KOM SG

Überarbeitung Sicherheitsvorschriften KOM SG

Alain Keller
Moritz Rauch

\ Vorstellung

- \ advact AG für KOM SG
  - \ Sicherheitsvorschriften
  - \ KOMSG Audits
  - \ Umfragen

advact
advise & act

- \ advact AG für Kanton St. Gallen und viele weitere
  - \ Penetrationtests
  - \ Individuelle sowie standardisierte Audits
  - \ Phishing Service

\ Agenda

- \ Vorstellung
- \ Ziel
- \ Ablauf & Einleitung
- \ Themengebiete
  - \ Schutz der Systeme
  - \ Active Directory
  - \ Email, M365, Azure
- \ Nächste Schritte
- \ Fragen

\ Ziel von Meeting

- \ Warum neue Sicherheitsvorschriften?
- \ Neuerungen / Änderungen der relevanten Abschnitte
- \ Offene Fragen sind geklärt
- \ Nächste Schritte sind bekannt

\ Ablauf & Einleitung

- \ Ablauf
  - \ 30 - 45min Präsentation
  - \ 30min Fragen/Diskussion
- \ Beauftragung zur Überarbeitung der Sicherheitsvor.
- \ Erfahrungen aus Audits und Penetrationtests

- \ Gültig ab 1. Januar 2023
- \ Umsetzung bis 30. Juni 2024

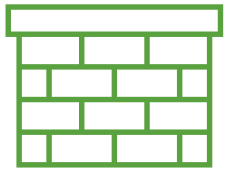
\ Einleitung

- \ Zwei Dokumente: Sicherheitsvor. & Anhang
- \ Anhang beinhaltet technische Details & Checkliste
- \ Checkliste besagt welche Kontrollen Pflicht oder Empfehlung sind

- \ (IT)-Partner müssen Vorgaben einhalten
  - \ Verträge ergänzen/anpassen
  - \ Pflichten

\ Themengebiet: Schutz der Systeme

- \ Serversysteme
  - \ Einschränkung Administrationsinterfaces
  - \ Persönliche Accounts



- \ Clientsysteme
  - \ Empfehlung Administrationsinterfaces
  - \ Virenschutz zentral
  - \ Verschlüsselung für mobile Clients

\ Themengebiet: Active Directory

\ Neuer Abschnitt / Zentral bei der Abwehr/Detektion

\ Hochprivilegierte Accounts/Gruppen

\ Lokal & Domäne

\ Veraltete/nicht benötigte Features deaktivieren

\ Zusätzliche Sicherheitsfeatures nutzen

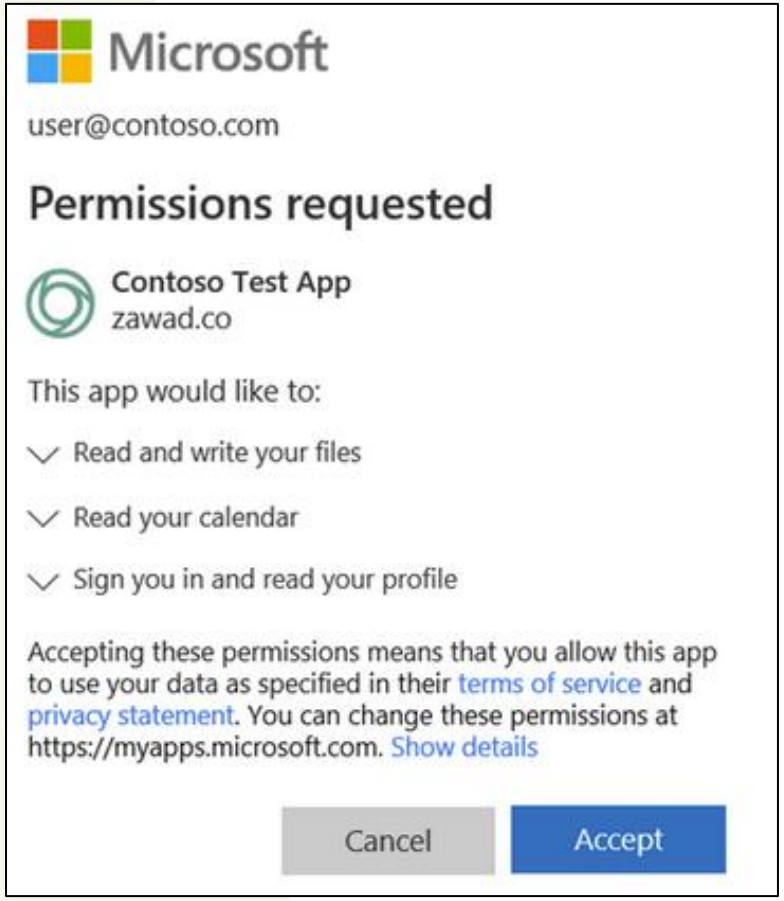
\ Passwortrichtlinie

\ Themengebiet: M365/Azure Cloud

- Sichern der Authentisierung zu M365
  - 2FA
  - Passwort Policy
  - Security Defaults oder Conditional Access Policies

- Einschränkung des Erteilens von Berechtigungen an Drittapplikationen

\ Consent Grant



\ Themengebiet: E-Mail

- \ Sandbox muss eingesetzt werden
  - \ KOMSG Service
  - \ M365 - Safe Links / Safe Attachments
  - \ Andere Sandbox – Sicherheitsvorschriften (Kapitel 7.3)

- \ Weiterleitung an private Mail

- \ Empfang von Spoofing Mail einschränken

- \ Grössenbeschränkung 20 MB / 200 Adressaten
  - \ KOMSG Service

\ Nächste Schritte

- \ Prüfen der Sicherheitsvorschriften/Anhang
- \ Beauftragung/Durchführung der nötigen Änderungen
- \ Keine Rückmeldung an KOM SG notwendig
- \ Audits
  - \ Auch weiterhin durchgeführt
- \ Überarbeitung Muster-Informatikweisung
  - \ Private Geräte - Geschäftsdaten

\ Fragerunde