Best Practice

Schutz vor Cyberangriffen während COVID-19.

Sieben Schritte zur Erhöhung der IT-Security von Collaboration Tools.

Campana Schott

Im Zuge der COVID-19-Krise haben viele Unternehmen neue Kommunikationslösungen kurzfristig eingeführt. Datensicherheit und Datenschutz wurden dabei nur oberflächlich betrachtet. Sieben Schritte helfen IT-Verantwortlichen, das Schutzniveau zu erhöhen.

Bei der Einführung neuer Tools denken Unternehmen im ersten Schritt meist an das Budget für Installation, Lizenzbedarf und möglichen Betrieb – und natürlich an die Freigabeprozesse. Das Thema Compliance und Datenschutz taucht häufig erst in einem späteren Schritt auf.

Dabei sollten Unternehmen von Anfang an darauf achten, denn allein in Bezug auf die EU-DSGVO wurden bis August 2020 insgesamt 320 Bussgelder in einer Gesamthöhe von mehr als 490 Millionen Euro verhängt. Davon entfallen mehr als 26 Millionen Euro auf Deutschland.

Um eine hohe Strafzahlung zu vermeiden, müssen alle Vorgänge im Zusammenhang mit personenbezogenen Daten auf DSGVO-Konformität geprüft und dokumentiert werden. Deshalb sind alle neuen Tools und Systeme auf IT-Sicherheit und Datenschutz zu untersuchen. Gerade diese beiden Punkte gelten laut 54,6 Prozent der Befragten im Future IT Report 2020 als grösste Hindernisse für die Digitalisierung. Aufgrund der COVID-19-Krise waren Unternehmen häufig gezwungen, trotz ihrer Bedenken schnell Collaboration Tools einzuführen. Deren Auswirkungen auf Datenschutz und IT-Sicherheit sind nun zeitnah zu analysieren und zu verbessern. Dies sollte anhand folgender sieben Punkte geschehen:

320 x

Bis August 2020 insgesamt 320 **Bussgelder** auf Grundlage der EU-DSGVO.

490 Mio. €

Gesamthöhe der Bussgelder in 2020 beträgt über 490 Mio. €.

26 Mio. €

Allein in Deutschland belaufen sich die verhängten Bussgelder auf über 26 Mio. €

Übersicht der Bussgelder für Verstösse gegen die EU-DSGVO im Jahr 2020

Schritte zur Erhöhung der IT-Sicherheit

1 Integration von Tools in die bestehende IT-Landschaft

Ein Collaboration Tool wie Microsoft Teams lässt sich meist in wenigen Schritten installieren. Schon die Standardeinstellungen ermöglichen produktives Arbeiten aus dem Home-Office und bieten eine zeitgemässe Kommunikationsplattform. Oft haben Unternehmen aus Zeitgründen jedoch nur die notwendigsten Schritte für die Integration von Teams in die bestehende IT-Infrastruktur durchgeführt.

Folgende Fragestellungen verdeutlichen den Handlungsbedarf:

- Welche vorhandenen Kommunikationslösungen werden parallel genutzt und wie lassen sich diese optimal mit Microsoft Teams integrieren?
- Welche Funktionsbereiche von Microsoft Teams können vorhandene Kommunikationslösungen ersetzen und wie kann ein solcher Prozess aussehen?
- Wie kann die IT-Sicherheit übergreifend und ganzheitlich gewährleistet werden, sowohl in der On-Premises-IT-Infrastruktur als auch in der Microsoft Cloud?
- Wie lässt sich weiterhin die Produktivität erhalten und steigern sowie gleichzeitig die Komplexität reduzieren, um den Supportbedarf gering zu halten?

2 Schutz von Identitäten

Insbesondere in hybriden Cloud-Umgebungen ist der Identitätsschutz wichtig. Das Prinzip „Zero Trust“ dient dem ortsunabhängigen Schutz. Es umfasst die anwendungsübergreifende Überprüfung und Risikobewertung von Identitäten zu jedem Zeitpunkt und in allen Vorgängen. Dies ermöglicht eine schnelle und zielgenaue Reaktion auf entsprechende Angriffsszenarien.

