



## Trennungsschmerzen vorbeugen

Viele Unternehmen erwägen, ihre IT-Security teilweise oder vollständig an externe Dienstleister zu vergeben. Doch nur die Berücksichtigung sehr vieler Faktoren führt zur richtigen Entscheidung.

von daniel krzyak, steffen weber und eberhard schott | markus.bereszewski@informationweek.de

Informationen brauchen sich nicht auf und lassen sich leicht vervielfältigen, verfälschen sowie verteilen. Unternehmen müssen daher Integrität, Vertraulichkeit und Verfügbarkeit der Informationen gewährleisten. Mit zunehmender Komplexität der Informationsinfrastruktur sowie Intensität der Angriffe auf IT-Funktionen stehen Unternehmen häufig vor dem Problem, der Lage mit eigenen Mitteln nicht mehr Herr zu werden. Auch das Fazit des Bundesamts für Sicherheit in der Informationstechnik (BSI) im Jahresbericht 2009 hinsichtlich der Bekämpfung von Cyberkriminalität ist mehr als deutlich: »Oft fehlen personelle und finanzielle Ressourcen sowie technisches Know-how. Technische Schutzmaßnahmen [...] sind jedoch besonders

wichtig, da Angriffe durch neue und komplexe Techniken zunehmend schwerer zur bekämpfen sind.« Eine im Auftrag von Symantec in den USA und Europa durchgeführte Studie unter 1000 IT-Managern und Sicherheitsexperten in Unternehmen zeichnet ein ähnliches Bild: Mit 98 Prozent haben fast alle der Befragten bereits spürbare Ausfälle des IT-Betriebs erlitten, die eindeutig auf Angriffe von außen zurückzuführen waren, bei 46 Prozent von ihnen standen die IT-Systeme vollständig still. Von den deutschen Teilnehmern der Umfrage haben 31 Prozent regelmäßig Bedrohungen dieser Art abzuwehren, 10 Prozent bezeichnen die Häufung der Vorfälle sogar als »extrem hoch«.



Eine angemessene Reaktion fällt den IT-Managern jedoch schwer. Die Mehrheit der Befragten geht davon aus, dass es in Zukunft teilweise deutlich schwieriger werden wird, die drohenden Gefahren einzudämmen. Gründe hierfür sind die ansteigenden Bedrohungen (64 Prozent), fehlendes Personal (56 Prozent), höhere gesetzliche Anforderungen (51 Prozent) sowie unzureichendes Budget (45 Prozent).

### Reduziertes Investitionsrisiko

Eine mögliche Lösung stellt ein effektiver Fremdbezug ausgewählter IT-Sicherheitsdienstleistungen dar. Frei werdende Ressourcen können so wieder verstärkt auf Kernkompetenzen im IT-Bereich konzentriert werden. Größere Einstiegsinvestitionen verwandeln sich in langfristige Zahlungsströme, was das Investitionsrisiko reduziert und die Flexibilität im Rahmen des Budgets erhöht. Entstandene Defizite

sondern auch tatsächlich sicherstellen? Verfügt er über hinreichend Wissen über und Interesse an den speziellen Anforderungen des Kunden, um diesen gerecht zu werden? Wie diese Fragen zeigen, ist eine umfassende Beurteilung der Situation unter Einbezug möglichst vieler Faktoren entscheidend.

Man unterscheidet im IT-Sicherheitskontext zwischen zwei Arten der Auslagerung: Zum einen kann die gesamte Abteilung für IT-Sicherheit inklusive kundenspezifischem Vermögen (Personal, Anlagen et cetera) an ein externes Unternehmen übergehen (IT Security Outsourcing, ITSO), welches fortan den Betrieb gewährleistet. Zum anderen können definierte Standardprodukte (beispielsweise Firewalls, Intrusion Detection and Prevention, E-Mail-Filtering, Public-Key-Infrastructures oder VPN-Services), die vom Anbieter standortunabhängig betrieben werden und stark von dessen IT-Infrastruktur geprägt sind, ausgelagert werden (Managed Security Services, MSS). Ein Übergang von Ressourcen zum Anbieter hin findet nicht statt, stattdessen werden diese Services flexibel nach Bedarf zugekauft und integriert. Dies eröffnet Unternehmen die Möglichkeit, kurzfristig die eingangs angesprochenen Problemstellungen zu adressieren und sie im Bereich IT-Sicherheit effektiv zu bewältigen.

