Kapitel 3 – Was haben wir da eigentlich? Die IT-Inventur als Basis jeder Sicherheitsstrategie

Bevor du etwas schützen kannst, musst du wissen, dass es existiert. Klingt banal, ist aber in der Realität oft überraschend schwierig.

Viele Unternehmen entdecken bei ihrer IT-Bestandsaufnahme Relikte aus vergangenen Jahrzehnten, Admin-Konten ohne Namen und Passwörter, die in Excel-Dateien oder Köpfen schlummern.

Dieses Kapitel zeigt, warum eine strukturierte IT-Inventur nicht nur der erste, sondern vielleicht der wichtigste Schritt zu mehr Sicherheit ist.

Wir schauen uns gemeinsam an, wie du mit Microsoft-Tools wie Entra, Intune, Defender & Co. den Überblick gewinnst, warum Berechtigungen regelmäßig geprüft werden sollten und wieso der nette Kollege mit dem gesamten Adminwissen im Kopf ein größeres Risiko ist als jede Malware.

Am Ende kennst du deine IT besser als deine Kaffeemaschine.
Und das ist auch gut so.

3.1 IT-Inventur mit Augenzwinkern: Der digitale Dachboden

Wenn Unternehmen anfangen, ihre IT zu inventarisieren, passiert oft das Gleiche wie beim Frühjahrsputz im Keller:

Man findet Dinge, die man längst vergessen hatte.

> *„Wieso steht hier ein Server namens Test-SRV-2008?“*
>
> *„Wer nutzt eigentlich noch diese Access-Datenbank?“*
>
> *„Das WLAN „Intern_BossOnly“ ist das offiziell?“*

Viele IT-Landschaften wachsen organisch. Das klingt romantisch, ist aber in Wahrheit: chaotisch.

Geräte, Anwendungen, Benutzer, Dienste, über Jahre entstanden, angepasst, erweitert. Und oft: nie wieder überprüft. Dabei ist eine saubere Bestandsaufnahme die Grundlage für jede Sicherheitsstrategie.

Denn man kann nur schützen, was man kennt. Oder um es mit dem Klassiker zu sagen: *„Was du nicht kennst, wird dich hacken.“*

Eine gute IT-Inventur umfasst:

- Hardware -> vom Server bis zur Kaffeemaschine mit WLAN
- Software -> lokal, in der Cloud, als Schatten-IT
- Identitäten -> wer hat Zugriff, wer hatte mal, wer nie hätte sollen
- Netzwerke -> intern, extern, VPN, Gastzugänge
- Schnittstellen -> wer spricht mit wem, wann und warum?

Microsoft bietet hier mit Defender for Endpoint, Microsoft Intune, Azure Arc und Entra ID viele Bordmittel, um Licht ins Dunkel zu bringen, automatisiert, zentralisiert und sogar mit Diagramm.

Aber bevor es technisch wird, reicht oft schon ein einfacher Satz:

> *„Lass uns mal auflisten, was wir wirklich haben.“*

3.2 Wer nutzt was und wer darf eigentlich was?

> *„Also der Kollege Müller hat noch Admin-Rechte, weil er vor drei Jahren mal eine App installiert hat.“*
>
> *„Das Konto Projekt123_test? Ach, das ist sicher alt… oder aktiv? Keine Ahnung.“*

Willkommen im Wildwuchs der Berechtigungen.

In vielen Unternehmen sind Benutzerkonten und Rechte ein historisch gewachsenes Labyrinth. Jeder darf irgendwie irgendwas,
aber niemand hat den Gesamtüberblick.

Da gibt es:

- Ex-Mitarbeitende, deren Konten noch aktiv sind
- Service-Accounts, die nie ablaufen
- Projektgruppen, die nie gelöscht wurden
- Lokal-Admins, die keiner kennt, aber alle sind’s

Das Problem?

Zugriffsrechte sind Macht. Und Macht ohne Kontrolle ist gefährlich.
Denn Angreifer lieben alte Konten, verwaiste Admin-Rechte und Systeme, bei denen nie jemand prüft, wer was darf.

Dabei ist die Lösung eigentlich einfach:

- Prinzip der minimalen Rechte: Jeder bekommt nur das, was er wirklich braucht.
- Regelmäßige Überprüfung: Was früher nötig war, ist heute vielleicht überflüssig.
- Zentrale Verwaltung: Mit Entra ID, PIM (Privileged Identity Management) und Azure RBAC lässt sich genau steuern, wer wann was darf und für wie lange.

Und nein, das ist kein Misstrauen. Das ist professionelles Risikomanagement. Denn nichts ist schlimmer als ein Admin-Konto mit Vollzugriff, das niemand mehr kontrolliert.

3.3 Passwort-Chaos, Excel-Listen und Admin-“Geheimwissen“

Jede Firma hat sie:

Die eine Excel-Datei mit dem Namen

„Kennwort_FINAL_NEU_NEU_2023 (1).xlsx“

Auf einem Netzlaufwerk. Ohne Passwort. Oder schlimmer:
mit dem Passwort in der ersten Zeile.

Oder sie haben keine Datei, weil es da „den einen Kollegen“ gibt, der „alles im Kopf“ hat.

- Der weiß, wie die Netzwerkinfrastruktur funktioniert.
- Der kennt alle Admin-Zugänge.
- Der weiß, wie man das ERP-System neustartet.

Und wenn er Urlaub hat? Oder kündigt? Oder krank ist?
Dann ist Panik angesagt.