Professionelles Sicherheitsmanagement zahlt sich aus

Von Erol Längle,
Security Manager Getronics Schweiz,

und Peter Wolf,
Senior Business Consultant, Getronics Deutschland

Ohne Internet-Kommunikation kommt heute kein Unternehmen mehr aus. Die Öffnung der Unternehmensnetze birgt aber auch erhebliche Gefahren. Security Management gehört daher in die Hände von Profis. Die Autoren stellen die These auf, dass Managed Security Services (MSS) sicherer und kosteneffizienter sind als eigene Lösungen.

Die Sicherheit des Firmennetzwerks gehört zu den Top-Prioritäten der ICT-Chefs. Entsprechend stark wird investiert in Virenscanner, Firewalls, Systeme für Intrusion Detection und Prevention sowie andere Sicherheitseinrichtungen. Mit dem Ergebnis, dass die Security-Kosten rasant steigen und die Schäden trotzdem nicht abnehmen – im Gegenteil: Sie erreichten im vergangenen Jahr weltweit eine neue Rekordsumme von 65 Mia. US-Dollar (Quelle: RSA Security). Und das betrifft nur die publizierten Fälle von erfolgreichen Hackerangriffen: Die Werte, die zusätzlich durch gezielte Einbrüche in Unternehmensnetze (zwecks Diebstahl, Manipulation oder Vernichtung von Daten) zerstört wurden, lassen sich bloss erahnen.

Schwachstellen nehmen zu

Was kann man dagegen tun? Das sicherste Rezept wäre natürlich, das Unternehmen elektronisch von der Umwelt abzunabeln und nur noch auf herkömmliche Art zu kommunizieren: persönlich, per Telefon, Fax oder Post. Mit dem Resultat, dass die Firma nicht mehr konkurrenzfähig und damit dem Untergang geweiht wäre.
Wer heute als Unternehmen bestehen will, ist auf Vernetzung nach aussen angewiesen – und damit auch zu sorgfältigen Schutzmassnahmen gezwungen. Wobei man sich vom Gedanken verabschieden muss, dass man ein vollkommen sicheres Netzwerk einrichten kann. Dafür ist der Einfallsreichtum der wachsenden und heute auf weltweit 19 Millionen Köpfe geschätzten Hackergemeinde viel zu gross. Und deshalb hat die Zahl der ausgenützten Schwachstellen in den IT-Systemen laufend zugenommen und ist heute so hoch[1], dass die Hersteller und Anwender mit dem Schliessen der Löcher nicht mehr nachkommen.

Security-Administratoren sind überfordert

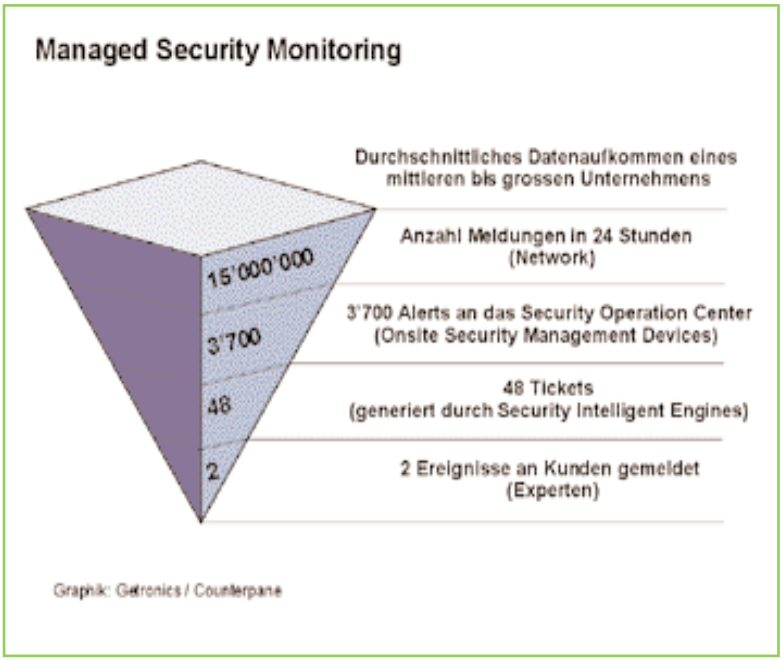
Technologie alleine kann also gar nicht alle Einbrüche verhindern. Das ist jedoch kein Grund zur Resignation: Security-Systeme erschweren zumindest elektronische Attacken und verschaffen damit Zeit zum Einleiten von Gegenmassnahmen – sofern der Angriff erkannt wird. Das alte Fliegersprichwort «Geschwindigkeit ist Sicherheit» gilt auch für Internet Security. Es ist erwiesen, dass nach der Erkennung einer typischen Attacke kaum mehr als 10 Minuten Zeit bleiben, um zu verhindern, dass diese grossen Schaden anrichten kann.
Und genau das bereitet den Unternehmen Kopfzerbrechen. Die heutigen Security Systeme erzeugen eine Flut von Alarmen, von denen aber ca.

