Cybersicherheit – Risiken, Massnahmen und Vorteile der OBT Swiss Cloud

Cyberattacken nehmen laufend zu. Nicht nur Unternehmen und Organisationen sind davon betroffen, sondern auch Gemeinden, Städte und öffentliche Institutionen. Die Zeiten, in denen ein Virenscanner und eine Firewall reichten, um sich mit einem sicheren Gefühl zurückzulehnen, sind längst vorbei. Security ist zu einem zentralen Thema der IT geworden – der Artikel zeigt auf, wie OBT seine Kunden dabei unterstützt.

Roman Grob
Leiter Markt Gemeinden und Städte
Zürich

Cyberattacken sind gezielte Angriffe auf einzelne Rechner und ganze computergestützte Informationssysteme, Infrastrukturen und Netzwerke. Dabei werden Daten manipuliert, gestohlen, verschlüsselt oder ganz gelöscht. Die Folgen für die betroffenen Organisationen sind beeinträchtigte oder ausfallende Services, Rufschädigung und im schlimmsten Fall auch die Verhinderung jeder operativen Geschäftstätigkeit – mit entsprechenden finanziellen Folgen.

Cyberattacken sind vielfältig

Es gibt viele verschiedene Wege, ein IT-System zu attackieren und Schaden anzurichten.

So zum Beispiel:

- Ransomware (Erpressungstrojaner) und Kryptoattacken: Eine eingeschleuste Schadsoftware verschlüsselt sämtliche Daten; erst gegen ein hohes Lösegeld werden sie wieder freigegeben.
- DDoS: Durch eine riesige Anzahl von Aufrufen/Anfragen werden Webseiten bzw. Internetdienste überlastet und lahmgelegt.
- E-Banking-Schadsoftware, E-Banking-Trojaner: Elektronische Banktransaktionen werden manipuliert bzw. Zahlungen an die Konten von Cyberkriminellen ausgelöst.
- Phishing- und Spear-Phishing-Angriffe: Angreifer beschaffen sich via E-Mail oder Telefon Zugangsdaten (Login und Passwort), um Daten abzugreifen oder Malware zu installieren.
- Social Engineering: Ausnutzen der «Schwachstelle Mensch», um an geheime Informationen oder Geldbeträge zu gelangen (Rechnungsmanipulationsbetrug, Scheckbetrug, CEO-Betrug etc.).

Die Auswirkungen dieser Angriffe sind unterschiedlich. Temporäre Einschränkungen der Verfügbarkeit oder der Verlust kleinerer Geldbeträge mögen zu verschmerzen sein; grosse kriminelle Attacken hingegen können die Betroffenen in schwerwiegende oder gar existenzbedrohende Situationen bringen.

OBT Swiss Cloud bietet hohe Sicherheit

Die Auslagerung der IT in eine sichere, verlässliche Cloudlösung kann die Abwehr vieler Bedrohungen wesentlich erleichtern. Allerdings weckt der Begriff «Cloud» bei vielen Leuten noch die irrige Vorstellung, dass Daten irgendwohin in eine schwer fassbare Wolke verschoben werden. Richtig ist: Die Cloud ist ein hochsicheres Rechenzentrum, in das Systeme und Daten ausgelagert werden. Das bietet auch entscheidende Vorteile bei der Arbeit im Home-Office oder unterwegs mit Mobilgeräten.

Die Rechenzentren der OBT Swiss Cloud sind besser gesichert als die meisten unternehmens- oder organisationsinternen Serverräume. Sie sind mehrfach

geschützt gegen Bedrohungen aller Art – auch gegen Elementarereignisse – und werden rund um die Uhr bewacht. Natürlich liegen sie in der Schweiz und unterliegen Schweizer Rechtsbestimmungen.

Die OBT Lösung: redundant, zertifiziert und preiswert

Alle Daten und Services werden als georedundante Lösung, das heisst in zwei redundanten Rechenzentren gleichzeitig, betrieben. So kann der Kunde selbst beim kompletten Ausfall eines ganzen Rechenzentrums ohne Unterbruch weiterarbeiten. Selbstverständlich sind alle Daten mit einer hochmodernen Back-Up-Lösung in mehreren Generationen auf unterschiedlichen Medien gesichert. Zudem betreibt OBT ein Informationssicherheits-Managementsystem, das anspruchsvolle technische und organisatorische Massnahmen vorgibt und ISO/IEC27001-zertifiziert ist.

Zu den weiteren Sicherheitsmassnahmen zählen unter anderem die Gliederung des Rechenzentrums in verschiedenen Sicherheitszonen, die Protokollierung aller Zugriffe und der durchgeführten Änderungen, weltweit agierende Services zur Erkennung von Bedrohungen und zeitnahes Aufspielen der neuesten Security-Patches, Viren- und Malwareschutz, professionelle Datensicherung und -wiederherstellung, Verschlüsselung sowie laufende Schulungen der Mitarbeitenden vor Ort.

Der Aufbau und der Betrieb einer sicheren Umgebung auf dem Niveau der OBT Swiss Cloud sind mit einem grossen finanziellen, personellen und organisatorischen Aufwand verbunden, der für einzelne Unternehmen oder öffentliche Verwaltungen meist nicht ohne Weiteres zu stemmen ist. Als grosser Cloud-Provider können wir die Kosten auf viele Kunden verteilen und uns ständig und intensiv mit Sicherheitsaspekten beschäftigen. Dadurch können sich unsere Kunden beruhigt auf ihre Hauptaufgaben konzentrieren.

Umgang mit «Schwachstelle Mensch»

Auch wenn eine privatwirtschaftliche Firma, ein Gemeinwesen oder ein öffentlich-rechtliches Unternehmen seine IT-Dienste ganz oder teilweise in die OBT Swiss Cloud auslagert, muss es sich grundsätzliche strategische Überlegungen zur IT-Security machen und diese auch kompromisslos umsetzen. Denn Sicherheit beginnt bei jedem eingesetzten Gerät und an jedem Arbeitsplatz. Die «Schwachstelle Mensch» muss durch die Sensibilisierung und die Schulung der Mitarbeitenden so weit wie möglich eliminiert werden.

Je sensitiver die Daten sind und je schwerwiegender die Konsequenzen eines möglichen Security-Vorfalls sein können, desto mehr lohnt sich der Abschluss einer Cyberversicherung. Sie deckt Schäden im Zusammenhang mit Hackerangriffen oder Attacken von Cyberkriminellen ab, zum Beispiel Ertragsausfälle, Wiederherstellung der IT-Infrastruktur, Krisenmanagement, Verhandlung mit Kriminellen und je nach Deckungsumfang auch weitere Leistungen wie Sicherheitsberichte, Handlungsempfehlungen, Prävention und Schulungen, Awareness-Trainings und Tests für Mitarbeitende.

FAZIT

Rund 40% der Schweizer KMU sowie viele Grossunternehmen, Gemeinden und Service-Public-Anbieter sind schon Opfer von Cyberkriminalität geworden. Das zeigt: Cybersicherheit betrifft alle, und niemand kann sich darauf verlassen, dass es ihn nicht treffen kann. Die OBT Swiss Cloud kann einen Beitrag zur Sicherheit leisten. Sie basiert auf hervorragend gesicherten Rechenzentren in der Schweiz. Ihr Informationssicherheits-Managementsystem ist nach den strengen Anforderungen von ISO/IEC27001 zertifiziert; zudem deckt eine umfassende Cyberversicherung auch allfällige Schäden auf Kundenseite ab, die im unwahrscheinlichen Fall einer erfolgreichen Cyberattacke durch Fehler von OBT entstehen könnten.