AD-Security: So richtig falsch gemacht

Nils Kaczenski
Head of Consulting
MVP Enterprise & Platform Security

Bild: Unsplash.com, Jonathan Borba

Ein Anruf auf der Mailbox:

> *Hi Nils, hier ist Mark.*
> *Kannst du mich mal dringend zurückrufen? Es geht um einen Notfall bei einem Kunden von mir.*
> *Ich stell grad ein Notfallteam zusammen und könnte dich gut dabei brauchen.*

- gehackt, vermutlich AD übernommen. Alles ist offline. Ein Forensik-Team analysiert gerade, was passiert ist.
- Kunde weiß überhaupt nicht weiter.

Nils Kaczenski
ATD | Systemhaus, Head of Consulting
MVP Enterprise & Platform Security

N.Kaczenski@atd.de

4 Fallbeispiele

Fallbeispiel: Eine Uni

- Killchain nachzeichnen
  - Große Netzwerkskizze Campus-Netzwerk mit Verzweigungen, Außenstellen usw.
  - Zoom auf Wohnheim-Netzwerk, Zoom auf Einzelrechner
  - Angreifer anzeigen, Weg des Angriffs auf der Skizze animieren, dabei Skizze zoomen und verschieben bis zum Zentrum

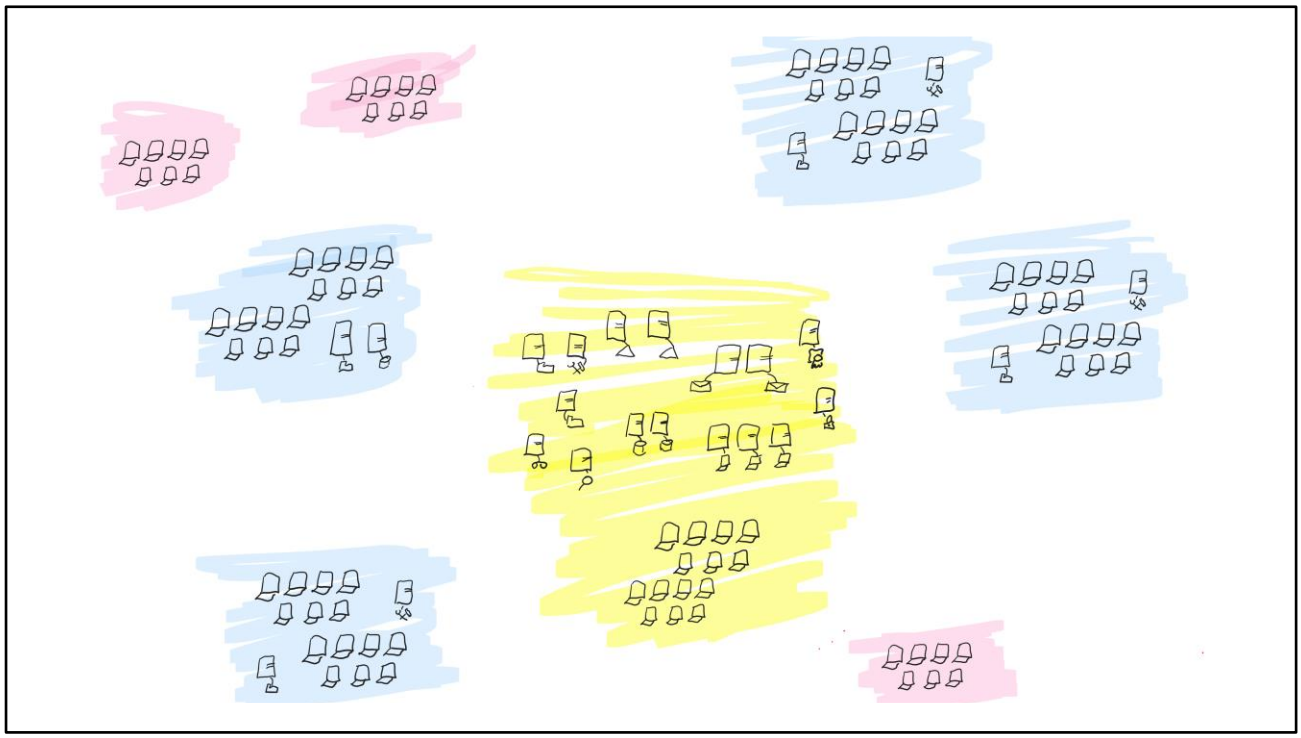


Bild: Unsplash.com, Andrew Winkler

- Verhalten des Kunden nach dem Incident
  - Shutdown
  - Große Ratlosigkeit
  - Verbale Bereitschaft, ab nun alles besser zu machen
  - … in der Realität aber: das mit den Fähnchen

