Checkliste
Wie Unternehmen Microsoft 365 sicher nutzen

Mit Microsoft 365 stehen für Unternehmen zahlreiche Schutzvorkehrungen zur Verfügung, die für eine hohe Sicherheit sämtlicher Anwendungen und Daten sorgen. Voraussetzung für eine sichere Verwendung von Microsoft 365 ist jedoch, dass die Security-Funktionen auch wirklich lizenziert, aktiviert, genutzt und aktiv verwaltet werden. Zudem müssen alle Nutzer und Administratoren über die Risiken informiert und für die sichere Verwendung geschult werden. Unsere Checkliste gibt Auskunft, welche Sicherheitsaspekte Sie für die Nutzung von Microsoft 365 berücksichtigen sollten.

swisscom

Microsoft 365: Populär bei Unternehmen – aber auch bei Hackern

Wenn Unternehmen ihre Daten und Anwendungen in die Cloud verlagern, bietet dies mehr Effizienz, Vorteile in der Zusammenarbeit und ein hohes Mass an Sicherheit. Bei Microsoft 365 ist dies nicht anders: Microsoft schützt seine Services mit den zahlreichen Sicherheits-Features. Doch da Microsoft 365 ein Cloud-Service ist, unterscheiden sich die Sicherheitsvorkehrungen gegenüber Applikationen in den eigenen Rechenzentren. Dies, weil sich die Bedrohungslage bei der Nutzung der Cloud gegenüber der On-Premise-Nutzung grundsätzlich unterscheidet. Unabhängig davon ist zu beachten, dass nicht nur die Security-Features korrekt konfiguriert und genutzt werden müssen, sondern auch der Mensch – also alle Benutzer und Benutzerinnen inklusive der Administratoren – als Risikofaktor miteinbezogen werden muss.

Microsoft 365 ist einer der meistgenutzten Cloud-Dienste im Bereich Productivity Services. Weltweit verwenden über eine Million Unternehmen die Cloud-basierte Version der Microsoft-Softwares wie Exchange, Sharepoint, Teams und die dazugehörigen Apps wie OneDrive oder die Kommunikations- und Kollaborationslösung Microsoft Teams, Planner, PowerBI und Co. In der Schweiz nutzen laut der Workplace-Studie 2023 von MSM Research rund 91 Prozent der Unternehmen Microsoft 365.

Künftig werden noch mehr Unternehmen in die Cloud wechseln, entsprechend wird der Datenverkehr zunehmen. Gemäss der Swiss IT 2022 Studie von IDC wird im Jahr 2025 der Wert neu erzeugter Daten bei 176 Zettabytes liegen, im Vergleich zu 18 Zettabytes im Jahr 2015. Zudem wird die Menge der gespeicherten Unternehmensdaten bis im Jahr 2025 auf 9 ZB ansteigen, 2015 waren es rund 0,8 ZB, also unter 1 ZB. Die jährliche Wachstumsrate der neuen Daten beträgt zirka 26 Prozent. Gerade weil Microsoft 365 derart verbreitet ist, stellen die Cloud-Dienste auch ein attraktives Ziel für Cyberkriminelle dar. Die Bedrohungen sind allgegenwärtig, Angriffe finden permanent statt.

91%

der Unternehmen in der Schweiz nutzen Microsoft 365.

Integrierter Standard-Schutz in Microsoft 365

Microsoft 365 bietet wirksame Sicherheitsfunktionen, die von Unternehmen ohne zusätzliche Kosten genutzt werden können. Diese schützen vor unterschiedlichsten Bedrohungen. Doch weil die Anwender bei der Nutzung nachlässig sein können oder das Know-how fehlt, kann es sein, dass der Schutz insgesamt mangelhaft ist. «Cyberkriminelle nutzen gestohlene oder manipulierte Identitäten von Nutzern und Administratoren, um an Daten und Services von Unternehmen zu gelangen», sagt Andreas Schmid, Product Manager bei Swisscom. Da Identitäten oft über Phishing gestohlen werden, sollten Mitarbeitende besonders auf die Gefahren von Phishing-Mails und die damit verbundenen Vorgehensweisen sensibilisiert werden. Denn die Angriffe zielen meist nicht auf die Microsoft-Cloud, sondern auf die Microsoft-365-Kunden. Die Folgen solcher Angriffe sind mannigfaltig und reichen von Datenverlust über hohe Kosten, die für Unternehmen entstehen, bis hin zur Übernahme von Azure-Ressourcen, mit denen heimlich Kryptowährungen geschürft werden.

Folgende Sicherheitsfunktionen bietet Microsoft 365

- **Multi-Faktor-Authentifizierung (MFA):** Neben Benutzername und Passwort sichert ein zweiter Faktor (z. B. ein auf den Benutzer registriertes Gerät, Microsoft Authenticator App auf dem Smartphone) den sicheren Anmeldevorgang ab. So wird verhindert, dass sich Unbefugte nur mit Username und Passwort am Account anmelden können.
- Ist die **Funktion Password hashsync** aktiviert, können kompromittierte Identitäten erkannt werden.
- **Password Protection:** Verhindert, dass häufig genutzte Kennwörter wie Firmennamen, Familiennamen, Automarken usw. verwendet werden können.

