Wie sicher sind Ihre E-Mails?

Immer häufiger verschicken Unternehmen sensible Daten wie Offerten, Verträge oder Lohnabrechnungen per herkömmliche E-Mail statt per physische Post. Was für Unternehmen praktisch und effizient ist, birgt jedoch Risiken hinsichtlich des Datenschutzes.

VON NORBERT KOLLER

Die aktuellen Gesetze verpflichten Unternehmen bereits heute zum sorgfältigen Umgang mit sensiblen Daten. Ein Unternehmen muss laut Gesetz alle notwendigen organisatorischen und technischen Massnahmen ergreifen, um die Datensicherheit sicherzustellen und den Datenmissbrauch möglichst zu verhindern. Mit dem neuen Schweizer Datenschutzgesetz (nDSG), das per 1. September 2023 in Kraft tritt, werden diese Pflichten verschärft und das Strafmass für Datenschutzverletzungen deutlich angehoben.

Neu gilt beispielsweise: Auch natürliche Personen können für Verstösse gegen das Gesetz gebüsst werden, und zwar mit bis zu 250 000 Franken. Bislang war das Schweizer Datenschutzgesetz das einzige Gesetz weltweit, das erlaubte, dass Mitarbeitende ihre Verantwortung für Datenschutzverstösse auf das Unternehmen übertragen konnten. Zudem besteht ab 1. September eine Meldepflicht bei Verletzungen der Datensicherheit.

Datenaustausch per E-Mail als Sicherheitsrisiko

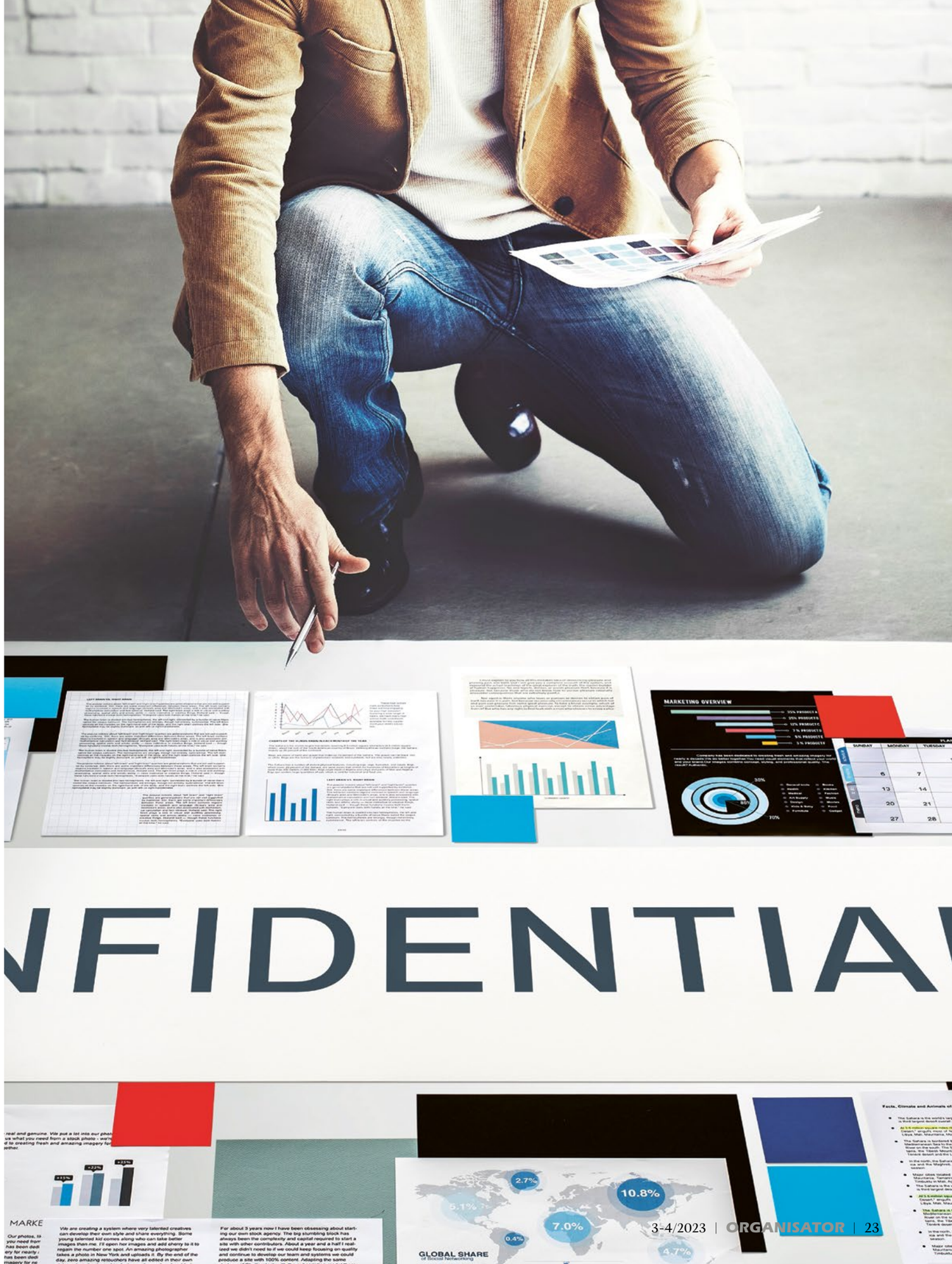
Die meisten Unternehmen haben inzwischen sichere IT-Umgebungen und stellen die Cybersicherheit ganz oben auf ihre Prioritätenliste. Sie beschäftigen sich mit grossen Themen wie Hacks von Cyberkriminellen. Jedoch wird oft nicht genügend aufgepasst, wenn Daten und Informationen häppchenweise über den täglichen E-Mail-Verkehr das Unternehmen verlassen.

