

Wir beraten Sie gerne!

Aktuelles Thema im Mittelstand: **Unternehmenssicherheit**

Antwort-Fax:
08142 / 4586 - 199

- Ja**, bitte beraten Sie mich unverbindlich zum Thema Unternehmenssicherheit mit Cisco SAFE. Bitte nehmen Sie dazu Kontakt zu mir auf.
- Ja**, ich möchte auch künftig Informationen von Ihrem Unternehmen erhalten.

_____	_____
Firma	Funktion/Abteilung
_____	_____
Name	Vorname
_____	_____
Straße/Postfach	PLZ/Ort
_____	_____
Telefon	Telefax
_____	_____
E-Mail	Branche

- Bitte entfernen Sie meine Adresse aus Ihrem Verteiler.

net Stemmer GmbH
Peter-Henlein-Strasse 2
D-82140 Olching
Tel. 08142 / 4586 - 100

www.stemmer.de



*FYI BERND (NETZWERKE)
wichtig: Bitte durchlesen
und auf mich zukommen,
glaube, wir haben
Handlungsbedarf.
Gruß Holger*

Wissen Sie wirklich, was sich
in Ihrem **Netzwerk** so tut?

Je mehr Internet, desto mehr Sicherheitsfallen

Das Internet ist heute ein unverzichtbares Werkzeug zur Kostensenkung und Effizienzsteigerung. Laut der Studie „Internet- und e-business-Einsatz im bundesdeutschen Mittelstand 2002“ von IBM und „impulse“ machen bereits 40 Prozent der Mittelständler im Internet erfolgreich Geschäft, bei 84 Prozent arbeitet E-Business innerhalb von 24 Monaten bereits profitabel.

Allerlei Gefahren von außen und innen

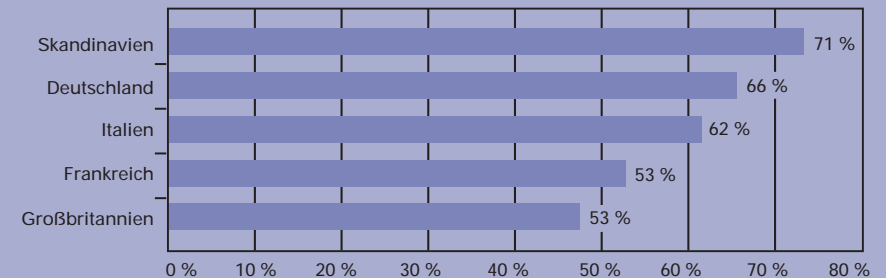
Dennoch sind viele dieser Unternehmen der Meinung, dass umfassende Sicherheitsmaßnahmen vor allem für Großunternehmen gelten. Dabei werden seriösen Studien zufolge 2003 die Hälfte aller mittelständischen Unternehmen mit erfolgreichen Attacken aus dem Internet konfrontiert.

Sicherheitsverletzungen können in vielfältiger Form auftreten von Virus-, Würmer- und Plattformlöcher-Attacken bis hin zum unerlaubten Zugriff auf vertrauliche Informationen (auch durch illoyale Mitarbeiter) und Denial-of-Service-Angriffen, die das Ziel haben, den Rechner zum Absturz zu bringen oder vom Netz zu trennen. Gemischte Sicherheits- und Integritätsbedrohungen wie der Nomad-, Goner- und Nimda-Virus werden von einzelnen Sicherheitsvorkehrungen gar nicht erst erkannt. Mittelständische Unternehmen sollten deshalb auf jeden Fall über Einzellösungen hinausgehen und durchgängige Sicherheitsebenen realisieren.

*Sind wir da auf der sicheren Seite oder wie läuft das bei uns?
Stichwort:
Zugang zum Logistik-Center
unseres Neukunden!!!!*

Sicherheit – Investitionen oder Unkosten?

Für den Erfolg und die Wettbewerbsfähigkeit ist ein sicheres technologisches Umfeld ohnehin ein Muss. Zudem erwirtschaften Sicherheitslösungen eine teils hohe und unmittelbare Investitionsrendite. Laut IDC (Infrastrukturumfrage 2002) fällt diese bei 23 Prozent der befragten Unternehmen deutlich höher aus als erwartet.



Quelle IDC 2002: Investitionsrendite aus Sicherheitsinvestitionen (Prozent Investitionsrenditen, die höher ausfielen als erwartet)

