Firmen und Freie Berufe ■ Cyberversicherung

Cloudnutzung und Cyberversicherung.

Immer mehr Unternehmen und Kanzleien lagern Bereiche ihrer Datenverarbeitung in eine Cloud (z. B. AWS (Amazon Web Services), T-Systems der deutschen Telekom, Microsoft, DATEV) aus. Das kann in unterschiedlichem Umfang geschehen:

- Auslagerung von Datenbeständen oder Back-ups
- Datenbestände und wesentliche Verarbeitungselemente
- Gesamte Datenverarbeitung und elektronische Kommunikation über die Cloud (z. B. in Form eines virtuellen Desktops)

Der Cloud-Dienstleister nutzt dabei üblicherweise alle technischen und organisatorischen Möglichkeiten, um seine Systeme und die dort gespeicherten Daten abzusichern. Dazu gehört ein sicherer Zugang z. B. über eine Zwei-Faktor-Authentifizierung oder sogar eine abgesicherte Verbindung (z. B. Virtual-Private-Network-Tunnel).

Warum kann hier ein Cyber-Angriff trotzdem erfolgreich sein?
Angriffspunkt ist in den wenigsten Fällen der Cloud-Dienstleister. Dieser ist meist sehr gut abgesichert. Die Schwachstelle ist das eigene IT-System (Clients, E-Mail-Server, Domain-Controller, Fileshare usw.) des Nutzers bzw. die eigene Organisation. Hier gelingt es oft nicht, die gleichen hohen Sicherheitsstandards der Cloud zu halten.

Wenn es einem Angreifer gelingt, einen Arbeitsplatz des Unternehmens oder der Kanzlei (von welchem regelmäßig auf die Cloud zugegriffen wird) zu kompromittieren, kann er hier Passwörter für den Cloud-Zugang aus dem Speicher (Cache) auslesen oder er installiert einen Keylogger, mit dem er das Passwort des Nutzers (User) mitschneidet, sobald dieser sich beim nächsten Mal in der Cloud anmeldet. Mit gestohlenen Zugangsdaten kann der Angreifer wie ein legitimer User agieren, ohne dass der Cloud-Dienstleister eine Chance hätte, die fehlende Legitimation zu erkennen.

Doch nicht nur die sensiblen Kundendaten auf den externen Servern sind gefährdet. Daneben gibt es noch eigene schützenswerte Daten (Abrechnungen, Mitarbeiterdaten, Löhne, Sozialversicherung etc.), welche in vielen Fällen lokal gespeichert werden. Bei einem Angriff können diese z. B. leicht Opfer eines Verschlüsselungstrojaners werden. Im schlimmsten Fall werden die Daten, auch wenn sie auf einem Server eines Dienstleisters liegen, ebenfalls befallen.

Zudem darf der menschliche Faktor nicht vernachlässigt werden, denn Datenverarbeitung und elektronische Kommunikation führen häufig zu einem Kompromiss zwischen Praktikabilität und Sicherheit. Angefangen von zu einfachen oder auf dem Notizzettel am Bildschirm notierten Kennwörtern über den nicht gesperrten Bildschirm beim Verlassen des Arbeitsplatzes bis hin zum Einstecken eines verseuchten USB-Sticks – für viele Risiken muss ein entsprechendes Bewusstsein bei den Mitarbeitern erst geschaffen werden. Auch der dauerhaft verbundene Verifizierungsschlüssel (Token) stellt ein potenzielles Risiko dar. Dann reicht ein ausgespähtes Passwort, um auch eine Zwei-Faktor-Authentifizierung zu überwinden.

Leicht zu übersehen ist auch ein Vertrauensschaden durch das Handeln eines Innentäters. Ein Mitarbeiter mit krimineller Energie kann seinen berechtigten Zugang zum Schaden seines Arbeitgebers missbrauchen und z. B. aus Wut über eine Abmahnung oder Kündigung Daten aus der Cloud stehlen oder die IT-Systeme des Arbeitgebers lahmlegen.

Fazit:
Die größtmögliche Sicherheit bei Datenverarbeitung und Kommunikation ergibt sich für den Nutzer nur, wenn ein hohes Maß an technischer Sicherheit mit einem hohen Risikobewusstsein verbunden wird und durch eine Cyberversicherung mit passgenauem Service (Incident-Response-Management) vervollständigt wird.

Eine Cyberversicherung ist also immer eine notwendige Komponente in einem umfassenden IT-Risikomanagement.

HDI Vertriebs AG
HDI-Platz 1
30659 Hannover
www.hdi.de/cyberversicherung

7003041167-201807