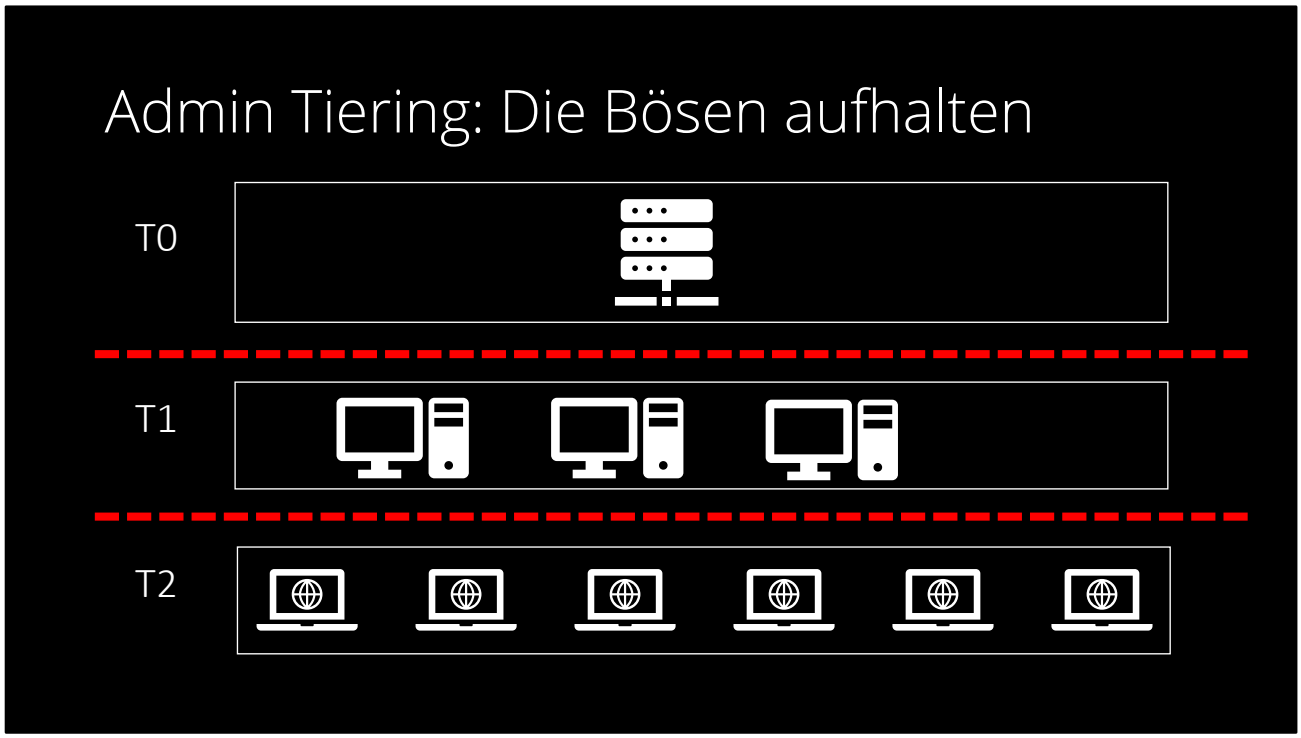
Fallbeispiel:
Mittelständische Unternehmensgruppe

Bild: Unsplash.com, Jelleke Vanooteghem

Mittelständische Unternehmensgruppe

- Major Incident: Ransomware-Befall
    - Mitarbeiter hat Mail geöffnet, die für ihn sehr plausibel aussah
    - Anhang wirkte ebenfalls plausibel
    - Der typische Ablauf: Makro fordert Berechtigungen an, lädt Malware nach, das Unheil nimmt seinen Lauf
    - Der Mitarbeiter reagiert gut und informiert die Admins …
    - … die ihrerseits auch schon bemerkt haben, dass was im Busch ist

Kompletter Shutdown, Neuaufbau durch Dienstleister
Ein wesentlicher Bestandteil: Admin Tiering (nach Microsoft-Vorlage)