Background-Information

Sicherheitsebenen

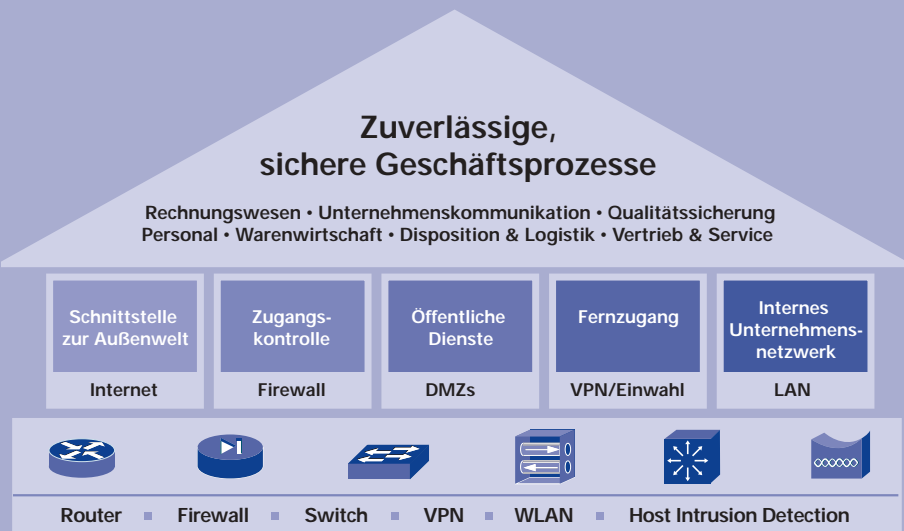
- Antivirenschutz für Desktop, Server und Gateway
- Content-Filtering für Internet und E-Mail
- Schwachstellenmanagement
- Intrusion Detection
- Firewalls
- Identity Management mit Benutzererkennung, Autorisierung, Beschaffungsmanagement der Nutzerdaten
- Intelligentes Netzwerkmanagement



Check doch mal unter www.cisco.de/mittelstandspartner, welcher Cisco Partner uns da helfen könnte.

Je mehr Sicherheitsfallen, umso wichtiger eine **lückenlose** Netzwerkstrategie

Ein durchgängiges, zuverlässiges und skalierbares Netzwerkfundament ist die beste Prävention vor Angriffen aller Art und damit der beste Schutz vor unkalkulierbaren Schäden. Cisco Systems liefert dazu einen wertvollen Beitrag: Produkte und Technologielösungen, mit denen Sie Ihr Netzwerk sicher und stabil auf- und ausbauen können. Das gesamte Portfolio basiert auf einer einheitlichen Technologie, so dass Sie jetzt und in Zukunft Ihr Netzwerk beliebig erweitern können – ohne teuren Wechsel auf andere Technologien und ohne Fehlinvestitionen.



Aktuelles Thema im Mittelstand: **Unternehmenssicherheit**

Cisco Security Produktportfolio

1. Internet

Zugangsroutern bilden die Schnittstelle zur Außenwelt, limitieren die Zugriffe und sind damit die erste Sicherheitsinstanz. Cisco Router integrieren höchste Sicherheitsvorkehrungen und bieten optional auch eine SW-Firewall.

2. Firewall

Firewalls kontrollieren den Datenverkehr und verhindern den unbefugten Zugriff. Sie trennen Bereiche mit verschiedenen Sicherheitsstufen innerhalb des Netzwerks.

3. DMZs

Die demilitarisierte Zone trennt das Unternehmensnetzwerk (LAN) vom Internet und sorgt für einen zusätzlichen Sicherheitsbereich. Die DMZ beinhaltet alle öffentlichen Dienste, die von außen erreichbar sein müssen (z. B. E-Mail, Webseite, Online-Bestellung usw.) und wird durch die Firewall geschützt.

4. VPN/Einwahl

Mobile Mitarbeiter oder Niederlassungen benötigen den sicheren Zugang zum Unternehmensnetz via Standleitung, ISDN oder DSL. Sichere Site-to-Site VPNs werden idealerweise mit VPN-optimierten Routern aufgebaut wie z. B. der Cisco 2600XM Serie. Der Cisco VPN Concentrator 3005 ist die VPN-Lösung für den Fernzugang.

5. LAN

Um Angriffe auch von innen zu verhindern, müssen Switches auch gesichert sein. Authentifizierungsmechanismen auf Benutzerbasis sorgen für die Datensicherheit. Im Bereich Security Monitoring liefert Cisco das Secure IDS, ein Werkzeug, das Netzwerkgefährdungen aufspürt.

Background-Information

Sicherheitsebenen

Sicherheitsrichtlinien oder Security Policies sind die Basis für das Sicherheitskonzept eines Unternehmens. Sie definieren das Sicherheitsniveau, Maßnahmen und Verantwortlichkeiten. Eine Security Policy beinhaltet Gesetze, Regeln und Verfahrensanweisungen für den Schutz der IT-Systeme sowie weiterer Ressourcen eines Unternehmens. Hier wird der Gebrauch von Daten und Informationen reglementiert, das heißt, die Verarbeitung, Speicherung, Verteilung und Präsentation. Sicherheitsrichtlinien sind Bestandteil der Sicherheitsarchitektur und werden mit Hilfe so genannter Security Services umgesetzt.

Alles rund um IT-Sicherheit unter cisco.de/security9:

WIRKSAME IT-SICHERHEITSSTRATEGIEN ■ ONLINE-SICHERHEITSCHECK ■ SICHERHEITSTIPPS ■ LÜCKENLOSE SICHERHEITSARCHITEKTUR ■ ONLINE-SEMINAR

Geh doch mal unter cisco.de/security9 und mach diesen Sicherheitscheck, damit wir mal kritisch unsere Situation beleuchten.

