- Eine Franchise-Restaurantkette wurde wegen kompromittierter Kreditkartendaten zu einer Strafe von 500.000 US-Dollar verurteilt und muss die Kosten für die Neuausgabe der Kreditkarten tragen
- Ein kleiner Lebensmittelladen musste eine Strafe von 50.000 US-Dollar wegen Non-Compliance an einen Kreditkarten-Interessenverband zahlen

Bedrohungsmodell erstellen: CIAA

Eine Möglichkeit, Bedrohungen und Schwachstellen eines Systems aufzuspüren, bevor die Sicherheitsmaßnahmen festgelegt werden, ist das CIAA-Bedrohungsmodell. Es teilt Schwachstellen und Sicherheitsanforderungen in vier Kategorien ein: Vertraulichkeit, Integrität, Verfügbarkeit und Auditierbarkeit, kurz CIAA!¹

¹ Das CIAA-Modell wird weltweit verwendet, aber das zweite A steht neben Auditierbarkeit oft auch für Authentifikation oder Accountability. Das Ziel ist freilich immer dasselbe.

Durch die Einteilung von Schutzmaßnahmen und Schwachstellen in diese vier Kategorien, können IT-Manager ein allgemeines Grundniveau festlegen, das dabei hilft, vorschriftskonforme Richtlinien aufzustellen. Das CIAA-Modell wächst mit neuen Bedrohungen, die sich ständig entwickeln; diese können leicht in das Modell integriert werden, ohne generell den Prozess zu verändern. Genauso lassen sich neu entdeckte Schwachstellen und neue Sicherheitsmaßnahmen integrieren, sobald sie bekannt werden.

Vertraulichkeit

Vertraulichkeit bezieht sich auf die Herausforderung des Datenschutzes beim Transport über das Netzwerk, das heißt die Frage, wie sichergestellt werden kann, dass niemand die Daten abfängt, und wie gewährleistet wird – falls die Daten doch abgefangen werden – dass die Daten nicht von Dritten gelesen oder ausgewertet werden können. IP-Spoofing, einschließlich des Man-in-the-Middle-Angriffs, sind Beispiele für Bedrohungen der Vertraulichkeit.

Vertraulichkeit betrifft das Netzwerk in drei Bereichen:

- Authentifizierung durch eindeutige Benutzererkennung und sichere Authentifizierungsprozesse
- Zugangskontrolle durch Vergabe von Zugriffsrechten auf einer Need-to-Know Basis
- Datenschutz, der auf einem hohen Verschlüsselungsgrad von Daten während des Transports oder im Speicher beruht

Technologien für Vertraulichkeit

Vertraulichkeit greift auf eine Reihe von etablierten Sicherheitsfunktionen in Cisco-Produkten zurück, darunter Firewalls, VPNs, Intrusion-Prevention-Systeme (IPS), Authentifizierung – Autorisierung – Accounting (AAA) und den Schutz von Endgeräten (Endpoint Protection).

Verschlüsselung ist für die Vertraulichkeit von Daten während des Transports besonders wichtig. Cisco Security-Lösungen, darunter Cisco IOS Software in Routern und Switches von Cisco, unterstützen die Verschlüsselung. Sie ist ein wesentlicher Schutzaspekt, sobald Daten durch unsichere Netzwerke wie das Internet, drahtlose Hot-Spots, ungesicherte Netzwerksegmente und Gastzugänge zu Netzwerken transportiert werden.

Weitere nützliche Funktionen und Technologien für die Vertraulichkeit in Routern und Switches sind:

- VLAN-Segmentierung
- Virtual Route Forwarding (VRF)
- Port Security bei Switches
- DHCP gegen Spoofing in Switches

Integrität

Die Kategorie Integrität enthält Maßnahmen, mit denen sich Daten vor unerlaubter Veränderung oder Zerstörung schützen lassen. Integrität bedeutet, dass Informationen korrekt und vollständig sind und dass deren Korrektheit und Vollständigkeit unantastbar garantiert ist. Zu den spezifischen Bedrohungen der Integrität gehören Datendiebstahl sowie das Kopieren, Speichern und Verändern von Daten, außerdem der unerlaubte Zugang zu Informationen.

