

## I. Einführung

Der Einsatz von Sicherheitssystemen wie Firewalls, Virenschutz-Gateways oder Intrusion Detection Systemen ist nichts Exotisches mehr. Entsprechend haben viele Organisationen die Anfangs-Euphorie hinter sich und kämpfen mit den täglichen Aufgaben beim Betrieb solcher Systeme. Wer zunächst glaubte, nur die Anschaffung einer Firewall wäre ein kostenintensives Vorhaben, der sieht sich heute mit einer Realität konfrontiert, in der die benötigten Software-Wartungsverträge sowie der Personalaufwand für die ständige Aktualisierung, Konfiguration, Fehlerbehebung oder auch nur die Überwachung die ursprünglichen Anschaffungskosten langsam aber stetig überholen.

Outsourcing ist kein neues Thema und so ist es nicht verwunderlich, dass sich auch im Sicherheitsbereich viele Anbieter bemühen, den Firmen diese Arbeiten gegen monatliche Bezahlung abzunehmen. In den Jahren 2000 und 2001, als die Technologie-Börsen noch euphorisch gestimmt waren, galten Anbieter von „Managed Security Services“ als lohnende Investitionen. Viele Sicherheitsfirmen investierten Millionen in den Aufbau von gesicherten Rechenzentren („Secure Operating Centers“, kurz SOC) von denen aus sie die Firewalls ihrer Kunden überwachen und betreiben wollten. Seit dem Einbruch der Technologie-Börsen sind viele dieser Anbieter wieder verschwunden oder haben ihre Outsourcing-Angebote eingestellt. Einige haben bis jetzt überlebt und der Kunde findet eine ganze Reihe von verschiedenen, mehr oder weniger überzeugenden Angeboten.

## II. Marktübersicht

Generell kann man die Angebote nach der Lage der Systeme und der Position des Personals unterscheiden. Die folgende Grafik soll die Unterschiede darstellen:

	<b>Equipment intern</b>	<b>Equipment extern</b>
<b>Personal intern</b>	<b>Interner Betrieb oder „Bodyleasing“</b>	<b>selten sinnvoll, evt. Hosting</b>
<b>Personal extern („Fernwartung“)</b>	<b>Firewalls/IDS Monitoring oder Management</b>	<b>Firewalls beim Provider, Scan oder Info-Service</b>

Im ursprünglichen Fall ohne externe Unterstützung stehen die Systeme im Rechenzentrum der Organisation selbst und sie werden von eigenem Personal betrieben. Gelegentlich kommt es vor, dass die Konfiguration und Pflege einzelner Systeme externem Personal übertragen wird, wobei diese Personen nicht über Remote Access auf die Systeme zugreifen, sondern dauerhaft beim Kunden vor Ort beschäftigt sind. Vom Kunden werden die externen Mitarbeiter oft wie eigene Mitarbeiter in interne Abläufe eingebunden. Der große Unterschied ist nur, dass die Mitarbeiter nicht beim Kunden, sondern bei einem externen Dienstleistungsunternehmen angestellt sind. In der Regel ist dieses Modell teurer, als eigene Mitarbeiter einzustellen. Falls entsprechend qualifizierte Personen jedoch nicht am Arbeitsmarkt zu haben sind, ihre Ausbildung zu teuer wäre oder innerbetriebliche Politik die Einstellung weiterer eigener Mitarbeiter verhindert, kommen derartige Modelle zum Tragen. Es gibt sicher noch weitere Argumente, die für oder gegen eine solche, landläufig

auch „Bodyleasing“ genannte Konstellation sprechen. Für die Betrachtung von Managed Security und Security Outsourcing ist sie jedoch nicht besonders interessant und wird daher im Folgenden nicht weiter behandelt.

Eine andere, weniger interessante Variante: Das Unternehmen stellt die Geräte zu einem externen Anbieter, lässt den Betrieb und die Konfiguration jedoch beim internen Personal. Der externe Anbieter übernimmt hier eigentlich nur den Anschluss an Strom und Netzwerk und die physikalische Zugangssicherung. Für IT-Sicherheitssysteme findet diese Variante nur selten Anwendung. Bei Webservern ist sie dagegen unter dem Namen Server Hosting oder Server Homing sehr verbreitet. Der Kunde profitiert dabei vor allem von einem kostengünstigen und gut ausgebauten Internet-Zugang des Anbieters.

Interessant für Sicherheitsanwendungen sind vor allem Modelle, bei denen qualifiziertes externes Personal von einem sicheren externen Rechenzentrum (SOC) aus Überwachungs- und Wartungsaufgaben für den Kunden übernimmt.

In diesem Segment findet man die meisten und vor allem die typischen Angebote wie „Managed-Firewall“ oder „Firewall-Monitoring“. Die Geräte selbst stehen dabei vorwiegend beim Kunden.