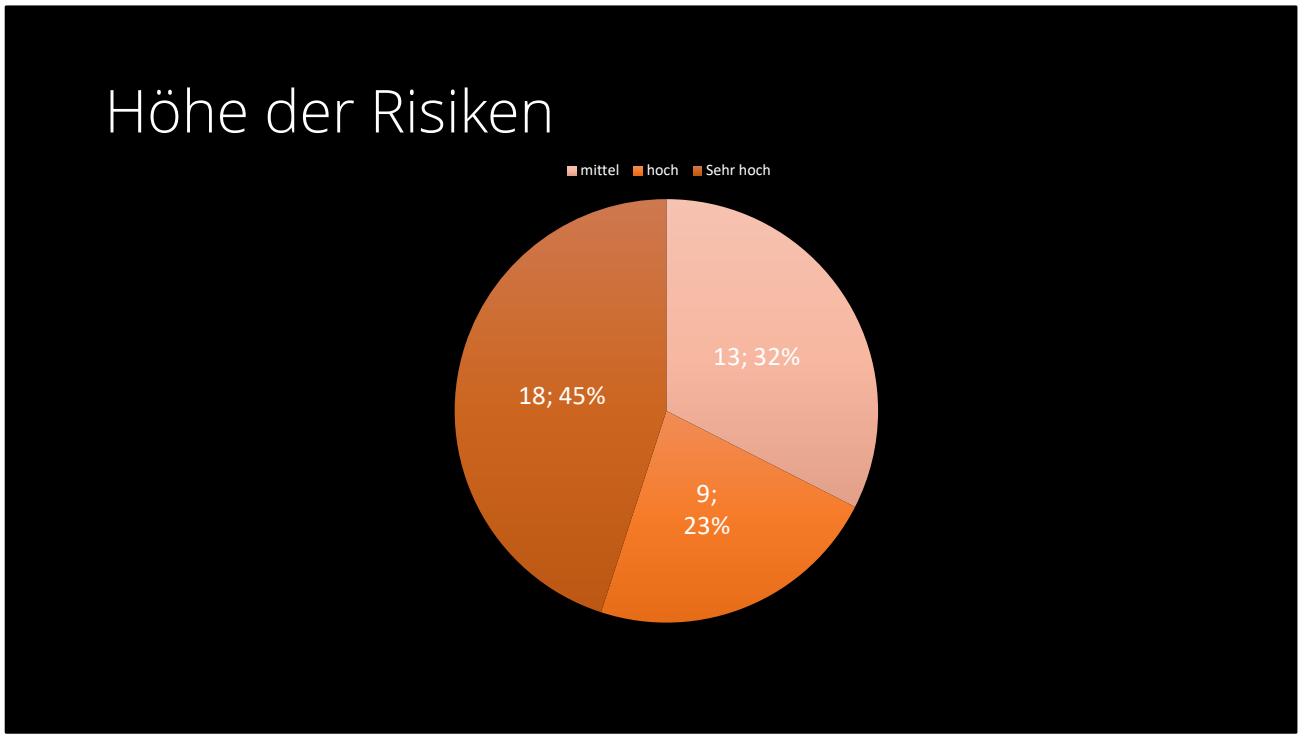
Rollentrennung ernst gemeint: Administrative Tiering

- Netzwerk in Sicherheits-Ebenen unterteilen
- Empfehlung: 3 Ebenen
- Ergänzend können Sicherheitszonen (vertikal) nützlich sein
- Jeder Account wird nur in einer Ebene (ggf. einer Ebene/Zone) verwendet

Warum der Mittelstand keine Pentests braucht

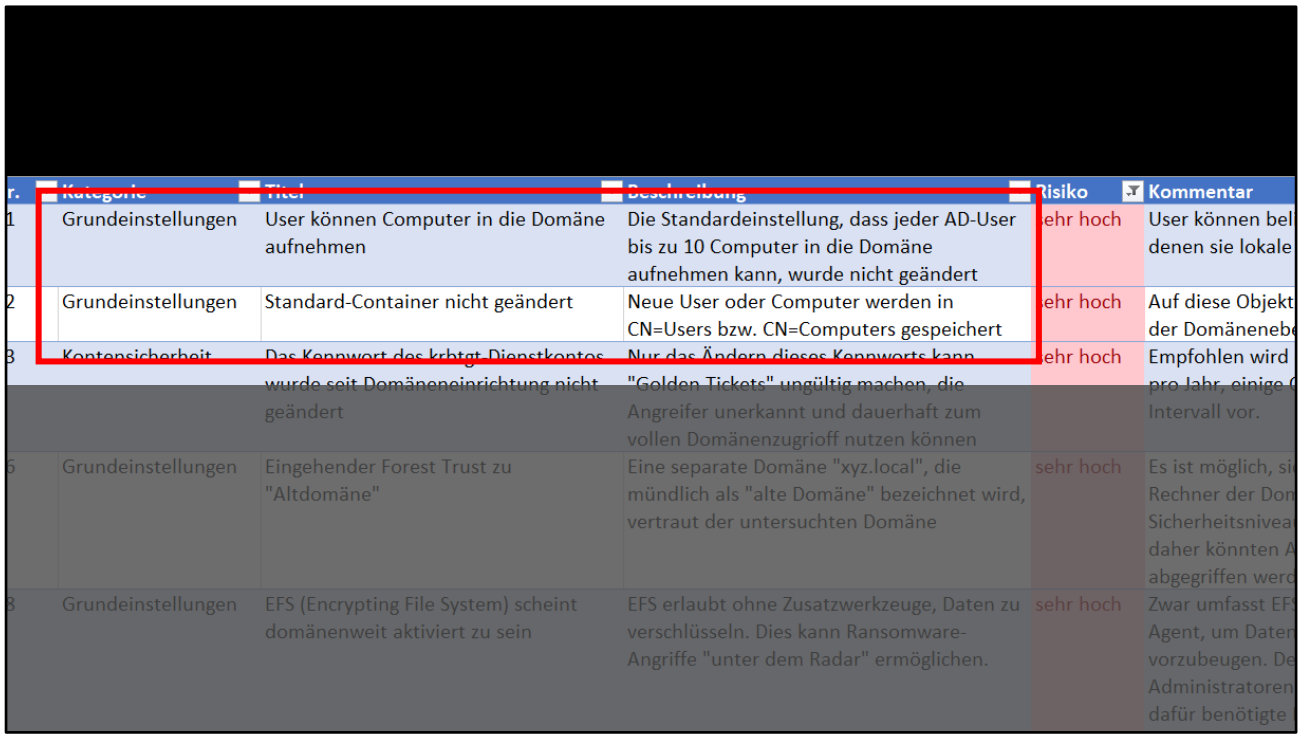
- Das typische „mittelständische“ Netzwerk ist durch Nachlässigkeit gekennzeichnet
  - Oft geht das durch Überlastung der IT auch gar nicht anders
- Daher sind diese Netze meist in einer Weise eingerichtet und betrieben, dass Pentests gar keinen Sinn ergeben: der Pentester wäre viel zu schnell drin, weil zu viele Grundlagen nicht beachtet sind

