



INTARGIA

Managed Security Services

Chancen & Risiken beim Outsourcing von IT-Sicherheit

Unternehmen als Teil der globalisierten Informations- und Wissensgesellschaft vertrauen auf eine Vielzahl von Applikationen, deren Absicherung von enormer Bedeutsamkeit für ein effizientes Wirtschaften ist. Diese Systeme gegen eine schnell wachsende Zahl komplexer räumlich und zeitlich verteilter Bedrohungen zu schützen erfordert nicht nur ein hohes Maß an Expertenwissen, sondern zieht auch eine Steigerung der Komplexität des Gesamtsystems nach sich. Diese Herausforderung bringt immer mehr IT-Abteilungen an die Grenzen ihrer Möglichkeiten. Externe Dienstleister bieten in Form von Managed Security Services die Gelegenheit, die interne IT zu entlasten, Effektivität und Effizienz der Schutzmaßnahmen zu steigern und die Kosten zu senken. Doch welchen Risiken sehen sich Unternehmen gegenüber, die den Schutz sensibler Datenbestände in fremde Hände geben? Ein Einblick in die Herausforderungen von IT-Sicherheit und die Möglichkeiten von Outsourcing in diesem Bereich.



Daniel Krzyzak
Berater



Steffen Weber
Berater



Prof. Dr. Eberhard Schott
Partner

Unternehmen bezüglich IT-Sicherheit mit schwieriger Situation konfrontiert

Unternehmen im 21. Jahrhundert sind Teil der globalen Informations- und Wissensgesellschaft. Treiber für die zunehmende Bedeutung von Informationen und Wissen sind die Globalisierung von Märkten, Produkten und Ressourcen, ansteigende Intensität von elektronischen Informationen und die zunehmende Ubiquität vernetzter Informations- und Kommunikationstechnologie. Analog zu der Chance, die diese Entwicklungen Unternehmen bieten, sehen sie sich auch einem wachsenden Risiko gegenüber. Anders als Industriegüter werden Informationen nicht verbraucht, sind leicht zu vervielfältigen, zu verfälschen und zu verteilen. Darauf muss ein Unternehmen reagieren, um seine Informationen zu schützen und deren Integrität, Vertraulichkeit und Verfügbarkeit zu gewährleisten. Mit zunehmender Komplexität der Informationsinfrastruktur sowie Intensität der Bedrohungen und Angriffe auf IT-Funktionen stehen Unternehmen oft vor dem Problem, der Lage mit eigenen Mitteln nicht mehr Herr zu werden.

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.“*

Studie bestätigt Einschätzung des BSI

Eine im Auftrag von Symantec in den USA und Europa durchgeführte Studie unter 1.000 IT-Managern und Sicherheitsexperten in mittelständischen und großen Unternehmen (davon 146 aus Deutschland) zeichnet ein ähnliches Bild: Mit 98% haben fast alle der Befragten bereits spürbare Ausfälle des IT-Betriebs erlitten, die eindeutig auf Angriffe von außen zurückzuführen waren. Ein Anteil von 46% hatte bereits einen kompletten Stillstand der ihrer IT-Systeme hinzunehmen. Von den deutschen Teilnehmern der Umfrage haben 31% regelmäßig Bedrohungen dieser Art abzuwehren, 10% bezeichnen die Häufung der Vorfälle sogar als „extrem hoch“.

In Sachen Abwehr derartiger Bedrohungen sehen IT-Manager sich zunehmend in die Defensive gedrängt. Die Mehrheit der Befragten geht davon aus, dass es in Zukunft teilweise deutlich schwieriger werden wird, die drohenden Gefahren einzudämmen. Die häufigsten Begründungen hierfür sind die ansteigenden Bedrohungen (64%), nicht

genügend Personal (56%), höhere gesetzliche Anforderungen / Compliance-Vorschriften (51%) sowie unzureichendes Budget (45%). Während 46% der Teilnehmer angeben, personell teilweise sogar signifikant unterbesetzt zu sein, sehen 42% ein großes Problem darin, Fachpersonal im Bereich IT-Sicherheit zu rekrutieren.

Somit stellt sich die Frage, inwieweit Unternehmen durch Fremdbezug ausgewählter IT-Sicherheitsdienstleistungen der „Komplexitäts- und Know-how-Falle“ entkommen und gleichermaßen Effektivität, Effizienz und Wirkungsgrad ihrer IT-Sicherheitsbemühungen steigern können.

