HELPDESK

MSS: Darauf sollten Firmen achten

Jede Woche beantworten Sicherheitsexperten Leserfragen und geben Ratschläge, wie sich die Sicherheit in einem Unternehmen erhöhen lässt.

Frage: Unsere Firma prüft die Option, die Betreuung der Firewall und den Antivirenschutz outzusourcen. Ist das sinnvoll?

Die Frage kann nicht pauschal beantwortet werden, weil die Antwort von individuellen Sicherheitsanforderungen und weiteren Rahmenbedingungen abhängt. Der Ausdruck «Managed Security Services» (MSS) steht für das Outtasking des operativen Betriebs verschiedenartiger technischer oder organisatorischer Security Services. Antiviren- und Antispamschutz gehören mittlerweile zum Basisangebot vieler Internet Service Provider (ISP).

Spezialisierte «Managed Security Services Provider» (MSSP) bieten zusätzlich gemanagte Firewalls, VPNs, Intrusion Detection/Prevention Systeme, Patchmanagement-Services oder periodische Security Scans an. Die Dienstleistungen inkl. Reaktionszeiten und Vertragsmodalitäten werden in einem Service Level Agreement (SLA) definiert. Bei MSS ist je nach Angebot mit externen monatlichen Kosten von wenigen Franken bis zu mehreren Tausend Franken zu rechnen, wobei Umfang und Qualität der Leistung meist linear zum Preis ansteigen. MSS bieten folgende Vorteile: Die MSSP verfügen über ein Team von Sicherheitsspezialisten, welches die gemanagten Komponenten überwacht, pflegt und im Ernstfall (z. B. Hackerangriff oder digitales Ungeziefer) situationsgerecht agiert.

Weil die Teams mehrere Kunden gleichzeitig betreuen, werden die Kosten von allen Kunden gemeinsam getragen – was die auf den einzelnen Kunden anfallenden Kosten im Vergleich zum Unterhalt eines eigenen Security Teams (Aufwand ca. 6 Personen für einen 365x24 Std.-Betrieb) massiv senkt. Ausserdem ist der MSSP um die kontinuierliche Weiterbildung seiner Mitarbeiter besorgt – ein bekannter Kostentreiber im eigenen Unternehmen. Spezialisierte MSSP betreiben erstklassig ausgestattete, sichere Kontrollzentren und verfügen über eine weltweite Vernetzung mit Backbonebetreibern und Antivirenherstellern, was eine Art Frühwarnsystem bildet. Selbstredend hat eine derartige Servicequalität ihren Preis.

«Trotz allem bleibt die Verantwortung für das IT-Risk-Management immer beim Kunden.»

Folgende Aspekte dürfen bei MSS-Projekten nicht vernachlässigt werden: Die IT-Sicherheit der Kundenumgebung liegt teilweise oder ganz in den Händen des MSSPs. Dennoch bleibt der Kunde verantwortlich für das IT Risk Management – der MSSP ist nur ausführendes Organ. Durch die Auslagerung des operativen Betriebs der Sicherheitskomponenten entsteht zwangsläufig ein Know-how-Manko im eigenen Betrieb. Selbst der bestorganisierte MSSP kann fehlende Organisation beim Kunden nicht ausgleichen – dieser Irrtum führte schon zum Scheitern manches Outtasking-Projekts. Je komplexer die MSS sind, welche ein Kunde bezieht, und je grösser die Zeitspanne zwischen Outtasking und erneutem Intasking ist, desto aufwändiger und teurer wird die Rückkehr zum Eigenbetrieb.

Generelle Empfehlungen: Organisationen, deren Kerngeschäft eng mit der IT Security verknüpft ist, wird generell von MSS abgeraten. Firmen oder Filialen, welche keine eigene DMZ betreiben, sondern das Internet nur für E-Mail und Surfen benötigen, bieten MSS eine gute Alternative zum Eigenbetrieb, da die Betreuung der Antivirenlösung oder der Firewall bei diesem Setup nicht sehr aufwändig ist – was sich in einem günstigen Preis für MSS äussert. Wenn eine VPN-Anbindung oder eigene Server in der DMZ ins Spiel kommen, ist mit massiv höherem Betriebs- und Wartungsaufwand zu rechnen, da diese Systeme potenzielle Ziele für Hacker, Phisher, Spammer und digitales Ungeziefer bilden. In diesem Fall ist abzuwägen, ob sich die eigene IT-Abteilung neben den täglich anfallenden Aufgaben auch dieser Aufgabe widmen muss, oder ob ein MSS-Anbieter eingebunden werden soll. Da sich die Rahmenbedingungen im Lauf der Zeit ändern können, sind Vertragslaufzeit und Ausstiegsklauseln im SLA von entscheidender Bedeutung.

MSS sind mit Medikamenten vergleichbar – richtige Diagnose und passende Dosierung bestimmen über Zustandsverbesserung oder unerwünschte Nebenwirkungen. ■

Der Autor
Christoph Baumgartner ist CEO und Senior Consultant bei OneConsult, Thalwil, www.oneconsult.com

Unsere Experten beantworten Ihre Fragen. Schreiben Sie uns: it-security@computerworld.ch

Ein Archiv der Helpdeskartikel finden Sie im Internet: www.computerworld.ch