Bild: fotolia

DOSSIER SECURITY
IN KOOPERATION MIT SWISSCOM

Seinen Gegnern stets einen Schritt voraus sein

jae. Wer für die IT-Sicherheit eines Unternehmens verantwortlich ist, sollte seinen Gegnern idealerweise stets einen Schritt voraus sein. Denn diese denken sich immer wieder neue Gemeinheiten aus, um die Sicherheitsabteilungen mit Angriffsmethoden bei Laune zu halten.

Aber wie kann man eine solche Mammutaufgabe angehen? Worauf ist zu achten? Markus Kägi ist Produktmanager für Managed Security Services beim Grosskundengeschäft von Swisscom. In seinem Beitrag auf Seite 31 liefert er Tipps für Unternehmen, die sich vertieft mit dem Thema IT-Sicherheit auseinandersetzen wollen, und zeigt Schritt für Schritt, worauf es ankommt.

Bedürfnisse definieren

Wichtig ist als Erstes, wie bei eigentlich jedem Vorhaben überhaupt, dass ein Unternehmen für sich selbst definiert, was es braucht und welche Sicherheitsvorkehrungen überhaupt nötig sind. Dabei muss beispielsweise definiert werden, welche Daten besonders schützenswert sind oder welche Applikationen wann verfügbar sein müssen. Daneben gibt es branchenspezifische Vorgaben, die beachtet werden müssen.

Wie umsetzen?

Danach gilt es zu überlegen, wo ein Unternehmen seine Daten speichern will. Sollen die Daten in der Schweiz verbleiben oder ins Ausland verlagert werden? Falls sie in der Schweiz gespeichert werden sollen, muss noch der genaue Standort geklärt werden. Und sind diese Fragen einmal beantwortet, müssen sich Unternehmen nur noch entscheiden, wie sie die Daten speichern wollen, in der Cloud, lokal oder mittels einer hybriden Lösung. <

> **Seite 31**
Umfassend definieren, kontinuierlich umsetzen

> **Seite 33**
Das Mobiltelefon als Security Token | Weltweit sicher Daten austauschen

Umfassend definieren, kontinuierlich umsetzen

Die ICT-Security ist eine dynamische Aufgabe. Was heute gilt, ist morgen bereits passé. Einmal grundlegend ausgerichtet muss ein Unternehmen das Sicherheitskonzept kontinuierlich überprüfen und justieren, denn Sicherheit definiert sich laufend neu. Welche Lösung aber eignet sich für welches Unternehmen? Markus Kaegi

Sicherheitslücken bei Smartphone-Apps, Cyberattacken oder Datenlecks bei Firmen: Derzeit vergeht kaum ein Tag ohne eine neue Meldung im Zusammenhang mit Datenschutz oder -sicherheit. Unternehmen befinden sich mittendrin. Als Verantwortliche für die Sicherheit ihrer Kunden- oder anderer sensibler Daten stehen sie in der Pflicht, die Sicherheit so weit wie möglich zu garantieren und sich mit zukunftsgerichteten Entwicklungen auseinanderzusetzen. Neue Technologien, Hersteller und ganze Megatrends werden von den Fachleuten ins Feld geführt. Worauf aber kann man vertrauen? Was ist tatsächlich nötig? Und in welchen Bereichen wittern Anbieter lediglich ein gutes Geschäft? Wer Sicherheit ernst nehmen will, sollte sich in einigen grundlegenden Punkten für eine Ausrichtung entscheiden. Nur so entsteht am Schluss ein Sicherheitskonzept, das zum Unternehmen passt und auch für die Kunden optimale Sicherheit gewährleistet.