Technologien für Integrität

Die wichtigsten Maßnahmen von Cisco zur Sicherung der Integrität von Daten ist der Einsatz von Firewall und IPS auf Netzwerkseite und der Cisco Network Admission Control (NAC) sowie des Cisco Security Agent auf Seiten des Endgeräts. Beide Verfahren sollten durch Cisco Identity-Based Networking Services (IBNS) zur sicheren Zugangskontrolle der Benutzer ergänzt werden.

Cisco Router und Switches enthalten Firewall und IPS-Funktionen, um unerlaubten Zugang zu Servern zu verhindern. Der Cisco Security Agent schützt Daten vor dem unzulässigen Verändern, Löschen, Kopieren und Drucken. Cisco NAC kann ein Profil aller Benutzer erstellen, sobald sie sich mit dem Netzwerk verbinden, und zusammen mit Cisco IBNS sowie Cisco Secure Access Control Server (ACS) Richtlinien und Zugangsrechte durchsetzen.

Wenn Daten übertragen werden, stellen Verschlüsselung und virtuelle private Netzwerke (VPN) deren Integrität sicher. Cisco IOS Software unterstützt eine ganze Reihe von Verschlüsselungsmethoden und VPNs, darunter:

- IP Security (IPSec) VPNs
- Secure Sockets Layer (SSL) VPNs
- Multiprotocol Label Switching (MPLS) VPNs
- Dynamic Multipoint VPNs (DMVPNs)
- Group Encrypted Transport VPNs

Verfügbarkeit

In mancher Hinsicht scheint Verfügbarkeit das Gegenteil von Vertraulichkeit zu bedeuten. Doch dieser Eindruck täuscht: Wenn es um Compliance geht, bedeutet Verfügbarkeit, dass **autorisierte** Benutzer zu jeder Zeit auf Daten zugreifen können und dass diese Daten für **nicht autorisierte** Benutzer nie erreichbar sind. Auch wenn viele Verfügbarkeit nicht als Sicherheitsfunktion betrachten, ist sie nichtsdestotrotz enorm wichtig für das Sicherheitskonzept. Verfügbarkeit muss auch garantieren, dass das Sicherheitssystem weit genug gefasst ist, dass es rechtmäßige Benutzer nicht von ihren Daten fernhält. Im Rahmen einiger Vorschriften wie HIPAA erfordert die Compliance auch, dass ein Unternehmen Verfügbarkeit im Sinne von Disaster Recovery und Verfügbarkeit der Geschäftsprozesse adressiert.

Einige spezifische aktive Angriffe auf die Verfügbarkeit sind Viren, Würmer und Denial-of-Service (DoS)-Angriffe. Auch Naturkatastrophen, Stromausfälle und verschiedene Notsituationen stellen eine Bedrohung dar.

Technologien für Verfügbarkeit

Cisco bietet Unternehmen jeder Größe eine ganze Reihe von Optionen, mit denen sie die Verfügbarkeit der Geschäftsprozesse durch verbesserte Widerstandsfähigkeit von Netzwerk und Anwendungen erhöhen und gleichzeitig die Betriebskosten senken können.

Network-Based Application Recognition (NBAR) ist ein solches Feature, mit dem Cisco Router und Switches die Verfügbarkeit angehen. Unternehmenswichtige Anwendungen wie Enterprise Resource Planning (ERP) und Applikationen zur Optimierung der Mitarbeiter lassen sich durch Cisco IOS Software intelligent identifizieren. Sobald diese Anwendungen erkannt wurden, kann man eine Grundbandbreite für sie reservieren, sie als besonders wichtig markieren und bevorzugt routen. Weniger wichtige Anwendungen lassen sich ebenfalls mit NBAR identifizieren und für Best-Effort Service kennzeichnen, einschränken oder ganz blockieren.

Nonstop Forwarding mit Stateful Switchover (NSF/SSO) ist eine weitere hilfreiche Technologie zur Sicherstellung eines hohen Maßes an Verfügbarkeit. Durch NSF/SSO wird der Status einer Session beibehalten, so dass die Kommunikation auch im Fall des Ausfalls einer Supervisor-Engine praktisch ununterbrochen weiterläuft.

