



Die Security-Policy als strategischer Unternehmensfaktor

* Pascal Schoch

Der Einbezug des Internets in die Unternehmenslandschaft wird in den nächsten Jahren immer zentraler und gleichzeitig auch komplexer und anspruchsvoller. Die Konzeption und Umsetzung einer Security-Policy wird

gerade in einem unübersichtlichen und vernetzten Umfeld zum strategischen Unternehmensfaktor, der den wirtschaftlichen Erfolg wesentlich beeinflusst.

Als Grundlage für alle Überlegungen zum Thema IT-Security muss gelten, dass es a priori keine Unternehmung gibt – und seien ihre Sicherheitsmassnahmen noch so gut konzipiert –, die gegen Hackerangriffe immun ist. Ebenso gibt es keine Firewall, die eine hundertprozentige Sicherheit garantiert. Denn mit der zunehmenden Vernetzung von Unternehmensnetzwerken mit dem öffentlichen Internet ist die Gefahr von Missbrauch und Hackerattacken exponentiell gestiegen.

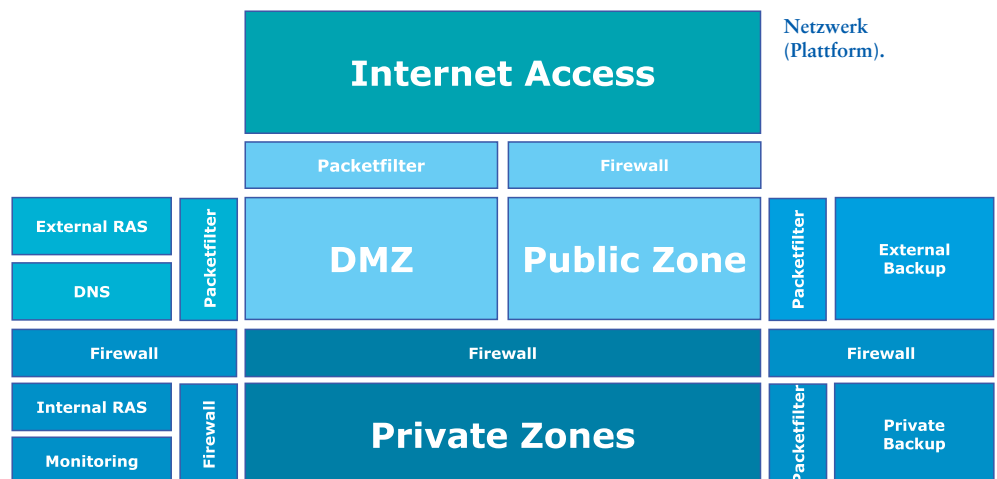
Trotzdem sind sich auch heute noch viele Unternehmen dieser Risiken nicht bewusst.

Waren in der Vergangenheit Telefon und Fax die Hauptkommunikationsmittel der Unternehmen, hat mittlerweile das E-Mail die Leitfunktion als neues Kommunikationsmittel übernommen. Das Internet nimmt sowohl im sozialen als auch wirtschaftlichen Bereich bereits eine zentrale Stellung ein. Mit der steigenden Verbreitung dieser netzgestützten Anwendungen steigt jedoch auch die Gefahr des Missbrauchs. So ist die Anzahl der Hackerattacken und Virenangriffe

in den letzten Jahren massiv gestiegen: Wurden im Jahre 1988 dem Koordinationszentrum für Internet-Sicherheit "Computer Emergency Response Team" (CERT), einer staatlich unterstützten Forschungsstätte der Carnegie Mellon Universität in Pittsburgh USA, ganze sechs Sicherheitsvorfälle gemeldet, zählte das CERT im Jahre 2001 beachtliche 52 658 Security-Incidents. Die Gefahr, dass vertrauliche Geschäftsdaten oder Kundeninformationen

von Hackern gestohlen oder zerstört werden, hat damit explosionsartig zugenommen. Durch das illegale Ausspionieren, Manipulieren oder Zerstören von Daten entstehen jährlich Schäden in Milliardenhöhe.