Eigenes Sicherheitsbedürfnis definieren

Als Erstes sollte dem Sicherheitsmanagement jeder Firma eine Risikoeinschätzung vorausgehen. Dabei müssen einerseits technische und prozessuale Fragen analysiert werden, zum Beispiel: Wie wichtig ist welcher Dienst? Welche Informationen sind besonders schützenswert? Welche Applikation muss wann verfügbar sein? Andererseits gibt es aber auch unternehmens- und branchenspezifische Vorgaben, die das Sicherheitsmanagement beeinflussen. Gibt es interne Datenschutzrichtlinien? Wer muss auf welche Daten zugreifen können? Was ist gesetzlich vorgegeben? Diese Risiko-Assessments können je nach internen Kompetenzen entweder selbst oder gemeinsam mit einem ICT-Vertrauenspartner durchgeführt werden. Generell ist eine Zweitmeinung beziehungsweise eine neutrale Beurteilung immer von Vorteil.

Ort der Datenlagerung bestimmen

Als Zweites gilt es zu überlegen, wo die eigenen Daten gespeichert werden sollen und von wo aus auf welche Daten zugegriffen werden muss. Angesichts der Relevanz von Sicherheit in der Öffentlichkeit ist es für jedes Unternehmen unabdingbar zu wissen, wo die eigenen Daten gespeichert sind und wie es diese wiederfindet. Es existieren rechtliche Vorgaben, die es zu beachten gilt. In manchen Branchen ist zum Beispiel klar vorgegeben, in welchen Ländern Daten gelagert werden dürfen. Wichtig hierbei: Bei der Speicherung im Ausland kommt immer auch das jeweilige ausländische Gesetz zur Anwendung. Da diverse Provider die Daten im Ausland lagern, kann sich dies unter Umständen auf die Datenbearbeitung oder -weitergabe auswirken. Grundsätzlich gilt: Dritte dürfen Daten, die ihnen anvertraut wurden, nur so bearbeiten, wie dies der Auftraggeber selbst tun dürfte. Ausnahmen sind gesetzliche oder vertraglich definierte Geheimhaltungspflichten. Besonders bei Personendaten müssen die geltenden Regelungen gemäss dem Datenschutzgesetz eingehalten und die Bearbeitung durch einen Dienstleister in jedem Fall vertraglich geregelt werden – egal, ob sich dieser in der Schweiz oder im Ausland befindet. Der Vorteil von externen, zertifizierten Providern ist, dass diese in der Regel sofort nachweisen können, wo die Daten gespeichert werden. Massgebende Zertifizierungen sind beispielsweise ISAE 3402 (ehemals SAS70) oder auch ISO27001. Wer ganz auf Nummer sicher gehen will, wählt einen Provider, der alle Daten in der Schweiz speichert.

Unternehmen, die die Daten weiterhin selbst speichern, sollten sicherstellen, dass die Infrastruktur immer auf dem aktuellen Stand ist. Da veraltete ICT-Infrastrukturen offene Türen für Attacken sind, sind regelmässige Updates zwingend nötig. Auch die physische Sicherheit darf nicht ausser Acht gelassen werden. Dazu gehören beispielsweise eine unterbrechungsfreie Stromversorgung, sichere Zutrittssysteme sowie Brandschutzanlagen.

Cloudbasiert, lokal oder Hybridlösung?

Eng mit dem Ort der Datenhaltung hängt auch zusammen, ob man sich für eine cloud- oder premisebasierte Sicherheitslösung entscheidet. Bei vielen Unternehmen herrscht immer noch Unsicherheit darüber, ob Services aus der Cloud sicher genug sind. Umgekehrt sind aber wie erwähnt auch lokale, physische Installationen nicht zwingend sicherer. Für grössere Unternehmensstandorte ergibt heute eine Kombination aus cloud- und premisebasierten Diensten am meisten Sinn. Funktionen, die problemlos aus der Cloud bezogen werden können, sind beispielsweise E-Mail und Web-Security-Lösungen. Diese Hightech-Schutzschilder wehren Malware, Viren, Spam oder Spionage schon ausserhalb der Unternehmensgrenzen zuverlässig ab. Der entsprechende Traffic aus dem Web kommt damit bereits gesäubert ins Unternehmen. Dies verbessert die Performance und spart gleichzeitig die lokale Infrastruktur. Auch für Cloud-Lösungen gibt es übrigens Anbieter, bei denen die Daten die Schweiz nicht verlassen. Es empfiehlt sich, beim Anbieter nachzufragen, ob die Lösung eine eigene Cloud ist oder lediglich den Wiederverkauf einer globalen Cloud darstellt. Diverse weitere Funktionen wie Firewall-, Intrusion-Detection-Systeme, umfassende Proxyfunktionen oder das Vulnerability Management (Schwachstellenma-