Weitere nützliche Funktionen und Technologien für die Verfügbarkeit von Routern und Switches sind:

- Clustering und Load-Balancing
- Widerstandsfähigkeit von Komponenten, Geräten, Systemen und Übertragung
- Cisco Generic Online Diagnostics (GOLD) und Cisco IOS Embedded Event Manager (EEM)
- Cisco NAC

Auditierbarkeit

Aus Sicht der Compliance ist die Auditierbarkeit wahrscheinlich die wichtigste der vier CIAA-Kategorien. Ihr Ziel ist es, Beweise in Form einer Belegsammlung dafür zu liefern, dass ein Unternehmen alle notwendigen Schritte unternimmt, um bestimmte Vorschriften einzuhalten und wichtige Daten zu schützen. Jede Maßnahme im Sicherheitsbereich, die eine Firma durchführt, muss erfasst und festgehalten werden – nur so lässt sich Compliance nachweisen und eine Untersuchung im Fall eines Ereignisses durchführen. Zu den wichtigsten Punkten in dieser Kategorie gehören das Reporting, die Überwachung sowie das Aufzeichnen von Protokollen. Um die Einhaltung der Compliance nachzuweisen und Ermittlungen bei einem Vorfall durchzuführen, müssen IT-Manager in der Lage sein, aufgezeichnete Informationen in ausreichender Zahl zu jeder sicherheitsrelevanten Aktion bereitzustellen, darunter:

- Wann fand die Aktion statt?
- Welche Einbruchversuche waren erfolgreich und welche scheiterten?
- Wer war der Angreifer?
- Wie und von wo gewann der Angreifer Zugriff?
- Welche Daten waren betroffen?
- Was geschah mit den Daten?

Technologien für die Auditierbarkeit

Um Compliance mit regulatorischen Vorgaben zu erreichen, muss der Networkbetreiber verstehen, wie sich das Netzwerk verhält, einschließlich dessen Reaktion auf Änderungen. Die wichtigste Lösung von Cisco für den Schutz vor, das Aufdecken von und die Reaktion auf Bedrohungen ist das Cisco Security Monitoring, Analysis, and Response System (MARS). Cisco Security MARS stattet das Netzwerk mit Intelligenz aus, MARS sammelt Alarmmeldungen und Benachrichtigungen von Firewalls, IPSs, Cisco NetFlow, drahtlosen Anwendungen, dem Cisco Security Agent und anderen Tools. Aufgrund dieser Daten identifiziert Cisco Security MARS die Bedrohung, stellt fest, von wo sie ausgeht, wie sie am effizientesten zu stoppen ist und die Daten vor ihr zu schützen sind. Des Weiteren zeichnet Cisco Security MARS alle Aktionen auf, um die Erstellung von Reports und Compliance-Audits zu ermöglichen.

Größere Unternehmen benötigen ein hoch skalierbares Tool für Audit-Reports. CiscoWorks Network Compliance Manager (NCM) regelt und protokolliert Konfigurations- und Softwareänderungen in einer Multi-vendor-Netzwerkinfrastruktur (einschließlich Cisco Router, Switches, Firewalls, Sicherheitsappliances und Load-Balancer). Es macht Änderungen im Netzwerk transparenter und kann die Einhaltung einer großen Zahl von Best-Practice-Maßnahmen aus den Bereichen Compliance, Technologie, IT und Corporate Governance sicherstellen.

Die Cisco Configuration Assurance Solution (CAS) führt Modellversuche durch, analysiert die Auswirkungen von Änderungen auf das Netzwerk und vergleicht sie mit regulatorischen Vorgaben. Die Lösung zeigt an, wenn Änderungen an der Netzwerkinfrastruktur (Router, Switches, Sicherheitsappliances und Geräte von anderen Herstellern) das Unternehmen dem Risiko von Schwachstellen oder Non-Compliance aussetzen.