- Im realen Fallbeispiel:
  - IT denkt, sie sei nun sicher … aber da sind Zweifel …
  - Daher ein Audit nach drei Jahren: wie sicher sind wir wirklich?



- Ein begrenztes Security-Audit (wenige Tage Budget, daher nur stichprobenartig) offenbarte gravierende Lücken
  - Weder Konzept noch Dokumentation vorhanden
  - Allein im untersuchten Bereich 40 relevante Findings …
  - … davon fast die Hälfte mit sehr hohem Risiko

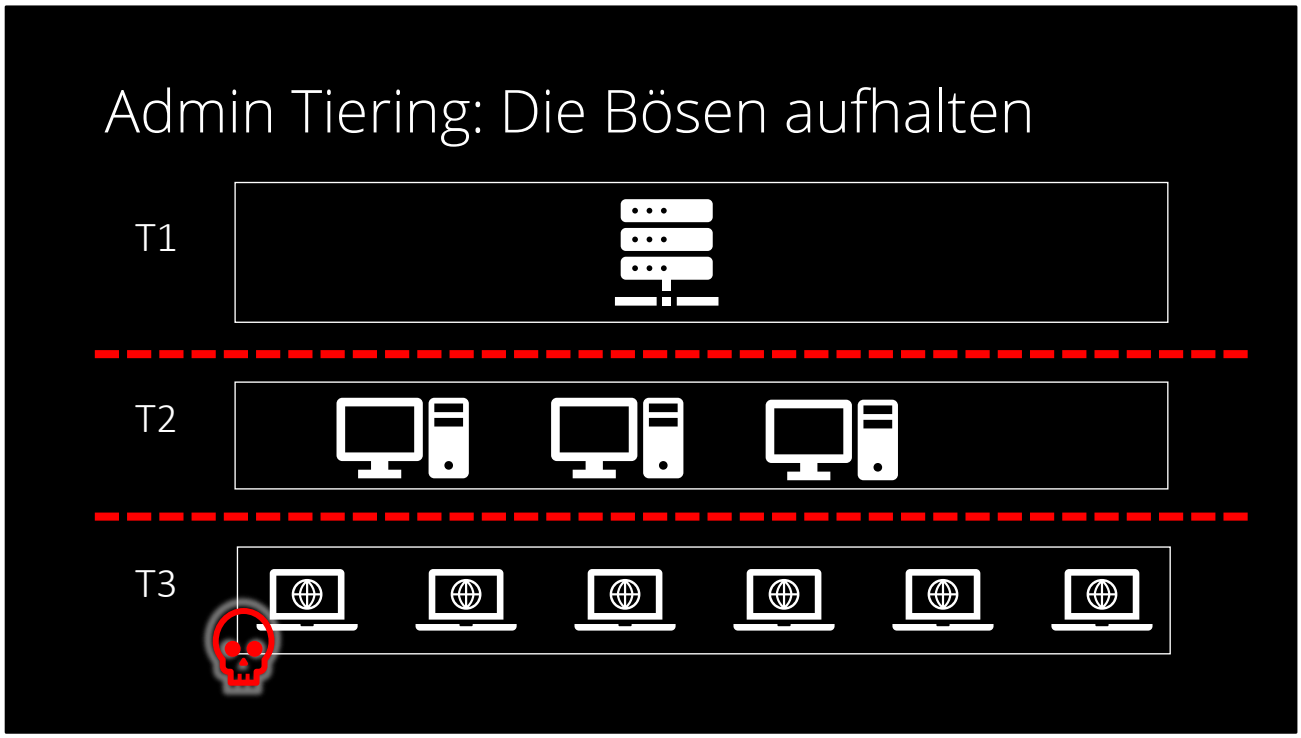
Nr.	Kategorie	Titel	Beschreibung	Risiko	Kommentar	Maßnahmen	Priorität
R1	Grundeinstellungen	User können Computer in die Domäne aufnehmen	Die Standardeinstellung, dass jeder AD-User bis zu 10 Computer in die Domäne aufnehmen kann, wurde nicht geändert	sehr hoch	User können beliebige Rechner aufnehmen, auf denen sie lokale Adminrechte haben	Die Konfiguration aufheben und das Aufnehmen von Clients mit per AD-Delegation steuern	sofort
R2	Grundeinstellungen	Standard-Container nicht geändert	Neue User oder Computer werden in CN=Users bzw. CN=Computers gespeichert	sehr hoch	Auf diese Objekte wirken keine GPOs (außer denen der Domänenebene)	Standard-Container ändern auf eine OU mit maximaler Restriktion	sofort
R3	Kontensicherheit	Das Kennwort des krbtgt-Dienstkontos wurde seit Domäneneinrichtung nicht geändert	Nur das Ändern dieses Kennworts kann "Golden Tickets" ungültig machen, die Angreifer unerkannt und dauerhaft zum vollen Domänenzugrioff nutzen können	sehr hoch	Empfohlen wird die Änderung mindestens zweimal pro Jahr, einige Quellen schlagen 40 Tage als Intervall vor.	Kennwort sofort ändern (zweimal hintereinander mit ca. 1-2 Stunden Abstand) und einen Turnus für den regelmäßigen Wechsel festlegen	sofort
R6	Grundeinstellungen	Eingehender Forest Trust zu "Altdomäne"	Eine separate Domäne "xyz.local", die mündlich als "alte Domäne" bezeichnet wird, vertraut der untersuchten Domäne	sehr hoch	Es ist möglich, sich mit Konten aus kunde.de an Rechner der Domäne xyz.local anzumelden. Das Sicherheitsniveau dieser Rechner ist unbekannt, daher könnten Anmeldedaten für kunde.de dort abgegriffen werden.	Die Vertrauensbeziehung auflösen. Bis das erreicht ist, das Sicherheitsniveau der Altdomäne verbessern.	kurzfristig
R8	Grundeinstellungen	EFS (Encrypting File System) scheint domänenweit aktiviert zu sein	EFS erlaubt ohne Zusatzwerkzeuge, Daten zu verschlüsseln. Dies kann Ransomware-Angriffe "unter dem Radar" ermöglichen.	sehr hoch	Zwar umfasst EFS einen vordefinierten Recovery Agent, um Datenverlusten durch Verschlüsselung vorzubeugen. Der Umgang damit ist vielen Administratoren aber unbekannt und oft liegt der dafür benötigte Private Key des zugehörigen Zertifikats nicht mehr vor.	Das Zertifikat des EFS-Recovery-Agents mit dessen Private Key sichern, sofern es noch vorhanden ist. EFS domänenweit deaktivieren, weil es vermutlich nicht aktiv verwendet wird.	kurzfristig