Outsourcing als Lösungsansatz

Nicht selten wird bei Problemen mit der internen Leistungserbringung in einem Bereich die Auslagerung der Unternehmensfunktion als Lösung propagiert. Die Gründe hierfür sind vielfältig: Frei werdende Ressourcen können wieder verstärkt auf Kernkompetenzen konzentriert werden. Größere Einstiegsinvestitionen verwandeln sich in langfristige Zahlungsströme, was das Risiko reduziert und die Flexibilität im Rahmen des Budgets erhöht. Entstandene Defizite innerhalb der Abteilung und deren Aufarbeitung werden zum Problem des Dienstleisters. Spezielle Kompetenzen und Technologien, die nur schwer aufzubauen bzw. zu betreiben sind, werden für das Unternehmen erreichbar. Das schlagende Argument ist meistens jedoch, dass die externe Leistungserbringung durch Skalenvorteile und Erfahrungswerte teilweise signifikant kostengünstiger sein kann.

Wie jede Entscheidung bringt auch die Erwägung eines Outsourcings Tradeoffs mit sich: Handelt es sich bei der Funktion möglicherweise doch um eine Kernkompetenz, deren Outsourcing 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, sondern auch tatsächlich sicherstellen? Verfügt er über hinreichend Wissen über und Interesse an den speziellen Anforderungen des Kunden, um diesen gerecht zu werden? Ist er auch in schwierigen Zeiten wirtschaftlich stabil und flexibel genug, um auf neue Anforderungen reagieren zu können? Wie wohl ist dem Management dabei, geschäftskritische Systeme und sensible Datenbestände in fremde Hände und das Unternehmen in eine nicht zu unterschätzende Abhängigkeit zu geben? Wie diese Fragen zeigen ist eine umfassende Beurteilung der Situation unter Einbezug möglichst vieler Faktoren entscheidend.



Managed Security Services vs. IT Security Outsourcing

Beschäftigt man sich mit dem Thema Outsourcing im Kontext der IT-Sicherheitservices eines Unternehmens ist eine grundlegende Unterscheidung nötig. Dreht es sich um die Auslagerung der gesamten Funktion bzw. Abteilung für IT-Sicherheit inkl. Übergang von kundenspezifischem Vermögen (Personal, Anlagen etc.) an ein externes Unternehmen spricht man von *IT Security Outsourcing (ITSO)*. Diese Art des Outsourcings findet meist in Verbindung mit der ganzheitlichen Auslagerung der Unternehmens-IT, zumindest aber der zentralen Einrichtungen wie Rechenzentrum, Support etc., an einen Dienstleister statt, und ist davon unabhängig bisher kaum verbreitet.

Größerer Beliebtheit erfreuen sich *Managed Security Services (MSS)*: Dabei handelt es sich primär um Standardprodukte (z.B. Firewalls, Intrusion Detection and Prevention, E-Mail-Filterung, Public-Key-Infrastructures (PKIs) oder VPN-Services), die vom Anbieter standortunabhängig betrieben werden und stark von dessen IT-Infrastruktur geprägt sind. Ein Übergang von Ressourcen zum Anbieter hin findet nicht statt, stattdessen werden diese Services flexibel nach Bedarf „von der Stange“ zugekauft und an den Grenzen des eigenen Netzes oder darin integriert. Dies eröffnet Unternehmen die Möglichkeit, kurzfristig die eingangs angesprochenen Problemstellungen zu adressieren und sich im Bereich IT-Sicherheit auch im Hinblick auf Audits im Rahmen überarbeiteter gesetzlicher Verpflichtungen besser aufzustellen.

MSS erreichen Mainstream in Europa

Die bereits zuvor zitierte Umfrage zeigt, dass sich der Markt für *Managed Security Services* gut entwickelt: Zum aktuellen Zeitpunkt nutzen 32% der befragten europäischen Unternehmen einen *Managed Security Service Provider (MSSP)*, weitere 35% erwägen diesen Schritt bereits oder planen eine Evaluation innerhalb der nächsten zwölf Monate. Nur 23% der Befragten schließen solche Überlegungen vorerst aus. Eine Steigerung des Marktanteils auf etwa 50% innerhalb der nächsten zwölf bis 24 Monate scheint also nicht unangemessen zu sein. 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, höhere Sicherheitsexpertise und sowie Konzentration auf das Kerngeschäft klassische Argumente für Outsourcing-Vorhaben genannt.

