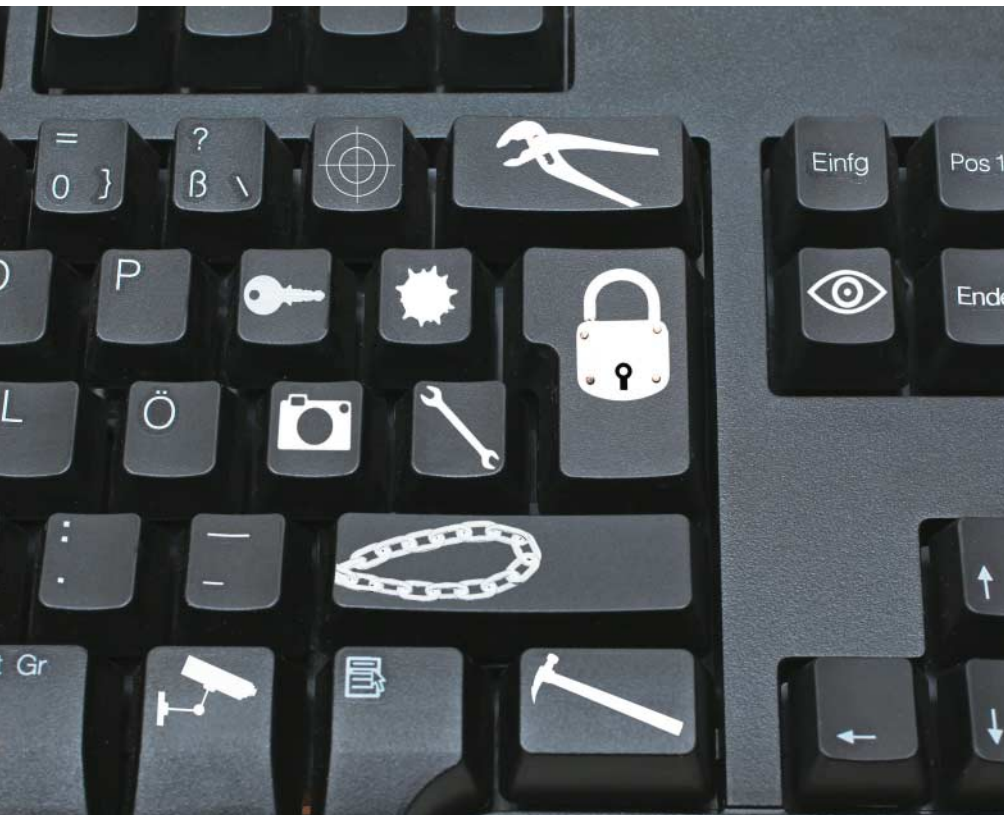



Managed Security Services: Sicherheit einkaufen

# Fremde Hilfe

**Uli Ries**

Gerade kleine Firmen haben oft weder Geld noch Know-how für IT-Sicherheit. Hier springen Anbieter von Managed Security Services in die Bresche: Kunden kaufen dort quasi per Modul die benötigten Dienste. Damit es weder teuer noch ein Reinfall wird, sind aber vorher einige Hausaufgaben zu erledigen.

An sich ist jetzt die Zeit, die sich IT-Verantwortliche immer herbeigesehnt haben: Die Geschäftsführung wünscht sich – nicht zuletzt aufgrund von Regelungen wie der nahenden EU-Datenschutz-Grundverordnung oder dem deutschen IT-Sicherheitsgesetz – mehr Fokus auf IT-Sicherheit. Bis dato mussten IT-Leiter meist um Budgets für neue Firewalls, Intrusion-Detection-Systeme oder moderne Antivirenlösungen feilschen. IT-Sicherheit wurde nur als Kostenblock gesehen und galt zudem als Bremser. Jetzt wandelt sie sich (eventuell gerade noch rechtzeitig) zur unabdingbaren Grundlage fürs Geschäft.

Dieser Wandel fegt aber in erster Linie den Markt an fähigen Mitarbeitern leer. IT-Sicherheit erforderte schon immer besondere detektivische Fähigkeiten, um die sprichwörtliche Daten-Nadel im Logfile-Heuhaufen zu finden. Und diese Fähigkeiten sind nicht breitflächig vorhanden. Insbesondere Mittelständler, die ihre Firmensitze abseits der Ballungszentren betreiben, tun sich typischerweise schwer beim Finden talentierter IT-Security-Experten. Die hohe Nachfrage führt automatisch auch zu steigenden Gehältern, was die Sache zusätzlich erschwert.