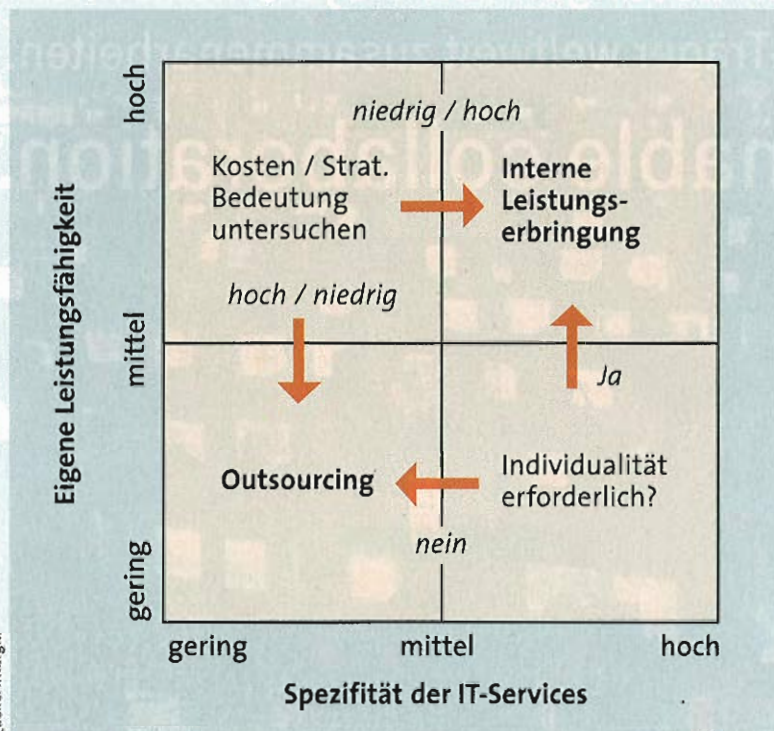
### Zunehmende Akzeptanz

Die genannte Umfrage zeigt, dass sich der Markt für MSS gut entwickelt: Zum aktuellen Zeitpunkt nutzen 32 Prozent der befragten europäischen Unternehmen einen Managed Security Service Provider (MSSP), weitere 35 Prozent erwägen diesen Schritt bereits oder planen eine Evaluation innerhalb der nächsten zwölf Monate. Bei der Frage nach den Motiven für die Nutzung von MSS werden mit der 24/7-Verfügbarkeit, also einem Mehrwert gegenüber der internen Leistungserbringung, niedrigeren Kosten, einer höheren Sicherheitsexpertise sowie der Konzentration auf das Kerngeschäft klassische Argumente für Outsourcing-Vorhaben genannt.

Ob ein IT-Service MSS-fähig ist, können folgende Faktoren annäherungsweise ermitteln:

1. **Spezifität:** Wie unternehmensindividuell muss der Service erbracht werden? Besteht Bedarf an individuellen Ressourcen, etwa spezielle Anwendungen oder speziell qualifizierte Mitarbeiter?
2. **Komplexität:** Wie umfangreich ist die Aufgabe, wie komplex die Systemlandschaft, wie hoch die Anforderungen an den Dienstleister?
3. **Strategische Bedeutung:** Wie hoch ist die strategische Bedeutung des Services für das Unternehmen?
4. **Interne Leistungsfähigkeit:** Kann der Service effektiv intern erbracht werden oder fehlen die notwendigen Kapazitäten?

Vorstehende Matrix ermöglicht die Einordnung der Security-Services nach den Kriterien der Spezifität →



innerhalb der Abteilung und deren Aufarbeitung werden zur Aufgabe des Dienstleisters. Spezielle Kompetenzen und Technologien, die nur schwer aufzubauen beziehungsweise zu betreiben sind, werden damit erreichbar. Darüber hinaus kann die externe Leistungserbringung durch Skalenvorteile und Erfahrungswerte teilweise signifikant kostengünstiger sein.

Trotzdem stellen sich hinsichtlich eines Outsourcings Fragen: Handelt es sich möglicherweise doch um eine Kernkompetenz, deren Auslagerung den Verlust von Wettbewerbsvorteilen nach sich ziehen könnte? Ist das Auslagern einer schlecht aufgestellten Funktion nicht viel teurer als die Reorganisation im eigenen Hause? Kann der Dienstleister die adäquate Qualität der Leistungserbringung nicht nur vertraglich garantieren,

sowie der eigenen Leistungsfähigkeit und gibt eine Entscheidungshilfe für unklare Situationen.

Alle Unternehmensnetze sind – abgesehen von gezielten Angriffen im Rahmen der Wirtschaftsspionage – den gleichen, nicht selektiven Bedrohungen ausgesetzt. Unternehmen benötigen also in jedem Falle ein Minimal-Set an Services, das sich zwar je nach Unternehmensgröße in Umfang und Komplexität unterscheidet, im Grunde aber die gleichen Leistungen bietet. Beispiele sind Internet-Nutzung, E-Mail-Dienste, Connectivity Services, PKI et cetera. Unter Berücksichtigung der vier genannten Faktoren handelt es sich in der Regel nicht um Services, die über eine hohe Spezifität verfü-

informeller Kommunikationswege oder mangelnde Kenntnis der Unternehmenskultur. Diese Befürchtungen können aber durch eine sorgfältige vertragliche Ausgestaltung der MSS (siehe hierzu auch Artikel ab Seite 33) gemindert werden. Der fehlenden Anwendernähe und dem Verlust informeller Kommunikationswege ist durch den hohen Standardisierungsgrad der beschriebenen IT-Sicherheitsdienstleistungen in diesem Bereich hinsichtlich des Qualitätsrisikos keine große Bedeutung beizumessen. Für den Client-Support und die Überprüfungsdienstleistungen ist es darüber hinaus so, dass Externe die Qualität durch ihre größere Erfahrung aus anderen Unternehmen massiv