R10	Admin-Tiering	Ein T1-Account ist Mitglied von Builtin\Sicherungsoperatoren und hat damit sehr hohe Rechte auf den T0-	Sicherungsoperatoren dürfen alle Daten sichern, also auch die AD-Datenbank vollständig kopieren.	sehr hoch	Ein T1-Account ist per definitionem nicht adäquat geschützt.	Den T1-Account aus der Gruppe entfernen	kurzfristig
R13	Admin-Tiering	Exchange-Gruppe "Organization Management" umfasst 13 Mitglieder, für die teils keine weiteren Einschränkungen gelten	Diese Gruppe hat nahezu vollständige administrative Rechte im AD	sehr hoch	Das widerspricht dem Konzept (dynamische Privilegien, gezielte Privilegien). Die betreffenden Gruppe sollte leer sein. Mitglieder gehören dem T0 an und sind entsprechend einzuschränken. Dem Anschein nach werden zumindest einige der Konten auch für T0-fremde Aufgaben verwendet.	Ein adäquates Gruppen- und Berechtigungskonzept einrichten, das die Privilegien und Berechtigungen zielgerichtet und dynamisch zuweist	kurzfristig
R18	Infrastruktur	Speichersystem der VM-Umgebung, auf der T0 teilweise läuft, wird auch für andere Zwecke und andere Tiers	Das Speichersystem kontrolliert die betreffenden VMs vollständig und muss daher sehr hohem Schutz unterliegen	sehr hoch	Die gemeinsame Nutzung des Systems für mehrere Tiers und Zwecke widerspricht dem Tiering und eröffnet sehr hohe Angriffsrisiken	Umstellen auf ein dediziertes Speichersystem für Tier-0	kurzfristig
R21	Gruppenrichtlinien	WSUS-Serverkonfiguration arbeitet teils ohne TLS (https)	In mehreren GPOs sind die WSUS-Adressen ohne https/TLS vorgegeben, auch im Tier-0 (in einem Fall sogar per IP-Adresse, nicht per Name)	sehr hoch	Dies ermöglicht DOS- oder Man-in-the-middle-Angriffe. Ein Angreifer kann das Ausspielen von Updates leicht verhindern oder gefälschte Updates zur Installation bringen.	WSUS nur per https/TLS anbinden	sofort
R23	Grundeinstellungen	Tier-0-Systeme anscheinend ohne erweiterte Härtungen	Es finden sich keine Gruppenrichtlinien, die für DCs und weitere T0-Systeme erweiterte Härtungen umsetzen	sehr hoch	Es sind nur die rudimentären Einstellungen aus der Microsoft-Referenz als GPOs vorhanden, die aber bei weitem nicht vollständig sind	Erweiterte Härtungen umsetzen	kurzfristig