Unter diesem Gesichtspunkt ist es offensichtlich, dass dem Sicherheitsaspekt gerade im Bereich Informatik und Internet in besonders hohem Masse Aufmerksamkeit geschenkt werden muss. Der Schaden, der bei-





spielsweise einer Bank entstünde, wenn ihre Kundendaten von einem Hacker gestohlen und publiziert würden, könnte unter Umständen zur Schliessung der Bank führen. Aber auch eine kleinere Handelsfirma mit weniger sensiblen Daten sollte sich über mögliche Sicherheitsrisiken klar sein.

Bedrohungen

Jede Privatperson, die sich ins Internet einwählt oder auch nur ihre Mailbox bei einem Provider leert, setzt sich Risiken aus. Dasselbe gilt für jedes Unternehmen, welches eine Verbindung der internen Informatiksysteme mit dem Internet unterhält. Die Schnittstelle zwischen dem heimischen PC, beziehungsweise dem Unternehmensnetz und dem Internet ist ein Einfallstor für ungebetene Gäste. Zwar können ausgefeilte mehrstufige Firewall-Systeme die ankommenden Daten nach vorgegebenen Kriterien filtern. Eine absolute Sicherheit ist damit jedoch nicht gegeben: Der stetigen technischen Weiterentwicklung folgend, müssen die Sicherheitssysteme permanent angepasst und erweitert werden. Veraltete Firewalls bieten gegen aussen keinen Schutz.

Gefahr droht aber auch von innen. Die Möglichkeit, dass Mitarbeitende gegen die Interessen des Arbeitgebers tätig werden oder dass Programme und Applets mit Schadenfunktion einen Einbruch in das lokale Netz von innen her vorbereiten, darf ebenfalls nicht ausser Acht gelassen werden.

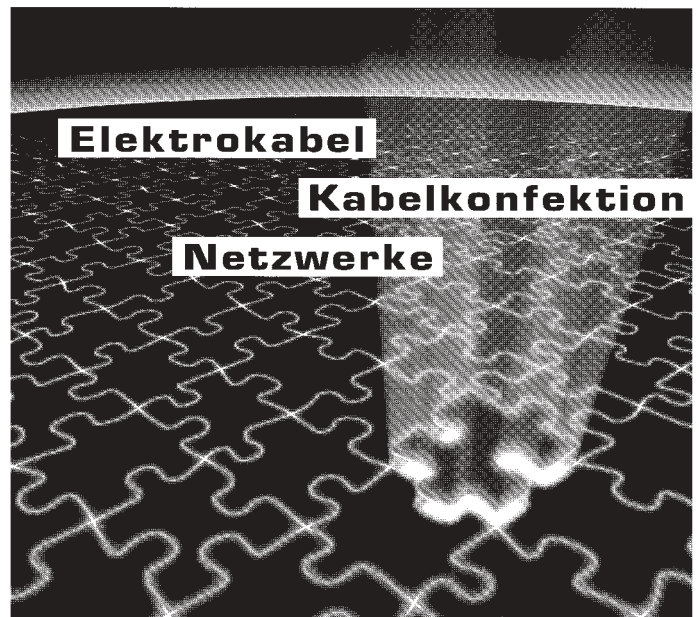
Die Security-Policy

Sicherheit ist ein Prozess, nicht ein Produkt. Oberstes Ziel dieses Pro-

zesses muss die Sicherung von Vertraulichkeit, Integrität und Verfügbarkeit sein. Technische Einrichtungen und Massnahmen unterstützen und begleiten diesen Prozess. Für sich alleine sind Sicherheitsmassnahmen jedoch noch kein Garant für Sicherheit. Die Begriffe "Sicherheit" und "Firewall" sind deshalb explizit nicht als Synonyme zu verstehen. Einem verlässlichen Sicherheitskonzept muss ein umfassenderes Sicherheitsverständnis zugrunde liegen.

