Sicherer Datenaustausch – eine spezifische Herausforderung in der Prozessoptimierung

Markus Richter, November 2022

Mit der fortschreitenden Digitalisierung werden in den Unternehmen immer mehr Daten erzeugt, gespeichert und sowohl intern als auch mit externen Partnern ausgetauscht. Seit Beginn der Pandemie und der damit verbundenen Verlagerung vieler Tätigkeiten ins Homeoffice steigt die digitale Kommunikation exponentiell, was neue Herausforderungen an die Datensicherheit stellt.

Sicherheitsrisiken durch digitale Prozesse

Eine Welt ohne E-Mail, Videokonferenzen, Cloud-Speichern und einem Austausch von zum Teil hochsensiblen Daten ist nicht mehr vorstellbar. Jedoch birgt jede Schnittstelle die Gefahr von unerwünschten Zugriffen von außen. Umso erstaunlicher ist es, dass laut einer Studie des deutschen Bundesministeriums des Inneren in 2020 nur etwa die Hälfte der deutschen Unternehmen Sicherheitsvorkehrungen für den Versand von Nachrichten getroffen hat, nur jedes fünfte Unternehmen auf verschlüsselte Nachrichten achtet und gerade mal 19 Prozent einen Passwortschutz für die Datenübertragung verwenden (veröffentlicht im DsiN-Praxisreport Mittelstand 2020)

Viele kleine Schritte erhöhen die Datensicherheit

Das größte Sicherheitsrisiko geht nach wie vor von E-Mail-Postfächern aus. Hier kann aber bereits mit wenig Aufwand im E-Mail-Programm selbst, beispielsweise durch das Aktivieren der Transportverschlüsselung, effektive Abhilfe geschaffen werden. Eine weitere Verschlüsselungsmethode der E-Mail-Kommunikation ist die sogenannte Ende-zu-Ende Verschlüsselung, für die man lediglich ein digitales Zertifikat benötigt, was nur wenige Euro pro Jahr kostet.

Sehr weit verbreitet ist auch der Datenaustausch über externe Datenträger, wie z.B. USB-Sticks und externe Festplatten. Da hier in den meisten Fällen keinerlei Prüfung der Daten vorangeht, stellt diese Vorgehensweise ebenfalls eine sehr große Gefahr für das Netzwerk dar.

Am sinnvollsten ist es, auf den Austausch von Daten per E-Mail oder über externe Datenträger gänzlich zu verzichten und dafür dedizierte Datenaustausch-Plattformen oder -Server zu nutzen, die als Datenschleuse fungieren. Dabei werden die Daten auf einen speziellen Server geladen, auf dem eine oder mehrere Anti-Schadsoftware-Lösungen laufen und nur die Daten durchgelassen werden, die die Prüfung bestanden haben. Sollte das Unternehmen keine eigene IT-Abteilung haben, die eine solche Datenschleuse aktuell halten und betreiben kann, gibt es zahlreiche Dienstleister, die unterschiedliche Modelle anbieten.

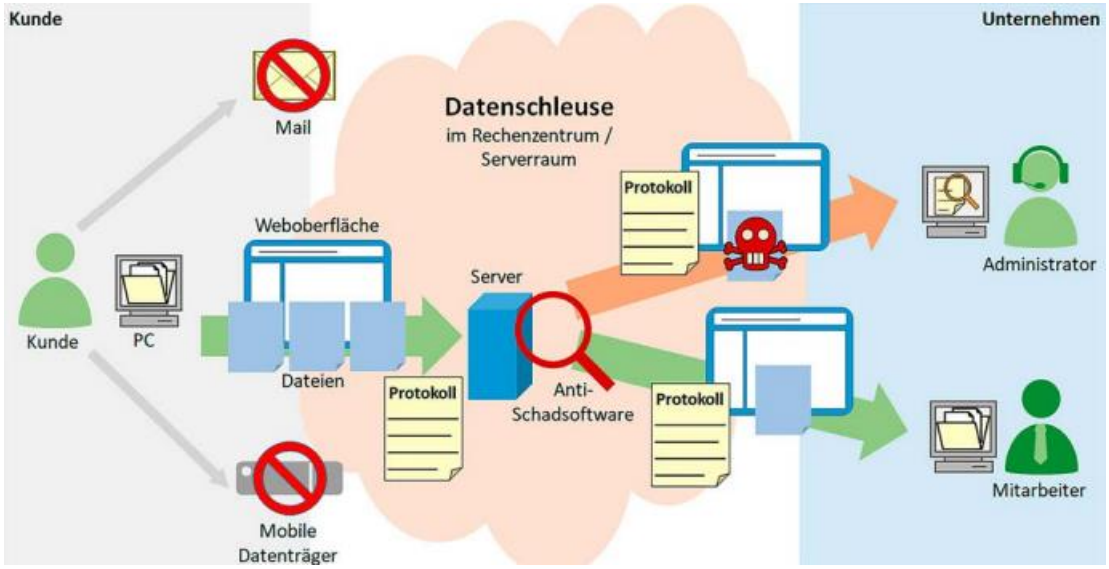

Abb.1: Datenschleuse (Quelle: Bundesministerium für Wirtschaft und Energie)

Egal welche Technologien man einsetzt, um die Datensicherheit zu erhöhen, der wichtigste Faktor ist die Sensibilisierung der Mitarbeiter in Bezug auf digitale Kommunikation. Ein unbedachter Klick auf den Anhang einer E-Mail kann ausreichen, um gefährliche Malware oder Trojaner in das Firmennetzwerk einzuschleusen, die einen erheblichen Schaden anrichten und sogar das gesamte Netzwerk lahmlegen können.

Sollte dennoch der Fall eintreten, dass Daten im eigenen Netzwerk zerstört oder gelöscht werden, kann ein Backup die Daten wieder herstellen, vorausgesetzt das Backup ist aktuell und wurde nicht ebenfalls schon durch Schadsoftware korrumpiert.

In der Prozessoptimierung auf Datensicherheit achten

Die **CONSENZUM** Managementberatung hat eine ihrer Kernkompetenzen in der Prozessoptimierung. Dabei setzen wir auf das Potenzial der Digitalisierung, um die Effektivität und Effizienz der Unternehmensprozesse zu heben. Der sicheren Übertragung von Daten zwischen internen und externen Prozessschnittstellen kommt dabei besondere Beachtung zu.

Markus Richter

CONSENZUM - Managementberatung
richter@consenzum.de | www.consenzum.de

Vertriebsentwicklung – Strategieentwicklung – Prozessoptimierung – Unternehmensnachfolge

---