Scheibchenweises Sicherheits-Know-how

Experten-Sharing Beim Security Outsourcing sollte die «Make-or-Buy»-Entscheidung nicht allein auf monetären Erwägungen beruhen. Für Klein- und Mittelunternehmen bietet sich das Experten-Sharing an.

Christoph Baumgartner*

Die primäre Zielgruppe für das Security Outsourcing sind Unternehmen mit zirka 50 bis 500 Mitarbeitenden. Grössere Unternehmen leisten sich meistens eine eigene IT-Security-Abteilung, bei kleineren Organisationen wird diese Funktion – wenn überhaupt – vom internen IT-Support abgedeckt.

Der Leistungsumfang der Dienstleistung wird, wie bei allen Outsourcing-Projekten üblich, in einem Service Level Agreement (SLA) definiert. Oftmals gehen die Kunden davon aus, dass mit der Unterzeichnung des Security-Outsourcingvertrages die Verantwortung für das IT-Riskmanagement (oder Teile davon) an den Outsourcer delegiert wird. Dies ist aber nur bedingt der Fall, weil von Gesetzes wegen die Verantwortung für das IT-Riskmanagement bei der Geschäftsleitung des jeweiligen Unternehmens selbst, also beim Kunden verbleibt. Der Outsourcer hat also nur beratende oder ausführende Funktion.

*Christoph Baumgartner ist IT-Berater bei der CDC IT und Geschäftsführer der Oneconsult.

Managed Security ist die am weitesten verbreitete Form des Security Outsourcing. Dabei werden bestimmte Komponenten wie Firewall, Virenscanner, Intrusion Detection Systeme (IDS) oder DNS-Server vom Outsourcer betrieben, überwacht und gewartet. Diese Komponenten stehen entweder beim Kunden oder in den Räumlichkeiten des Outsourcers. Die Dienstleistungen des Outsourcers sind in hohem Masse standardisiert, um Transaktionskosteneinsparungen seitens Outsourcer zu ermöglichen, welche dieser dann zu einem gewissen Teil an die Kunden weiter gibt. Die wiederkehrenden jährlichen Kosten für den Managed Firewall Service beginnen bei wenigen hundert Franken und sind gegen oben hin offen.

Security (Officer) Services

Aus sicherheitstechnischer Sicht gesehen ist der Mensch für rund 90 Prozent aller Pannen, Informationsdiebstähle und Manipulationen verantwortlich. Aber nur ein kleiner Teil dieser Risiken kann durch geeignete technische Massnahmen wie Firewalls, Datenverschlüsselung oder Smartcards verhindert oder vermindert werden. Dem Grossteil der Risiken kann nur durch die Planung und Umsetzung von organisatorischen Massnahmen wie Security Policies begegnet werden.

Dies ist der Ansatzpunkt für Security (Officer) Services. Da es sich hierbei um eine relativ junge Form des Security Outsourcing handelt, existieren dafür noch keine Standardausdrücke. Im Gegensatz zur Managed Security stehen bei den Security (Officer) Services organisatorische und konzeptionelle Dienstleistungen im Vordergrund.

Die Kunden kaufen beim Outsourcer je nach Anforderung ein gewisses Jahres-Stundenkontingent ein. Gemäss Kundenwunsch teilt der Outsourcer dem Kunden einen oder mehrere Security Officer zu. Der Beschäftigungsgrad des Security Officers bestimmt dabei, ob es sich um eine Vollzeit- oder Teilzeitstelle handelt. Im Falle einer Teilzeitbeschäftigung teilen sich verschiedene Kunden einen Security Officer beziehungsweise ein Team. Während der vertraglich vereinbarten Arbeitszeit steht der Security Officer dem Kunden exklusiv für jegliche Arbeiten im Security-Umfeld zur Verfügung wie Mithilfe bei der Entwicklung und Umsetzung der Sicherheitspolitik, verfassen oder überarbeiten von Security Policies, Benutzersensibilisierungen und Schulungen, Dokumentationen, Evaluationen, IT Verwundbarkeitstests, Bedrohungs- und Risikoanalysen. Der Ort der Leistungserbringung wird dabei vom Kunden bestimmt.