IT-Sicherheit, verstanden als Prozess, ist demnach eine Methode, um den autorisierten Zugriff auf Ressourcen (Applikationen, Datenbanken, Webseiten, FTP-Server oder zentrale Computer-Systeme) zu erlauben. Eine solche Policy ist ein dokumentierter Plan für den unternehmensweiten Schutz der Infor-

matik-Umgebung. In allen ihren Vorgaben beschreibt dieses Sicherheitsdokument den Konsens der Firmenleitung bezüglich IT-Sicherheit. Die Policy liefert ein Rahmenwerk, um spezifische Entscheide zu treffen, und legt fest, wann welcher Abwehr-Mechanismus zu wählen ist. Die Security-Policy regelt auch, wie sich Benutzer, Administratoren und Software-Entwickler hinsichtlich der Sicherheit zu verhalten haben. Darüber hinaus definiert die Policy, in welchen Bereichen weitergehende Sicherheitsprozesse zu etablieren sind, um eine sichere Arbeitsumgebung zu schaffen. In die Security-Policy integrierte Massnahmenkataloge mit Verantwortlichkeiten und Umsetzungsterminen stellen sicher, dass die theoretischen Überlegungen in der Praxis angewandt werden.

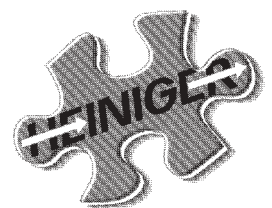


A. Heiniger & Cie. AG
Sagestrasse 65, CH-3098 Koniz

Bereich Kabel Tel. 031 970 55 70 Fax 031 970 55 79	Bereich Netzwerke Tel. 031 970 55 50 Fax 031 970 55 59
Bereich Konfektionen Tel. 031 970 55 30 Fax 031 970 55 39	

A. Heiniger & Cie. AG
Sumpfstrasse 22, CH-6312 Steinhausen

Bereich Konfektionen
Tel. 041 749 16 55 Fax 041 741 29 01



Qualität verbindet.

Internet: www.heiniger-ag.ch
e-mail: heiniger@heiniger-ag.ch

Ohne Security-Policy entbehrt ein Unternehmen der Grundsätze, die bei der Implementierung von neuen Systemen und Sicherheitsmassnahmen herangezogen werden können. Der Aufbau und die Pflege der Security-Policy verdienen deshalb oberste Priorität und müssen in einer Unternehmung fest verankert sein.

Bestandteil einer Security-Policy

In der Praxis gehören folgende Bereiche und Abläufe in einer Security-Policy detailliert behandelt und geregelt:

- Zugangskontrollen zu Gebäuden, Server-Räumen, Verteilerschränken etc.
 - Zugriffsschutz für Systeme und Ressourcen (IDS, Firewall, etc.)
 - Sicherheitsrichtlinien für interne und externe Software- oder System-Entwickler
 - Konfigurationsmanagement
 - Patch- und Release-Management
 - Einrichtung von Benutzer-Accounts (Remote Access Policy, inklusive Regeln für die Wahl von Passwörtern)
 - Definition und Pflichten des Informations-eigentümers
 - Datensicherung und Lagerung von vertraulichen Daten (inklusive Disaster-Recovery-Verfahren)
 - Periodische Log-File-Analyse und entsprechendes Incident Handling
 - Planung und Ablauf von Schwachstellenanalysen und Revisionen
 - Schulungsmassnahmen für Mitarbeiter
 - Regelungen im Umgang mit Verstössen gegen die Richtlinien
- Für die sinnvolle Konzeption einer unternehmenseigenen, individualisierten Security-Policy müssen

IT Security Audit

Jährliche, dem CERT gemeldete Security-Vorfälle.

Bestandesaufnahme

Schützenswerte
Ressourcen
Applikationen
Netzwerktopologie
Schutzmassnahmen

Bedrohungsanalyse

Intern (90%)
Menschliche Fehler
Betriebssysteme
Netzwerke
Applikationen
Transaktionen
Passwörter

Extern (10%)
Hacker / Cracker
Wettbewerb
Spionage / Sabotage
Viren / Trojaner
Service Provider
Partnernetze

die festgehaltenen Regeln und Vorschriften implementierbar, durchsetzbar und allgemeinverständlich formuliert sein. Auch muss eine Abwägung der Sicherheit gegenüber der Produktivität erfolgen. Eine regelmässige Erneuerung und Überarbeitung der Security-Policy garantieren einen aktuellen Sicherheitsstandard.

