Datensicherheit intern oder extern abhandeln

In kleinen und mittleren Betrieben wird dem Thema Datensicherheit häufig ein unzureichender Stellenwert zugeschrieben. Daher sind gerade KMU oftmals Opfer von Hacker- sowie Spionageangriffen.

Armin Baumann

KMU verfügen, im Vergleich zu multinationalen Grosskonzernen, häufig nicht über millionenschwere IT-Budgets, um dieses wichtige Thema intern vollumfassend abhandeln und sauber aufgleisen zu können. Hierzu fehlen oft einfach schlichtweg die finanziellen Mittel. Eine Lagerung ihrer Daten bei einem externen Datacenter oder Cloud-Provider kann hier kostengünstig und effektiv Abhilfe schaffen. In meinem Beitrag in der Ausgabe 3/2019 mit dem Titel «Der Weg ist das Ziel in die Cloud für das KMU» bin ich auf die verschiedenen Punkte zur Cloud-Providerwahl eingegangen. Im vorliegenden Beitrag möchte ich einige weitere allgemeine Punkte beleuchten, welche KMU bei ihrer Entscheidung, ob sie ihre Datensicherheit intern oder extern verwalten lassen möchten, in Betracht ziehen sollten.

Relevante Aspekte zur Sicherheit der Firmendaten

Bei der Entscheidung, ob eine Firma die Sicherheit der Daten intern oder extern handhaben möchte, kommen einige relevante Aspekte zum Tragen. Unter anderem sollten folgende Punkte bei der Evaluierung und der entsprechenden Entscheidungsfindung miteinbezogen werden:

Physische Sicherheit

Eine angemessene physische Infrastruktur ist für eine sichere Datenhaltung unabdingbar. Wenn die Daten in-house auf den eigenen Rechnern bzw. Servern im Büro lagern, welche nicht hermetisch sowie mit den entsprechenden Sicherheitsvorkehrungen und erweiterten Zugangskontrollen vom Rest der Firma abgetrennt sind, besteht das potenzielle Risiko, dass jemand Externes sich Zugang zu der IT-Infrastruktur sowie den Daten verschaffen könnte, beispielsweise zwecks Industriespionage, Diebstahl oder Manipulation. Dies könnten unter anderem externe Firmen sein, welche bei der Firma Aufträge ausführen, oder aber auch mutwillige kriminelle Organisationen sowie Konkurrenten, welche zum Beispiel mittels Social Engineering vortäuschen, ein Mitarbeiter der Firma zu sein, und sich somit unrechtmässig Zugang zu den Räumlichkeiten verschaffen.
Um diese und weitere damit verbundene Risiken effektiv einzudämmen, empfiehlt es sich, die Server, statt in-house, in einem professionellen Datacenter zu betreiben. Datacenter sind so konzipiert, dass das unrechtmässige Eintreten Fremder effektiv vermieden wird. Durch die starken Sicherheitsvorkehrungen ist es nahezu ausgeschlossen, dass Unbefugte sich Zutritt zum Datacenter verschaffen können. In Datacenters mit einem hohen Sicherheitsstandard kommt in der Regel die sogenannte 3-Faktor-Authentifizierung zum Einsatz: Hierbei erhalten zutrittsberechtigte Personen ein Badge mit PIN, mit welchem die äussere Schleusentür zum Datacenter geöffnet werden kann. Anschliessend werden mittels eines biometrischen Scanners die Handvenen der zutrittsberechtigten Person ausgelesen und mit dem vorliegenden Datenbankeintrag des Überwachungssystems abgeglichen. Erst nach erfolgreicher 3-Faktor-Authentifizierung öffnet sich die innere Schleusentür und die Person kann eintreten. Innerhalb des Datacenters sind die verschiedenen Racks wiederum in viele verschiedene Räume aufgeteilt, welche wiederum erst nach erfolgreicher Legitimation mit Badge und PIN geöffnet werden können. Des Weiteren sind alle Schleusen sowie das gesamte Datacenter mit Kameras und zusätzlichen Sensoren ausgestattet. Eine Unregelmässigkeit, wie zum Beispiel das mutwillige Eindringen in die Schleuse, würde daher vom System sofort identifiziert und entsprechende Gegenmassnahmen könnten vom Sicherheitspersonal eingeleitet werden.

