

Verantwortlichkeiten bei Managed Security Services

Verantwortungsübertragung hat Grenzen

Rechtsanwalt Tim Faulhaber und Rechtsanwalt Robert Niedermeier

Managed Security Services (MSS) erlauben eine selektive oder umfassende Ausgliederung von Sicherheitsfunktionen der IT an einen externen Spezialisten. Es leuchtet ein, dass bei einer Übertragung dieser höchstkritischen Funktionen schnell die Frage nach der Haftung im Schadensfall aufkommt. Dieser Artikel möchte dem Leser einen Kurzüberblick über die Verantwortlichkeiten im Bereich der IT-Security im Kontext der Managed Security Services vermitteln. Hierzu werden die rechtlichen Anforderungen der IT-Sicherheit und deren praktische Umsetzung mittels Managed Security Services dargestellt.

Unternehmen steht mit Managed Security Services eine kostengünstige Alternative zum eigenen Betrieb der sehr komplexen Sicherheitstechnik zur Verfügung. Aber nicht nur Kostenfaktoren können für ein Outsourcing sprechen. Ein spezialisierter Managed Security Service Provider (MSSP) ist nicht selten besser über die aktuellen sicherheitsrelevanten Themen und Problematiken informiert als die eigene IT-Abteilung. Nachdem anfänglich nur Grundfunktionen wie das Firewall-Management ausgegliedert wurden, werden zwischenzeitlich alle denkbaren IT-Security-Funktionalitäten auf dem Markt angeboten und genutzt. So übergeben Unternehmen inzwischen auch Inhaltsfilterfunktionen, Intrusion-Detection-Systeme (IDS), Intrusion-Prevention-Systeme (IPS)

und E-Mail-Security-Funktionen an spezialisierte MSS-Provider.

IT-Security im Brennpunkt der IT-Compliance

Der Begriff der IT-Compliance ist wegen mehrerer öffentlichkeitswirksamer Negativbeispiele in jüngster Zeit zu einem allgegenwärtigen Schlagwort geworden. Unter dem Oberbegriff „Compliance“ wird generell die Befolgung von rechtlichen Pflichten und Geboten sowie von ethischen Unternehmensregeln und die entsprechende Verantwortung der Unternehmensleitung diskutiert. Im Hinblick auf die in den Unternehmen angesiedelte Informationstechnik sowie die starke Abhängigkeit zahlreicher Geschäftsprozesse von

der IT rücken gesetzgeberische und behördliche Aktivitäten im Bereich der IT-Sicherheit und im Bereich der mittels IT umzusetzenden, nicht IT-spezifischen Anforderungen im Zusammenhang mit dem Thema „Compliance“ immer stärker in den Mittelpunkt des Interesses.

Unternehmen und die Unternehmensleitung treffen in diesem Zusammenhang zunehmend umfangreiche Pflichten, deren Nichtbeachtung eine Haftung des Unternehmens als solches sowie – vor dem Hintergrund der in den letzten Jahren zunehmenden persönlichen Inanspruchnahme von Mitgliedern der Unternehmensleitung – eine persönliche Haftung der Unternehmensleitung nach sich ziehen kann. Die Unternehmensleitung steht nach § 93 Absatz 1 AktG sowie § 43 Absatz 1 GmbHG für eine ordentliche und gewissenhafte Unternehmensführung sowie ein gesetzeskonformes Verhalten des Unternehmens ein. Bei mehreren Vorständen oder Geschäftsführern gilt der Grundsatz der Gesamtgeschäftsführung und der Gesamtverantwortung. Dies ist vorwiegend dann der Fall, wenn im Unternehmen die notwendigen Sicherheitsstrukturen nicht oder unzureichend implementiert wurden.