Praxistipp

Microsoft 365 in der Praxis

- Alle Benutzer und Administratoren sollten ihre Accounts mit einer Multi-Faktor-Authentifizierung (MFA) schützen.
- Konfigurieren und überwachen Sie aktiv alle Security Alerts (z. B. Exchange Online Protection, Password Protection usw.).
- Regeln Sie die Nutzungsmöglichkeiten für die Mitarbeitenden in der Rechte- und Identitätsverwaltung.

- **Microsoft Information Protection:** Entdeckt, klassifiziert und schützt Ihre vertraulichen Informationen in Dokumenten oder E-Mails – von der Speicherung bis zur Übertragung.
- **Mobile Device Management (MDM):** Ermöglicht selektives Löschen von Geschäftsdaten auf mobilen Endgeräten und macht sichere Resets von mobilen Endgeräten.
- **Conditional Access:** überprüfen vom «Gesundheitszustand» der Endgeräte die sich auf die Microsoft 365 Services verbinden wollen. Blockieren von Zugriffen aus nicht vertrauenswürdigen Standorten (Darkweb).
- **Information Rights Management:** Regelt die Kontrolle über Zugriffe auf Unternehmensdaten.
- **Secure Score:** Informiert über den aktuellen Stand, wie sicher die Services zurzeit konfiguriert sind. Es werden Risiken und Schwachstellen aufgezeigt und Vorschläge gemacht, wie die Sicherheit erhöht werden kann.

Punkt 1

Basis-Security-Features: aktivieren, nutzen und verwalten

Multi-Faktor-Authentifizierung aktivieren

Die MFA gehört zu den wichtigsten und wirkungsvollsten Sicherheitsmassnahmen, da sie den Zugriff zu Daten und Anwendungen sichert. Doch in der Praxis wird diese jedem User zur Verfügung gestellte Möglichkeit nur wenig benutzt: Laut einer Untersuchung von 2018 sollen nur gerade 3 Prozent aller Administratoren die Multi-Faktor-Authentifizierung verwendet haben. Deshalb muss im Unternehmen darauf Wert gelegt werden, dass möglichst viele Nutzerinnen und Nutzer die MFA benutzen.

Reporting

DLP aktivieren und konfigurieren: inklusive Echtzeit-Überwachung und Berichte über Vorfälle.

«Die besten Sicherheitsfunktionen in Microsoft 365 nützen nichts, wenn sie nicht aktiviert, korrekt konfiguriert und professionell verwaltet werden.»

Andreas Schmid, Product Manager bei Swisscom

Punkt 2

Korrekte Nutzung: Mitarbeitende und Administratoren sensibilisieren und ausbilden

Identitätssicherheit erhöhen
Die Identitätssicherheit zu erhöhen, gehört zu den wichtigsten Massnahmen. Einfallstor Nummer 1 ist der Identitätsdiebstahl. Hacker übernehmen die Zugangsdaten, um über das gekaperte Konto weitere Angriffe zu starten. So können sie etwa ins Unternehmensnetzwerk eindringen und an Daten gelangen.

Dedizierte Admin-Konten anlegen
Administratoren sensibilisieren und deren Accounts von ihren User-Accounts trennen.

Passwort-Richtlinien einführen
Einführung strenger Passwort-Richtlinien bei allen Benutzern und Administratoren.

Nutzer schulen
Schulungen, Sensibilisierung, Sicherheitsbewusstsein aufbauen. Sämtliche Nutzerinnen und Nutzer speziell über Phishing informieren.

Starke Passwörter verwenden
Nur starke Passwörter verwenden und diese in einem Passwort-Manager verwalten.

Admin-Konten korrekt verwenden
Admin-Konten nur für Tätigkeiten verwenden, die im Zusammenhang mit der Administration stehen.

Cloud konsequent nutzen
Die Cloud konsequent nutzen. Falls Daten lokal gespeichert werden, sollten sie immer mit der Cloud synchronisiert werden.

Sensibilisieren
6 von 10 Nutzer von Microsoft 365 nutzen weder die integrierten Datenschutzfunktionen noch verfügt ihr Unternehmen über einen Präventionsplan zum Datenschutz.

Handeln Sie jetzt!

Schützen Sie Ihre Netzwerke, Datacenter und Clouds vor den Gefahren aus dem Cyberspace. Wir beraten Sie gerne!

Microsoft 365 von Swisscom

Wollen Sie mehr wissen über die Business-Komplettlösung aus der Cloud? Swisscom bietet die entsprechenden Services für jede Unternehmensgrösse. Mehr Informationen zu Microsoft 365 von Swisscom.