Zumal ein einzelner Sicherheitsspezialist schon in einem mittelgroßen, aus wenigen Hundert Endgeräten und einer Handvoll Servern bestehenden Netzwerk mit den zu bewältigenden Aufgaben überfordert sein dürfte. Ganz zu schweigen davon, wenn die Überwachung der IT-Systeme den Zwei-Schicht-Betrieb erfordert, weil der Schutzbedarf entsprechend hoch ist. Gänzlich aussichtslos würde das Unterfangen, müsste der Kollege sich auch noch um herkömmliche IT-Administration kümmern. Typischerweise würde das alleine gut drei Viertel der Arbeitszeit in Beschlag nehmen. Das verbleibende Viertel ist viel zu wenig für eine erfolgreiche Abwehr von Angriffen – die es zuerst einmal zu verstehen gilt, was wiederum Weiterbildung erfordert.

## Angebote für jedes Budget

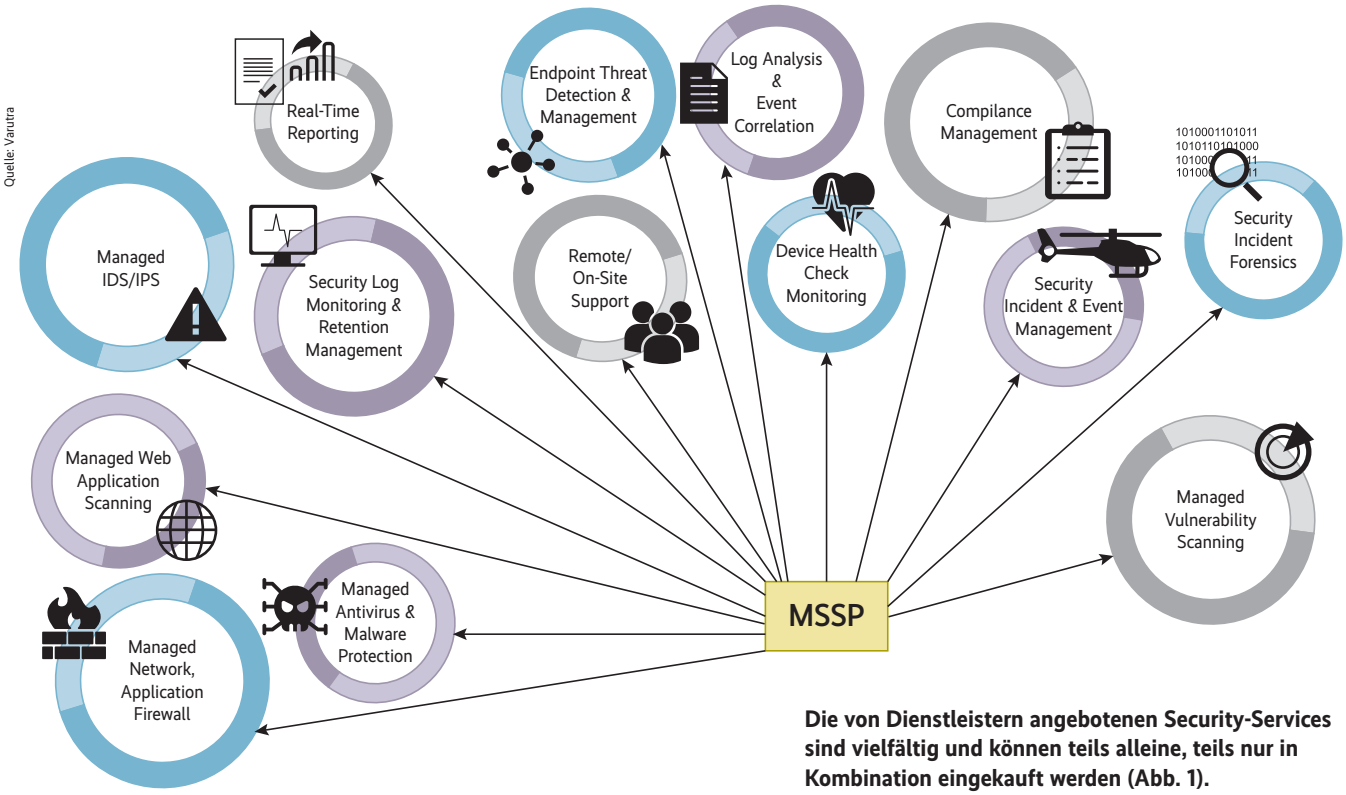
Die Lösung für dieses Ressourcenproblem nennt sich Managed Security Services (siehe Tabelle „Anbieter verschiedener Managed Security Services“). Ähnlich wie beim klassischen Outsourcing von IT-Aufgaben übernimmt ein Dienstleister die zuvor abgesprochenen Aufgaben. Und die können vielfältig sein: Identitäts- und Zugriffskontrolle, Schwachstellenscans, Patch-Management, Management von (Web Application) Firewalls und Antivirenlösungen, Logfile-Analyse/Netzwerk-Monitoring, Incident Response, Penetrationstests (Einbruchtests), E-Mail-Filterung und so weiter (Abbildung 1). Netzwerk-Monitoring beispielsweise liegt im niedrigen vierstelligen Eurobereich pro Monat. Der komplette Betrieb aller IT-Sicherheitskomponenten inklusive Rund-um-die-Uhr-Überwachung kostet je nach Dienstleister 20 000 Euro und aufwärts.