Ein weiteres hilfreiches Tool ist Cisco NetFlow, eine Komponente der Cisco IOS Software, die das Netzwerkverhalten bewertet und tieferen Einblick in das Netzwerk gewährt. Cisco NetFlow untersucht und protokolliert Problembereiche wie Netzwerkanomalitäten und Sicherheitsschwachstellen. Administratoren bekommen mit Cisco NetFlow ein Tool, das ihnen zeigt, wie, wann, wodurch und wohin der Netzwerkverkehr fließt. Cisco NetFlow gibt diese Informationen dann an Cisco Security MARS zur tiefergehenden Auswertung weiter.

VLAN-Segmentierung, ein Feature der Cisco IOS Software in Routern und Switches, ist besonders hilfreich, wenn es um die Auditierbarkeit geht. Durch VLAN-Segmentierung lassen sich Bereiche des Netzwerks logisch abtrennen, die Auditierung bleibt auf einen genau festgelegten Fokus beschränkt und sorgt so für niedrigere Betriebskosten. So lässt sich beispielsweise der Fokus eines Audits auf ein Segment beschränken, ohne auf das gesamte Netzwerk ausgedehnt werden zu müssen. Diese Fähigkeit ist besonders für die Reduzierung der Audit-Kosten entscheidend, weil sich der Fokus einer Untersuchung auf exakt diejenigen Bereiche konzentrieren lässt, die sensible Informationen enthalten.

Weitere nützliche Tools für die Kategorie Auditierung umfassen:

- Switched Port Analyzer (SPAN), Remote SPAN (RSPAN) und Encapsulated RSPAN (ERSPAN)
- Firewall und IPS-Alarme
- Syslog Reports
- Cisco Security Agent

Umfassende Technologielösung für regulatorische Compliance

Das Netzwerk spielt eine maßgebliche Rolle in der regulatorischen Compliance, da es jeden Aspekt des erweiterten Unternehmens berührt und alle Geschäftsprozesse verbindet. Weil das Unternehmensnetzwerk heute auch Außenstellen und Telearbeiter mit einbezieht, benötigen Firmen einen systembasierten End-to-End-Ansatz. Er muss integriert und wandelbar sein, um das Unternehmen dabei zu unterstützen, Sicherheitslücken und regulatorische Anforderungen in den Griff zu bekommen.

Firmen, die sich Compliance-Herausforderungen gegenübersehen, finden im Cisco Self-Defending Network, einschließlich Cisco Router und Switches, eine Lösung. Das Cisco Self-Defending Network besteht aus der Cisco IOS Software und Cisco Appliances, deren Sicherheitsfeatures direkt auf die IT-Anforderungen der Vorschriften eingehen. Der Einsatz oder Upgrade auf die aktuellen Routing- und Switching-Plattformen, die das Cisco Self-Defending Network unterstützen, hilft Firmen nicht nur dabei, Compliance zu erzielen, sondern kann zudem Kosten senken und Sicherheitsrisiken verringern.

Cisco Self-Defending Network

Das Cisco Self-Defending Network ist ein immens wichtiger Bestandteil bei der Verbesserung der gesamten Sicherheitssituation eines Unternehmens und für das Einhalten von Compliance-Vorgaben. Das Cisco Self-Defending Network bietet einen End-to-End-Systemansatz, der eine elegante und weniger komplexe Möglichkeit bietet, Netzwerk-Sicherheitsrisiken und Compliance-Vorgaben zu verwalten. In ein übergreifendes Systemkonzept integriert, kann das Cisco Self-Defending Network Management Überschneidungen und redundante Kosten reduzieren, weil es Standardprozesse zur Einhaltung der Compliance nutzt. So können Firmen ihre Geschäftsziele und Strategien umsetzen und gleichzeitig ihre Netzwerksicherheitsrisiken effektiv im Auge behalten.

Voraussetzung für das Cisco Self-Defending Network ist eine sichere Netzwerkplattform: Die branchenweit führenden Router und Switches von Cisco. Weil Sicherheitsfunktionen und Technologien bereits in die Struktur des Netzwerks eingebunden sind, wird die Sicherheit zu einem integralen Grundbestandteil.

