10.02.2026

zurück

Wie sicher sind Ihre Daten?

Zum heutigen internationalen „Safer Internet Day“ haben wir ein Gespräch mit zwei IT-Experten des Dienstleisters Konverto geführt. Wie gut schützen wir unsere Daten, und was sollten vor allem jene beachten, die Daten vulnerabler Personen handhaben?

Mara Ierace verantwortet bei Konverto als Legal Expert und Data Protection Officer (DPO) den Datenschutz , Michele Fiorese ist Experte in der Abteilung „Security Operations“ tätig. Beide haben sehr konkrete Vorstellungen davon, wie IT-Sicherheit gewährleistet werden kann, vor allem mit Blick auf Sozialgenossenschaften, die mit Daten vulnerabler Personen konfrontiert sind.

Warum ist IT-Sicherheit in sozialen Organisationen besonders wichtig, da sie doch Daten vulnerabler Personengruppen handhaben?

Mara Ierace: Soziale Organisationen verarbeiten täglich personenbezogene Daten, darunter sogenannte „besondere Kategorien personenbezogener Daten“, die einem erhöhten Schutz unterliegen. Dazu zählen unter anderem: Gesundheitsdaten, Sozial- und Finanzdaten, Daten von Kindern, älteren Menschen oder Menschen in schwierigen Lebenssituationen

Diese Daten unterliegen nach der DSGVO einem besonderen Schutz. Ein Verlust oder Missbrauch hätte nicht nur rechtliche Konsequenzen, sondern kann für betroffene Personen auch spürbare persönliche Nachteile mit sich bringen – etwa in Form von Stigmatisierung, Diskriminierung oder Vertrauensverlust.

Also geht es hier auch über den technischen Aspekt hinaus?

Mara Ierace: Ja, aus Datenschutzsicht ist IT-Sicherheit keine rein technische Angelegenheit, sondern eine Frage des Schutzes der Menschen und ihrer Würde. Gerade soziale Organisationen tragen hierbei eine besondere Verantwortung.

Gibt es eigentlich typische Datenschutz- oder IT-Sicherheitsrisiken, die Sozialgenossenschaften beachten sollten?

Michele Fiorese: Sozialgenossenschaften sind häufig mit mehreren typischen IT- und Datenschutzrisiken konfrontiert. Da sie oft besonders schützenswerte personenbezogene Daten von Mitgliedern, Klientinnen und Klienten oder Mitarbeitenden verarbeiten, ist das Risiko von **Datenabflüssen** besonders kritisch. Kleinere Organisationen sind zudem oft anfälliger für **Phishing und Social Engineering**, da Schulungen und Sicherheitsbewusstsein im Alltag begrenzt sein können – ebenso wie die Ressourcen, um Bedrohungen laufend zu überwachen.
Viele Sozialgenossenschaften nutzen Cloud- oder SaaS-Lösungen, wodurch Risiken durch **Fehlkonfigurationen** oder zu schwache Zugriffskontrollen entstehen können.

Gilt es auch, die Geräte im Blickfeld zu halten?

Michele Fiorese: Ja, ein weiterer Schwachpunkt ist die **Endgerätesicherheit**, da Laptops, Tablets oder Smartphones oft sensible Daten enthalten, aber nicht konsequent aktualisiert, abgesichert oder verschlüsselt sind.
Auch eine unzureichende Rechteverwaltung (z. B. zu weitreichende Berechtigungen) erhöht das Risiko interner Vorfälle. Remote-Zugriffe sind zwar notwendig, stellen aber ebenfalls ein häufiges Einfallstor dar, wenn sie nicht sauber abgesichert sind. Besonders relevant ist das Risiko durch **Ransomware**, wenn Backup- und Wiederherstellungsprozesse nicht zuverlässig funktionieren. Insgesamt sollten Sozialgenossenschaften den Schwerpunkt auf **strenge Zugriffskontrollen, Verschlüsselung, sichere Geräteverwaltung, Monitoring von Cloud/SaaS und belastbare Backup-Strategien** legen.