Sicherheits-technologien

Es existieren für Unternehmen die verschiedensten Technologien und Werkzeuge, um ihre Systeme und Informationen vor Schaden zu bewahren. Diese Tech-

nologien schützen gegen Angriffe, entdecken unübliche oder verdächtige Aktivitäten und reagieren automatisch auf Sicherheitsvorfälle. Grundsätzlich kann zwischen operationeller Technologie einerseits

und Verschlüsselungstechnologie auf der anderen Seite unterschieden werden. Der Hauptzweck der operationellen Technologie liegt in der Wartung und Sicherstellung der Verfügbarkeit von Ressourcen wie Daten oder Applikationen. Die Verschlüsselungstechnologie dient der Sicherung von Vertraulichkeit und Integrität

von Datenressourcen.

One-Time-Passwörter

Eindringlinge installieren so genannte Sniffer-Tools, die unbemerkt Passwörter abfangen, wenn diese über das Netzwerk gesendet

werden. Die Passwörter werden dann automatisch an nicht-autorisierte Drittpersonen weitergeleitet. Sämtliche Passwörter sollten deshalb vor einem allfälligen Versand verschlüsselt werden. Noch sicherer sind One-Time-Passwörter, wie sie bereits von Banken für das Online-Banking an ihre Kunden abgegeben werden. Wie bei der Frage nach der Systemperformance, ist auch bei der Anwendung von One-Time-Passwörtern vorgängig abzuschätzen, wie weit es den Benutzern zumutbar ist, komplizierte Einwahlprozeduren zu durchlaufen.

Firewalls

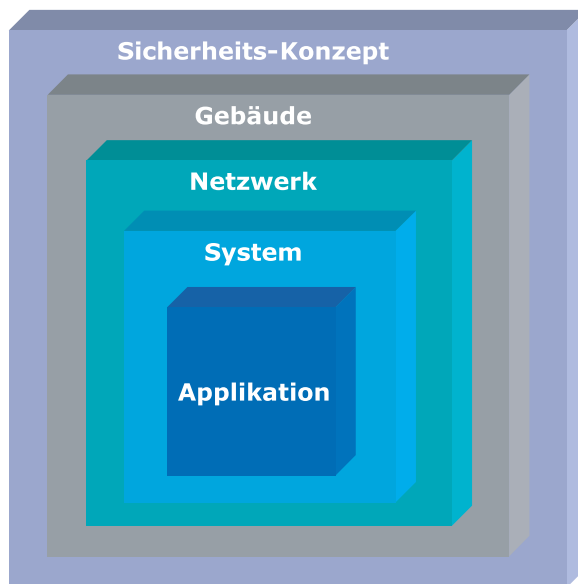
Um Zugang zu einem geschützten Bereich zu erhalten, kann eine normale Verbindungsaufnahme zwischen autorisierten Systemen vorge-täuscht und missbraucht werden. Da Firewalls die erste Abwehrlinie bilden, muss ihre Konfiguration besonders sorgfältig erfolgen.

Monitoring Tools

Um den Sicherheitsstandard auf hohem Niveau halten zu können, bedarf es einer ständigen Überwachung des Netzwerkes und der Systeme. So genannte Monitoring Tools, welche permanent Informationen über das gesamte System sammeln und überprüfen, erledigen diese Aufgabe.

Auf einer noch höheren Komplexitätsstufe finden sich die so genannten "Intrusion Detection Systeme" (IDS). Diese Systeme kombinieren verschiedene bereits genannte Werkzeuge und bilden somit ein umfassendes, komplexes Abwehrsystem. Hauptaufgabe von IDS ist die Überwachung ganzer Netzwerke und Systeme, meist kombiniert mit automatisierter Alarmierung und Auslösung von ersten Abwehrmechanismen.