Das Cisco Self-Defending Network bietet zudem weitergehende Technologien und Sicherheitsdienste, darunter Lösungen wie:

- Bedrohungskontrolle und Eindämmung, damit die Mitarbeiter trotz einer herausfordernden und dynamischen Bedrohungssituation produktiv bleiben
- Vertrauliche Kommunikation, um sicherzustellen, dass wichtige Telefonate, Daten und drahtlose Verbindungen geschützt bleiben
- Sichere Transaktionen, egal ob sie intern oder mit Kunden abgewickelt werden, um die empfindlichsten und wichtigsten Aktivposten der Firma zu schützen

Um das Cisco Self-Defending Network zu vervollständigen, liefert Cisco eine ganze Familie von Tools, die einen Rahmen für das Management der Betriebsprozesse und die Verwaltung von Richtlinien bilden. Miteinander ergeben diese Elemente eine stabile Strategie, um CIAA anzugehen.

Beispiel: PCI Data Security Standard

Der PCI Data Security Standard ist ein gutes Beispiel für die Unterstützung eines Unternehmens bei der Erzielung von Compliance durch das Cisco Self-Defending Network. Jede Organisation, die Kreditkartendaten speichert, verarbeitet oder übermittelt, unterliegt dem PCI-Standard.

Cisco kann Unternehmen dabei helfen, den PCI-Anforderungen zu entsprechen, indem es integrierte, aufeinander abgestimmte und wandelbare Lösungen bietet, die auf bestimmte Bereiche des PCI-Standards zugeschnitten sind. Zu den Komponenten einer PCI-konformen Lösung von Cisco gehören:

- Sichere Router: Router mit Cisco IOS Software enthalten weitergehende Sicherheits- und Kommunikationsfähigkeiten wie VPN, drahtlose Kommunikation, Sprache, Firewall, Intrusion Prevention und Netzwerkverkehrsanalyse.
- Network Admission Control: Cisco NAC stellt fest, welcher Client-PC Zugriff auf das Netzwerk erhält und welcher abgewiesen wird. Die Kontrolle über den Netzwerkzugang reduziert die Gefahr eines unbefugten Zugriffs auf Kreditkartendaten.
- Compliance Reporting und Management: Cisco Security MARS, der Cisco Security Manager und andere Managementprodukte stellen vielfältige Dienste zur Verfügung – Berichte über die Ausnutzung des Netzwerks und Ereignisse, Provisionierung, Richtlinien und Change-Management sowie Kontrolle des Workflows im Netzwerk. Diese Daten können in Compliance-Berichten zur Auditierung genutzt werden. Mit diesen Cisco-Managementprodukten lassen sich auch die Betriebskosten senken.

Aktuellere Technik aus Compliance-Gründen einsetzen

Organisationen sehen sich mit der Herausforderung konfrontiert, der wachsenden Liste von Compliance-Anforderungen im IT-Bereich nachzukommen. Viele stellen fest, dass die vorhandenen Netzwerke zwar ihren Zweck in den letzten Jahren gut erfüllt haben, deren Sicherheitsfunktionen aber nicht mehr ausreichen, um die wachsenden Compliance-Forderungen zu erfüllen. Wie eine Studie von Forrester ermittelte, nennen 42 Prozent der befragten Firmen das Thema Sicherheit als Grund für Updates im Netzwerk. Weil viele der aktuellen Produkte und Technologien von Cisco noch weitere Vorteile bieten, darunter verbesserte Produktivität, geringeren Stromverbrauch und vereinfachten Betrieb, entscheiden sich zahlreiche Kunden von Cisco für ein Upgrade. Dadurch wird nicht nur die Einhaltung von Compliance-Vorgaben erleichtert, nebenbei ist es auch eine wertvolle Investition, um die Total Cost of Ownership (TCO) des Netzwerks zu senken.

Der Austin Independent School District war mit der Einhaltung von drei verschiedenen gesetzlichen Vorgaben konfrontiert. Sie sollten den Schutz der Schülerdaten gewährleisten und sie vor unzulässigen und nicht altersgemäßen Inhalten schützen (Childrens Internet Protection Act (CIPA), Family Educational Rights and Privacy Act und HIPAA). Der District entschied sich für eine integrierte Netzwerklösung von Cisco. Durch deren erweiterte Sicherheitsfunktionen wurde nicht nur die Compliance mit den Vorgaben erreicht, sondern auch die Produktivität erhöht und die Kosten gesenkt.