Welche niedrigschwelligen Maßnahmen im Bereich Datenschutz können demnach Mitarbeitende ohne IT-Vorkenntnisse sofort umsetzen?

Mara Ierace: Datenschutz beginnt im Alltag – auch ohne IT-Vorkenntnisse. Besonders wirksam sind einfache, aber konsequent umgesetzte Maßnahmen wie zum Beispiel starke, individuelle Passwörter und keine Weitergabe von Zugangsdaten, das Sperren des Bildschirms, wenn man den Arbeitsplatz verlässt und auch die Vorsicht bei E-Mails mit Anhängen oder Links (Phishing). Ich rate allen dringend, sensible Informationen niemals offen liegen zu lassen und nur Daten zu verarbeiten, die man für die eigene Arbeit wirklich braucht (Datenminimierung). Auch mobile Geräte sollten nur verwendet werden, wenn sie freigegeben und geschützt sind.

Kann man dabei auch typische Datenschutz- oder IT-Sicherheitsrisiken nennen, die Sozialgenossenschaften besonders beachten sollten?

Mara Ierace: Aus der Praxis zeigen sich immer wieder ähnliche Risikobereiche, dazu zählen unzureichend geschützte E-Mail-Kommunikation, veraltete Software oder fehlende Sicherheitsupdates, die mangelnde Sensibilisierung der Mitarbeitenden für Datenschutz und IT-Sicherheit, die die Nutzung privater Geräte oder nicht freigegebener Cloud-Dienste und auch zu weit reichende Zugriffsrechte nach dem Prinzip „alle sehen alles“.

Ist das schon als Fehlverhalten der Mitarbeitenden anzusehen?

Mara Ierace: Nein, häufig handelt es sich nicht um vorsätzliches Fehlverhalten, sondern um Herausforderungen des Arbeitsalltags. Um dem vorzubeugen und um Risiken nachhaltig zu reduzieren, empfehlen wir Schulungen, klare Zuständigkeiten und einfache, praxistaugliche Prozesse.

Mit Blick auf die Sicherheitsanforderungen, wie verändern KI und Cloud-Dienste dieselben?

Michele Fiorese: Künstliche Intelligenz und Cloud-Dienste verschieben die Sicherheitsanforderungen deutlich. Da in Cloud-Umgebungen immer mehr Daten und Services online verfügbar sind, greifen klassische Schutzmodelle am „Firmennetz-Perimeter“ zunehmend zu kurz. Organisationen müssen daher stärker auf eine saubere **Identitäts- und Zugriffsverwaltung (IAM)** sowie auf **kontinuierliches Monitoring** setzen.
KI-Systeme arbeiten mit großen Datenmengen, die häufig sensible Informationen enthalten – dadurch steigen die Anforderungen an **Verschlüsselung, Anonymisierung und rechtliche Compliance**. Gleichzeitig nutzen auch Angreifer KI, um Angriffe zu automatisieren und Phishing deutlich glaubwürdiger zu machen, etwa durch **Stimmenklonen**. Das erfordert Sicherheitslösungen, die flexibel sind und sich laufend an neue Bedrohungen anpassen.

Wie können sich Unternehmen dabei schützen?

Michele Fiorese: In Cloud-Konstellationen gilt das Prinzip der **geteilten Verantwortung**: Unternehmen können sich nicht vollständig auf den Cloud-Anbieter verlassen, sondern müssen ihre eigenen Cloud-Dienste aktiv absichern. Entscheidend ist daher eine klare Abgrenzung, welche Aufgaben beim Kunden liegen und welche beim Provider. Insgesamt geht der Trend weg von statischen, regelbasierten Schutzmaßnahmen hin zu **dynamischen, automatisierten Sicherheitsstrategien**, die Bedrohungen in Echtzeit erkennen und beantworten können.