IDS arbeiten auf zwei Funktionsebenen: Sie entdecken abnormale Vorgänge oder erkennen bestimmte Musterabläufe (Patterns). Ein IDS kann nicht als einmalige Massnahme implementiert werden, sondern muss permanent gewartet und aktualisiert sein.



Das Sicherheits-konzept.

Datensicherung und Aufbewahrung

Für ein Unternehmen kann es geschäftskritisch sein, im Falle eines Angriffes oder eines Schadenfalls innert kürzester Zeit wieder auf die Originale der manipulierten oder zerstörten Ressourcen zurückgreifen zu können. Diverse Datensicherungs-Praktiken stehen dazu zur Verfügung, angefangen beim lokalen Backup-Tape bis hin zum zentralen Backup-System mit eigenem Netzwerk. Auch wenn die Datensicherung kein aktiver Schutz gegen Angriffe ist, kommt ihr gerade für das Recovery eine zentrale Rolle zu und muss darum unbedingt in die Planung und den Aufbau einer Security-Umgebung integriert werden.

Verschlüsselung

Ein Hauptgrund für den Erfolg von Hackerangriffen ist der unkomplizierte Einblick in den Datenverkehr einer Unternehmung. Bedenkt man, wie viele Millionen von elektronischen Nachrichten pro Tag unverschlüsselt über das Internet versendet werden, ist es nachvollziehbar, wie einfach ein Hacker an vertrauliche Daten gelangen kann.

Verschlüsselung sichert Informationen, indem sie ihre Vertraulichkeit schützt. Auch der E-Mail-Verkehr lässt sich ebenfalls verschlüsseln. Eine der populärsten Verschlüsselungssoftwares für E-Mails ist "Pretty Good Privacy" (PGP), welche im Internet zum Download angeboten wird.

Outsourcing der Sicherheit

Durch die steigenden Anforderungen an Security-Systeme kann davon ausgegangen werden, dass auch die zur Erfüllung der Security-Bedürfnisse benötigten Ressourcen weiter steigen werden. IT-Manager sehen sich damit in der unangenehmen Situation, verringerte Budgets

Ziele und Inhalt der Security-Policy

Für einen wirkungsvollen Einsatz muss eine Security-Policy die folgenden Vorgaben erfüllen und über die hier aufgeführten Komponenten verfügen:

- Sie enthält alle Sicherheitsanforderungen an die IT-Infrastruktur
- Sie umfasst eine detaillierte Beschreibung aller implementierten Sicherheitsmassnahmen
- Sie liefert die Begründung für den Einsatz der gewählten Sicherheitsmassnahmen (beispielsweise durch den Verweis)
- Sie beschreibt den korrekten Umgang mit den Sicherheitsmassnahmen
- Sie dient als Basis zur Ableitung der rechtlichen Verpflichtungen zwischen den beteiligten Partnern in einer IT-Infrastruktur
- Sie erleichtert die Identifizierung von zusätzlichen Sicherheitsmassnahmen und die Einhaltung von Sicherheitsstandards
- Sie ist ein Instrument zur periodischen Prüfung des Sicherheitsniveaus einer Unternehmung.

mit steigenden IT-Sicherheitsrisiken in Einklang zu bringen. Dieser Hintergrund führt dazu, dass intensiv nach Alternativen Ausschau gehalten wird.

Bei der Realisierung einer Outsourcing-Lösung im IT-Sicherheitsbereich wird mit einem Dienstleister ein Aufgabenkatalog definiert. Die Bandbreite der auszulagernden Tätigkeiten reicht dabei vom Netzwerk-Design und dem Installations-support bis zum umfassenden und unternehmensweiten Security-Management.

Dem Umfang und der Komplexität der Aufgaben entsprechend, kann es sich bei den Outsourcing-Anbietern um kleinere Softwarehändler handeln, die beispielsweise Antiviren-Software beim Kunden installieren und in regelmässigen Abständen warten. Auf der anderen Seite der Skala finden sich die so genannten Managed Service Provi-



IBM Learning Services



IBM Learning Services – Education for IT-Security

Eine nachhaltige Ausbildung und professionelle Beratung können wirksame Unterstützung bieten, um Risiken und Gefahren für unternehmenseigene Datenbestände zu verringern. IBM Learning Services ist ausgewiesener Experte in den Bereichen Ausbildung und Beratung.

