Informationssicherheit in der Ära des Cloud Computing

Digitalisierung und Mobilität verursachen neue Gefahren, exponieren sensible Unternehmensdaten und stellen für die Unternehmen eine grosse Herausforderung dar. Auch das Verhalten der Mitarbeitenden und der Benutzer hat sich massiv verändert. Diese sind immer vernetzter und verfügen oft nur über ein geringes oder gar kein Sicherheitsbewusstsein. Für Systemadministratoren gilt es, die Balance zwischen «Sicherheit und Bedienbarkeit» zu finden. Keine einfache Aufgabe.

DER AUTOR

Wolfgang Sidler
Inhaber, Sidler Information Security

Mobile Kommunikation ist für Hacker zum wichtigen Ansatzpunkt geworden, um an sensitive geschäftliche und persönliche Informationen zu gelangen. Denn an keiner anderen Stelle kann man so schnell so viele persönliche und wichtige Informationen abgreifen. Wenn ein Smartphone gehackt wird, merkt das der Benutzer meistens nicht. Und normalerweise ist auch keine IT-Abteilung vor Ort, um die Sicherheit der Datenverbindung zu überprüfen. Kommt hinzu, dass ein Smartphone heute gleichzeitig im Mobilfunknetz und über WLAN im firmeneigenen Netzwerk eingeloggt sein kann. Über diese «Funkbrücke» werden abgeschottet geglaubte Bereiche in einem Unternehmen plötzlich von aussen mit schnellen Mobilfunk-Zugängen erreichbar. Mit dem neuen Datenschutzgesetz (2018) werden Unternehmen in Zukunft mehr als heute in die Pflicht genommen. Sie müssen dafür sorgen, dass Daten trotz Mobile-Boom und Cloud Computing gesetzeskonform gesichert sind.

> Bei Verstössen gegen das neue Datenschutzgesetz drohen empfindliche Bussen bis 500 000 Franken.

Neues Datenschutzgesetz und hohe Bussen

Unternehmen ist dringend zu empfehlen, sich bereits jetzt auf das neue Schweizerische Datenschutzgesetz einzustellen und die notwendigen Vorbereitungsarbeiten zur Sicherstellung der künftigen Datenschutzkonformität an die Hand zu nehmen. Dazu gehören etwa die Analyse der Datenbearbeitungsprozesse und der damit verbundenen Risiken sowie die bestehenden internen Richtlinien und Weisungen sowie der Verträge mit Dritten. Unternehmen drohen empfindliche Bussen bis 500 000 Franken, falls sie gegen die entsprechenden Rechtsnormen verstossen, etwa wenn sie es unterlassen, Betroffene zu informieren, keine angemessenen Massnahmen zur Gewährleistung der Datensicherheit treffen, die Datenschutz-Folgenabschätzung oder die Dokumentation der Datenbearbeitung versäumen. Zudem müssen Datenschutz-Vorfälle neu dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gemeldet werden.

Der Hype um die Clouds verschärft das Thema. Nutzer wissen in der Public Cloud bei Amazon, Apple, Google, Microsoft und Co. nicht, auf welchen Systemen, in welchem Rechenzentrum und in welchem Land der Provider die Nutzerdaten speichert. In den entsprechenden Service Level Agreements (SLA) kann zum Beispiel der folgende Passus stehen «Unter bestimmten Umständen kann (Name des Providers) Daten ohne Ihre vorherige Zustimmung weitergeben. Dazu gehört die Befolgung rechtlicher Anforderungen». Für ein rechtlich abgesichertes Cloud-Szenario sind dedizierte Anforderungen an den Cloud-Provider sowie wasserdichte Verträge ein Muss.

Fazit

Die Bedrohungen und der damit verbundene Datenabfluss sind Realität. Durch die wachsende Komplexität und Vernetzung der IT-Systeme und die Globalisierung ergeben sich neue Herausforderungen an den Schutz der Daten und Informationen. Schützen Sie Ihr Firmen-Know-how mit Ihren Möglichkeiten und lassen Sie sich, wenn nötig, von einem Sicherheitsspezialisten beraten.

WIE KÖNNEN SIE SICH SCHÜTZEN?

- Sensibilisieren Sie alle Mitarbeitenden in Bezug auf die Informationssicherheit.
- Beginnen Sie, ein Informationssicherheits-Managementsystem (ISMS) aufzubauen (Notfall- und Krisenmanagement-Konzept, ein Risiko-Management-Konzept, eine Cloud-Strategie, eine Mobile-Device-Strategie etc.), das Sie später gemäss ISO 27001 zertifizieren lassen können.
- Erstellen Sie eine IT-Nutzungsweisung, etwa im Umgang mit E-Mails und Internet, Aktenvernichtung oder USB-Sticks.
- Führen Sie Security-Audits und Schwachstellen-Scans durch, um mögliche Schwachstellen (technischer wie auch organisatorischer Natur) im Unternehmen zu finden und zu beheben.
- Führen Sie mithilfe eines Sicherheitsspezialisten eine Risikoanalyse in Ihrem Unternehmen durch. Dabei geht es darum, die Unternehmenswerte zu identifizieren, damit die Risiken und Gefahren explizit richtig eingeschätzt werden können. Ermitteln Sie die möglichen Szenarien mit den entsprechenden Gegenmassnahmen.