Cloud-Dienste

KONZEPT ZUM UMGANG

SMART-IT GMBH
Roter Str. 11
88416 Erlenmoos

Fon: 07352 60239-0
Fax: 07352 60239-99
Mail: info@smart-it.gmbh
Web: www.smart-it.gmbh

Der Umgang mit Cloud-Diensten

Cloud-Dienste werden für Unternehmen immer wichtiger. Beinahe jedes Unternehmen hat einen oder mehrere Dienste (E-Mail, Dropbox, OneDrive, SharePoint) in der Cloud.

Die Cloud bietet diverse Vorteile in Bezug auf die Verfügbarkeit und Ausfallsicherheit. Die Anbieter setzen viel daran, dass die Dienste immer verfügbar sind. Diese Verfügbarkeit hat aber nicht nur Vorteile.

Früher war der E-Mail-Server nur im Unternehmensnetzwerk erreichbar. Heute ist der E-Mail-Server in der Cloud weltweit für jeden erreichbar. Deshalb müssen gewisse Vorkehrungen getroffen werden, damit böswillige Externe/Interne nicht an Daten des Unternehmens gelangen oder manipulieren.

Umsetzung durch die SMART-IT:

Wir empfehlen ein Konzept für den Umgang mit Cloud-Diensten. Dieses Konzept beruht auf aktuelle Erfahrungswerten und dem Stand der Technik.
Die Umsetzung setzt auf insgesamt drei Säulen.

Die 3 Säulen
zum Umgang mit Cloud-Diensten

SECURITY	DATENSICHERHEIT	RECHTSSICHERHEIT/ DSGVO
Multi-Faktor-Authentifizierung (MFA) für Mitarbeiter	Backup der Cloud-Dienste	E-Mail-Archivierung

Cloud-Dienste (E-Mail, OneNote, Sharepoint, Cloud-Server, Teams, usw.)

1 SECURITY

Multi-Faktor-Authentifitierung (MFA)

Multi-Faktor-Authentifizierung (MFA) für Cloud-Dienste

Cloud-Dienste sind aus der täglichen Arbeit nicht mehr wegzudenken. Viele Kunden setzen bereits auf Microsoft365. Dadurch sind z.B. E-Mails von überall auf der Welt verfügbar. Diese Verfügbarkeit bringt allerdings auch einen großen Nachteil mit sich. Mit der Kombination aus Benutzernamen und Kennwort können die Daten von Externen eingesehen und verändert werden. Diese “Schwachstelle” kann mit der Multi-Faktor-Authentifizierung (MFA) abgeschwächt werden.

Was ist MFA?

Die MFA kombiniert mehrere Berechtigungsnachweise. Im ersten Schritt wird das Passwort verlangt. Dies ist für eine erfolgreiche Anmeldung allerdings nicht ausreichend. Für die Anmeldung ist ein weiterer Nachweis notwendig. Dieser kann in Form eines Einmalpassworts oder einer biometrischen Verifizierung erfolgen.

Umsetzung durch die SMART-IT:

Empfohlen: Bestätigung der Anmeldung via Microsoft Authenticator-App auf dem Smartphone (Android oder iOS). Nach der Eingabe des Benutzernamen und Passwort wird eine Genehmigungsnachricht an das hinterlegte Smartphone geschickt. Erst wenn die Anfrage bestätigt wird, ist eine Anmeldung erfolgreich.

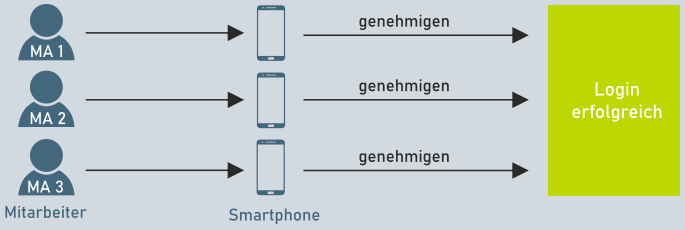
Alternativ: Bestätigung der Anmeldung via SMS. Nach der Eingabe des Passworts wird eine SMS an die hinterlegte Rufnummer verschickt. Erst mit dem Code in der SMS kann eine Anmeldung erfolgreich durchgeführt werden.

Alternativ: Bestätigung der Anmeldung via Security Token. Für die Anmeldung ist ein sogenannter Security Token notwendig. Dieser zeigt den Code für die Anmeldung an. Der Code wechselt alle 30 Sekunden.

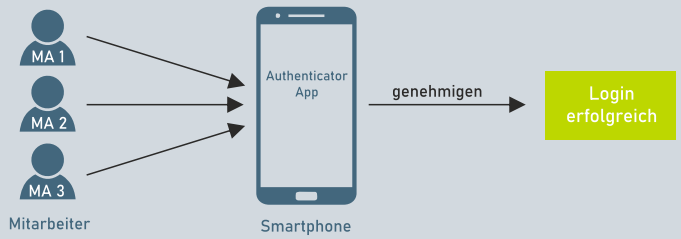
(siehe Anleitung)

Umsetzung beim Kunden:

A) Der Mitarbeiter bekommt den zweiten Faktor (Authenticator-App, SMS oder Security Token) auf sein geschäftliches/privates Gerät ausgehändigt. Dies kann den Nachteil haben, dass sich der Mitarbeiter außerhalb des Unternehmens einloggt. Zusätzlich muss beim Security Token berücksichtigt werden, dass ein Token ca. 25 € kostet. Es wird pro Mitarbeiter ein Token benötigt.