Beim „Firewall-Monitoring“ sind sowohl Personal als auch die Geräte bei einem externen Dienstleister zu finden. Ein typisches Beispiel ist ein „sicherer“ Internet-Anschluß, der schon beim Provider über eine Firewall und einen Virenschanner geht. Der Kunde nutzt damit eine zentrale Sicherheitsinfrastruktur des Providers gemeinsam mit anderen Kunden. Ähnlich verhält es sich bei externen Trustcentern, die digitale Zertifikate für Kunden ausstellen. Auch hier stehen die Geräte in einem sicheren Rechenzentrum des Anbieters und werden auch von ihm betrieben. Die Kunden bekommen nur das fertige Zertifikat zugestellt.

### III. Aufgaben beim Security-Outsourcing

Um die einzelnen Security-Outsourcing-Angebote bewerten zu können, ist es sinnvoll, sich zunächst einen realistischen Überblick über die tatsächlich anfallenden Aufgaben und ihre Verknüpfung mit den übrigen organisatorischen Abläufen zu verschaffen. Gelegentlich erscheint es auf den ersten Blick zwar plausibel, bestimmte Aufgaben einem externen Anbieter zu übergeben, bei genauerem Betrachten jedoch sind die Aufgaben mit so vielen internen Rollen und Abläufen verknüpft, dass eine externe Vergabe den intern anfallenden Aufwand nur noch vergrößert.

Bei der Gliederung der Aufgaben, die für Outsourcing in Frage kommen, findet man eine Reihe von offensichtlichen Punkten, die immer wieder angeboten werden. Diese Liste ist zwar nie vollständig, da die Kreativität der Anbieter sich nicht beschränken lässt, sie zeigt jedoch die wichtigsten Punkte:

#### • Externes Monitoring von Sicherheitssystemen beim Kunden

Beim Monitoring werden Zustände und Events von Geräten kontinuierlich überwacht und gegebenenfalls Reaktionen ausgelöst sowie bei Bedarf eskaliert. Je nach Art des überwachten Sicherheitssystems fallen primär Log-Informationen über den Zustand des Geräts oder Alarme an.

Die Angebote selbst variieren in der Betrachtung der Systeme. Einige fokussieren sich auf sicherheitsrelevante Informationen über Angriffe und entsprechende Alarme. Andere kontrollieren vor allem die Verfügbarkeit der Geräte.

Klassische Ausprägungen sind hier die externe Überwachung von Firewalls und von Intrusion Detection Systemen.

- **Externes Management von Sicherheitssystemen beim Kunden**

Im Gegensatz zum Monitoring steht beim Management mehr die Konfiguration der Systeme oder das Einspielen von neuen Software-Versionen im Vordergrund. Die Überwachung hinsichtlich sicherheitsrelevanter Vorgänge oder Ereignisse wie beim Monitoring ist je nach Anbieter enthalten oder nicht.

Die konkreten Angebote sind meist das Management von Routern, Firewalls, IDS und Virenschutz-Gateways.

- **Externer Betrieb von Sicherheitssystemen im SOC des Anbieters**

In diesem Fall stehen die Geräte beim Anbieter, der sich sowohl um die Verfügbarkeit und Software-Updates als auch um die Überwachung bezüglich potentieller Angriffe kümmern muss.

Typische Beispiele sind Kunden-Firewalls bei einem Internet-Provider oder externe Trustcenter.

- **Informationsservices über neue Verwundbarkeiten in bestimmten Produkten, neue Viren und neu bekannt gewordene Einbrüche**

Im Gegensatz zu verschiedenen kostenlosen Mailinglisten, die ähnliche Inhalte liefern können, nehmen die kommerziellen Services dem Kunden die Vor-Auswahl der relevanten Daten ab. Der Kunde bekommt meist einen oder mehrere Accounts, wo er seine Interessen bezogen auf Betriebssysteme, Produkte und Versionen online definieren kann. Danach bekommt er nur noch die Meldungen zugeschickt, die in sein Interessensgebiet fallen.

- **Dauerhafte Überprüfung der Kunden-Infrastruktur auf Schwachstellen**

In der Vergangenheit wurden solche Überprüfungen vor allem auf Projektbasis durchgeführt. Ein externer Dienstleister wurde beauftragt, die Sicherheit der extern sichtbaren Server eines Kunden zu testen und einen Bericht über mögliche Angriffspunkte zu erstellen. Neue Services erledigen dies automatisch und als „Managed Service“, der die Überprüfung jede Nacht oder automatisch bei jeder Änderung der Firewall-Policy durchführen kann. Für den Kunden wird es damit zu einem outsourcing-ähnlichen Geschäft, bei dem er eine feste Jahresgebühr zahlt und jeden Morgen den aktuellen Sicherheits-Zustand seiner externen Zugänge im Überblick bekommt.

Im nächsten Newsletter werden einige konkrete Angebote näher betrachtet und die Argumente für und gegen ihren Einsatz diskutiert.