Prüfung der Eignung von Services für Outsourcing

Ob diese Wünsche der Unternehmen erfüllbar sind hängt in erster Linie davon ab, wie gut sich die IT-Security Services, welche außerhalb der eigenen Organisation erbracht werden sollen, hierfür eignen. Die Antwort auf diese Frage lässt sich durch Einschätzung von vier Faktoren zumindest annäherungsweise ermitteln:

1. **Spezifität:** Wie stark muss die entsprechende Leistung auf das Unternehmen abgestimmt sein? Werden hierfür individuelle Mittel (z.B. Tools, Systeme, etc.) oder hochspezifische Humanressourcen benötigt? Oder ist es eine Anforderung, die in der Mehrzahl von Unternehmen in dieser oder ähnlicher Form benötigt wird?
2. **Komplexität:** Handelt es sich um eine umfangreiche Aufgabe mit hohen Anforderungen an den Dienstleister, die einen komplexen Prozess mit großem Fehlerpotential und hohen Transaktionskosten mit sich bringt? Oder geht es um eine Problemstellung, deren Komplexität wenig ausgeprägt oder wenn vorhanden sogar nicht in der Kompetenz des Unternehmens liegt und dies damit von Schwierigkeiten bei der Leistungserbringung entlastet wird?
3. **Strategische Bedeutung:** Ist die Erbringung der Leistung von hoher strategischer Bedeutung für das Unternehmen, vielleicht sogar ein Alleinstellungsmerkmal oder eine wichtige Stärke aus Sicht der Kunden? Oder handelt es sich eher um einen Hygienefaktor, der nur bei Nichterfüllung für die Entwicklung des Unternehmens von Relevanz ist?
4. **Interne Leistungsfähigkeit:** Ist das Unternehmen selbst (vielleicht sogar besser) dazu in der Lage, die Aufgabe zu erfüllen? Oder fehlt es hier an Kompetenz, Ressourcen und Erfahrung, um die Leistung selbst zu ähnlichen oder geringeren Kosten wie Anbieter am Markt zu erbringen?

Anhand dieser Faktoren kann für jede Anforderung aus dem IT-Sicherheitsmanagement eine Argumentenbilanz erstellt werden, deren Saldo oft einen optimalen Lösungsweg aufzeigt, zumindest aber in aller Regel eine Tendenz erkennbar macht.



Viele Services im Bereich IT-Sicherheit sind auslagerbar

Auch wenn die IT-Infrastruktur eines jeden Unternehmens einzigartig ist, so ergeben sich doch in nahezu jedem Falle zwei Gemeinsamkeiten: Alle Unternehmensnetze sind abgesehen von gezielten Angriffen im Rahmen der Wirtschaftsspionage den gleichen, nicht selektiven Bedrohungen ausgesetzt, die in der Regel auf bekannten Wegen versuchen, Systeme zu kompromittieren und / oder deren Betrieb zu stören. Außerdem sind alle Unternehmen auf ein bestimmtes grundlegendes Set an Services angewiesen, die sich zwar je nach Unternehmensgröße in Umfang und Komplexität unterscheiden, im Grunde aber die gleichen Leistungen bieten. Hierzu zählt z.B. die Anbindung des Unternehmensnetzes an das Internet, E-Mail-Dienste, Connectivity Services wie z.B. VPN oder Terminalsdienste, Private Key Infrastructures etc. Wendet man auf die Absicherung dieser Services die Prüfung auf Eignung zum Outsourcing mittels der vier zuvor vorgestellten Faktoren an ist das Ergebnis wenig überraschend: Es handelt sich in der Regel nicht um Services, die über eine hohe Spezifität verfügen, sondern in dieser oder ähnlicher Form von nahezu allen Unternehmen eingesetzt werden. Auch die Komplexität der Anforderungen wie z.B. Filterung von E-Mails, den Schutz von Rechenzentren durch Firewalls oder den Betrieb von VPN Gateways ist als gering einzustufen. Gleiches gilt für die strategische Bedeutung dieser Anwendungen, die mit wenigen Ausnahmen klare Hygienefaktoren für Kunden und das Unternehmen selbst sind. Abhängig vom Unternehmen ist natürlich die interne Leistungsfähigkeit – mit Zunahme der Anforderungen an die interne IT-Abteilung wie zu Beginn dargestellt dürfte dieser Aspekt aber weiter an Bedeutung gewinnen.