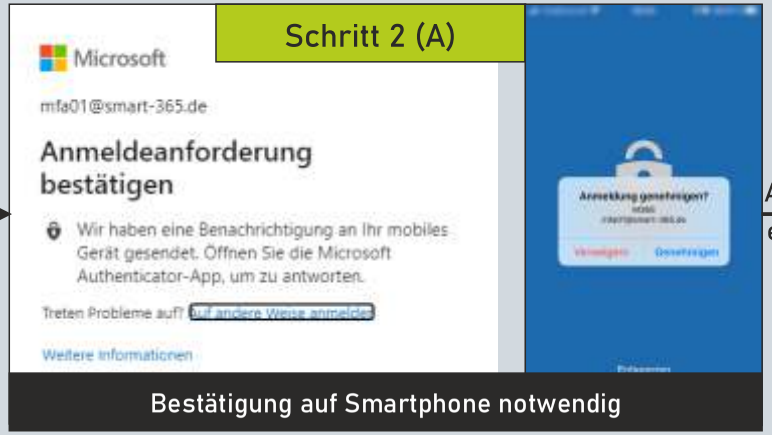
B) Der zweite Faktor wird zentral verwaltet. Dies bedeutet, dass es ein zentrales Smartphone für alle Mitarbeiter gibt. Mit dem Vorteil, dass die Geschäftsleitung den Überblick über die Logins hat. Ein Mitarbeiter/Externer kann sich nicht unbefugt mit einem Gerät einloggen.



ANLEITUNG: Bestätigung der Anmeldung via Microsoft Authenticator-App auf dem Smartphone (Android oder iOS).

Nutzer gibt Passwort ein.

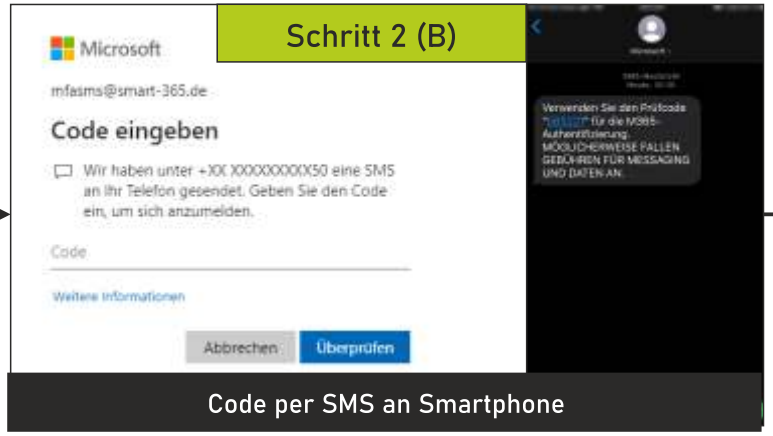
Passwort ist korrekt



Bestätigung auf Smartphone notwendig

Anmeldung erfolgreich

B
Alternativ:
Bestätigung via SMS.



Code per SMS an Smartphone

C
Alternativ:
Bestätigung via Security Token.

Code vom Security-Token

2 DATENSICHERHEIT

Backup der Cloud-Dienste

M365-Backup für E-Mails, Sharepoint und OneDrive

Beim Einsatz der Cloud-Dienste von Microsoft liegen die Daten in der Cloud. Microsoft bietet eine hohe Verfügbarkeit und eine Ausfallsicherheit durch die redundante Datenhaltung. Allerdings weißt Microsoft darauf hin, dass die Datenverwaltung dem Kunden obliegt. Das bedeutet, dass der Kunde selbst für die Daten verantwortlich ist. Microsoft gibt keine Garantie für die Integrität der Daten. Des Weiteren hält Microsoft kein Backup der Daten vor.

Beispiele, die für ein zusätzliches Backup der Daten sprechen:

- Ein Mitarbeiter löscht versehentlich eine Datei aus Teams/ OneDrive.
- Ein Mitarbeiter löscht absichtlich diverse E-Mails und Daten aus Teams. Der Mitarbeiter verlässt das Unternehmen.
- Ein Mitarbeiter führt einen Verschlüsselungstrojaner aus. Auf dem Rechner ist die Unternehmens-OneDrive synchronisiert. Dadurch werden die Unternehmensdaten verschlüsselt.
- Eine Datenbankdatei wird aufgrund eines Softwarefehlers korrupt. Nur die Vorgängerversion der Datei kann das Problem lösen.
- Trotz Ausfallsicherheit bei Microsoft kann ein Fehler im Rechenzentrum auftreten.

Umsetzung durch die SMART-IT:

Wir bieten eine Backuplösung für die Cloud-Dienste von Microsoft 365 an.

