Best Practices für eine geschützte Zusammenarbeit

Know-how Im September wird das neue Schweizer Datenschutzgesetz eingeführt. Ein guter Grund, sich mit den Sicherheitsaspekten von Microsoft Teams auseinanderzusetzen. Denn: Die Plattform wie vorkonfiguriert einzusetzen, ist der erste Schritt in die Datensicherheitsfalle.

Von Christian Dunkel

Microsoft Teams hat sich zu einer beliebten, ja nicht mehr wegzudenkenden, Kommunikations- und Kollaborationsplattform für Unternehmen entwickelt. Die Vorteile sind vielfältig: Teamarbeit wird vereinfacht, die Produktivität gesteigert und die Zusammenarbeit über geografische Grenzen hinweg ermöglicht – und das alles, ohne besondere Kosten zu verursachen (mehr dazu im Artikel ab Seite @@).

Soweit die Theorie, denn was während der Pandemie oft schnell installiert wurde, um die (Zusammen-)arbeit im Home Office überhaupt zu ermöglichen, stellt viele Unternehmen heute vor das eine oder andere Sicherheits- und Compliance-Problem. Denn in der Regel werden in Unternehmen nicht nur allgemeine Informationen, sondern auch viele sensible Daten geteilt – da können Sicherheitslücken durchaus teuer werden.

Die gute Nachricht lautet jedoch: Microsoft 365 bietet jede Menge Möglichkeiten, Teams sicher einzusetzen. Bei individueller Konfiguration der zur Verfügung stehenden Tools kann sowohl den Datenschutzbestimmungen genüge getan als auch die Vertraulichkeit Ihrer Unternehmensinformationen gewährleistet werden.

Die Problematik: Keine Zeit und fehlendes Bewusstsein

2020 überschlugen sich mit der plötzlichen Pandemie die Ereignisse und viele Unternehmen waren froh darüber, dass es eine App wie Teams überhaupt gab. Meist geriet in den Hintergrund, dass Teams (nur) als Hub dient und dass jeder User (intern und extern) – wenn die Rechte nicht explizit eingeschränkt werden – in der Grundkonfiguration Teams mit hunderten weiteren Business-Applikationen verknüpfen kann, und zwar unabhängig vom Nutzen für das jeweilige Unternehmen. Vernachlässigt wurde zudem, dass Teams den Datenschutz-Richtlinien des Entwicklers Microsoft unterliegt, sich rechtlich also an den USA orientiert.

Auch nach der Installation und mit der Nutzung von Teams in den letzten drei Jahren erwiesen sich die immer vielfältigeren und optional einzustellenden Features, Apps und Tools nicht als offensichtlich notwendig zu konfigurieren. Und bis heute lässt Microsoft von vornherein bei Teams immer noch sozusagen alle Türen offen: Aktuell sind beispielsweise erst einmal alle über 800 kooperierenden Apps freigeschaltet. Das hat einerseits den Grund, dass von Herstellerseite natürlich eine reibungslos funktionierende und möglichst umfassende Nutzung der Anwendung ohne Einschränkungen, gewünscht ist. Es hängt andererseits aber auch damit zusammen, dass die gesetzlichen Sicherheitsvorschriften und unternehmensinternen Regelungen von Land zu Land und von Unternehmen zu Unternehmen verschieden sind – und deshalb von Microsoft gar nicht berücksichtigt werden können. Diese Richtlinien muss also jedes Unternehmen selbst für sich erst mal definieren.

Das Bewusstsein für Datenschutz und Sicherheit hat sich allerdings gewandelt. Wer heute Microsoft Teams geplant ein-

MICROSOFT TEAMS ABER SICHER

Folgende Punkte sind zu beachten, um Teams sicher einzuführen oder für Ordnung zu sorgen, falls das (Sicherheits-)Chaos bereits wütet.