r.	Kategorie	Titel	Beschreibung	Risiko	Kommentar
1	Grundeinstellungen	User können Computer in die Domäne aufnehmen	Die Standardeinstellung, dass jeder AD-User bis zu 10 Computer in die Domäne aufnehmen kann, wurde nicht geändert	ehr hoch	User können bel denen sie lokale
2	Grundeinstellungen	Standard-Container nicht geändert	Neue User oder Computer werden in CN=Users bzw. CN=Computers gespeichert	ehr hoch	Auf diese Objekt der Domäneneb
3	Kontensicherheit	Das Kennwort des krbtgt-Dienstkontos wurde seit Domäneneinrichtung nicht geändert	Nur das Ändern dieses Kennworts kann "Golden Tickets" ungültig machen, die Angreifer unerkannt und dauerhaft zum vollen Domänenzugrioff nutzen können	ehr hoch	Empfohlen wird pro Jahr, einige Intervall vor.
6	Grundeinstellungen	Eingehender Forest Trust zu "Altdomäne"	Eine separate Domäne "xyz.local", die mündlich als "alte Domäne" bezeichnet wird, vertraut der untersuchten Domäne	sehr hoch	Es ist möglich, si Rechner der Dom Sicherheitsnivea daher könnten A abgegriffen werd
8	Grundeinstellungen	EFS (Encrypting File System) scheint domänenweit aktiviert zu sein	EFS erlaubt ohne Zusatzwerkzeuge, Daten zu verschlüsseln. Dies kann Ransomware-Angriffe "unter dem Radar" ermöglichen.	sehr hoch	Zwar umfasst EF Agent, um Daten vorzubeugen. De Administratoren dafür benötigte

Nr.	Kategorie	Titel	Beschreibung	Risiko	Kommentar
1	Grundeinstellungen	User können Computer in die Domäne aufnehmen	Die Standardeinstellung, dass jeder AD-User bis zu 10 Computer in die Domäne aufnehmen kann, wurde nicht geändert	sehr hoch	User können be denen sie lokale
2	Grundeinstellungen	Standard-Container nicht geändert	Neue User oder Computer werden in CN=Users bzw. CN=Computers gespeichert	sehr hoch	Auf diese Objek der Domäneneb
3	Kontensicherheit	Das Kennwort des krbtgt-Dienstkontos wurde seit Domäneneinrichtung nicht geändert	Nur das Ändern dieses Kennworts kann "Golden Tickets" ungültig machen, die Angreifer unerkannt und dauerhaft zum vollen Domänenzugrioff nutzen können	sehr hoch	Empfohlen wird pro Jahr, einige Intervall vor.
6	Grundeinstellungen	Eingehender Forest Trust zu "Altdomäne"	Eine separate Domäne "xyz.local", die mündlich als "alte Domäne" bezeichnet wird, vertraut der untersuchten Domäne	sehr hoch	Es ist möglich, s Rechner der Do Sicherheitsnivea daher könnten abgegriffen wer
8	Grundeinstellungen	EFS (Encrypting File System) scheint domänenweit aktiviert zu sein	EFS erlaubt ohne Zusatzwerkzeuge, Daten zu verschlüsseln. Dies kann Ransomware-Angriffe "unter dem Radar" ermöglichen.	sehr hoch	Zwar umfasst EF Agent, um Date vorzubeugen. D Administratore dafür benötigte Zertifikats nicht
10	Admin-Tiering	Ein T1-Account ist Mitglied von Builtin\Sicherungsoperatoren und hat damit sehr hohe Rechte auf den T0-	Sicherungsoperatoren dürfen alle Daten sichern, also auch die AD-Datenbank vollständig kopieren.	sehr hoch	Ein T1-Account geschützt.
13	Admin-Tiering	Exchange-Gruppe "Organization	Diese Gruppe hat nahezu vollständige	sehr hoch	Das widersprich

13	Admin-Tiering	Exchange-Gruppe "Organization Management" umfasst 13 Mitglieder, für die teils keine weiteren Einschränkungen gelten	Diese Gruppe hat nahezu vollständige administrative Rechte im AD	sehr hoch	Das widerspricht Privilegien, gezie Gruppe sollte le an und sind ents Anschein nach w auch für T0-frem
18	Infrastruktur	Speichersystem der VM-Umgebung, auf der T0 teilweise läuft, wird auch für andere Zwecke und andere Tiers	Das Speichersystem kontrolliert die betreffenden VMs vollständig und muss daher sehr hohem Schutz unterliegen	ehr hoch	Die gemeinsame Tiers und Zwecke eröffnet sehr ho
21	Gruppenrichtlinien	WSUS-Serverkonfiguration arbeitet teils ohne TLS (https)	In mehreren GPOs sind die WSUS-Adressen ohne https/TLS vorgegeben, auch im Tier-0 (in einem Fall sogar per IP-Adresse, nicht per Name)	ehr hoch	Dies ermöglicht Angriffe. Ein Ang Updates leicht v zur Installation b
23	Grundeinstellungen	Tier-0-Systeme anscheinend ohne erweiterte Härtungen	Es finden sich keine Gruppenrichtlinien, die für DCs und weitere T0-Systeme erweiterte Härtungen umsetzen	sehr hoch	Es sind nur die r Microsoft-Refere bei weitem nicht