In diesen Fällen riskiert der Geschäftsführer beziehungsweise der IT-Verantwortliche eine Exponierung des Unternehmens, aber auch seiner eigenen Person. Wer grob fahrlässig Sicherheitsmaßnahmen unterlässt, muss auch in Kauf nehmen, dass eine grundsätzlich vorhandene Versicherung nicht einspringt oder den Einwand des Mitverschuldens im Schadensfall anführt. Darüber hinaus greift aber auch das Strafrecht. Wird eine IT-spezifische Straftat im Aufgabenbereich eines IT-Verantwortlichen entdeckt, so exponiert sich dieser gegebenenfalls auch strafrechtlichen Sanktionen.

Die Schlussfolgerung hieraus ist, dass ein umfassendes Compliance-Konzept nicht ohne eine effiziente IT-Security erfolgen kann.

Grundsätzliche Anforderungen an die IT-Security

Bei der IT-Security kommen insbesondere folgende Anforderungen auf die Unternehmen zu:

Organisationsverpflichtung

Ein Unternehmen ist nach den Vorschriften der Gewerbeordnung und des Handelsgesetzbuchs gehalten, seine Applikationen entsprechend Art und Umfang des Geschäfts so auszugestalten, wie dies für eine ordentliche Durchführung des Geschäfts erforderlich ist. Hierzu zählen über die unerlässlichen Sicherheitsmaßnahmen hinaus verschiedene Organisationspflichten, die die einwandfreie Abwicklung eines IT-Betriebs ermöglichen und sicherstellen.

Dies hat die Rechtsprechung jetzt bestätigt. Nach dem Urteil des Landesgerichts Nürnberg-Fürth ist eine im Online-Bereich tätige Bank dazu verpflichtet, geeignete technische und organisatorische Vorkehrungen zu treffen, die sicherstellen, dass im Internet erteilte unplausible und offensichtlich irrtümliche Aufträge als solche erkannt werden. Der Irrtum des Kunden bei der Auftragserteilung ist bei unzureichender Organisation der Auftragsbearbeitung durch eine Online-Bank nicht als Mitverschulden des Kunden anzusehen. Hat eine Bank die notwendige Sicherung bei der Auftragserteilung nicht eingebaut, ist sie dem Kunden zum Ersatz des hieraus entstandenen Schadens verpflichtet. Die gleichen Pflichten bestehen im Bereich der IT-Sicherheit.

Internes Kontrollsystem

Die interne Revision kann sich jederzeit erkundigen, inwieweit die notwendigen technischen und organisatorischen Maßnahmen der IT-Sicherheit im Unternehmen getroffen worden sind. Stellt die interne Revision fest, dass ein dringender Hand-

lungsbedarf zur Sicherstellung der ordentlichen Geschäftsabwicklung besteht, könnten entsprechende Konsequenzen gezogen und die Verantwortlichen haftbar gemacht werden.

Verfügt das Unternehmen gemäß § 91 Absatz 2 AktG über ein eigenes Risikomanagement, so muss dieses Risikomanagement nicht nur für die Sicherheit der IT-Infrastruktur im Allgemeinen, sondern auch für die Sicherheit der Applikationen Sorge tragen. Dies gilt besonders bei Aktiengesellschaften, die dem sogenannten KonTraG unterliegen. Hier sind für kritische Entwicklungen entsprechende Früherkennungs- und Steuerungssysteme zu implementieren. Das aktuelle Bekanntwerden von Sicherheitslücken leitet eine solche kritische Entwicklung ein.

Datenschutz

Bei der Verarbeitung von personenbezogenen Daten ist das Bundesdatenschutzgesetz (BDSG) zwingend zu beachten. Gerade im Bereich der IT-Sicherheit sind personenbezogene Daten in einem erheblichen Ausmaß betroffen. Zum Verständnis soll an dieser Stelle kurz auf die Definition personenbezogener Daten gemäß § 3 Absatz 1 BDSG eingegangen werden. Personenbezogene Daten sind demnach Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person. Unter Heranziehung dieser Definition fallen schon Logdateien mit IP-Adressen aufgrund der Möglichkeit der Zuordnung zu einer bestimmten natürlichen Person unter den Anwendungsbereich des BDSG. Aber auch im Bereich der E-Mail-Filterung oder beim Content-Scanning sind in der Regel personenbezogene Daten in erheblichem Umfang betroffen. Für den Bereich der IT-Security sind vorrangig die von § 9 BDSG und seiner Anlage geforderten angemessenen technischen und organisatorischen Maßnahmen einzuhalten. Wenn