INFO: MANAGED SECURITY SERVICES
DIE DIENSTLEISTUNG MANAGED SECURITY SERVICES (MSS) BESTEHT IM WESENTLICHEN AUS:

Managed Security Monitoring
Expertensystem-unterstützte Sammlung, Filterung, Korrelation und Echtzeit-Analyse der Log-Dateien und Messages von Firewalls, IDS-/IPS-Systemen, Server, Router und anderen ICT-Infrastruktur-Geräten sowie sofortige Einleitung von Gegenmassnahmen im Falle eines Angriffs.

Security Management
Configuration Management, Patch Management, Policy Management, IMACs (Installations, Moves, Adds, Changes), Installation von SW-Updates und Security Patches, SW-Konfiguration, Durchführung von Regeländerungen in Absprache mit dem Kunden.

Managed Vulnerability Assessment
Regelmässiger Scan der Netzwerkinfrastruktur, Identifikation der installierten Geräte, Erkennung der Schwachstellen, Empfehlungen für notwendige Security Patches.



80 Prozent keine sicherheitsrelevanten Ereignisse darstellen. Die Folge davon ist, dass die Security-Administratoren bei der Analyse der Meldungen hoffnungslos überfordert sind und diese verständlicherweise gar nicht mehr beachten.

Weiterhin ist in der Regel kein Personal für das – will man Security ernst nehmen – notwendige 24 x 7-Security-Monitoring vorhanden. Hierzu werden mindestens sechs gut ausgebildete Mitarbeiter benötigt. Zusammen mit der erforderlichen räumlichen und technischen Infrastruktur schätzen Fachleute die jährlichen Kosten auf mindestens 500 000 Schweizer Franken. Das ist für die meisten Unternehmen nicht tragbar.

MSS-Dienstleister bringen Transparenz in die ICT-Security

Abhilfe aus diesem Dilemma schaffen externe Security Management Services. Managed Security Service Provider sind in der Lage, diese aufwändige und technisch anspruchsvolle Aufgabe kosteneffizient und rund um die Uhr anzubieten. Dazu stehen die besten Remote-Monitoring- und Analyse-Systeme zur Verfügung sowie exzellent ausgebildete Security-Spezialisten, die stets auf dem neusten Wissensstand sind.

Service Provider wie Getronics bieten «24 x 7 Managed Security Monitoring» (MSM) an. Gemäss Marktbeobachtern wie Forrester Research betragen die Kosten dafür nur knapp ein Drittel eines vergleichbaren unternehmenseigenen Service. Mit anderen Worten: die externen Kosten für eine solche Sicherheits-Lösung sind rund 70 Prozent tiefer als die internen.

