AWK Group
Enabling digital performance.

DIGITALER ARBEITSPLATZ:

Sichere Zusammenarbeit mit Microsoft 365

Tom Schons | Daniel Kaufmann

COVID-19, Digitaler Arbeitsplatz und Sicherheit

Als die Massnahmen zu Beginn der COVID-19 Epidemie verschärft wurden, haben viele Unternehmen ihre Mitarbeitenden ins Home-Office geschickt. Innerhalb von kurzer Zeit mussten neue Tools für die Zusammenarbeit – z. B. für Videokonferenzen – ausgerollt und Kapazitäten für den Fernzugriff auf das Unternehmensnetzwerk auf- oder ausgebaut werden.

Kurz nachdem dies endlich geschafft war, tauchten in Medien Mitteilungen über Sicherheitslücken und Datenschutzmängel auf. Der Videokonferenz-Anbieter Zoom war davon besonders betroffen[1]. Zoom sammelte unerlaubt Daten seiner Benutzer und hatte diverse Schwachstellen. Dadurch konnten unter anderem Windows-Passwörter gestohlen werden. Zudem traten häufig Fremde einer Konferenz bei und verbreiteten unangemessene Inhalte. Auch etablierte Anbieter mussten Lücken schliessen. Mit einem manipulierten GIF-Bild gelang es Forschern, Konten in Microsoft Teams zu übernehmen[2]. Damit einhergehend stellte das Nationale Zentrum für Cybersicherheit in den vergangenen Monaten einen deutlichen Anstieg der Cyber-Angriffe fest[3].

Die AWK Group konnte die Einführung von MS Teams kurz vor dem Ausbruch der COVID-19 Pandemie in der Schweiz erfolgreich umsetzen. Die damit verbundenen Governance Aspekte, das verwendete Framework sowie einige «lessons learned» haben wir anschliessend veröffentlicht und im Dokument *«Die erfolgreiche Einführung von Microsoft Teams innerhalb der AWK Group»* ausführlich beschrieben.

Mittlerweile wurden die COVID-19 Massnahmen wieder gelockert. Die Krise hat jedoch gezeigt, dass Home-Office und die Zusammenarbeit mithilfe von modernen Tools auch viele Vorteile haben. Dies ist eine gute Gelegenheit, den Stand des digitalen Arbeitsplatzes zu hinterfragen, die Übernahme und Nutzung der neuen Tools durch die Mitarbeitenden zu evaluieren oder die Sicherheit von bestehenden Systemen zu überprüfen.

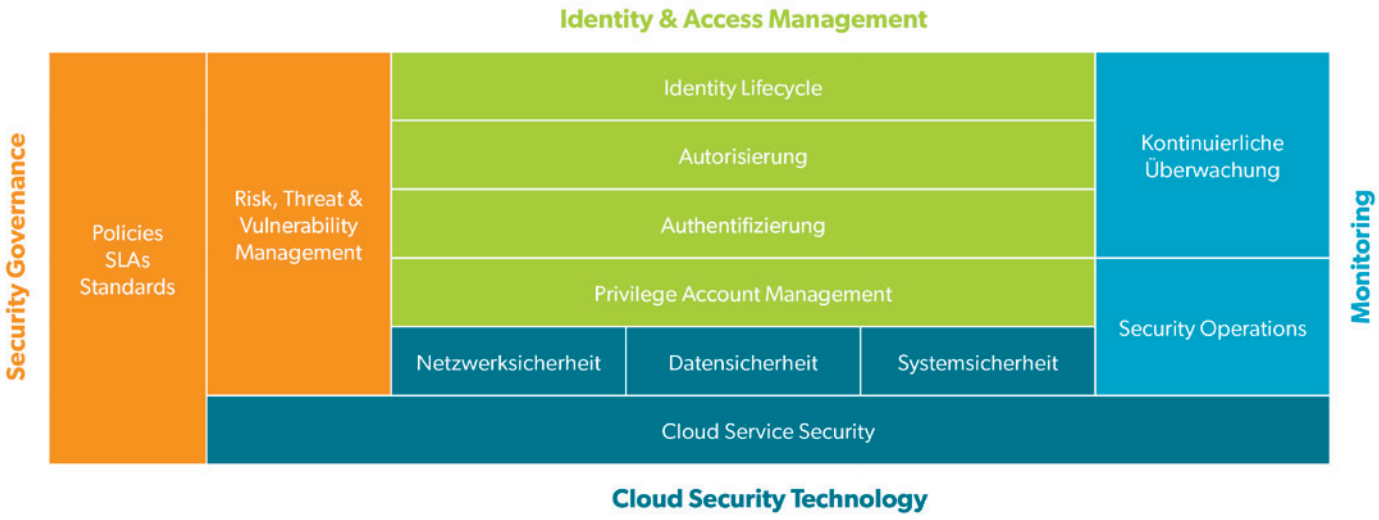
---

1 https://www.schneier.com/blog/archives/2020/04/security_and_pr_1.html
2 https://www.heise.de/security/meldung/Boese-GIFs-Microsoft-Teams-Konten-mit-verminten-Bildern-kapern-4711282.html
3 https://www.melani.admin.ch/melani/de/home/ueber_ncsc/meldeeingang.html