Je nach Anforderungen und Größe des Budgets lassen sich die Dienste kombinieren. Es gibt kein Patentrezept, welches Unternehmen welche Services benötigt. Schon eher lassen sich Angebote ausmachen, die man wahrscheinlich nur selten abruft und für die daher keine laufenden Kosten eingeplant werden sollten. Dazu gehört Incident Response, also die Reaktion auf einen erfolgreichen Angriff beziehungsweise ein entdecktes Datenleck. Schwachstellenscans und das Überwachen des Netzwerks auf Anomalien sind hingegen dauerhaft benötigte Dienste.

Egal, welche Aufgaben ein Unternehmen einem MSS-Anbieter überträgt, die-



© Copyright by Heise Medien
Persönliches PDF für Tatjana Kassilova aus 14532 Kleinmachnow




**Die von Dienstleistern angebotenen Security-Services sind vielfältig und können teils alleine, teils nur in Kombination eingekauft werden (Abb. 1).**

ser muss nicht vor Ort angesiedelt sein. Verwaltungsaufgaben lassen sich via Fernwartung oder Desktop-Sharing per TeamViewer & Co. erledigen. Der eigentliche Datenverkehr im Kundennetzwerk lässt sich mittels eines von drei gängigen Modellen überwachen: Bei einer Variante wird der gesamte Traffic in Richtung Cloud geleitet und dort durch die Filter des MSS-Anbieters geschickt.

Mit weniger Datenschutzbedenken einher geht wahrscheinlich das Ausleiten der Daten zum Rechenzentrum des Dienstleisters, wo die Filter ans Werk gehen. Am wenigsten Kontrollverlust über die eigenen Daten bedeutet es, wenn der Dienstleister sämtliche Schutzkomponenten vor Ort im Rechenzentrum des Auftraggebers betreibt, zumeist in eigens gesicherten Schränken. Diese Variante ist jedoch auch die teuerste, da die zum Analysieren der Datenströme notwendige Hard- und Software exklusiv vom Kunden verwendet wird und demnach auch alleine von ihm bezahlt werden muss. Der Skaleneffekt von Cloud-Angeboten fällt weg.

## Hausaufgaben erledigen

Bevor ein Unternehmen den Umfang der beim Anbieter zu buchenden Services festlegen kann, muss es erst einmal wissen, was es eigentlich zu schützen gilt. Das klingt simpler, als es in jahrelang gewachsenen IT-Umgebungen ist. Zumal IT-Fachleute oftmals gar nicht wissen, welches die kritischen Geschäftsprozesse in den jeweiligen Fachabteilungen sind. Die vor dem Beauftragen des MSS-Providers notwendige Risikoanalyse lässt sich also nur im Zusammenspiel zwischen IT- und Fachabteilungen erstellen.