CHECKLISTE

- Qualitätsausweise: Seriöse Anbieter haben glaubwürdige Referenzen und häufig auch spezifische Zertifizierungen in der Informationssicherheit (z.B. Finma, ISAE 3402- oder ISO-Zertifizierungen).
- Dedizierte Betriebseinheit: Der Anbieter sollte über eine Abteilung verfügen, die sich ausschliesslich Sicherheits-Services widmet, die Leistung 7x24 erbringen kann und über ein mehrstufiges Zutrittskonzept verfügt.
- Erfahrung: Je länger ein Anbieter im Bereich der Managed Security Services tätig ist und je mehr Kunden er hat, umso grösser ist seine Erfahrung.
- Persönliche Beratung: Ein persönliches Gespräch oder ein Besuch in der Betriebsorganisation sind vor der Auslagerung sensitiver Geschäftsbereiche zwingend und ermöglichen es, sich ein persönliches Bild vom Unternehmen zu machen.
- Internationale Erfahrung: Unternehmen mit Standorten in verschiedenen Ländern sollten auch auf Anbieter mit internationaler Erfahrung setzen.

Überwachung rund um die Uhr: In einem Security Operation Center werden die Daten rund um die Uhr überwacht und gemanagt. Bild: Swisscom

nagement) können allerdings nach wie vor lokal sinnvoll sein. Gerade für Unternehmen mit einer umfangreichen Demilitarized Zone, beispielsweise am Hauptsitz, wird so ein optimales Sicherheits-Level erreicht. Wer sich für eine solche Mischform zwischen cloud- und premisebasierten Diensten entscheidet, sollte darauf achten, dass die verschiedenen Services Hand in Hand arbeiten und so eine Art Hybridlösung bilden.

Ein Ansprechpartner für alle Standorte

Eine weitere Dimension ist die geografische Vernetzung. Organisationen expandieren und wachsen oder lagern die Produktion ins Ausland aus. Für solche multinationalen Unternehmen stellt sich die Frage, wie die ganze Organisation am besten geschützt werden kann. Gerade die Aussenstellen sind logistisch sehr aufwändig zu sichern. Da das interne IT-Know-how meist am Hauptsitz angesiedelt ist, ist an den Aussenstellen häufig kein IT-Fachmann vor Ort. Viele Unternehmen setzen deshalb im Ausland auf lokale Serviceprovider, die den jeweiligen Standort «betreiben». Dies stellt zwar ein Grundniveau an Sicherheit sicher, bringt jedoch auch Schwierigkeiten mit sich. So verteilt sich die Expertise auf verschiedene Ansprechpartner, und nach einem Angriff gestaltet sich beispielsweise die Fehleranalyse schwieriger, da mehrere Anbieter das Problem eruieren müssen. Wer verschiedene Standorte mit Sicherheitslösungen ausstatten muss, sollte deshalb eine möglichst ganzheitliche Lösung anstreben. Ob eigene Betriebseinheit oder verschiedene Anbieter spielt dabei eine weniger entscheidende Rolle als klare Abläufe und Kompetenzverteilungen, eine gute Vernetzung und ein regelmässiger Wissensaustausch untereinander.