Für die Planung vorbereiten:

- Change-Management aufsetzen
- User-Research
- Netzwerk und Internetverbindung anpassen
- Governance, Compliance und Security
- Coachings und Updates

Für Struktur und Sicherheit sorgen:

- Compliance Policies
- Data Loss Prevention Policies
- Multi-Faktor-Authentifizierung (MFA)
- Conditional Accesss
- Sharing-Konfiguration
- Provisionierung
- Phasenweise Implementierung

Um die Sicherheit in Microsoft Teams zu erhöhen, empfiehlt es sich zuallererst alles nicht unbedingt Notwendige zu deaktivieren. Anschliessend gilt es entsprechende Governance-, Compliance- und Security-Strukturen aufzubauen.

führt, profitiert natürlich von den Erfahrungen der vergangenen Jahre und kann mit den nötigen Einstellungen gleich von Anfang an alles richtig machen. Aus unserer Erfahrung als IT-Berater wissen wir jedoch, dass bei Kunden gerade in Bezug auf Governance, Compliance und Security immer noch grosse Unsicherheiten bestehen und viele mit den umfangreichen Möglichkeiten stark überfordert sind. Insbesondere kleine Unternehmen wissen nicht genau, welche Daten sie teilen, wo welche Daten gespeichert sind und wer alles Zugriff darauf hat.

Die Vorbereitung: Wieviel Teams brauche ich wirklich?

Tatsächlich sind nach wie vor viele Unternehmen eher IT- und nicht Business-gesteuert unterwegs, wenn es um Change-Prozesse in der Digitalisierung geht. Da die IT meist nicht direkt in das aktuelle Tagesgeschäft involviert ist, fehlen ihr oft genaue Informationen über die Abläufe. Wir empfehlen Verantwortlichen in einem ersten Schritt deshalb immer die User-Bedürfnisse abzufragen und dann zu überlegen, was wirklich benötigt wird, damit das Business reibungslos, sprich profitabel, arbeiten kann.

Gleichzeitig sollte man aber auch die technischen Voraussetzungen für eine störungsfreie Nutzung der Plattform im Auge behalten – Teams ist schliesslich keine eigene Technologie, sondern als Hub hohen Anforderungen ausgesetzt. In seiner Schnittstellenfunktion werden hier verschiedenste Microsoft-365-Dienste in einer Anwendung vereint. Dadurch ist Teams sehr ressourcen-intensiv und benötigt eine dementsprechende Netzwerkplanung und Internetverbindung.

Ebenfalls in die Vorbereitungsphase fallen individuelle Architekturen für den schon erwähnten Datenschutz, die Sicherheit sowie die internen und externen Unternehmens- beziehungsweise Mitarbeiterinteressen (Governance, Compliance & Security), sowie die Anpassung der sich durch Teams ändernden Arbeitsabläufe. Im Idealfall werden auch die User durch regelmässige Updates immer auf dem Laufenden gehalten und durch Coachings auf die effiziente Nutzung und die Arbeit mit Teams vorbereitet. Denn missglückt die Einführung, leidet die Akzeptanz und eine schlechte Erfahrung seitens der User wieder auszugleichen ist extrem schwierig. Grundsätzlich gilt: Weniger ist mehr. Teams sollte idealerweise phasenweise implementiert und Features erst nach und nach freigeschaltet werden.

Im Nachhinein, aber auch generell: Es gibt immer eine Lösung

Ist Teams bereits installiert und etabliert – wie es meist der Fall ist – gilt es aufzuräumen und die Sicherheit hochzuschrauben. Dazu empfehlen wir zuallererst alles nicht unbedingt Notwendige zu deaktivieren. Die wenigsten der hunderten Features und Apps werden genutzt und daher von den Usern auch nicht vermisst. Ausserdem sind diese mit weiteren Cloud-Diensten vernetzt und Unternehmen wissen in der Regel nicht, welche Daten genutzt werden und wohin sie fliessen oder abgelegt werden.

Anschliessend sollten Governance-, Compliance- und Security-Strukturen eingerichtet werden. Dazu gehört als ein besonders wichtiges Element etwa die Multi-Faktor-Authentifizierung (MFA), um den Zugriff auf Teams zu schützen. Ebenso können geobasierte Ausschlüsse vorgenommen werden (Conditional Access) – wenn nicht immer oder von überall, etwa aus dem Ausland oder einem öffentlichen Internetzugang, ein Zugriff auf das Netzwerk erlaubt werden soll.