Microsoft 365 bietet eine umfassende Plattform mit Windows 10 und Office Anwendungen für die tägliche Arbeit im Büro, unterwegs oder im Home-Office. Ergänzend dazu bietet Microsoft auch zahlreiche Security Funktionen für die Sicherheit dieses digitalen Arbeitsplatzes. Wie bei allen Cloud-Lösungen gilt das Prinzip der geteilten Verantwortung. Dies bedeutet, dass auch der Cloud-Nutzer eine Verantwortung für die Umsetzung von bestimmten Sicherheitsmassnahmen hat und nicht alles an den Cloud-Anbieter delegieren kann.

Was sind die zentralen Elemente für die Sicherheit von Microsoft 365?

Mit der *AWK Cloud Security Architektur* können diese Aspekte analysiert und strukturiert werden. Die Security Architektur beinhaltet die Bausteine Security Governance, Identity und Access Management, Cloud Security Technology sowie Monitoring. Diese Bausteine können weiter detailliert und mit einem standardisierten Framework abgeglichen werden.



AWK Cloud Security Architektur

Security Governance

1. Prüfen Sie die Audit-Berichte von Microsoft. Nutzen Sie das Service Trust Portal von Microsoft, um Audit-Berichte (z. B. SOC2, ISO 27001) und Informationen zum Datenschutz (z. B. GDPR Control Mapping) zu finden und zu studieren. Dokumentieren Sie, dass Sie diese überprüft haben und welche Schlussfolgerungen Sie gezogen haben.

2. Erstellen Sie ein Datenschutzkonzept. Prüfen Sie den Einfluss von Cloud-Dienstleistungen auf die von Ihnen verarbeiteten Daten.

3. Identifizieren, klassifizieren und kennzeichnen Sie Ihre Informationen. Definieren Sie den Schutzbedarf für die Informationen und setzen sie entsprechende Massnahmen um.

4. Setzen Sie Massnahmen zur Verhinderung von Datenverlust um. Definieren Sie Massnahmen auf verschiedenen Ebenen, z. B. Sharing und Gäste-Zugriff, E-Mail-Versand sowie Conditional Access Regeln.

5. Fördern Sie das Sicherheitsbewusstsein in Ihrer Organisation. Dazu gehören z. B. Phishing-Awareness und der Umgang mit Daten in der Cloud. Binden Sie Microsoft in Ihre Sensibilisierungskampagne ein oder starten Sie hierzu eine separate Kampagne.

6. Etablieren Sie ein effektives Change Management. Beobachten Sie die Änderungen, die Microsoft laufend einführt. Prüfen Sie den Einfluss auf Ihre Prozesse und informieren Sie bei Bedarf die Benutzer.

Identity und Access Management

1. Schützen Sie Ihre Administratorenkonten. Halten Sie die Anzahl von globalen Administratoren klein und verwenden Sie dedizierte Administratorenkonten. Aktivieren Sie die Multi-Faktor-Authentisierung und verwenden Sie spezifische, besonders gesicherte Geräte für Administrationstätigkeiten.

2. Schützen Sie Ihre Benutzer. Definieren Sie Regeln für die Länge, Komplexität und Gültigkeitsdauer von Passwörtern. Aktivieren Sie wenn möglich die Multi-Faktor-Authentisierung für alle Benutzer. Überwachen Sie die Benutzer-Identitäten auf Risiken.

3. Erstellen Sie Regeln für Microsoft 365 Gruppen und Teams. Setzen Sie die Standardeinstellungen für Gruppen und Teams auf «Privat». Konfigurieren Sie Regeln für das Life-Cycling, wie beispielsweise die Identifikation von inaktiven oder verwaisten Gruppen.

4. Konfigurieren Sie Conditional Access Regeln, um die Konten ihrer Standard- und privilegierten Benutzer zu schützen.

5. Setzen Sie «need-to-know» um und prüfen Sie regelmässig die Zugriffsrechte.

Cloud Security Technology

1. Erarbeiten Sie ein Zero-Trust Konzept und setzen Sie dieses konsequent um.

2. Aktivieren Sie Microsoft 365 Advanced Threat Protection zum Schutz vor gefährlichen E-Mail-Anhängen und Dateien, verdächtigen Links und Phishing-Angriffen.