Hierzu ist in erster Linie die Definition der eigenen Messlatte für Risiken unabdingbar, je nach Branche und IT-System drohen unterschiedliche Gefahren. So ist die Manipulation der IT-Systeme einer Finanzinstitution durch Insider mit ganz anderen Bedrohungen verbunden, als dies bei einem E-Commerce-Anbieter der Fall ist. In größeren Organisationen variiert das Risiko zudem: Verliert die Entwicklungsabteilung eines Maschinenbauers die Konstruktionsdaten der nächsten Maschinengeneration, sind die Folgen sehr viel schwerwiegender, als wenn der lediglich zu Marketing- und Informationszwecken genutzte Webserver erfolgreich attackiert wird.

Entscheidend ist also, in jedem Geschäftsbereich die kritischen Informationen – die sogenannten Kronjuwelen – zu identifizieren. Ausgangspunkt jeder Risikoeinschätzung ist der jeweilige Businessprozess. Anschließend werden die hierfür notwendigen IT-Systeme unter die Lupe genommen und zuletzt die zu verarbeitenden Daten klassifiziert. Aufgabe der IT-Organisation ist es, den Fachbereichen bei eventuellen Fragen zur Risikoabschätzung unter die Arme zu greifen.

Traut sich ein Unternehmen diese notwendige Risikoanalyse nicht selbst zu, hilft der Managed-Security-Services-Anbieter erfahrungsgemäß auch hierbei. Wenngleich dieser Teilbereich am besten vom Unternehmen selbst erbracht wird, da er sonst ins Geld gehen kann: Das Risikoprofil ändert sich laufend. Mit jedem neuen Angebot, das das vorhandene Geschäftsmodell erweitert, mit jeder Rabattaktion, die kurzzeitig vertrauliche Kundendaten an einem neuen Speicherort zusammenzieht, wird eine erneute

### iX-TRACT

- Mangelndes Know-how in den eigenen Reihen, Budgetknappheit und in manchen Fällen auch Fachkräftemangel lassen es in kleinen Unternehmen um die IT-Sicherheit schlecht stehen.
- Managed Security Services sind häufig die Lösung: Hier können Unternehmen jeder Größe einzelne Dienste oder Pakete an Sicherheitsleistungen einkaufen, die sie selbst nicht erbringen können.
- Vor dem Einkauf ist eine Risikoanalyse und das Identifizieren der „Kronjuwelen“ im Unternehmen erforderlich. Ein weiterer nicht zu vernachlässigender Aspekt ist das Sensibilisieren der Mitarbeiter als Teil des Sicherheitskonzepts.



© Copyright by Heise Medien
Persönliches PDF für Tatjana Kassilova aus 14532 Kleinmachnow

Risikoanalyse fällig. Unter Umständen genügt ein erstmaliges, vom MSS-Anbieter geführtes Analysieren und das Vermitteln der Denkweise von Angreifern; ohne sich in die Rolle von kriminellen Hackern zu versetzen, dürfte kaum ein Unternehmen auf Lücken in der eigenen Verteidigung stoßen. Ist das Wissen vom MSS-Provider ins Unternehmen geflossen, kann es die folgenden Analysen selbst stemmen.

Allen Beteiligten muss dabei klar sein, dass der Schutz einzelner Endgeräte oder Server immer weiter in den Hintergrund rückt. Aus zwei simplen Gründen: Zum einen finden talentierte Angreifer immer eine Lücke, mit der sie die jeweilige Maschine – und damit unter Umständen das ganze Netzwerk – unter ihre Kontrolle bekommen. Hundertprozentig dichte Systeme waren schon immer entweder unerreichbar oder unbezahlbar. Zum anderen haben sich Angreifer auf das massenhafte Ausspähen von Login-Daten konzentriert und sitzen auf Milliarden von funktionierenden Anmeldedaten für Webdienste. Da viele Anwender Passwort-Recycling betreiben, öffnen diese Daten eventuell auch die Türen ins Unternehmensnetzwerk.

Daher sollte ein Augenmerk auf das Management von Firewalls und Antivirenlösungen gelegt werden. Zumal die Empfehlung des Bundesamts für Sicherheit in der Informationstechnik lautet, verschiedene Virenscanner für Gateway, Server und Endgeräte zu verwenden, damit dieser Mix die jeweiligen Schwächen einer einzelnen Lösung minimiert. Dies erhöht natürlich den Managementaufwand. Mehr Aufmerksamkeit – und damit auch ein größeres Stück des Budgets für MSS-Dienstleistungen – sollten hingegen das Identitäts- und Zugriffsmanagement (Identity and Access Management, IAM) sowie das Netzwerk-Monitoring bekommen.