Über folgende Technologien lassen sich Identitäten nachhaltig schützen:

- Multi-Faktor-Authentifizierung verhindert den Missbrauch von gestohlenen Identitäten
- Bedingter Zugriff, um eine Anmeldung mit kompromittierten oder risikobehafteten Identitäten automatisch zu verhindern
- Kennwortschutz zum Erkennen und Vermeiden schwacher und kompromittierter Kennwörter
- Passwortlose Anmeldung, zum Beispiel mit FIDO2-Sicherheitsschlüssel
- Zuweisung von privilegierten Berechtigungen, bei Bedarf beschränkt auf den benötigten Zeitraum

3 Schutz von Informationen

Der Verlust digitaler Informationen kann existenzbedrohend sein. So schreibt nicht zuletzt die DSGVO einen angemessenen Schutz von relevanten digitalen Informationen vor. Versehentliches und vorsätzliches Teilen, Verändern und Löschen von Informationen sowie Diebstahl und unerwünschter Abfluss von Daten sind zu erkennen und zu verhindern.

Die Klassifizierung und Kennzeichnung von Informationen mit Vertraulichkeitsstufen ermöglichen gezielte automatisierte Massnahmen gegen den Verlust vertraulicher Daten. Durch Verschlüsselung lassen sie sich im gesamten Lebenszyklus vor nicht autorisierten Zugriffen geräte- und anwendungsübergreifend schützen. Aufbewahrungskennzeichen stellen die Verfügbarkeit von Daten sicher, auch wenn diese versehentlich oder vorsätzlich beschädigt oder gelöscht wurden. Sie ermöglichen auch die Datensparsamkeit durch automatisiertes Löschen von Daten nach Ablauf der definierten Aufbewahrungszeiten.

Schritte zur Erhöhung des Datenschutzes

1 Identifizierung und Dokumentation personenbezogener Daten

Personenbezogene Daten befinden sich an vielen Stellen im Unternehmen. Bei Tools zur Zusammenarbeit sind mindestens die Mitarbeiterdaten zu berücksichtigen. Dazu gehören die Unternehmens-E-Mail-Adresse sowie Vorname und Nachname jedes Mitarbeitenden. Um aus Datenschutzsicht mit einem Collaboration Tool arbeiten zu dürfen, muss unter bestimmten Voraussetzungen vorab eine Datenschutzfolgeabschätzung (DSFA) inklusive Risikobewertung durchgeführt werden. Ist dies aufgrund der Krisensituation nicht geschehen, ist sie zeitnah nachzuholen. Auch wenn keine DSFA erforderlich ist, muss eine Risikobewertung stattfinden.

Notwendige Schritte zur Absicherung des Datenschutzes

2 Festlegung von Zugriffs- und Nutzungsbedingungen für die Daten

Nach der Identifizierung und Dokumentation der personenbezogenen Daten erfolgt die Ergänzung der neuen Bearbeitungsprozesse in den bestehenden Dokumentationen zum Datenschutz (Verzeichnis von Verarbeitungstätigkeiten). Dabei ist zu prüfen, ob bereits entsprechende Richtlinien für die Verwendung des neuen Tools im Unternehmen verankert sind, zum Beispiel für **Remote Work** oder **Bring your own Device.** Fehlen solche Richtlinien, müssen sie Unternehmen entwickeln und einführen. Im Sinne des Grundsatzes der Datensparsamkeit sind zusätzlich Rollen und Verantwortlichkeiten in Bezug auf Zugriff, Verwaltung, Speicherung und Löschung von Daten innerhalb des neuen Tools zu klären.

3 Einrichtung von Massnahmen zur Gewährleistung der Datensicherheit

Die DSGVO fordert von Unternehmen geeignete technische und organisatorische Massnahmen zum Schutz personenbezogener Daten. Beim Auftreten von Verstössen müssen sie die zuständigen Behörden innerhalb von 72 Stunden informieren, in einigen Fällen auch einzelne Personen benachrichtigen. So sind für jedes neue Tool solche dokumentierten und nachweisbaren technisch-organisatorischen Massnahmen zu ergreifen.

4 Verwaltung der Dokumente, um auf Anfragen reagieren zu können

Unternehmen müssen auch nachweisen können, wie sie personenbezogene Daten erheben, verwenden, speichern, übermitteln und vernichten. Zum Beispiel stellt Microsoft für die Kunden von Teams entsprechende Dienste bereit, die bei der Verwaltung der erforderlichen Dokumente unterstützen. Dazu gehören Security und Compliance Center oder Audit Logs.

Fazit

In dringenden Fällen können Unternehmen neue Tools ad hoc einführen, sollten aber im Nachgang IT-Security und Datenschutz schnellstmöglich auf den aktuellen Stand bringen. Dies ist zum Schutz des Persönlichkeitsrechts der Mitarbeitenden und der Unternehmensdaten relevant. Dazu sind sieben wichtige Punkte zu beachten. Dann lassen sich auch moderne Collaboration Tools nachhaltig sicher und datenschutzkonform nutzen.