Vorteile

Die Kunden profitieren beim Security Outsourcing einerseits vom üblicherweise auf dem neuesten Stand befindlichen Fachwissen und der Erfahrung der Sicherheitsspezialisten des Outsourcers. Andererseits bekommen die Kunden diese Dienstleistung dank Experten-Sharing günstiger, als wenn sie die dafür benötigte Infrastruktur (Personal, Organisation und Technik) selbst aufbauen, betreiben und pflegen müssten. Ein KMU kann oder will sich oft keine eigenen System- oder Sicherheitsadministratoren leisten, welche rund um die Uhr die Aktivitäten auf der Firewall beobachten, die neuesten Security- und Anti-Viren-Updates innert nützlicher Frist installieren und bei Hackerattacken sofort gemäss Notfallplan einschreiten. Gute Security Outsourcer haben ihre Kunden erfolgreich vor den Auswirkungen der aktuellen Attacken des digitalen Ungeziefers (W32.Blaster. Worm) geschützt, indem sie die Firewall und die Kundensysteme entsprechend konfiguriert und Updates rechtzeitig eingespielt haben. Die Grundlage liefern dabei Notfallplan und Security Policy, für deren Erstellung der Security Officer verantwortlich ist.

Nachteile und Risiken

Die Qualität des Security Outsourcings und den damit zusammenhängenden Dienstleistungen hängt wie bei allen Outsourcingprojekten von der richtigen Wahl des Outsourcing-Partners ab. Bei den kostengünstigen Managed Security-Angeboten muss sich der Kunde beispielsweise in der Regel für ein, beziehungsweise das unterstützte Firewallprodukt und das vordefinierte Dienstleistungspaket entscheiden. Wer mehr Entscheidungsspielraum benötigt, muss diesen teuer berappen. Manche Anbieter binden ihre Kunden mittels Outsourcingverträgen mit mehrjähriger Laufzeit, wobei die durchschnittliche Laufzeit für die kostengünstigen Standardangebote bei sechs bis zwölf Monaten liegt.

Der fehlende Wissenstransfer in Richtung Kunde kann als weiterer Nachteil der Managed Security empfunden werden. Je nach SLA werden dem Kunden alle oder gewisse Administrationsrechte für die outgesourcten Komponenten entzogen. Wenn der Kunde Glück hat, wird er vom Outsourcer über Hackingversuche mit Ziel Kundensysteme informiert. Oftmals werden die outgesourcten Komponenten für den Kunden aber zur reinen «Black Box».

Fazit und Empfehlungen

Security Outsourcing ist in vielen Fällen die passende Lösung für Unternehmen, bei denen die Informatik nicht zum Kerngeschäft gehört, sondern als Basistechnologie gesehen wird. Allerdings gilt es, vor Vertragsabschluss einige Punkte zu beachten. Die Ziele, welche mit dem Security Outsourcing erreicht werden sollen, sollten schriftlich festgehalten werden. Ausserdem müssen die Geschäftsprozesse des Outsourcers mit denen des Kunden kompatibel sein. Besonderes Augenmerk gilt auch der Schnittstelle zwischen Kunde und Outsourcer, welche Rechte, Pflichten und Stellvertretungen präzise definieren muss. Zu guter Letzt sollte regelmässig von einer unabhängigen Instanz überprüft werden, ob der Security Outsourcer – gilt vor allem für Managed Security – auch hält, was er gemäss SLA verspricht. Diese Überprüfung sollte Bestandteil des Vertrages mit dem Outsourcer sein. Andernfalls kann sich der Outsourcer gegen derartige Qualitätssicherungsmassnahmen wehren. Darum prüfe, wer sich (ewig) bindet.

Info/http://www.oneconsult.com, http://www.cdcit.ch