Hier eine Auswahl von Kursen zum Thema:

Networking

Internet and Security (IS010ACH)

Managing Cisco Network Security (2NMCNAIC)

Cisco Secure PIX Firewall Advanced (CSPA0ACH)

Microsoft Windows

Designing a Secure MS Windows 2000

Network (2M215OIC)

Deploying and Managing MS Internet Security

and Acceleration Server 2000 (MS2159CH)

AIX/Linux

Linux as a Firewall (LX240AIC)

iSeries AS400

iSeries Sichern und wiederherstellen (2FS36AIC)

iSeries Arbeiten mit BRMS/400 (2FS39BIC)

iSeries System-Sicherheit (2FG40AIC)

iSeries Netzwerk-Sicherheit (2FG42ACH)

OS/390 zSeries

RACF Grundlagen (2EH95BIC)

Implementing and Using LDAP (ES650ACH)

Tivoli

Tivoli Disaster Recovery Manager (2AT171K)

Tivoli Data Protection für R/3 (2AT13K)

Tivoli Data Protection für Oracle (2AT14K)

Weitere Informationen, Kursdaten und Anmeldung:

ibm.com/services/learning/ch

Tel. 0844 80 32 32, education@ch.ibm.com

generation @ business



IT-Kurse zum 1/2-Preis:

Swiss EducationCard!

Mehr dazu unter:

ibm.com/services/learning/ch

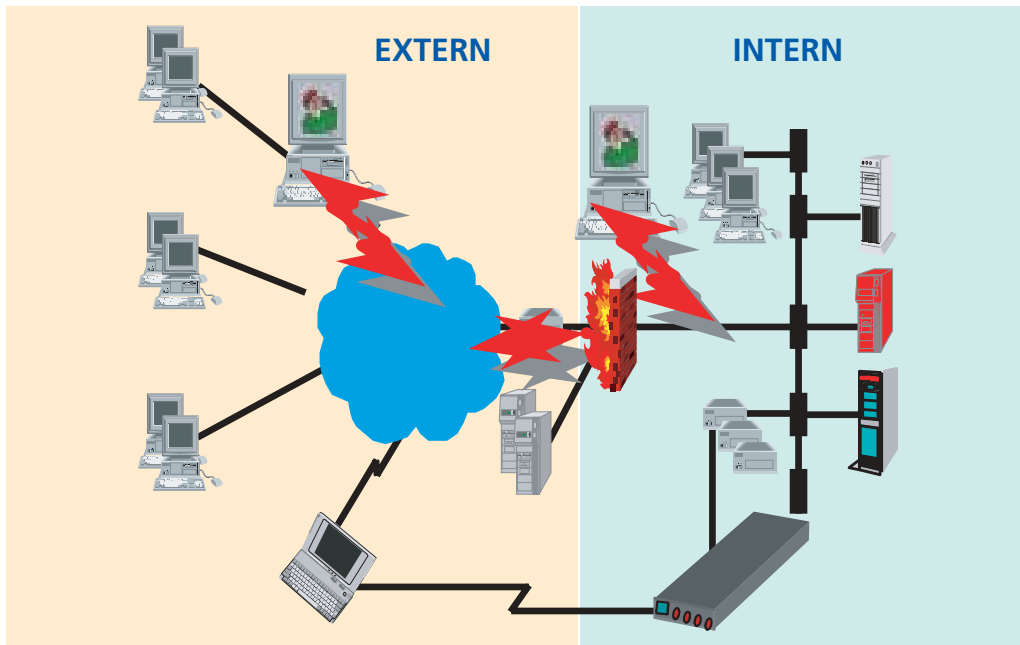
der, die sich auf das vollumfängliche Security-Management von ganzen Netzwerken und Systemen konzentrieren.