IAM-Systeme regeln, welcher (berechtigte) Mitarbeiter auf welchem Weg Zugriff auf welche Datenspeicher im Unternehmen bekommt. Je nach Leistungsfähigkeit solcher Systeme lassen sich zur Zutrittskontrolle beziehungsweise den nach dem Login gewährten Zugriffsrechten noch weitere Faktoren heranziehen: Kommt der Client per VPN von außen oder greift er über das lokale (W)LAN zu? Ist die Uhrzeit des Anmeldeversuchs ungewöhnlich? Erfolgt der Zugriff aus dem Homeoffice, einer Filiale oder aus dem Hauptsitz des Unternehmens? All diese Angaben lassen sich vom MSS-Anbieter in Regeln gießen, die dann den Zugriff definieren. So lässt sich festlegen, dass Mitarbeiter, die außerhalb der Bürozeiten vom Heimarbeitsplatz aus auf das Netzwerk zugreifen, nur Zugang zu ihren E-Mails haben. Die Fileserver stehen nur bei Anmeldungen aus dem Büronetzwerk zur Verfügung.

Grundsätzlich lässt sich ein funktionierendes IAM auch von den festangestellten Mitarbeitern überwachen. Die erstmalige Einführung verlangt aber nach mehr Zeit und Konzentration, als es das Tagesgeschäft erlauben dürfte. Denn bis die Reglements stehen und getestet sind, können einige Tage ins Land ziehen. Zumal verschiedene Spezialisten aus dem IT-Team – für WLAN, Switches, Sicherheit – an einem Strang ziehen müssen zur Definition der Regeln und deren Implementation. Vorteile durch ein IAM-Angebot eines MSS-Providers ergeben sich auch durch die je nach Service Level Agreement (SLA) verfügbare Rund-um-die-Uhr-Überwachung. Denn es nützt wenig, wenn die IT-Mitarbeiter des Unternehmens am Mittwoch nach den Weihnachtsfeiertagen in den Logdateien sehen, dass Freitagnacht vor dem Fest etliche unerlaubte Login-Versuche stattgefunden haben. Angreifer versuchen üblicherweise außerhalb der Bürozeiten ihrer Opfer in deren Systeme einzudringen, in der Hoffnung, dass die Admins im Feierabend weilen. Auch ein Mischbetrieb – Kunde übernimmt die Überwachung während der Bürozeiten, der MSS-Anbieter die übrige Zeit – ist machbar.

## Mehr Augen sehen mehr

Neben der eventuellen Dauerüberwachung von Login-Versuchen und Netzwerken bringen einzelne MSS-Anbieter einen weiteren großen Vorteil mit. Sie bündeln die Überwachung der Kundennetzwerke in sogenannten Security-Operation-Centern (SOC). Dort laufen dann alle Warnmeldungen auf. Auf diese Weise reichen einige wenige Spezialisten aus, eine große Zahl an Netzwerken im Blick zu behalten, und die Kunden profitieren von einem weiteren Punkt: Werden die Monitoring-Experten auf eine bisher nicht gekannte Attacke aufmerksam, kön-

**Anbieter verschiedener Managed Security Services**

| | 8com | Atos | Axians IT Security | Bechtle | British Telecom | Computacenter | Concat | Controlware | Deutsche Telekom | DXC Technology | ESC | Fujitsu | IBM | IT-Cube | Konica-Minolta | Netfox | NTT Security | Secunet AG | Secure Works | SHE Informationstechnologie AG | Verizon Business |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Anti-DDoS | – | ✓ | ✓ | ✓ | ✓ | – | ✓ | ✓ | ✓ | – | ✓ | ✓ | – | – | – | ✓ | ✓ | – | – | – | ✓ |
| Anti-Spam | – | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | – | ✓ | ✓ | – | – | ✓ | ✓ | ✓ | ✓ | – | ✓ | ✓ |
| Awareness-Schulungen | ✓ | ✓ | ✓ | ✓ | – | – | ✓ | ✓ | ✓ | ✓ | – | ✓ | ✓ | – | ✓ | ✓ | ✓ | ✓ | – | – | ✓ |
| Forensik | ✓ | ✓ | – | – | – | ✓ | – | – | ✓ | ✓ | – | ✓ | ✓ | – | ✓ | ✓ | ✓ | ✓ | ✓ | – | ✓ |
| Incident Response | ✓ | ✓ | ✓ | ✓ | – | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Managed Antivirus | – | ✓ | ✓ | ✓ | – | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | – | – | ✓ | ✓ | ✓ | – | ✓ | ✓ | ✓ |
| Managed Firewall | – | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Managed IPS/IDS | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | – | – | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Managed Proxys (E-Mail / Web) | – | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | – | ✓ | ✓ |
| Managed SIEM/Log-Überwachung | ✓ | ✓ | ✓ | ✓ | – | ✓ | ✓ | ✓ | ✓ | – | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | – | – | ✓ |
| Schutz von Webservern/Webanwendungen | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Vulnerability Management | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | – | ✓ | ✓ | ✓ |