„Das Netzwerkupgrade hatte deutliche Vorteile für den District. Die Schüler haben nun mehr Möglichkeiten zum Lernen, darüber hinaus konnte der Austin Independent School District sein bestehendes Netzwerk länger nutzen, die Effizienz der Mitarbeiter verbessern, die Kosten senken und dem District die Vorteile einer leistungsfähigen neuen Technologie zur Verfügung stellen. So wurden die Steuergelder umsichtig eingesetzt.“

Gray Salada, Chief Information Officer, Austin Independent School District

Das aktuelle Portfolio der Cisco Routing- und Switching-Plattformen, wie die Cisco Integrated Services Router und die Cisco Catalyst Switches der 3750er, 4500er und 6500er Serie, verfügen über viele neue Fähigkeiten, die die Vorgängerplattformen bisher nicht boten. Die Tabelle zeigt einige der Sicherheitsfeatures und Technologien der neuen Cisco-Plattformen für den Campus, das WAN-Headend und Außenstellen im Überblick.

Sicherheitsfeatures und Technologien von neuen Cisco Plattformen

Campus (1)	WAN Headend (2)	Außenstelle (3)
<ul style="list-style-type: none"> · VLAN-Segmentierung · Cisco In-Service Software-Upgrades (ISSU) · Distributed DoS-Schutz · Man-in-the-Middle-Schutz · Cisco IBNS-Fähigkeit · Cisco NAC-Fähigkeit · NFS/SSO · Hardware-basierte Applikations-Intelligenz (mit NBAR) · Hardware-basierte flexible Paketzurordnung (FPM) · Cisco GOLD · Cisco IOS EEM · ERSPAN · Cisco NetFlow-Unterstützung · VRF-fähige Dienste 	<ul style="list-style-type: none"> · Cisco ISSU · DDoS-Schutz · Stateful und VRF-fähige Firewall · IPS-Funktion · Cisco NetFlow Netzwerk-Über-sichtstools · IPSec und SSL VPN-Unterstützung · Cisco NAC-Fähigkeit · Reverse Path Forwarding (RPF) · Control-Plane-Richtlinien · Anwendungsintelligenz (mit NBAR) · Cisco Secure Multicast · DMVPN · Group Encrypted Transport VPN 	<ul style="list-style-type: none"> · DDoS-Schutz · Stateful und VRF-fähige Firewall · ISP-Fähigkeit · Cisco NetFlow Netzwerk-Über-sichtstools · Cisco NAC-Fähigkeit · Anwendungsintelligenz (mit NBAR) · Eingebaute Verschlüsselungs-Hardware · Cisco IOS Software IPSec und SSL VPN · Secure Wireless · WAN-Optimierung

(1) Cisco Catalyst Switches 4500er und 6500er Serie, verglichen mit Cisco Catalyst Switches 5000er und 5500er Serie

(2) Cisco Router der 7600er Serie und Cisco Catalyst Switches der 6500er Serie, verglichen mit Cisco Routern der 7500er Serie

(3) Cisco Integrated Services Router der 3800er und 2800er Serie, verglichen mit den Vorgängermodellen der Router für Außenstellen

Anwendergeschichte: Metropolitan Transit System

Montreals öffentliches Nahverkehrssystem, die Société Transport de Montreal (STM), betreibt Bus- und U-Bahnlinien. Jeden Tag werden die Transportmittel 1,3 Millionen Mal in Anspruch genommen. Das Herz der großen und vielgestaltigen Organisation ist die IT-Abteilung. Sie gewährleistet die Verfügbarkeit, Integrität und Vertraulichkeit für die 120 Informationssysteme, welche die STM einsetzt. Um diesen gewaltigen Betrieb zu unterstützen, investierte die STM in ein sorgfältig designtes Netzwerk von Cisco. Weil das Dienstleistungsunternehmen von mehreren Behörden gelenkt und überwacht wird, betreibt die STM ein umfangreiches Berichtswesen und muss verschiedenen Daten- und Netzwerksicherheitsvorschriften entsprechen.