Mögliche Vorteile beim Einsatz von MSS für Unternehmen

Nachdem geklärt ist, dass die Auslagerung von IT-Sicherheitsservices an einen externen Dienstleister nach anerkannten Faktoren der Outsourcing-Praxis sinnvoll erscheint, muss die Situation nun aus der Perspektive der IT-Sicherheit bewertet werden. Dies soll am Beispiel der gängigsten Sicherheitsanwendungen geschehen, die als Managed Service angeboten werden.

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“, also

fälschliche Treffer, zu generieren. Dies trifft auf eine große Bandbreite von Applikationen zu: Von der Filterung von E-Mails hinsichtlich Spam, Malware und Social Engineering über Firewalls zum Block von Datenverkehr mit potentiell böswilligen Hosts bis hin zur Sperrung bestimmter Webpräsenzen aus dem Unternehmensnetz sind Kriterienkataloge nötig, anhand deren die Applikationen entsprechend reagieren können. Zu diesem Zweck kommen Filtersets, Black- und / oder Whitelists sowie Signaturen zum Einsatz, die nicht nur aufgebaut und gepflegt, sondern vor allem beim Auftreten neuer Bedrohungen schnell, zuverlässig und fehlerfrei (also ohne „False Positives“) aktualisiert werden müssen. Hierbei profitieren MSSPs von der Bündelung der Überwachungs- und Abwehrmaßnahmen vieler Kundenetze an zentralen Stellen, nämlich den Security-Operations-Centern (SOCs), die weltweit betrieben werden und in ständigem Austausch stehen. Durch die automatisierte Überwachung können Muster, die auf eine neue Bedrohung hinweisen, und gleichzeitig an mehreren Stellen auftauchen, zuverlässig und schnell erkannt werden. Kursiert beispielsweise bei einer Vielzahl von Kunden eine E-Mail mit sehr ähnlichem Inhalt, kann diese in kürzester Zeit als Spam- oder Malwareträger identifiziert und geblockt werden. Durch die Auswertung von Datenverkehr aus Kundennetzen mit bestimmten Servern können Steuerserver von Botnetzen identifiziert und durch zentrale Regeln in den Firewalls ohne Verzögerung geblockt werden. Webseiten mit Inhalten, die gegen die Unternehmenspolitik verstoßen (z.B. Pornographie, Glücksspiel etc.) können an zentraler Stelle kategorisiert und je nach Wunsch für Websurfer aus bestimmten Unternehmen gesperrt werden. Alle diese Maßnahmen sind nur möglich, da sie kollektiv für eine Vielzahl von Unternehmen durchgeführt werden, und können in dieser Art von kaum einer internen IT-Abteilung erbracht werden.

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-Servicesdesks 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. Unklar ist jedoch, ob diese Befürchtungen gerechtfertigt sind. Die aus den Eignungsfaktoren für Outsourcing resultierenden Gegenargumente wurden bereits zuvor besprochen, wie aber verhält es sich mit den generischen Risiken des Outsourcings, von denen einige zu Beginn dieses Textes vorgestellt wurden?

Hierzu zählen z.B. Qualitätsrisiken durch fehlerhafte Durchführung, fehlende Anwendernähe, Verlust informeller Kommunikationswege oder mangelnde Kenntnis der Unternehmenskultur. Diese sind zwar vorhanden, können aber durch eine sorgfältige vertragliche Ausgestaltung der MSS 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. Diese Dienstleistungen benötigen nach erfolgreicher Übergabe nur geringe Kommunikation mit dem Nachfragerunternehmen. Für die Client-Support-Dienstleistungen und die Überprüfungsdienstleistungen ist es darüber hinaus so, dass Externe die Qualität durch ihre größere Erfahrung aus anderen Unternehmen massiv 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. Zusätzlich lassen sich Anforderungen, Umfang und Auswirkungen auf die jeweilige Organisation aufgrund des hohen Standardisierungsgrades schon ex ante erarbeiten und im notwendigen Maße in den Planungen berücksichtigen. Überprüfungen wie Audits etc. profitieren sogar von einer externen Sicht auf die IT-Sicherheitslage.

Hinsichtlich der großen Abhängigkeit im Kontext möglicher wirtschaftlicher Instabilität ist festzuhalten, dass es sich in der Regel um hochgradig standardisierte Dienstleistungen handelt, welche von vielen externen Dienstleistern am Markt angeboten werden. Es wird bei der Übernahme des Services auch kein oder nur sehr wenig unternehmensspezifisches Know-how übernommen. Sollte der Anbieter nicht mehr lieferfähig sein, ist es für den Nachfrager deshalb leicht, einen neuen Anbieter am Markt zu identifizieren. Dasselbe gilt für die Nutzung von Standards (z.B. ISO/IEC 27001) im Rahmen von IT-Sicherheitschecks oder -audits.