✓: ja; –: nein. Tabelle beruht teilweise auf Herstellerangaben. Je nach Anbieter/SLA lassen sich einzelne Dienste nur im Paket buchen zusammen mit anderen Diensten des Providers. Einige Anbieter führen nicht alle Dienste auf ihren Webseiten auf, im Zweifel nachfragen.



© Copyright by Heise Medien
Persönliches PDF für Tatjana Kassilova aus 14532 Kleinmachnow

nen sie in allen übrigen ihnen unterstellten Netzwerken nach ähnlichen Angriffsmustern suchen. Einzelkämpfern in Unternehmen fehlt nicht nur dieser Einblick und das damit verbundene Tempo bei der Informationsgewinnung. Sie müssten zusätzliche Threat-Intelligence-Dienste abonnieren, um überhaupt an solche Informationen zu gelangen, und dann rund um die Uhr auf Alarme achten.

Die Kunden müssen sich diese dauerhafte Überwachung jedoch sichern. Genau wie beim Umgang mit Cloud-Anbietern gilt im MSS-Umfeld: Nur was im Vertrag beziehungsweise dem SLA steht, wird auch geliefert. Die kritischen Kennzahlen sind die Zeiten, zu denen die Dienstleistungen erbracht werden, sowie die Reaktionszeiten, binnen derer der Dienstleister eine vereinbarte Reaktion auf eine festgestellte Aktion zu erbringen hat. Diese Kennzahlen variieren je nach Kunde. Ein Krankenhaus benötigt für seine zentralen IT-Dienste andere Reaktionszeiten und Verfügbarkeiten als ein Logistikunternehmen, das sein Tagesgeschäft für eine Weile notfalls auch ohne IT abwickeln kann.

Je nach Detailgrad der SLA lassen sich auch Zeiten festschreiben, binnen derer durch einen Angriff ausgefallene Systeme wieder in Betrieb sein müssen. Die jeweiligen Verantwortlichkeiten gilt es unbedingt im Vertrag festzuhalten: Wofür ist der Dienstleister zuständig, wofür das beauftragende Unternehmen? Backups sind oftmals ein Stolperstein, da Kunden blindlings davon ausgehen, dass Dienstleister eine so grundlegende Absicherung von sich aus erbringen. Immens wichtig ist auch eine Regelung, die dem Dienstleister das Abschalten infizierter Systeme erlaubt, um das Abfließen sensibler Daten zu unterbinden. Zwar sollten Verantwortliche im Fall einer entdeckten Infektion Ruhe bewahren und durch Beobachten der Angreifer möglichst viel über die verwendeten Tools und eventuelle weitere infizierte Maschinen in Erfahrung bringen. Machen sich die Kriminellen jedoch an zuvor durch die Risikoanalyse identifizierten und im Vertrag spezifizierten Datenspeichern zu schaffen, hilft eventuell nur das virtuelle Ziehen des Steckers.