«Ab 1. September besteht eine Meldepflicht bei Verletzungen der Datensicherheit.»

Informationen und Dokumente aller Art werden heute häufig und gerne per E-Mail versendet und empfangen – und zwar über alle Abteilungen hinweg. Human Resources verschickt Arbeitsverträge per elektronische Post, der Verkauf nutzt sie für Offerten oder Preiskalkulationen an die Kunden und die Sekretärin sendet dem Verwaltungsrat vertrauliche Protokolle. Alles Daten, die nicht in falsche Hände geraten dürfen.

E-Mails sind wie Postkarten

Sobald eine E-Mail über das Internet an externe Empfänger übertragen wird, ist sie möglichen Angriffen ausgesetzt. Eine E-Mail ist wie eine Postkarte. Unbefugte Dritte können ungesicherte E-Mails wie eine Postkarte mitlesen oder verändern. Schlimmer noch: E-Mails lassen sich im Gegensatz zur Postkarte einfach nach Schlüsselbegriffen durchsuchen.



© RAWPIXEL / DEPOSITPHOTOS.COM

Ein weiteres Risiko sind Nachrichten, die versehentlich falsch versendet werden. Trotz aller Vorsorge: Im Arbeitsalltag kommt es vor, dass Mitarbeitenden Datenpannen unterlaufen. Schnell ist ein vertrauliches E-Mail aus Unachtsamkeit an die falsche Adresse verschickt.

Herausforderung grosser Datentransfer

Eine weitere Herausforderung bei E-Mails ist der Austausch grosser Datenmengen. Die Datei ist mal wieder zu gross für die E-Mail? Wir alle kennen dieses Problem. Schliesslich können viele E-Mail-Clients nur Dateien bis 20 Megabytes versenden – und die sind bei den heutigen Datenmengen schnell erreicht.

Einige Unternehmen benutzen für den Austausch grosser Datenmengen eine FTP- oder S/FTP-Lösung oder versenden die Dateien nach wie vor per Post auf USB-Sticks. Oder aber, die Mitarbeitenden weichen kurzerhand auf Notlösungen aus, die ihnen bekannt sind, wie Whatsapp oder Dropbox – ein echter Albtraum für jede Unternehmens-Compliance.