Unterbruchfreier Betrieb und Redundanz

Für Firmen ist es von höchster Priorität, Ausfallsicherheit für ihre IT-Systeme und Daten zu gewährleisten. Nichts ist ärgerlicher, als wenn ein Systemausfall plötzlich das gesamte Netzwerk lahmlegt und wichtige Kundenaufträge nicht mehr speditiv und fristgemäss ausgeführt werden können. Dies führt im schlimmsten Fall zu Kundenverlust und hohen finanziellen Einbussen. Die Auslagerung der internen IT-Systeme in ein Datacenter bzw. zu einem Cloud-Provider schafft hier Abhilfe: Mittels Service Level Agreements (SLAs) wird ein unterbruchfreier Betrieb für die Firma sichergestellt. Sie kann von jedem Ort der Welt und zu jedem Zeitpunkt auf deren Daten zugreifen – 24/7/365.
Im professionellen Datacenter sind die Strom- und Internetanbindung redundant aufgebaut, sodass bei einem Ausfall eines Anbieters sofort ein alternativer Internetprovider bzw. Batterien und dieselbetriebene Notstromaggregate anspringen und einen Unterbruch effektiv verhindern.
Bei vielen Firmen ist die konstante Aufrechterhaltung des Geschäftsbetriebes Teil eines sogenannten Business Continuity Plans (BCP). Sollte die Firma sich entscheiden, die primäre IT-Infrastruktur in-house zu betreiben, so ist es auch möglich, im Rahmen der Disaster-Recovery-Massnahmen eine Redundanz im externen Datacenter aufzubauen, welche im Falle eines Ausfalls der primären Systeme den laufenden Betrieb aufrechterhält. In diesem Punkt gibt es sogar bestimmte Datacenter, welche sich komplett nur auf diesen Bereich spezialisiert haben.
Des Weiteren bieten Datacenter sowie Cloud-Provider eine hervorragende Möglichkeit, Backups der Firmendaten sowie virtuellen Maschinen zu erstellen, welche darüber hinaus noch gespiegelt werden können. Dies bedeutet, dass die Systeme redundant betrieben werden, sodass sogar im Falle eines einzelnen Serverausfalls der Betrieb ohne Unterbruch und ohne Datenverlust weiterläuft. Dies geschieht mittels Zuschaltens eines Backup-Servers innert Millisekunden, welcher den reibungslosen Betrieb sicherstellt.

Umgebungskonditionen für die Hardware

Falls die Firma intern eigene Server betreibt, ist zu beachten, dass die sensible Hardware anfällig ist für Schwankungen der äusseren Umstände. Im Datacenter werden Temperatur und Luftfeuchtigkeit mittels umfangreicher Kühlung und weiteren Equipments stets konstant auf Idealniveau gehalten, sodass die Langlebigkeit der Hardware gewährleistet wird.

Cyber Security und Updates
Die Firma möchte sich keine Gedanken mehr machen müssen um allfällige Hackerangriffe und Virenbefall auf ihrer IT-Infrastruktur. Bei einem externen Hosting kümmern sich die Fachkräfte der Datacenter und Cloud-Provider um alle relevanten Aspekte der Cyber Security und halten die Systeme stets up-to-date.
Zahlreiche Schutzmechanismen können bei Bedarf aufgeschaltet werden, wie beispielsweise Anti-Virenscanner, die Verschlüsselung der Daten, die Abwehr von Denial-of-Service Attacken (DDoS), der Einsatz von Web Application Firewalls, Intrusion Detection und Prevention, sowie viele weitere Services.

Know-how, Professionalität und Kosten
Eine interne IT-Abteilung samt Infrastruktur aufzubauen, erfordert starke finanzielle, fachliche sowie personelle Ressourcen.
Extern wird die Lagerung im Regelfall professionell abgehandelt. Bei Datacenters und Cloud-Providern sollten man darauf achten, dass diese über die ISO-27001-Zertifizierung verfügen, welche dem Betreiber einen professionellen Umgang unter anderem in Bezug auf relevante Aspekte rund um die Datensicherheit attestiert.
Kostenmässig ist es viel günstiger, eine hochsichere IT-Infrastruktur in einem externen Datacenter bzw. Cloud-Provider aufzubauen als diese intern zu betreiben, da die Fix- sowie laufenden Kosten auf viele verschiedene Kunden umgelegt werden können. Nicht zu vernachlässigen sind die Kosten für die Schulung der IT-Mitarbeiter, welche stets auf dem neuesten Stand der Datensicherheit gehalten werden sollten. Einer der grössten Risikofaktoren bei der Datensicherheit ist immer noch der Mitarbeiter selbst. Insgesamt kann man durch eine gänzliche oder teilweise Auslagerung der IT ihre Kapitalbindungskosten deutlich senken.
Zudem kann sich die Firma bei einer Auslagerung voll und ganz auf das Kerngeschäft konzentrieren und damit deren Agilität steigern.

Regulatorische Aspekte
Abschliessend ist noch darauf hinzuweisen, dass für einige Schweizer Firmen besondere regulatorische Anforderungen in Bezug auf das IT-Outsourcing gelten. So müssen Treuhänder und Banken beispielsweise ihre Daten zwingend in der Schweiz lagern sowie weitere Anforderungen sicherstellen, um sich FINMA-konform zu verhalten. Dies stellt jedoch für eine Auslagerung kein Hindernis dar, da es einige Datacenter in der Schweiz gibt, welche diese FINMA-Anforderungen vollumfassend erfüllen.

Fazit

Falls die Firma in-house über eine angemessene Infrastruktur zur sicheren Datenverwahrung sowie über die entsprechenden fachlichen und finanziellen Ressourcen verfügt, könnte eine Lagerung in-house für die Firma in Betracht kommen. Ansonsten lohnt sich die Überlegung, Teile oder gar die gesamte IT-Infrastruktur an einen externen professionellen Dienstleister im Datacenter bzw. Cloud-Bereich auszulagern.
Bei einer gewöhnlichen Büro-Infrastruktur muss man sich im Hinblick auf die Datensicherheit sinnbildlich die Frage stellen, ob man seine Goldvreneli lieber zu Hause unter dem Kopfkissen oder doch lieber im sicheren Bankschliessfach lagern möchte. Die Entscheidung liegt bei jedem selbst. ■