## Cloud: Schutz für hybride Umgebungen per MSS?

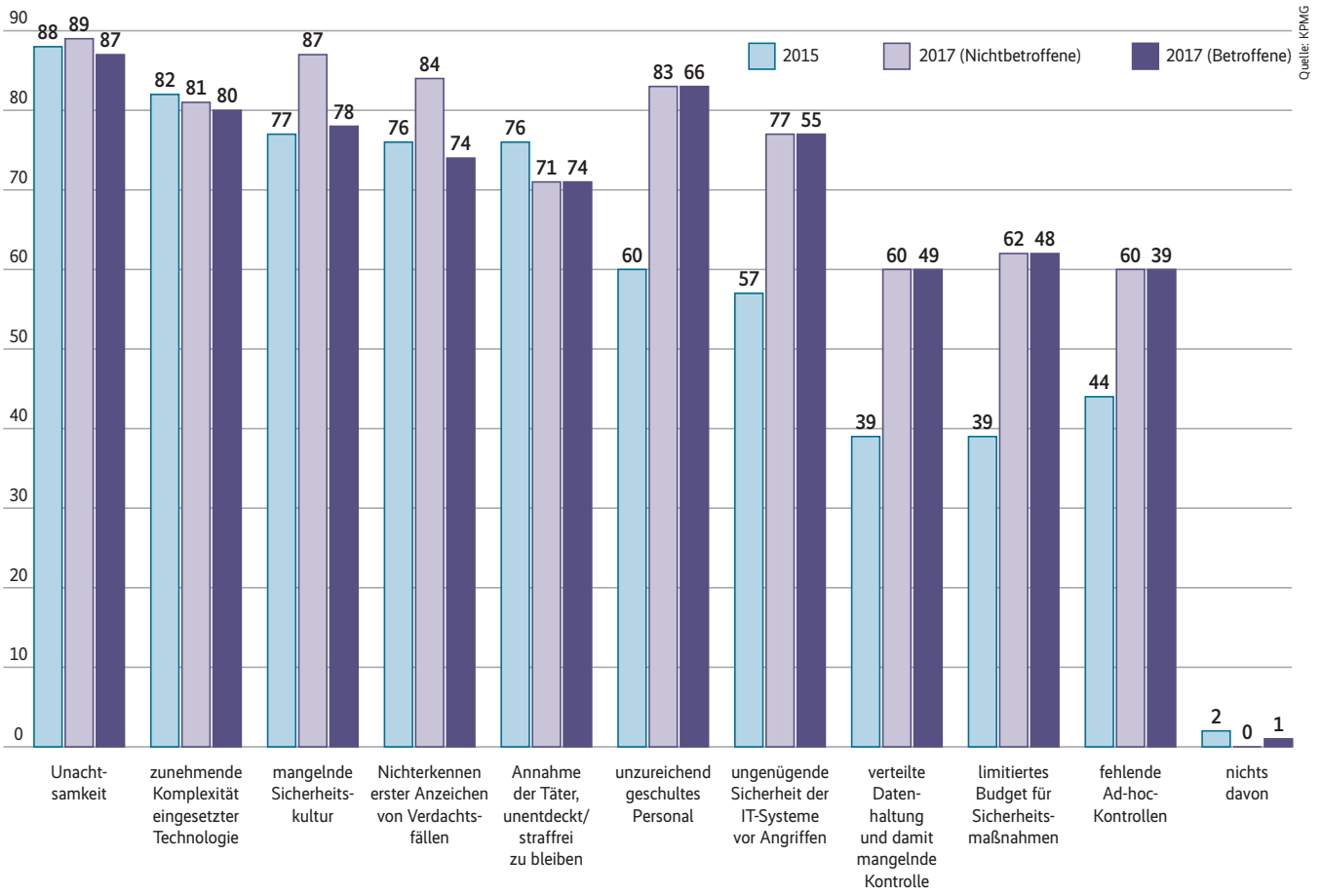
Nachdem auch kleine und mittelgroße Unternehmen (KMU) Nutzer von Cloud-Diensten sind, stellt sich natürlich die Frage, wie sich die zumeist hybriden IT-Landschaften schützen lassen und welche Rolle Managed Security Services hierbei spielen können. Grundsätzlich liefern Cloud Access Security Broker (CASB) die gewünschte Funktion. Diese Gateways klinken sich in die Datenströme zwischen lokalen Geräten sowie Cloud-Diensten ein und setzen die Sicherheits-Policies des Unternehmens auch in der Cloud-Umgebung durch. Noch ist CASB ein eher junges Thema. Entsprechend dünn ist derzeit noch das Angebot an Managed Security Services, die CASB mit anbieten.

Grundsätzlich ist aber nach wie vor unbestritten, dass Cloud-Anbieter Daten besser schützen können als die meisten Unternehmen. Kein KMU kann sein eigenes Rechenzentrum so aufwendig schützen, wie Cloud-Anbieter dies können: von der physischen Sicherheit (Löschanlagen, Einbruchsschutz, Zutrittskontrolle, Energieversorgung und so weiter) bis hin zum Absichern der Anwendungen wie Microsoft Exchange, SAP oder das Speichern der Daten im Internet.