personenbezogene Maßnahmen verarbeitet werden, stehen die Ziele der Vertraulichkeit, Verfügbarkeit und der Integrität im Mittelpunkt der Sicherheitsmaßnahmen. Bei Nichteinhaltung drohen Geldbuße und im Extremfall auch Freiheitsstrafe.

Das Unternehmen zeichnet dabei auch dann noch als verantwortliche Stelle für einen datenschutzkonformen Umgang verantwortlich, wenn es die Datenverarbeitung durch einen externen Dienstleister vornehmen lässt.

Weitere Anforderungen

Für gewisse Branchen sind weitere Anforderungen beim Outsourcing zu beachten. So sind im Falle des MSS im Finanzsektor sowohl § 25a KWG als auch die Mindestanforderungen an das Risikomanagement (MaRisk) zu beachten. Diese Regelungen können ebenfalls als Best-Practice auf andere Tätigkeitsfelder übertragen werden. Neben gesetzlichen und untergesetzlichen Vorschriften sind vom Unternehmen weitere Vorgaben zu berücksichtigen. An dieser Stelle soll nur kurz auf ein ordnungsgemäßes Lizenzmanagement, die Risikobewertung bei Kreditvergaben im Rahmen von BASEL II sowie die individuellen Vorgaben der betrieblichen Versicherung hingewiesen sein. Versäumnisse können auch in diesem Bereich das Unternehmen empfindlich treffen. Denkbar sind der Ausfall des Versicherungsschutzes aufgrund von Mitverschulden, die Ablehnung von lebenswichtigen Betriebskrediten durch die Banken und Schadensersatz aufgrund von Urheberrechtsverletzungen.

Einzelheiten bei MSSPs

Wie bereits dargestellt, richten sich die gesetzlichen und sonstigen Anforderungen bezüglich der IT-Sicherheit an die Geschäftsleitung des Unternehmens. Die dargestellten Grundsätze und die damit verbundenen Anforderungen an die IT-Security gelten dabei auch bei Auslagerung

der Funktionen an einen externen MSSP fort.

Eine pauschale Verantwortungsübertragung auf den MSSP kann aufgrund der Vorschriften, die die Verantwortung begründen, per se nicht erfolgen. Lediglich die Haftungsrisiken bei Vermögensschäden können in einem gewissen Umfang und nur im Innenverhältnis zwischen Auftraggeber und MSSP vertraglich aufgeteilt werden. Daneben kann es sowohl im deliktischen als auch im vertraglichen Bereich zu Exkulpationsmöglichkeiten des Auftraggebers bei einem Verschulden des MSSP kommen. Grundvoraussetzung sind hierbei aber immer eine ordnungsgemäße Auswahl und Überwachung des MSSP. Aber auch unter diesem Aspekt ist MSS gerade bei kleineren und mittleren Unternehmen empfehlenswert, da hierdurch eine ordnungsgemäße IT-Sicherheit durch die Beanspruchung von Spezialisten sichergestellt werden kann. Dies führt im Ergebnis zu einer Minimierung der ohnehin bestehenden Risiken für die Geschäftsleitung.

