Sicherheitsmanagement

Sicherheit ist keine Frage der Unternehmensgrösse

Geschäftsdaten sind das wertvollste Gut vieler Unternehmen. Um sie zu schützen, reichen physische Vorkehrungen längst nicht mehr aus. Das digitale Zeitalter erfordert ein systematisches Sicherheitsmanagement: von A wie Analyse bis Z wie Zertifizierungen.

› Markus Kaegi

Die eigene Sicherheit ist uns wichtig. Im Alltag haben wir teils bewusst, teils unbewusst Mechanismen entwickelt, die uns als Person und unser Eigentum schützen. Wir schliessen die Haustür ab, wenn wir zur Arbeit gehen, wir haben eine Haftpflichtversicherung und hängen ein zusätzliches Schloss an den Koffer, wenn wir in ferne Länder reisen. Viele Sicherheitsvorkehrungen haben wir selbst oder andere in unseren Alltag integriert, ohne dass wir sie noch als solche wahrnehmen. Der Airbag ist fix im Auto installiert und den Sicherheitsgurt legen wir automatisch vor der Abfahrt an.

Unvermeidbare Digitalisierung

In einem Unternehmen ist die Sicherheit nicht ganz so einfach zu regeln. Es gibt keinen Airbag, der sich bei Gefahr schützend um die Güter legt. Dass diese zudem häufig nicht greifbar sind, erschwert die Sache. Mit der Digitalisierung sind sensible Daten in vielen Unternehmen heute unsichtbar. Was früher in Ordnern verstaut wurde, ist heute auf Servern gespeichert. So geht schnell vergessen, dass in vielen Unternehmen grosse Teile des Kapitals in Form elektronischer Daten gelagert sind. Ob Adressen von Kunden oder Buchhaltungsabrechnungen – insbesondere in der Dienstleistungsbranche wird ein immer grösserer Teil des Geschäfts digital abgewickelt. Aber auch in der Industrie hat das digitale Zeitalter längst Einzug gehalten. Pläne und Prozesse werden elektronisch festgehalten, Maschinen mit Software-Programmen konzipiert und gesteuert. So gibt es immer weniger Firmen, die auf digitale Sicherheit verzichten können. Die meisten Unternehmen sind heute auf eine kontinuierlich funktionierende IT angewiesen – unabhängig davon, wie gross sie sind. Die Folgen, wenn ein Unternehmen nicht mehr auf die Geschäftsdaten zugreifen kann oder diese gar zerstört wurden, sind entsprechend schwerwiegend.

kurz & bündig

- Dem Sicherheitsmanagement der Firma sollte eine Risikoeinschätzung vorausgehen. Dabei müssen einerseits technische und prozessuale Fragen analysiert werden, andererseits sollten unternehmens- und branchenspezifische Vorgaben sowie gesetzliche Rahmenbedingungen mit berücksichtigt werden.
- Sobald die Analyse des Risikos abgeschlossen ist, stellt sich die Frage, wie man das Sicherheitsmanagement im Alltag tatsächlich umsetzt. Dies kann entweder mit oder ohne externe Unterstützung geschehen.
- Eine Möglichkeit, Sicherheit teilweise auszulagern, sind Managed Security Services.

Sicherheitsbedürfnis definieren

Trotz der offensichtlichen Bedeutung von Daten für ein Unternehmen ist in vielen Betrieben kein systematisches Sicherheitsmanagement etabliert. Besonders in kleinen und mittelgrossen Betrieben, wo die Ressourcen ohnehin knapp sind, fehlt dafür häufig die Zeit. Das kann gefährlich sein – denn Sicherheit ist keine Frage der Grösse. Auch kleinere Unternehmen können sehr hohe Anforderungen an die Sicherheit haben. Je nach Geschäftsfeld haben Sicherheitslücken unterschiedlich gravierende Folgen. Dem Sicherheitsmanagement von jeder Firma sollte deshalb eine Risikoeinschätzung vorausgehen. Dabei müssen einerseits technische und prozessuale Fragen analysiert werden, wie zum Beispiel: Welche Dienste sind wie wichtig? Was muss wann verfügbar

Bilder: Swisscom (Schweiz) AG

sein? Andererseits gibt es aber auch unternehmens- und branchenspezifische Vorgaben sowie gesetzliche Rahmenbedingungen, die das Sicherheitsmanagement beeinflussen. Gibt es interne Datenschutzrichtlinien? Wer braucht auf welche Daten Zugriff? Was ist gesetzlich vorgegeben? Diese sogenannten 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.

Updates schützen vor Angriffen

Ist die Risikoanalyse abgeschlossen, stellt sich die Frage, wie man das Sicherheitsmanagement im Alltag tatsächlich umsetzt. Dies kann entweder mit oder ohne externe Unterstützung geschehen. Firmen, die die Sicherheit selbst managen möchten, müssen vor allem darauf achten, dass die Infrastruktur stets auf dem aktuellsten Stand ist. Nur wer seine Hard- und Software mit regelmässigen Updates oder neuen Releases versorgt, ist auch gut geschützt. Veraltete Programme und Geräte laden potenzielle Täter geradezu ein, Daten zu hacken. Auch das lokale Netzwerk, das sogenannte Local Area Network (LAN), muss professionell verschlüsselt und so vor Angriffen geschützt werden. Mitarbeitende, die von unterwegs auf das Firmennetz zugreifen müssen, sollten dies nur über eine verschlüsselte Verbindung tun. Solche «Virtual Private Networks» (VPN) übertragen Daten sicher und binden mobile Arbeitsplätze oder das Home Office an das Firmennetzwerk an.