Tatsächlich war die Rollentrennung halbherzig und somit unwirksam

Fallbeispiel:
Unternehmen mit hohem Finanzvolumen

Bild: Unsplash.com, Dave Goudreau

- Killchain nachzeichnen
    - Nur kurz, weil ähnlich zu den anderen Fällen

Bild: Unsplash.com, Santiago Lacarta

- Kompetenz- und Dienstleister-Gerangel nach dem Incident
    - Der DL, der das Design verbockt hatte, übernimmt durch geschicktes Taktieren die Führung im Neuaufbau

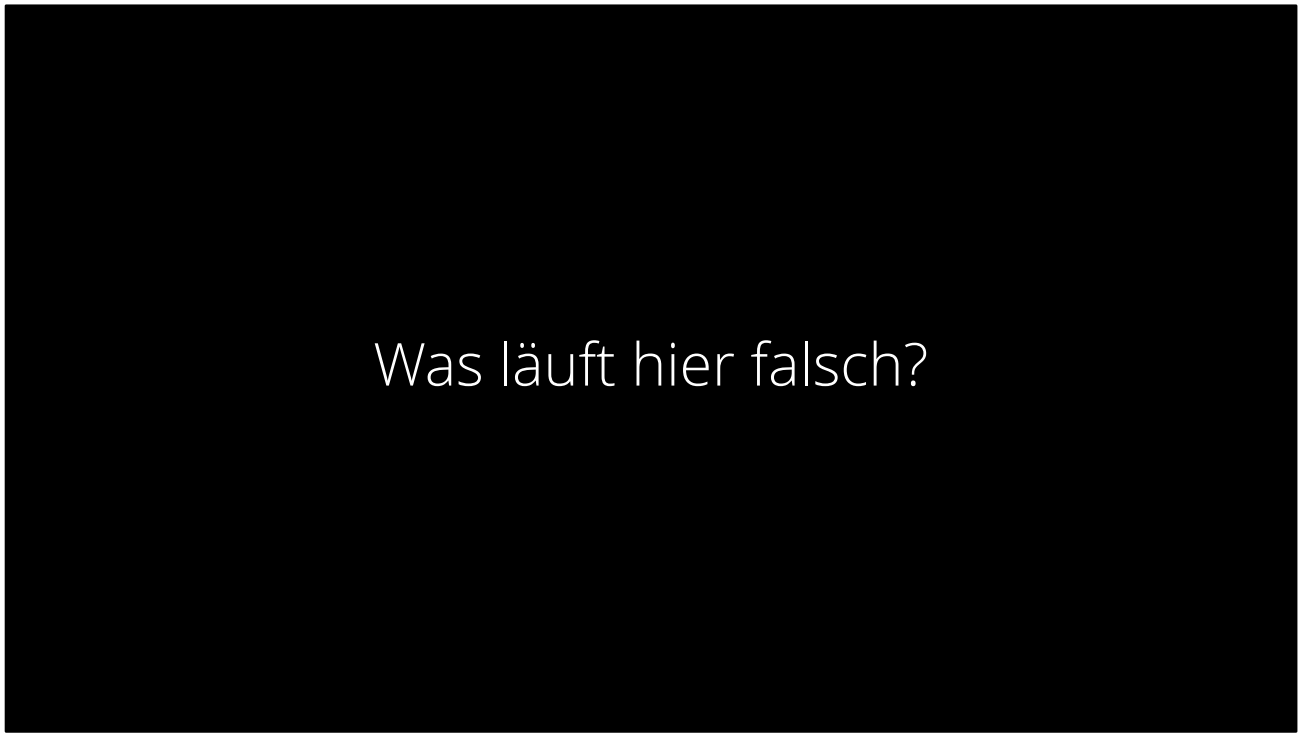
Fallbeispiel:
Gezielter Angriff auf Hi-Tech-Unternehmen

Bild: Chris Linnett, Unsplash.com

- Typischer Vorfall, alles steht
- Hinweise, dass es ein gezielter Angriff war
- Kein externer IR und Forensiker
    - … sondern Versicherung
    - … die ihre eigenen Interessen vertritt