Dies beinhaltet:

- Sichern von Postfächern, einschließlich E-Mails, Anlagen, Kalendern sowie Kontakten
- Sichern von Dateien innerhalb von OneDrive und SharePoint
- Die Backups werden mit einer AES-256-Bit Verschlüsselung erstellt

3 RECHTSSICHERHEIT

E-Mail-Archivierung

SMART-MAILS, die rechtssichere E-Mail-Archivierung

Die in Deutschland, Österreich und der Schweiz geltende rechtlichen Anforderungen verpflichten Unternehmen grundsätzlich dazu, ihre E-Mails über viele Jahre hinweg vollständig, originalgetreu, manipulationssicher und jederzeit verfügbar aufzubewahren. Dazu kann jegliche Korrespondenz gehören, durch die ein Geschäft vorbereitet, abgewickelt, abgeschlossen oder rückgängig gemacht wird.

Die DSGVO und E-Mail-Archivierung

Die DSGVO legt Grundlagen für die rechtskonforme Verarbeitung personenbezogener Daten fest. Darunter fallen auch die E-Mail-Korrespondenzen. Die DSGVO verlangt Schutzmaßnahmen zur Gewährleistung der Datensicherheit. Dies umfasst das Zugriffsmangement oder auch eine Verschlüsselung. Das “Recht auf Löschung” (Art. 17 DSGVO) muss ebenso berücksichtigt werden.
Aber nicht nur die Sicherung der Daten ist ein wichtiges Kriterium. Das Auskunftsrecht für die betroffene Person muss ebenso erfüllt sein. Die hat zur Folge, dass das Archiv schnell und einfach durchsuchbar sein muss.

Weitere Informationen unter www.smart-mails.de

Umsetzung durch die SMART-IT:

- Für Sie wird eine exklusive Archivinstanz eingerichtet, die völlig separat betrieben wird.
- Unterstützung bei der Erfüllung rechtlicher Anforderungen
- SMART-MAILS ist keine Einbahnstraße. Alle E-Mails können zu jeder Zeit und in Standardformaten aus dem Archiv heraus wiederhergestellt werden. Dies garantiert eine langfristige Unabhängigkeit auch von SMART-MAILS selbst.
- Ihre Mitarbeiter können über eine nahtlose Integration in Microsoft Outlook, über Web Access oder auch mobil auf die archivierten E-Mails zugreifen und diese schnell durchsuchen.

E-Mail-Backup vs. E-Mail-Archivierung

Auf den ersten Blick könnte der Einsatz eines E-Mail-Backups die E-Mail-Archivierung überflüssig erscheinen lassen. Dies ist bei einer genaueren Betrachtung allerdings nicht der Fall. Ein Backup dient dazu, Daten über einen limitierten Zeitraum aufzubewahren. Die Daten können im Bedarfsfall wiederhergestellt werden. Ein Zugriff auf das Backup im laufenden Betrieb ist nicht vorgesehen. Des Weiteren können Daten manipuliert werden. Vor der Ausführung des Backups werden bestimmte Mails gelöscht. Diese Mails befinden sich dann nicht im Backup.
Ein Archiv dient der Wiederauffindbarkeit und Verfügbarkeit der Daten über einen langen Zeitraum hinweg. Durch Mechanismen wie Hashwerte und Verschlüsselng wird die Manipulationssicherheit gewährleistet. Die E-Mails werden in das Archiv aufgenommen, noch bevor der Mitarbeiter die E-Mail in seinem Postfach empfängt. Dadurch kann der Mitarbeiter das Archiv nicht manipulieren. Die Löschung der E-Mail aus seinem Postfach hat keine Auswirkung auf das Archiv.

Aufklärung
ÜBER DIE NUTZUNG VON CLOUD-DIENSTEN

Unternehmen

Geschäftsführung

Anschrift

E-Mail

BESTÄTIGUNG & BEAUFTRAGUNG

Hiermit bestätige ich, dass unser Unternehmen zum Umgang mit Cloud-Diensten von der SMART-IT aufgeklärt wurde.

Ich beauftrage die SMART-IT folgende Themen für unser Unternehmen umzusetzen (bitte ankreuzen):

- ☐ 1- SECURITY: Multi-Faktor-Authentifizierung (MFA)
- ☐ 2- DATENSICHERHEIT: Backup der Cloud-Dienste
- ☐ 3- RECHTSSICHERHEIT (DSGVO): E-Mail-Archivierung

Hierzu habe ich von der SMART-IT ein separates Angebot (AG_____) erhalten.

Sofern nicht alle drei Säulen zur Umsetzung gewünscht werden:

- ☐ Mir ist bewusst, dass ich für die eingesetzten Cloud-Dienste in unserem Unternehmen selbst verantwortlich bin und die SMART-IT keine Haftung übernimmt.

Anmerkungen:

UNTERSCHRIFT

Ort, Datum

Unterschrift & Firmenstempel

vertreten durch die Geschäftsführung/
Vorstand oder bevollmächtigten Vertreter