Fragen im Nachgang an Hr. Wahlefeld aus Live-Chat im IT Sec Talk am 27.02.25

- Wie sensibel reagieren die IAM Lösungen auf Software Produkt Updates und einhergehender möglicher Schnittstellen Anpassungen für angebundene Systeme?

Dirk Wahlefeld: IAM-Lösungen reagieren zum Teil sehr sensibel auf solche Anpassungen und Änderungen. Wenn von Herstellern dieser externen Systeme Änderungen an Schnittstellendefinition, Konfigurationsparametern, Architektur, Datenmodell etc. vorgenommen werden, sollte eine abgestimmte Aktualisierung der Systeme durchgeführt werden, um die Betriebsfähigkeit der Integration garantieren zu können. Aus Erfahrung kann ich von einer entkoppelten Aktualisierung der integrierten Systeme nur abraten und empfehle einen abgestimmten Vorgang im Sinne eines Changes.

- Haben Sie eine Quelle für die Statistik, dass 80% der Verursacher von Cyberattacken menschliche Fehler sind?

Dirk Wahlefeld: Diese Statistik (https://decoded.avast.io/threatresearch/avast-q1-2024-threat-report/) zeigt einen sehr guten Überblick über die Anteile der verschiedenen Angriffsszenarien, wobei Social Engnieering den größten Anteil hat.

- Wenn ALLES in EINEM PAM-System verwaltet wird, wie abgesichert muss das dann sein, damit nicht AD(FS), alle Windows-Server, alle Linux-Server, alle Cloud-Server/Accounts usw. übernommen werden können, wenn das PAM mal hopsgenommen wird bzw. wenn es (geplant/ungeplant) ausfällt?

Dirk Wahlefeld: Unabhängig davon, ob Ansätze mit hohen Risikofaktoren zentralistisch oder verteilt umgesetzt werden, gilt es die Evaluierung der

Sicherheitsstufe und der Definition des Risikoindex in den Vordergrund zu stellen. Fragen wären bspw.:

- Wer muss auf ein PAM-System Zugriff erhalten? Nur interne MA oder auch externe Anwender.
- Wenn externe Anwender, wie ist der Genehmigungsprozess definiert?
- Wie soll der Zugriff erfolgen, bzw. wie wird der Zugriff angebahnt (Außen nach innen – traditionell oder von innen nach außen).
- Weiter wäre zu hinterfragen, inwieweit Überwachungsmechanismen implementiert sind, um Angriffsszenarien präventiv erkennen zu können. Welche „Notaus"-Routinen sind vorbereitet, um im Fall der Fälle „den Stecker ziehen" zu können.

Diese Frage ist lässt (leider) keinen simplifizierten Lösungsansatz zu, um es qualitativ hochwertig in dieser Form beantworten zu können.