Bild: Patrick Hendry, Unscplash.com

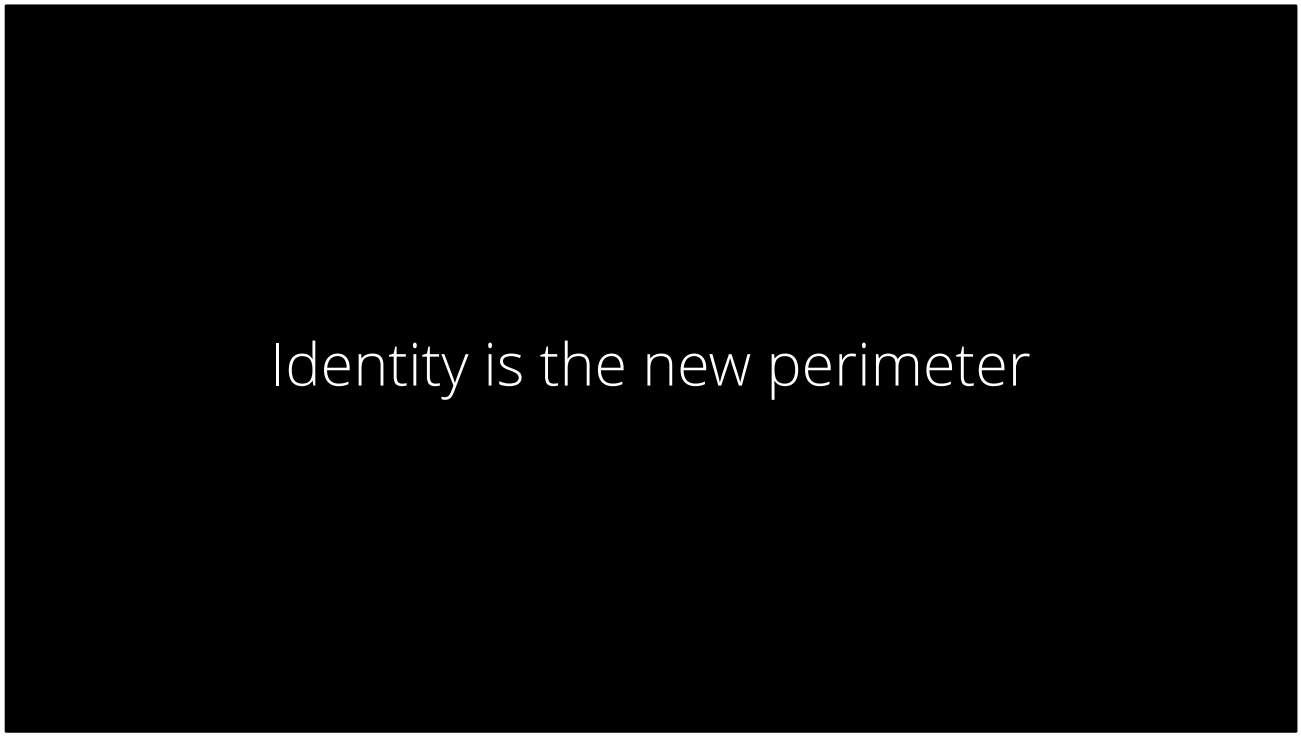
- Glück gehabt: Produktion kaum betroffen
    - Dadurch unbedingter Fokus auf "Business muss laufen"
- Recovery mit enormem Aufwand, aber immer "Business First"
    - Notfall-Modus nicht verlassen
    - Viel "erstmal eingerichtet"
    - … dadurch die typischen Fehler wiederholt



Was lernen wir daraus?

Bild: Oleksandr K, Unsplash.com

Technische Sorgfalt fehlt



Warum AD gerade im Cloud-Zeitalter gepflegt werden muss

- Identity is the new perimeter
- AD ist überall, aber nicht mehr im Fokus
    - Sorgfalt lässt nach
    - Gewohnheit und Nachlässigkeit
    - Basiskenntnisse an Nachwuchskräfte schlecht vermittelt
    - Angriffsziel wird attraktiver, weil AD die Verbindung zwischen Cloud und on-prem ist

State of the Nation

State of the Nation

- AD-Analysen offenbaren immer noch dasselbe Bild wie seit 25 Jahren
- Admin = Gottmodus
- Zu hohe Berechtigungen für User
- Einmal erteilt, niemals entzogen

Admin Tiering

Tiering, ESAE, Enterprise Access Model

- Typische Missverständnisse
  - ESAE als Kochrezept verstehen
  - Nur die Beispiele der (ehemaligen) Webseite umsetzen
  - ESAE = PAW
  - ESAE = einheitliche Vorgabe für alle
- Folge: Das ist so komplex, dass man lieber gar nichts macht

Bild: Jason Goodman, Unsplash.com

Organisation zu schwach

- Gemeinsame Strukturen fehlen
    - Jeder macht alles
    - … wie es ihm gerade einfällt
    - Zu laxe Organisation erzeugt zu laxe Technik
- Keine Konzepte für den Notfall
    - Headless Chicken Mode
    - Keine Führung in der Krise

Notfallplan

- Und bevor es so weit ist: Erstreaktion organisatorisch vorbereiten
  - Minimaler Notfallplan

Minimaler Notfallplan

- Und bevor es so weit ist: Erstreaktion organisatorisch vorbereiten
  - Minimaler Notfallplan

Bild: NASA Hubble Space Telescope, Unsplash.com

IT und Business sind auf verschiedenen Planeten

- IT: Kein Verständnis, was das Business braucht
- Business: Kein Verständnis, wie man Prozesse sicher einrichtet

Bild: Dimitri Iakymuk, Unsplash.com

Fragen & Antworten

Nils Kaczenski
ATD | Systemhaus, Head of Consulting
MVP Enterprise & Platform Security

N.Kaczenski@atd.de