Je wichtiger das Netzwerk, umso klarer der Fall für Cisco SAFE

Cisco SAFE (Security Architecture for Enterprises) ist die Sicherheitsarchitektur für Unternehmensnetzwerke, die lückenlos alle Sicherheitsaspekte abdeckt. Die flexible Komplettlösung kann – je nach Unternehmensgröße und Anforderung – beliebig skaliert und erweitert werden, und ist damit die zuverlässige Plattform für Investitionsschutz und Wachstum.

Bestandteile von Cisco SAFE sind die sicheren Systemkomponenten von Cisco wie Firewall, Router, Switches sowie eine Reihe integrierter Module für die aktive Abwehr und das intelligente Netzwerkmanagement.

Cisco Secure Intrusion Detection System

Cisco Secure IDS ist ein netzwerkbasierendes Expertensystem zur Aufdeckung und Abwehr von Einbruchsversuchen. Es erfasst und beendet unautorisierte Aktivitäten.

Cisco Secure Access Control Server

Cisco Secure ACS für Windows NT erlaubt die zentrale Authentifizierung, Autorisierung und das Accounting von Access-Servern, VPNs und Firewalls, Voice-over-IP-Lösungen. Integriert sind die vom Standard IEEE 802.1x abgeleiteten Erweiterungen für die Schlüsselverwaltung und Zugriffskontrolle für drahtlose Netzwerke der Cisco AIRONET-Serie sowie das Management von Benutzerauthentifizierungen an Cisco LAN-Switches.

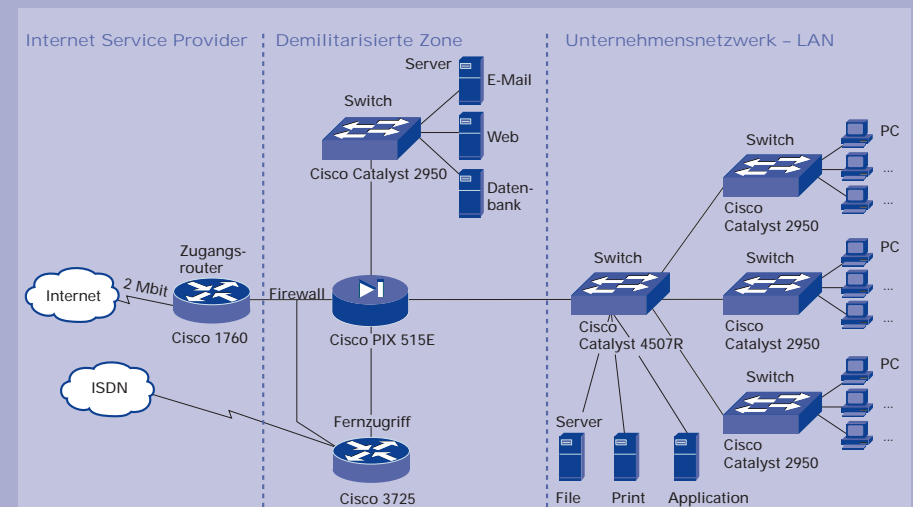
Background-Information

Host IDS (HIDS)

Bei Host IDS werden auf jedem Host Agenten installiert. Diese prüfen Event Logs, kritische System-Daten, unautorisierte Zugriffe oder suspekten Daten und schlagen Alarm. Zum Beispiel kann ein HIDS die Login-Zugriffe überwachen und falsche Passwort-Eingaben aufzeichnen. Oder es kann den Status eines Systems und der Daten überwachen, zumeist über einen Snapshot-Mechanismus. Will ein Angreifer Veränderungen im System erreichen, löst das HIDS Alarm aus.

Cisco Secure Policy Manager

Der Cisco Secure PM ist ein skalierbares, umfassendes Sicherheitsmanagementsystem für Cisco SAFE Systemkomponenten. Es erlaubt die zentrale Definition, Verteilung, Durchsetzung und Überprüfung von Sicherheitsrichtlinien.



Beispiel einer Cisco SAFE Gesamtlösung

Hier wird die PIX515 verwendet, eine dedizierte Firewall mit hoher Bandbreite. Die Einwahl und VPN-Lösung wird durch den Router Cisco 3725 gelöst. Er bietet hohe Leistung und Flexibilität, um auch zukünftige Erweiterungen abzudecken. Der Cisco 1760 wird vom ISP als Leitungsabschluss installiert. Das LAN besteht aus dem Cisco Catalyst 4507R als Backbone-Switch, an dem alle Etagenverteiler und Server angeschlossen sind. Auf den Etagen werden Cisco Catalyst 2950-24T eingesetzt. Dieses Design erlaubt sowohl hohe Leistung und Ausfallsicherheit durch redundante Anbindungen der Switches über Gigabit als auch Erweiterungsmöglichkeiten und ein ausgezeichnetes Preis-/Leistungsverhältnis.