Die Faktoren, die einen Entscheid für oder gegen das Security-Outsourcing beeinflussen, sind das vorhandene Budget, der gegenwärtige Stand des Sicherheitsrisikos, das abrufbare unternehmensinterne Sicherheitswissen sowie verfügbare Kapazitäten von kompetenten Mitarbeitern (Ressourcen).

Aus der Sicht eines Unternehmens ermöglichen Security-Outsourcer den kostengünstigen Zugriff auf Best-of-Breed-Security-Lösungen. Gleichzeitig werden die anfallenden Implementierungskosten im Vergleich zu einer eigenen, internen Lösung drastisch reduziert.

Security-Aufbau

Der Aufbau und Roll-out einer Inhouse-Lösung kann ein langwieriger Prozess sein. Die Berücksichtigung eines externen Dienstleisters verkürzt diesen Prozess, da auf bewährte und bekannte Abläufe und Techniken zurückgegriffen werden kann. Abzuklären ist zudem, wie sicher bzw. hackeranfällig die Unternehmenssysteme



Bedrohungsanalyse.
Intern (90%): menschliche Fehler, Betriebssysteme, Netzwerke, Applikationen, Transaktionen, Passwörter.
Extern (10%): Hacker / Cracker, Wettbewerb, Spionage / Sabotage, Viren / Trojaner, Service Provider, Partnernetze.

während der Security-Implementierungsphase sind, vor allem dann, wenn sich der Projektablauf über mehrere Monate hinzieht. Auch hier kann die beschleunigte Projektabwicklung durch einen externen Dienstleister von Vorteil sein.

Wahl des geeigneten Security Service Providers

Hat sich ein Unternehmen für ein Security-Outsourcing entschieden, sollten bei der Wahl des externen Service-Providers folgende Punkte in der Evaluation berücksichtigt werden:

- Erfahrung und Reputation des Dienstleisters – Gute Anhaltspunkte betreffend die Erfahrung und die Reputation eines Dienstleisters sind dessen Kernkompetenzen (Netzwerkbereich oder System-Sicherheit): Wie lange ist der Anbieter schon in diesem Bereich tätig und welche Referenzen kann er vorweisen?
- Angebotene Produkte und Dienstleistungen – Wichtig ist die Abklärung, ob ein Dienstleister Lösungen von verschiedenen Herstellern anbietet, ob er sich auf einen einzigen Hersteller verlässt oder ob er eigene Lösungen entwickelt und verkauft. Alle Varianten haben ihre Vorteile: Eine Berücksichtigung von verschiedenen Herstellern lässt darauf schließen, dass der Provider die besten

Lösungen anbieten will und sich nicht lediglich auf den Produktverkauf eines einzigen Herstellers konzentriert. Ausserdem kann bei der Offerierung von verschiedenen Plattformen davon ausgegangen werden, dass der Provider einen guten Überblick über die verfügbaren Sicherheitstechnologien und -anbieter besitzt und den Kunden daher in der Auswahl der passenden Komponenten gut beraten kann. Das Angebot von selbst entwickelten Lösungen wiederum lässt auf profunde Fachkenntnisse schliessen. Finden sich nur Lösungen eines Zulieferers im Portfolio des Dienstleisters, werden sich die Schnittstellenprobleme zwischen den einzelnen Komponenten in Grenzen halten. Diese verschiedenen Vorteile sind je nach Projekt gegeneinander abzuwägen.

* Pascal Schoch war nach seinem Betriebswirtschaftsstudium als Product Manager im Bereich Electronic Commerce Solutions bei Swisscom tätig. Seit dem Sommer 2000 ist er als Product Manager bei Aspectra für die Bereiche Dedicated Hosting und Application Hosting verantwortlich.
 E-Mail: pascal.schoch@aspectra.ch

IT-Sicherheit



Dieser Bericht ist eine Kurzfassung eines Whitepapers, welches von Pascal Schoch verfasst und von der Aspectra AG herausgegeben wurde. Die Originalfassung kann über www.aspectra.ch bestellt werden.

Kontakt:

aspectra ag
 Zeughausstrasse 31
 Postfach 4013, 8021 Zürich
 Tel. 01 296 56 56
 Fax 01 296 56 57
www.aspectra.com