DATENSICHERHEIT IM UNTERNEHMEN

5-Punkte-Checkliste

In Zeiten der Digitalisierung gewinnt der Schutz von Daten enorm an Bedeutung. Das betrifft sowohl Kundendaten als auch die für digitalisierte Geschäftsprozesse erforderlichen Daten. Daten - das heutzutage wertvollste Gut für viele Unternehmen - müssen permanent verfügbar sein, aber gleichzeitig vor Manipulationen und technischen Defekten geschützt werden und eine Vertraulichkeit erfüllen, die den gesetzlichen Datenschutzvorgaben entspricht.

Das stellt IT-Abteilungen von E-Commerce-Firmen und digitalen Dienstleistungsunternehmen vor viele Herausforderungen und Fragen: Wie lässt sich die Datensicherheit gewährleisten? Welche technischen und organisatorischen Maßnahmen sind zu ergreifen? Sind alle Punkte der Datenschutz-Grundverordnung (DSGVO) erfüllt? Die folgende Checkliste soll Ihnen helfen, den Stand der Datensicherheit in Ihrem Unternehmen zu prüfen. Dabei werden die fünf wichtigsten Aspekte beleuchtet.

Physische Datensicherheit im Rechenzentrum

TIPP #1

Sofern Sie Ihr Datacenter Inhouse betreiben, sind folgende Punkte sicherheitsrelevant:

- Klimatisierung und Brandschutz (Kühlung, Schutzvorrichtungen, Früherkennungssysteme, Brandlöschanlage)
- Stromversorgung und USV (Umschaltung auf Notstrombetrieb, Blitzschlagsicherung)
- Gebäudeschutz (Zutrittsregelungen und -kontrollen, Überwachung, Meldeanlagen)
- Kommunikationsanbindung (Glasfaserverkabelung, Kommunikationssysteme)

Jeder dieser Punkte sollte in einem ganzheitlichen Sicherheitskonzept, inklusive Notfallpläne, Redundanzsysteme und Störungsmanagement, Berücksichtigung finden. Nur so lässt sich im Fall des Falles ein unterbrechungsfreier Betrieb gewährleisten.

Schutzmaßnahmen gegen Datenmanipulation

TIPP #2

Hackerangriffe, Distributed-Denial-of-Service-Attacken (DDoS) und Viren nehmen im Zuge der digitalen Transformation zu. Datendiebstahl oder -manipulation sowie die Nichtverfügbarkeit von Internetdiensten, Echtzeitanwendungen und Multi-media-Dienstleistungen haben für die betroffenen Unternehmen verheerende Konsequenzen.

Hohe Umsatzausfälle, verlorenes Kundenvertrauen und die Haftung für Schäden können existenzgefährdend sein. Der Angriffsprävention und Cybersicherheit kommen somit ein hoher Stellenwert zu.

Wie steht es um folgende Maßnahmen in Ihrem Unternehmen?

- Firewall, Malware- und Virenschutz
- Abwehr-Monitoring
- Abwehr-Technologien inklusive Hardware-Applikationen
- Gegenmaßnahmen bei Attacken
- Redundanzsysteme als Ausweichmöglichkeit im Angriffsfall

Management der IT-Systemlandschaft

TIPP #3

Informationstechnologie will gepfl egt und gewartet werden. Regelmäßige Updates und Patches, Datensicherungen und Backups, Störungsanalyse und -behebung - all das sind originäre Aufgaben der IT-Wartung.

Hinzu kommt die Planung, ein System zukunftssicher aufzusetzen und bei Bedarf schnell skalieren zu können. Hardwareausfälle und Softwarefehler behindern nicht nur Arbeitsprozesse, sondern gefährden auch die Datensicherheit.

Sicherheit von Cloud Services und Server

TIPP #4

Haben Sie Services, Anwendungen und Speicher in der Cloud, liegt das Thema Datensicherheit weitgehend nicht mehr in Ihrer Zuständigkeit. Das entbindet Unternehmen jedoch nicht von der Verantwortung, die Anbieter zu prüfen und so Sicherheitsrisiken zu minimieren.

Das beginnt beim Check der Datenschutzregelungen am Firmensitz des Anbieters (entsprechen sie der DSGVO?) und dem physischen Standort seiner Server und reicht bis zu Zugriffsrechten im Dienstleistungsvertrag.

Prüfen Sie außerdem:

- wie die Zugriffskontrolle aussieht,
- ob die Verschlüsselung bei der Datenübertragung ausreicht,
- ob eine zusätzliche Datensicherung außerhalb der Cloud erfolgt,
- und wie der Umgang mit den Daten nach Vertragsende geregelt ist.

Anforderungen der DSGVO

TIPP #5

Neben dem physischen Schutz der Daten ist ein sicherer Umgang mit ihnen zu beachten. Die DSGVO gibt hier im Hinblick auf persönliche Daten klare Richtlinien vor, die in Unternehmen umgesetzt werden müssen.

Dazu gehören der Schutz vor unbefugten Zugriffen, Dokumentationspfl ichten bezüglich der Datenverarbeitung, eine saubere Datentrennung, das Vorhandensein eines Datenschutzbeauftragten und vieles mehr.

Konkret sind folgende Punkte wichtig:

- Rollen- und Berechtigungskonzept
- Benutzerauthentifizierung
- Compliance
- Datenverschlüsselung
- Aufbewahrung von Datenträgern

Datensicherheit ist ein Fall für Spezialisten

FAZIT

Angesichts der Fülle und Komplexität an technischen und strukturellen Sicherheitsmaßnahmen entscheiden sich immer mehr Unternehmen für das Auslagern ihrer Daten in ein externes Rechenzentrum. Das senkt die Betriebs- und Kapitalkosten und spart Platz.

Als Premium-Anbieter für Colocation und Housing gibt firstcolo Ihren IT-Systemen ein sicheres Zuhause. Die firstcolo Datacenters-Experten sorgen dafür, dass Sie an alle Punkte der Checkliste einen Haken setzen können und Ihre Daten hochverfügbar, vertraulich und integer bleiben.

Und das mit Brief und Siegel, denn der TÜV hat das firstcolo Rechenzentrum nach der Norm ISO/IEC 27001:2013 zertifiziert.

firstcolo

firstcolo ist Ihr Partner für Datacenter und Managed Services

Über firstcolo

Mit den Kernkompetenzen Colocation- und Cloud-Services, Managed Services und DDoS-Schutz betreibt firstcolo als IT-Infrastrukturanbieter Hochverfügbarkeits-Rechenzentren an deutschen und europäischen Server-Standorten. firstcolo bietet sachverwandte IT-Dienstleistungen für Mittelstand und Großkunden an. Die IT-Systeme zahlreicher Branchen bekommen bei firstcolo ein sicheres, kostengünstiges und zeitgemäßes Zuhause. Zum Kundenstamm gehören vornehmlich Unternehmen mit überdurchschnittlichen Ansprüchen an Servicequalität und IT-Sicherheit.

First call us – firstcolo ist Ihr Assistent für Datensicherheit. Weitere Informationen zu unserem hochmodernen Rechenzentrum erhalten Sie unter www.firstcolo.net.