Die Geschäftsleitung muss daher auch bei Beanspruchung eines MSSP imstande sein, unternehmenskritische Entwicklungen in der IT frühzeitig zu erkennen. Hierbei können sich durch die Einschaltung externer Dienstleister sogar negative Entwicklungen ergeben. So steht zu befürchten, dass bei einer mangelhaften Umsetzung die unternehmensinternen Sicherheitsprozesse nicht mehr richtig greifen und dass es zu Friktionen an der Schnittstelle zwischen Auftraggeber und MSSP kommt. Abhilfe kann hier eine optimale Abstimmung der Organisationsprozesse schaffen. Hierzu sind die Verantwortlichkeiten der Beteiligten möglichst detailliert zu fixieren und entsprechend in den Verträgen zu verankern. Zu jeder Zeit ist für reibungslose Kommunikation durch Bereitstellung von Kontaktpersonal auf beiden Seiten zu sorgen. Detaillierte Krisenpläne stellen im Notfall sicher, dass beide Seiten die erforderlichen Maßnahmen in

der richtigen Reihenfolge treffen. Allerdings kann auch eine optimale Abstimmung ins Leere gehen, wenn die IT-Security-Lösung des MSSP nicht auf das einschlägige Gepräge des Unternehmens abgestimmt ist. So hilft einem Unternehmen, dessen Kommunikation sensible personenbezogene Daten oder streng geheime Forschungsdaten umfasst, das beste IDS nicht weiter, wenn an der verschlüsselten Kommunikation gespart wurde. Im Rahmen einer Risikoanalyse muss deswegen zwingend festgestellt werden, wo die Schwerpunkte zu setzen sind und welche Bereiche für das Kerngeschäft von nachrangiger Bedeutung sind. In diesem Zusammenhang ist auch zu erwähnen, dass die vertragliche Ausgestaltung zwischen den Parteien so flexibel gehalten sein muss, dass ohne eine Neustrukturierung der Verträge zeitnah Änderungen in der Risikoanalyse entsprechend in die Realität umgesetzt werden können. Hierzu bietet sich ein modulares Vertragskonglomerat anhand von einem Rahmenvertrag sowie austauschbaren und erweiterbaren Unterverträgen an.

Für den Bereich des Datenschutzes muss sichergestellt sein, dass auch beim MSSP die erforderlichen technischen und organisatorischen Maßnahmen in einem angemessenen Umfang gewährleistet sind. Hierzu bietet es sich an, dass vor Beauftragung eine Besichtigung des Rechenzentrums des MSSP durchgeführt wird, um sich einen Überblick über die dort getroffenen Maßnahmen verschaffen zu können. Auch für den Bereich des Datenschutzes ist es ratsam, Informations- und Prüfungsrechte in die Verträge aufzunehmen.

Fazit

Zusammenfassend kann festgehalten werden, dass durch MSS eine pauschale Verantwortungsübertragung nicht erreicht werden kann. Aufgrund der Spezialisierung des

MSSP kann jedoch ein hoher Sicherheitsstandard erreicht werden, was zu einer Minimierung der Risiken beiträgt. Hierfür sind jedoch in der vertraglichen Ausgestaltung, zur Absicherung der gesetzlichen Vorgaben und der privatrechtlichen Haftungsszenarien, folgende Punkte zwingend zu berücksichtigen:

- Flexible Vertragsgestaltung, um aktuelle Bedrohungsszenarien effizient berücksichtigen zu können;
- detaillierte Abstimmung der Organisationsprozesse, detaillierte vertragliche Festlegung der Verantwortlichkeiten, Erstellung von Notfallplänen, Bereitstellung von Mitarbeitern auf beiden Seiten;
- Erstellung einer Risikoanalyse zur Abdeckung der individuellen Anforderungen;
- Analyse des bestehenden Versicherungsschutzes und individuelle Anpassung;
- vertraglich festgelegte Einstandspflicht des MSSP bei verursachten Schäden und
- vertragliche Aufnahme von Informations- und Prüfungspflichten.

Zu den Autoren

Rechtsanwalt Tim Faulhaber beschäftigt sich als niedergelassener Rechtsanwalt in München überwiegend mit Fragen rund um die IT und deren rechtssicherer Ausgestaltung. Rechtsanwalt Robert Niedermeier ist Mitglied der Heussen Rechtsanwalts-gesellschaft und ebenfalls auf IT-Recht spezialisiert.