Anzeige



© Copyright by Heise Medien
Persönliches PDF für Tatjana Kassilova aus 14532 Kleinmachnow




**Von den laut KPMG häufigsten Ursachen für Datenlecks lassen sich etliche mithilfe von Managed Security Services in den Griff bekommen (Abb. 2).**

Zwar ist moderne Schutztechnik unabdingbar im Hase-und-Igel-Wettrennen zwischen Cyberkriminellen und Unternehmen. Vergessen Letztere aber beim Konzipieren der Schutzmaßnahmen, ihre Mitarbeiter einzubeziehen, lassen sie ein Scheunentor offen stehen. Denn professionelle Onlinekriminelle stürzen sich laut dem aktuellen Data Breach Investigations Report von Verizon Business zufolge bei 50 Prozent aller erfolgreichen Angriffe erst im zweiten Schritt auf einen Server oder PC. Zuerst attackieren sie einen Mitarbeiter eines Unternehmens durch Social Engineering. Dem IT-Sicherheitsexperten Karsten Nohl zufolge verraten 80 Prozent der Angestellten einem geschickt vorgehenden Angreifer per Telefon ihr Passwort. Auf Phishing-E-Mails fällt immerhin noch die Hälfte aller Mitarbeiter herein.

## Den Menschen im Visier

Um hier gegenzusteuern, empfiehlt sich ein Mix aus MSS und Eigeninitiative: Ein Dienstleister kann beim Konzipieren von Awareness-Maßnahmen helfen. Diese versorgen die Mitarbeiter mit dem nötigen Hintergrundwissen. Wichtig hierbei ist, alle Mitarbeiter einzubeziehen. Denn so gut wie nie wenden sich die Kriminellen an das eigentliche Ziel ihrer Bemühungen, also etwa den Forschungschef, Finanzvorstand oder Geschäftsführer, sondern stattdessen an Kollegen aus Personal- oder Marketingabteilung oder Buchhalter. Letztere stehen im Fokus beim sogenannten CEO-Fraud.

Laut Karsten Nohl haben sich statische Schulungen, die mehr oder weniger zufällig übers Jahr verstreut zu absolvieren sind, als wenig wirksam erwiesen. Deutlich effektiver sei es, Mitarbeiter durch gezielt verschickte Phishing-E-Mails oder vom MSS-Anbieter gestartete Anrufe einzeln aufs Glatteis zu führen. Anschließend erhalten nur die Kollegen einen (weiteren) Anruf, die auch auf Anhang oder Link geklickt oder allzu freigiebig Auskunft erteilt haben. Inhalt des Anrufs: eine Erläuterung des Fehlverhaltens und Tipps, woran das Opfer E-Mail oder Anruf als Betrugsversuch hätte erkennen können. Wichtig ist hierbei laut Nohl, dass der Anruf binnen weniger Minuten nach dem Klick erfolgt. Dies könne die Klickrate bei künftigen Phishing-Kampagnen um zwei Drittel senken.

Erfordert das Erstellen der Skripte für den Anruf des vermeintlichen Kriminellen oder das Formulieren einer überzeugenden Phishing-Mail noch die Hilfe des MSS-Anbieters, kann das Unternehmen die Nachsorge und weitere Penetrationstests durchaus selbst stemmen. Der Anbieter sollte in diesem Fall nur Hilfe zur Selbsthilfe geben sowie bei der Lernzielkontrolle unterstützen.

Insbesondere für kleine und mittelgroße Unternehmen sind Managed Security Services heute quasi der einzige Weg, um sicherheitstechnisch mit dem Niveau professioneller Angreifer mithalten zu können (Abbildung 2). Auch wenn es ein bisschen frustrierend klingt: Unterm Strich dürfte es oftmals sogar zielführender sein, sich gleich nach einem MSS-Anbieter umzuschauen als nach personeller Verstärkung der eigenen IT-Mannschaft. (ur)

**Uli Ries**

ist Fachjournalist mit Schwerpunkt auf IT-Sicherheit.



© Copyright by Heise Medien
Persönliches PDF für Tatjana Kassilova aus 14532 Kleinmachnow