Traditionelle Verschlüsselungsmethoden haben ausgedient

Um Daten sicher per E-Mail zu übertragen, sind zusätzliche Massnahmen erforderlich. Traditionelle E-Mail-Verschlüsselungsmethoden sind etwa S/MIME oder PGP. Die gängigen Verschlüsselungsmethoden erfüllen jedoch drei grundlegende Anforderungen nicht. Erstens, die Lösungen setzen eine meist komplexere Beschaffung und Einrichtung von öffentlichen und privaten Schlüsseln voraus. Sie können nicht ad hoc zwischen zwei Kommunikationsteilnehmern respektive ohne Einrichtungsprozedur eingesetzt werden. Zweitens, die Anwendung ist für Unternehmen und ihre Kunden teils sehr umständlich. Drittens, sie sind in Anschaffung und Betriebsführung teuer.

Auf Verschlüsselung zu verzichten kann teuer werden

Jüngste Cyberbedrohungen, neue Gesetze und einfachere Technologien sind Grund genug, jetzt tätig zu werden und bei der E-Mail-Kommunikation neue und sichere Wege einzuschlagen. Denn nur wenn die Mitarbeitenden über die nötigen Tools verfügen, werden sie die gesetzlichen und unternehmensinternen Datenschutzregelungen auch umsetzen können.

Ja, die zusätzlichen Sicherheitsmassnahmen beim E-Mail kosten Geld. Es ist jedoch deutlich günstiger, in Sicherheit zu investieren, als einen Datenschutzvorfall zu riskieren. Denn dann drohen nicht nur Sanktionen – auch der Schaden, der durch den Reputationsverlust entsteht, ist nicht zu unterschätzen. Die Frage lautet also nicht: Kann ich mir die Investition in die E-Mail-Sicherheit leisten? Sondern vielmehr: Kann ich es mir leisten, darauf zu verzichten?

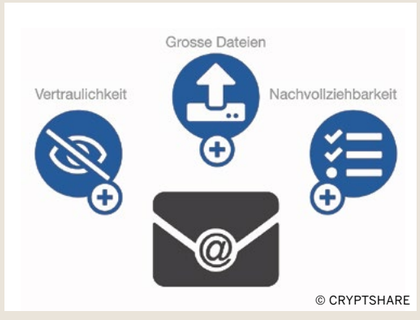
CHECKLISTE

Wichtige Kriterien bei der Software-Auswahl

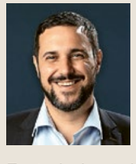
Eine zeitgemässe Lösung für den sicheren Datenaustausch geht heute über die herkömmliche E-Mail-Verschlüsselung hinaus.

Die Markterfahrung und Kundenbefragungen von Cryptshare (Cryptshare unterstützt mit der gleichnamigen Softwarelösung den sicheren Datenaustausch per E-Mail) zeigen, worauf Unternehmen bei der Auswahl einer Softwarelösung Wert legen. Die folgende Liste ist geordnet nach der Wichtigkeit, basierend auf der Anzahl der Kunden, die dieses Kriterium geäussert haben:

- **Usability:** einfach zu bedienende und leicht zugängliche Lösung
- **Nachvollziehbarkeit:** Möglichkeit zum Aufzeichnen von Transaktionen
- **Policy Management:** Nutzungsrichtlinien sollen verwaltet und technisch durchgesetzt werden können
- **Grosse Dateien:** Versand von grossen Dateien möglich, in einigen Fällen grösser als 100 Gigabyte
- **Flexible Bereitstellungsoptionen:** verschiedene Bereitstellungsmethoden verfügbar
- **Integration:** einfache Integration in die vorhandene IT- und Sicherheitsinfrastruktur
- **Corporate Design:** Anpassung der Benutzeroberfläche an das Corporate Design



Eine zeitgemässe Lösung für den sicheren Datenaustausch geht über die herkömmliche E-Mail-Verschlüsselung hinaus.



Autor

Norbert Koller ist Standortleiter Zentralschweiz bei T&N, einem Schweizer ICT-Dienstleister für Informatik und Telekommunikation. T&N unterstützt Unternehmen mit IT-Lösungen bei der Umsetzung der Datensicherheit.

> *www.tn-ict.com*