Sicheres Firmennetz

Sicherheit muss aber nicht zwingend selbst gemanagt, sondern kann auch als Dienstleistung eingekauft werden. Die Palette der Anbieter ist hier extrem breit und Unternehmen müssen sich entscheiden, wie viel sie tatsächlich abgeben möchten. Die Möglichkeiten reichen von einem externen Datenserver über das Abgeben des Sicherheitsmanagements bis hin zum kompletten Outsourcing. Je nach Ausprägung behält man mehr oder weniger Sicherheitsbestandteile in der eigenen Hand. Eine Möglichkeit, Sicherheit teilweise auszulagern, sind sogenannte Managed Security Services. Dabei werden einzelne Aspekte, beispielsweise das

Checkliste Sicherheitsprovider

- **Erfahrung:** Je länger ein Anbieter im Sicherheitsgeschäft tätig ist und je mehr Kunden er hat, umso grösser ist seine Erfahrung.
- **Qualitätsausweise:** Seriöse Anbieter haben glaubwürdige Referenzen und häufig auch spezifische Zertifizierungen in der Informationssicherheit (z. B. ISO-Zertifizierungen).
- **Dedizierte Betriebseinheit:** Der Anbieter sollte über eine Abteilung verfügen, die sich ausschliesslich Sicherheits-Services widmet.
- **Persönliche Beratung:** Ein persönliches Gespräch ist vor der Auslagerung sensitiver Geschäftsbereiche zwingend und ermöglicht, sich ein persönliches Bild vom Unternehmen zu machen.
- **Internationale Erfahrung:** Unternehmen mit Standorten in verschiedenen Ländern sollten auch auf Anbieter mit internationaler Erfahrung setzen.

VPN-Netzwerk, die Firewall oder die E-Mail-Sicherheit ausgelagert. Bei Letzterem kommen die E-Mails bereits gesäubert in das Firmennetzwerk, sodass schädliche Inhalte gar nicht erst Schaden anrichten können. Generelles Ziel ist immer, die Sicherheit und Stabilität des Firmennetzes zu gewährleisten und gegen Angriffe von aussen optimal zu schützen. Der Vorteil dieser Managed Services ist, dass man als Unternehmen Teilbereiche der Sicherheit weiterhin selbst managen kann und lediglich besonders schützenswerte Bereiche an Experten abgibt. Beim Outsourcing dagegen ist man von jeder Mitwirkungspflicht befreit und gibt die Verantwortung komplett ab.

Seriöse Dienstleister wählen

Unabhängig davon, welcher Anteil des Sicherheitsmanagements ausgelagert wird, sollte man bei der Wahl des Providers Vorsicht walten lassen. Durch die Diskussion rund um Datenspionage ist die Sicherheit für viele Anbieter auch zu einem guten, aber leider nicht immer seriösen Geschäft geworden. Dies macht die Wahl externer Dienstleister nicht einfacher. Einige Kriterien, beispielsweise internationale Zertifizierungen, können bei der Auswahl helfen (siehe Box). Trotz Auslagerung bleibt aber eines immer in der Eigenverantwortung der Unternehmer: Sie sollten stets wissen, wo sich die eigenen Daten befinden. In manchen Branchen ist klar vorgegeben, in welchen Ländern die Daten gelagert werden dürfen. Der Anbieter wiederum muss nachweisen können, wo die Daten gespeichert werden und wer darauf zugreifen kann. Der beste Schutz ist hier, sich beim Anbieter fundiert zu erkundigen und sich falls nötig juristisch beraten zu lassen. Denn der beste technische Schutz feit einen nicht vor rechtlichen Misstritten.

Fazit

Sicherheit lohnt sich: Für die meisten Unternehmen ist ein durchdachtes Sicherheitsmanagement heute Pflicht. Dieses beginnt mit einer Risikoanalyse und endet in der Entscheidung, die schützenden Massnahmen entweder selbst umzusetzen oder auszulagern. Egal, welchen Weg man dabei einschlägt: Wer Sicherheit explizit adressiert, hat schon viel gewonnen. «

Porträt

Markus Kaegi
Produktmanager Sicherheit Geschäftskunden

Markus Kaegi ist Produktmanager Sicherheit Geschäftskunden bei der Swisscom (Schweiz) AG. Swisscom bietet Geschäftskunden als führende Full-Service-Anbieterin zuverlässige Kommunikationslösungen. Die Unternehmen werden von der ICT-Beratung über die Integration bis zum Betrieb und Support begleitet. Bei Bedarf übernimmt Swisscom im Rahmen von Outsourcing-Verträgen auch die Gesamtverantwortung für die ICT-Infrastruktur von Geschäftskunden.

Kontakt

markus.kaegi@swisscom.com
www.swisscom.com