## Das Auslagern bestimmter Anwendungen ist ein probates Mittel, um den Herausforderungen im Bereich IT-Sicherheit zu begegnen.

gen, sondern in dieser oder ähnlicher Form von nahezu allen Unternehmen eingesetzt werden. Auch die Komplexität der Anforderungen ist als eher gering einzustufen. Gleiches gilt für die strategische Bedeutung dieser Anwendungen. Abhängig vom Unternehmen ist natürlich die interne Leistungsfähigkeit.

Eine der großen Herausforderungen im IT-Sicherheitsmanagement liegt darin, Bedrohungen zu erkennen und erste Signale für einen Zwischenfall frühzeitig und zuverlässig aus dem »Hintergrundrauschen« des täglichen Betriebs zu filtern, ohne dabei zu viele »False Positives« zu generieren. Hierbei profitieren MSSPs von der Bündelung der Überwachungs- und Abwehrmaßnahmen vieler Kundennetze an zentralen Stellen. Durch die automatisierte Überwachung können Muster, die auf eine neue Bedrohung hinweisen, und gleichzeitig an mehreren Stellen auftauchen, zuverlässig und schnell erkannt werden. Der Effizienzgrad solcher Maßnahmen hängt direkt mit der Anzahl von Unternehmen zusammen, die diese Services nutzen.

Die Spanne an Dienstleistungen, die an zentraler Stelle aufgrund von Skalenvorteilen und der Konzentration von Know-how in höherer Qualität und zu günstigeren Preisen erbracht werden kann, ist aber deutlich größer. Sie reicht von 24/7-Erreichbarkeit des Security-Servicedesks für Mitarbeiter über Expertenunterstützung im Rahmen von 3rd-Level-Support bis hin zur zentralen Verwaltung der Private Key Infrastructure für die sichere Kommunikation innerhalb und außerhalb des Unternehmens sowie des zentralen Roll-Out von Patches und Updates auf Systemen innerhalb der Unternehmen.

### Risiken von MSS sind überschaubar

Unternehmen mangelt es oft an Vertrauen, Dienstleistungen im Bereich IT-Sicherheit in Anspruch zu nehmen. Befürchtet werden Qualitätsrisiken durch fehlerhafte Durchführung, fehlende Anwendernähe, Verlust

steigern können. In Bezug auf die mangelnde Kenntnis der Unternehmenskultur lässt sich festhalten, dass es bei MSS größtenteils um technische Routineaufgaben geht, welche nur sehr begrenzt von der Unternehmenskultur des Nachfragers geprägt sind.

Das Gegenargument der Abhängigkeit vom Anbieter wird durch den hohen Grad an Standardisierung der Services entkräftet, was bei Unzufriedenheit einen möglichen Wechsel zu einer Vielzahl an externen Dienstleistern ermöglicht. Es wird bei der Übernahme des Services auch kein oder nur sehr wenig unternehmensspezifisches Know-how übernommen. Das eigentliche Risiko von MSS stellt der problematische Schutz sensibler Datenbestände dar. Hier muss deshalb schon bei der Auswahl des Anbieters und der Vertragsgestaltung ein hohes Maß an Sorgfalt angewandt werden. Vertrauensbildende Maßnahmen zwischen Anbieter und Nachfrager, Datenschutz-Klauseln und vertraglich fixierte Sanktionen sind daher Pflicht. Ein möglicher Qualitätsnachweis kann zum Beispiel durch die Kommunikation von Compliance-Nachweisen wie Zertifizierungen sowie Referenzen seitens des MSSPs erbracht werden.

### Fazit

Das Auslagern bestimmter Anwendungen im Rahmen von MSS ist ein probates Mittel, um den komplexen Herausforderungen im Bereich IT-Sicherheit besser gewachsen zu sein. Die zunehmende Akzeptanz dieser Dienstleistungen signalisiert die wachsende Reife des Marktes und die Zuverlässigkeit der Angebote. Gerade durch die hohe Standardisierung von IT-Sicherheitsdienstleistungen und die verbesserte Qualität der Leistungserbringung bietet sich ein Fremdbezug zunehmend an. ■

\* Daniel Krzyzak und Steffen Weber sind Berater, Prof. Dr. Eberhard Schott ist Partner der INTARGIA und lehrt an der Hochschule Aschaffenburg.