Das eigentliche Risiko beim Outsourcing von IT-Sicherheitservices stellt der problematische Schutz sensibler Datenbestände dar. Dem MSS-Anbieter sind sicherheitsrelevante Aspekte des Nachfragers bekannt, er erhält Zugriff auf sensible Unternehmensinformationen. 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 z.B. durch die Kommunikation von Compliance-Nachweisen wie Zertifizierungen seitens des MSSPs erbracht werden.

Wichtige Faktoren bei der Auswahl eines Managed Security Service Providers

Bei der Suche nach einem passenden MSSP ist aufgrund der zuvor angesprochenen Risiken daher mit erhöhter Sorgfalt vorzugehen. Folgende Faktoren sollten im Rahmen des Auswahlprojekts berücksichtigt werden:

- Umsatz von mindestens 20 Mio. USD aus dem MSSP-Geschäft bei öffentlich gehandelten Firmen.
- Über Produkte und Services verteilter, sowie geographisch gut aufgestellter Channel-Vertrieb.
- Erfahrung des Managements, welche über Technik hinausgeht und sich auch auf die Bereiche Business Development sowie Managed Services erstreckt.
- Hinreichend große Präsenz auf dem Markt
- Rund 10 % des Personals sollte in Forschungs- und Entwicklungstätigkeiten eingebunden sein.
- Hohe Breite des Serviceangebots über die wichtigsten Dienstleistungen.
- Dokumentierte und extern auditierte Sicherheitsmanagementprozesse.
- Optimale Skalierbarkeit der eingesetzten Technologie.
- Nachvollziehbare Dokumentation relevanter Ereignisse, leicht zu erstellende ad-hoc Reports.
- Passende Referenzen hinsichtlich Unternehmensgröße und IT-Durchdringung der Kernprozesse.

Fazit

Wie die dargestellten Überlegungen zeigen ist das Auslagern bestimmter Anwendungen im Rahmen von Managed Security Services ein probates Mittel, um den komplexen Herausforderungen in kommenden Jahre besser gewachsen zu sein. Die zunehmende Akzeptanz dieser Dienstleistungen in Europa und weltweit signalisiert die nötige 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 an.

Gerne stehen wir Ihnen bei der Auditierung und Verbesserung Ihres internen Sicherheitsmanagements, der Prüfung hinsichtlich Möglichkeiten des Outsourcings bei höherer Professionalität, Steigerung der Qualität und Reduzierung der Kosten sowie bei Auswahl von und Transition zu einem Anbieter zur Verfügung.

Quellen

Baqué, M. (2009): „Partner gesucht“, in <kes> Ausgabe 2, Mai 2009, SecuMedia, Ingelheim

Autoren

Daniel Krzyzak und **Steffen Weber** sind seit 2007 Berater im Bereich IT-Risikomanagement der INTARGIA und verfügen über umfassende Erfahrung aus beruflichen Stationen und Projekten rund um Sicherheit in der IT.

Prof. Dr. Eberhard Schott ist seit 2004 Professor im Bereich Wirtschaftsinformatik an der Hochschule Aschaffenburg und seit 2006 Partner der INTARGIA. Von 1996 bis ins Jahr 2000 war er als Manager in verschiedenen Rollen (Business Development, Due Diligence & Transition Manager, Program Manager, HR- und Integrations-Manager) im Outsourcing-Bereich tätig. Seither folgten viele Projekte in der Rolle als Berater und Projektleiter (Ausgliederungen, Integrationen, Aufbau von Service-Organisationen). Neben Outsourcing ist die Organisation von Service-Bereichen sein wichtigstes Thema. Seit 2008 ist er auch CIO / Rechenzentrumsleiter der Hochschule Aschaffenburg.

Kontakt

Daniel Krzyzak, Berater
Steffen Weber, Berater
Prof. Dr. Eberhard Schott, Partner

INTARGIA Managementberatung GmbH
Max-Planck-Strasse 20
63303 Dreieich

Tel.: +49 (0) 6103 / 5086-0
Fax: +49 (0) 6103 / 5086-45

E-Mail: it-risikomanagement@intargia.com
Website: <http://www.intargia.com>