3. Nutzen Sie die E-Mail-Authentifizierung für einen besseren Schutz vor E-Mail-Bedrohungen.

4. Konfigurieren Sie Mail-Flow-Regeln zum Schutz vor Ransomware und anderer Malware. Blockieren Sie die automatische Weiterleitung von E-Mails an Empfänger ausserhalb Ihrer Organisation.

5. Prüfen Sie die Backup- und Wiederherstellungsfunktionen von Microsoft und vergleichen Sie diese mit Ihren eigenen Vorgaben.

Überwachung

1. Aktivieren Sie das Audit-Log für Microsoft 365. Integrieren Sie das Log in eine bestehende SIEM-Lösung oder nutzen Sie das Cloud-SIEM von Microsoft.

2. Etablieren Sie eine Bedrohungserkennung durch die Identifikation von Anomalien und riskanten Aktivitäten.

3. Überwachen Sie kritische Einstellungen Ihrer Microsoft 365-Konfiguration und alarmieren Sie bei nicht autorisierten Änderungen

4. Prüfen Sie regelmässig Ihr Secure und Compliance Score. Setzen Sie Verbesserungen um.

5. Definieren Sie Prozesse für die Behandlung von Sicherheitsvorfällen. Setzen Sie diese um und bestimmen Sie Verantwortlichkeiten.

Zusätzliche Sicherheitsmechanismen für kritische Infrastrukturen

Betreiber kritischer Infrastrukturen, wie etwa Banken und Versicherungen oder Grundversorger (Wasser, Strom), werden aufgrund hoher Sicherheitsanforderungen und regulatorischer Vorgaben zusätzliche Sicherheitsmechanismen umsetzen müssen.

Als Beispiel besonders hervorheben möchten wir die neuen Schweizer Data Center, die Microsoft kürzlich eröffnet hat. Betreiber kritischer Infrastrukturen sollten die Verlagerung ihrer bestehende Microsoft 365 Umgebung in ein Schweizer Data Center prüfen oder, im Falle von Neukunden, besser gleich mit einem Schweizer Data Center starten.

Ein weiteres sinnvolles Beispiel ist das Thema «Bring Your Own Key». Hierbei bringen Sie als Kunde zur Verschlüsslung der Microsoft 365 Umgebung ihren eigenen Schlüssel mit. Dieser stellt sicher, dass Microsoft keinerlei Zugriff auf Ihre Daten und Informationen hat. Ein besonderes Augenmerk erfordert hier allerdings die professionelle Schlüsselverwaltung, da im Falle eines Schlüsselverlustes niemand ihre Daten wiederherstellen kann.

Als abschliessendes Beispiel möchten wir die feingranulare Rechtevergabe sowie die zeitgemässe Dokumentenklassifikation und -verschlüsselung hervorheben. Der Schutz von Informationen sollte nicht ausschliesslich auf dem Gerät oder beim Benutzer liegen. Vielmehr sollte anstelle der Ablage oder des Gerätes möglichst die kleinste Entität (z. B. das Dokument) geschützt werden.

Microsoft stellt ausführliche Dokumente zur Sicherheit von Microsoft 365 zur Verfügung[4]. Nutzen Sie diese und andere Ressourcen auf dem Weg in die Cloud[5].

Unsere Experten stehen Ihnen bei der konkreten Umsetzung gerne unterstützend zur Seite.

[4] https://docs.microsoft.com/de-de/microsoft-365/security/
[5] https://docs.microsoft.com/de-de/microsoft-365/security/office-365-security/security-roadmap

Tom Schons
Manager
AWK Group AG
tom.schons@awk.ch

Daniel Kaufmann
Senior Consultant
AWK Group AG
daniel.kaufmann@awk.ch

AWK Group AG
Leutschenbachstrasse 45
CH-8050 Zürich
T +41 58 411 95 00
www.awk.ch

Zürich • Bern • Basel • Lausanne

© Copyright 2020 – AWK Group AG

AWK Group
Enabling digital performance.

Über AWK

AWK ist mit über 330 Mitarbeitenden eines der grössten unabhängigen Schweizer Beratungsunternehmen für Strategieentwicklung, Informationstechnologie und Digitalisierung. Das Unternehmen ist schweizweit tätig mit Standorten in Zürich, Bern, Basel und Lausanne. Seine Kernkompetenzen umfassen Digital Strategy & Innovation, Data Analytics & AI, Project Management & Transformation, IT Advisory und Cyber Security & Privacy.