Sicherheit definiert sich laufend neu

Beim internationalen Austausch über Zeitzonen hinweg gilt es auch, die Erreichbarkeit der jeweils verantwortlichen Personen sicherzustellen. Ein gutes Sicherheitsmanagement regelt die Verantwortlichkeiten ohne Unterbrechung und bedingt eine vorausschauende Planung. Dies gilt für alle Massnahmen: vom Wartungsvertrag über die Gerätelizenz bis zur anstehenden Pensionierung des Security-Verantwortlichen. Unter Umständen wirkt sich also auch das Wissensmanagement oder die Nachfolgeplanung des Unternehmens auf die Sicherheit aus. Im Sicherheitsmanagement gilt es zu überlegen, welche Szenarien wann selbst abgedeckt werden können. Am besten dient das Worst-Case-Szenario als Ausgangslage, nämlich dass der Ausfall oder der Datenverlust ausserhalb der Geschäftszeiten stattfindet. Dies zeigt rasch auf, zu welchen Zeiten im Notfall keine kompetente Ansprechperson oder kein Back-up zur Verfügung stehen würden. Ziel muss am Ende sein, eine Rund-um-die-Uhr-Lösung zu gewährleisten. Security-Fachkräfte müssen sieben Tage die Woche während 24 Stunden verfügbar sein. Am besten sind sie immer «on duty», also aktiv bei der Arbeit, da Pikett-Lösungen die Problemlösung verzögern. Zudem wird bei Pikett-Lösungen häufig via Internet auf das System zugegriffen, was eine Sicherheitslücke darstellen kann. Wer diesen umfangreichen Betrieb nicht selbst sicherstellen und auf einen Partner setzen will, sollte zwingend eine Vereinbarung mit garantiertem Leistungsversprechen abschliessen. Nur dann bietet der externe Partner effektiv einen Mehrwert.

Kontinuierliche Aufgabe

Der Grundsatz, dass Sicherheit ein 7x24-Thema ist, gilt nicht nur gegen aussen, sondern auch für das Sicherheitsmanagement selbst. Es ist eine kontinuierliche Aufgabe, die nie beendet ist. Da die Sicherheit so eng an die ICT und damit an eine sehr dynamische Technologie gekoppelt ist, ist eine heute installierte Lösung bereits morgen nicht mehr aktuell. Sowohl potenzielle Angreifer als auch Anbieter von Sicherheitskomponenten finden im Wochenrhythmus neue Ansätze, um anzugreifen oder Angriffe zu verhindern. Genau diese Dynamik in der ICT-Security macht vielen Unternehmen das Leben schwer. Damit die Gesamtlösung stabil bleibt, muss die aktuelle Infrastruktur immer wieder überprüft und müssen neue Ansätze darin integriert werden. Dabei ist es nicht ganz einfach zu beurteilen, welche der neuen Ideen nachhaltig sind und auch zu den bestehenden Komponenten passen. Zudem erfordern auch die vielen durchzuführenden Updates hochqualifiziertes Personal und ein Verständnis der übergeordneten Zusammenhänge zu weiteren Systemen.

Konsistente Gesamtlösung entscheidend

Bei der Ausgestaltung des Sicherheitsmanagements gilt es also zahlreiche Punkte zu beachten. Je nach Branche oder spezifischen Firmenanforderungen können zu den erwähnten Aspekten weitere dazu kommen. Entscheidend ist auch die Priorisierung. Abhängig vom Geschäftsfeld, der Unternehmensgrösse, der Internationalität oder den Kundensegmenten müssen einzelne Aspekte höher gewichtet werden als andere. Wer bei diesem komplexen Prozess Unterstützung braucht, sollte sich an Anbieter von Managed Security Services wenden. Diese bieten neben Managed Services auch Beratungsleistungen und Analysen an. Zentral dabei ist, immer die Gesamtlösung im Auge zu behalten. Auch wenn nur Teilbereiche ausgelagert werden, müssen die Teillösungen aufeinander abgestimmt werden und zusammen funktionieren. Denn egal ob selbst machen oder auslagern: Wer sich in der ICT-Welt sicher bewegen will, muss den Blick immer aufs Ganze richten. <

Markus Kaegi ist Produktmanager im Bereich Managed Security Services für Geschäftskunden bei Swisscom.