Die STM setzte Sicherheitsfunktionen von Cisco ein, darunter die Cisco Catalyst Switch-basierten Firewall- und IPS-Dienste sowie die Cisco VPN-Konzentratoren der 3000er Serie für sichere Fernzugänge. Doch die zusätzlichen Sicherheitskomponenten im Netzwerk sorgten für einen exponentiellen Zuwachs an Sicherheitsrohdaten. Schädliche Vorgänge in einem so großen Netzwerk zu identifizieren – und Gegenmaßnahmen zu ergreifen – stellte eine enorme Herausforderung dar. Die IT-Manager benötigten eine effizientere, proaktive Lösung, um die Sicherheitsdaten des Netzwerks zu überwachen.

Um diesen Herausforderungen zu begegnen, implementierte die STM Cisco Security MARS, einen Bestandteil der Cisco Security Management Suite. Cisco Security MARS Appliances sind in der Lage, die großen Mengen der typischerweise in einem solchen Netzwerk generierten Sicherheitsinformationen zusammenzufassen und aufzubereiten. Events können mit anderen Vorkommnissen korreliert werden, und eine Gültigkeitsprüfung hilft bei der Erkennung von und Reaktion auf Bedrohungen in Echtzeit.

Die Lösung konnte sehr einfach in das bestehende Netzwerk und die Prozesse der STM integriert werden. Heute sind die IT-Manager der STM in der Lage, Bedrohungen schneller zu erkennen und darauf zu reagieren als jemals zuvor. Diese Vorteile hatten beträchtliche Produktivitätszuwächse beim IT-Personal der STM zur Folge. Die Lösung erwies sich zudem als Gewinn für die regulatorischen Compliance-Anforderungen der STM. Vor der Einführung von Cisco Security MARS musste der IT-Leiter vor einem Sicherheitsaudit Daten aus verschiedenen Quellen zeitaufwendig zusammensuchen. Das nahm mehrere Tage in Anspruch. Nun verursachen Audits so gut wie keine Vorbereitung mehr, und die IT kann sich auf andere wichtige Aufgaben konzentrieren.

Schlussfolgerung

Auch wenn der Unterschied zwischen einer sorgfältig geplanten Sicherheitsstrategie und einer Strategie aus dem Stegreif enorm ist, was die Wirksamkeit angeht, gibt es in der Regel keine vollständige Sicherheit oder Compliance. Allerdings haben Firmen, die sich dem Thema Compliance mit einer soliden Sicherheitsbasis, einem erprobten IT-Managementkonzept, Best Practices und dem CIAA-Ansatz nähern, mit hoher Wahrscheinlichkeit einen besseren Stand, wenn es zu einer Compliance-Begutachtung kommt. Darüber hinaus bereitet die Wahl des aktuellen Cisco-Portfolios aus Routern, Switches und Cisco IOS Software Unternehmen schon auf die Compliance-Herausforderungen der Zukunft vor. Denn die Cisco-Systeme wurden entwickelt, um solchen Herausforderungen nachhaltig die Stirn zu bieten.

Weitere Informationen:

- Regulatorische Compliance
http://www.cisco.com/en/US/netsol/ns625/networking_solutions_package.html
- Cisco Sicherheitsfeatures
<http://www.cisco.com/go/security>
- Soci t  Transport de Montreal – Anwendergeschichte
http://www.cisco.com/en/US/products/ps6241/products_case_study0900aecd8047bc61.shtml



Cisco Systems GmbH
Kurfürstendamm 21-22
10719 Berlin

Cisco Systems GmbH
Neuer Wall 77
20354 Hamburg

Cisco Systems GmbH
Hansaallee 249
40549 D sseldorf

Cisco Systems GmbH
Ludwig-Erhard-Stra e 3
65760 Eschborn

Cisco Systems GmbH
Wilhelmsplatz 11 (Herold Center)
70182 Stuttgart

Cisco Systems GmbH
Am S ldnermoos 17
85399 Hallbergmoos

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

 2006 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)