Auch eine Data Loss Prevention (DLP)-Policy, durch die unter anderem die Datenklassifikation festgelegt und Sharing-Einstellungen klar definiert werden, erhöht die Sicherheit. Darunter fällt beispielsweise, welche Daten welcher Klasse wie genutzt werden oder gar den internen Bereich verlassen dürfen. Oder ob es möglicherweise Datenklassen gibt, die generell nur per Anfrage oder Genehmigung oder einer bestimmten Gruppe eingesehen werden dürfen, zum Beispiel Mitarbeiterdaten, Arbeitsverträge oder Dokumente von in der Entwicklung befindlichen Patenten. Nicht zuletzt finden hier viele individuelle Regelungen zum Datenschutz Platz.

Sowohl für Sicherheit als auch für Ordnung sorgt darüber hinaus die Auswahl, wer überhaupt Teams-Kanäle erstellen darf.

Denn auch, wenn es anfänglich zum Ausprobieren einlädt und die Akzeptanz steigern mag, kann eine unüberlegte Nutzung schnell in Überfüllung mit leeren, ungenutzten beziehungsweise Test-Channels ohne Zuordnung, Namenskonzept oder fehlender Pflege enden. Nicht selten greifen Mitarbeitende aufgrund von Unsicherheiten (wer, wo, wie, was) dann plötzlich lieber wieder auf die gute alte E-Mail zurück.

Um die Übersicht in Teams zu behalten, gibt es verschiedene Provisionierungs-Anwendungen – darunter auch die «Request-a-team» App von Microsoft selbst. Diese lässt sich den Anforderungen entsprechend anpassen und setzt dem Wildwuchs in Teams ein Ende. Denn vor der Erstellung neuer Teams wird ein Approval-Prozess in Gang gesetzt und die Verantwortung (Genehmigung neuer Kanal: ja nein) an einen vorher festgelegten Entscheider delegiert.

Schliesslich können nach und nach wieder mehr, jedoch nur die individuell sinnvollen, Features und Apps zugelassen werden, um die vielfältigen Möglichkeiten und Vorteile, die Teams unbestritten bietet, nutzen zu können.

Neues Datenschutzgesetz im Anmarsch

Microsoft Teams ist eine durchaus sinnvolle Plattform, die den Arbeitsalltag erheblich erleichtern und effizienter gestalten kann. Die von Haus aus gegebenen Schwachstellen lassen sich im Grossen und Ganzen eliminieren – vorausgesetzt Unternehmen wissen, was sie brauchen (User-Research) und gehen einmal alle Sicherheitseinstellungen durch.

Im Auge behalten sollte man auch, dass in der Schweiz am 1. September 2023 der Datenschutz mit der europäischen Datenschutz-Grundverordnung (EU-DSGVO) harmonisiert wird und ein neues Schweizer Datenschutzgesetz (DSG) in Kraft tritt. Das wirkt sich vor allem durch eine erhöhte Transparenz (Information über Datenverarbeitung) und in einer Stärkung der Rechte von betroffenen Personen aus. In diesem Zuge wurde auch die Datenschutzbehörde ausgebaut und Strafbestimmungen verschärft.

Die Pandemie war ein grosser Beschleuniger für Digitalisierungen im Allgemeinen und den Digital Workplace im Unternehmen. Doch was ad-hoc eingeführt wird, kann eben nur selten auf soliden Füssen stehen. Für zahlreiche Unternehmen gilt es jetzt, das Fundament in Form von Compliance, Governance und Security nachzuziehen, denn es ist nicht die Software oder der digitale Arbeitsplatz an sich, der Probleme mit sich bringt, sondern der individuelle Umgang damit. ■

DER AUTOR

Christian Dunkel ist Head of Infrastructure & Workplace Services bei Allgeier Schweiz. Der IT-Dienstleister begleitet Unternehmen aus verschiedenen Branchen auf ihrem Weg zum Digital Workplace, zur Data-driven Company und zu einer Business-driven IT.