Weshalb, so fragt man sich, zögern denn so viele Unternehmen immer noch, ihr dringendes Sicherheitsproblem in gute Hände zu legen, oder geben sich mit einer teuren und meist weniger zuverlässigen Eigenlösung zufrieden? Das liegt insbesondere am weit verbreiteten Irrtum, mit einem externen Partner gehe die Kontrolle über die IT-Sicherheit verloren. Das ist etwa vergleichbar mit der Aussage, mit einem Outsourcing an einen Dienstleister wie die Securitas verliere man die Kontrolle über die physischen Zugänge zum Firmengelände. Dabei ist genau das Gegenteil der Fall: Ein guter MSS-Dienstleister bringt Transparenz in die ICT-Security, sowie ein besseres Informationsmanagement und Reporting, als dies die eigene IT-Abteilung liefern könnte.

Fazit

Auch wenn es keine absolute IT-Sicherheit gibt, so bieten Managed Security Services zumindest das Optimum des Machbaren. IT-Sicherheit ist und bleibt Sache von Experten, denn die Bedrohung nimmt ständig zu. Die Kosten für ein professionelles Security-Management sind zudem wesentlich günstiger als eine vergleichbare Inhouse-Lösung. Misst man den Aufwand gar an den möglichen Schäden, so lohnt sich die Sache erst recht.

---

[1] *Die Anzahl der neu entdeckten Sicherheitslücken hat massiv zugenommen: von 170 im Jahr 1995 auf 1090 im Jahr 2000 auf 3780 im vergangenen Jahr. Insgesamt wurden in diesem Zeitraum beinahe 13 000 Sicherheitslücken rapportiert. Diese betreffen nicht nur Microsoft-Produkte – auch Linux Software hat ihre Schwachstellen. Von Januar bis Oktober 2002 gingen gemäss dem Computer Emergency Response Team (CERT) 16 von 29 publizierten Lücken auf das Konto von Linux und nur 7 auf jenes von Microsoft.* ◆

MANAGED SECURITY MONITORING VON GETRONICS UND COUNTERPANE

Beispielhaft für hochklassiges Managed Security Monitoring sind die Dienste, die der globale ICT-Dienstleister Getronics zusammen mit dem amerikanischen MSM-Spezialisten Counterpane in über 130 Ländern anbietet, rund um die Uhr, an 365 Tagen im Jahr.

Getronics betreibt für Counterpane das europäische Security Operations Center. Die MSM-Lösung besteht aus dem so genannten «Sentry» Security Device, das ins Kundennetz installiert wird. Es sammelt, filtert, korreliert und analysiert Log-Daten und Nachrichten von Firewalls, Intrusion-Detection-Systemen, Servern, Routern und anderen Geräten und sendet Alarme ans «Socrates»-Expertensystem im Security Operations Center. Socrates checkt die empfangenen Muster mit einer über 34 Terabyte grossen Datenbank ab, die laufend mit den neusten sicherheitsrelevanten Informationen der Hersteller und Alert Services sowie allen auftretenden Vorfällen in den Kundennetzen aktualisiert wird. Die dabei ausgefilterten und als mögliche ernsthafte Angriffe erkannten Vorfälle werden automatisch an die Experten des Security Operations Center weitergeleitet. Falls ein ernst zu nehmender Angriff vorliegt, werden die Kunden innert zehn Minuten benachrichtigt.

Der MSM Service von Getronics und Counterpane unterstützt über 300 unterschiedliche Gerätetypen und bietet die Möglichkeit, zusätzliche Geräte schnell und ohne hohe Entwicklungskosten zu integrieren. Die Kosten sind transparent und kundenfreundlich: Fällig ist ein monatlicher Festpreis, der abhängt vom Gerätetyp, vom Service-Umfang und vom Service Level Agreement.

WEITERE INFORMATIONEN

Getronics (Deutschland) GmbH
Am Prime Parc 10-12
65479 Raunheim
Tel. 06142 925 214
www.getronics.de

LESERDIENST **126**