Das Mobiltelefon als Security Token

Die Nutzung mobiler Geräte ist heute selbstverständlich. Die Mobilität stellt Unternehmen, Behörden und Serviceprovider vor neue Herausforderungen bezüglich der Authentisierung von Benutzern. Dabei ist die Lösung ganz einfach: die Kombination von Mobiltelefon und Security Token.

Wer hat das nicht schon erlebt? Der Security Token für das Log-in ins Firmennetzwerk oder zu einem Portal ist wieder einmal unauffindbar. Zudem sollte eine Banktransaktion sofort erledigt werden, der Token des Finanzinstituts liegt aber daheim in der Schreibtischschublade. In diesen Situationen wäre eine einfache und sichere Authentisierungsmöglichkeit gefragt.

Digitale Identität immer in der Tasche

Dies haben Telekommunikationsanbieter erkannt und machen das Mobiltelefon zum Authentisierungstoken. Dabei ist die SIM-Karte der sichere Träger der Verschlüsselung. Die notwendigen Funktionalitäten sind darin integriert. Um diese zu nutzen, müssen keine Apps installiert werden.

Digitale Identitäten lassen sich damit genauso eindeutig feststellen, wie Zugänge und Interaktionen effektiv schützen. Unterschiedliche Tokens gehören der Vergangenheit an, die Benutzer haben eine einzige Log-in-Lösung für die unterschiedlichsten Applikationen immer mit dabei.

Die Authentisierung mit dem Mobiltelefon eröffnet Serviceprovidern und Behörden neue Möglichkeiten bei der Interaktion mit Kunden, Partnern und Mitarbeitern. Mögliche Anwendungen sind zum Beispiel die Bestätigung von Transaktionen im E-Banking, das fälschungssichere Signieren von Dokumenten oder die Anmeldung bei Onlineportalen.

Autor: Adrian Humbel, Leiter Identity und Access Management, Swisscom

Das Mobiltelefon kann als Authentisierungstoken verwendet werden. Bild: Fotolia

Bild: Fotolia

Weltweit sicher Daten austauschen

Die Zusammenarbeit in einer globalisierten Welt erfolgt bevorzugt elektronisch übers Internet. Die möglichen Risiken werden dabei häufig unterschätzt. Denn nicht zuletzt mit dem Bekanntwerden der Spionagetätigkeiten der Geheimdienste weiss man um die Verletzlichkeit von elektronischen Daten.

Der physische Austausch von Daten birgt jedoch den Nachteil, dass die benötigten Unterlagen nicht überall und jederzeit zugänglich sind. In vielen Branchen und Geschäftsfällen ist dies aber von entscheidender Bedeutung.

Ein virtueller Hochsicherheitsraum für Besprechungen

Für den sicheren und weltweiten Austausch von sensitiven Daten bietet sich eine webbasierte Kollaborationsplattform an, ein sogenannter Swiss Trust Room. In diesem virtuellen Hochsicherheitsraum können Unternehmen ihre Kunden und Partner treffen, vertrauliche Daten austauschen und gemeinsam bearbeiten. Wo sich ein Sitzungsteilnehmer befindet, ist dabei unerheblich. Ein sicherer Authentifizierungsschlüssel erlaubt den Zutritt zum virtuellen Sitzungsraum.

Dabei durchläuft der Sitzungsteilnehmer eine mehrfach gesicherte Anmeldung Sicherheits- und Berechtigungsstufen können individuell vergeben werden. Dank der revisionssicheren Protokollierung aller Aktionen ist die Erfüllung von Compliance-Anforderungen garantiert. Die Daten sind physisch auf Servern in der Schweiz gespeichert und rund um die Uhr verfügbar.

Autor: Adrian Humbel, Leiter Identity und Access Management, Swisscom