advisio
CORPORATE CONSULTING

Automatisiertes Identitätsmanagement in einer Active Directory Umgebung

Nicht nur die ISO 27001 gibt vor, dass der Lebenszyklus von Identitäten verwaltet werden muss, sondern es gebietet auch der gesunde Menschenverstand, dass nur diejenigen Personen Zugriff auf das Unternehmen-Netzwerk haben, die den Zugriff benötigen.

Die Zugriffs-Verwaltung bedeutet für viele Unternehmen einen manuellen Aufwand. Automatisierte Anbindungen an Personal-Systeme oder andere Management-Systeme sind eher selten.

Beiliegender Artikel möchte Anregungen für Automatisierungen und somit der Erhöhung der Sicherheit und der Reduktion von Aufwänden geben.

Ein Bericht von Martin Zeyer, Senior Consultant für Informationssicherheit bei der advisio GmbH.

advisio
CORPORATE CONSULTING

Inhaltsübersicht

1. Einleitung

Sehr viele Unternehmen und Institutionen nutzen ein Active Directory (AD) zur Verwaltung ihrer digitalen Ressourcen und deren Zugangsschutz. Das AD speichert dazu alle relevanten Assets, wie Server, Computer, Drucker, Benutzer, … in ihrer zugehörigen Datenbank (ESE). Über das Active Directory (AD) lassen sich dann Eigenschaften speichern, Beziehungen definieren und vor allem Zugriffe auf die Objekte regeln. Im Normalfall wird dies über die Anmeldung in Windows realisiert. Daran verknüpft sind eine Vielzahl von weiteren Zugängen, Berechtigungen und Zugriffsmöglichkeiten. Viele Applikationen nutzen die Authentifizierung über das AD, wie zum Beispiel das Mail-System. Damit muss sich der Anwender nur noch ein Kennwort merken bzw. er hat nur einen Zugang, an dem er sich authentifizieren muss.

Andererseits birgt dieser sogenannte „Single-Sign-On“ (SSO) auch jede Menge Gefahren. Das AD ist der Dreh- und Angelpunkt für den Zugang zum Unternehmensnetzwerk und ist daher interessant für Angriffe jeglicher Art. Eine penible, strukturierte Verwaltung, die zeitnah auf Veränderungen und Meldungen jeglicher Art reagiert, ist daher ein MUSS für die Informationssicherheit. Ein hoher Automatisierungsgrad kann hier deutlich entlasten.

Note: Um die Lesbarkeit zu erhöhen, verzichten wir auf Gender-Sternchen oder die Aufzählung aller möglichen Gender. Mit Anwender, Nutzer, Bearbeiter oder anderen Singularitäten meinen wir hier Menschen aller Art.

2. Active Directory

Ein Active Directory ist ein Verzeichnisdienst, der von Microsoft mit Windows 2000 eingeführt wurde. Bis dahin war eine zentrale Zugangs- und Objektverwaltung nur unter Novell verbreitet. Die zentralen Dienste nennen sich auch „Active Directory Domain Services“ (ADDS). Dieser Dienst läuft auf einem (oder auch mehreren) Windows-Servern (AD-Controller) und beherbergt Abbilde der Objekte der realen Umgebung. Dies sind Benutzer, Computer, Drucker, Server, Dienste, Gruppen, Freigaben, …. Die Objekte werden auf dem Server in einer Jet-Datenbank abgelegt und ggf. auf den beteiligten Servern bei Änderungen abgeglichen. Zusätzlich zu den Objekten werden Zusammenhänge der Objekte und Berechtigungen zwischen den Objekten gespeichert. Ebenso finden sich in der AD auch Informationen zur Konfigurationen von Objekten.

Wenn sich ein Anwender an einem Computer (z.B. Notebook) authentifizieren will, so schickt der Computer die Anfrage zu dem AD-Controller, der zum einen bestätigt, dass der Anwender bekannt ist, sein Kennwort korrekt ist und dass er sich an diesem Computer heute und jetzt Zugang verschaffen darf (Anmeldung). Wenn das der Fall ist, wird der Rechner entsperrt und der Anwender kann auf die Funktionen des Rechners zugreifen. Weiterhin können bei der Anmeldung Konfigurationen aus dem AD für die Nutzung des Computers oder/und diesem Anwender übertragen werden. Das können z.B. individuelle Druckerverbindungen sein oder Einstellungen, welche Software zur Verfügung steht.

Beginnt der Anwender zu arbeiten und nutzt weitere Dienste, Software, Datenbanken, Server, Drucker, …, die mit dem AD verknüpft sind, so wird bei jedem Zugriff eine Abfrage an das AD geschickt, um zu überprüfen, ob der Anwender dieses Recht besitzt und den Arbeitsschritt tätigen darf. Dies erfolgt über das „Lightweight Directory Access Protocol“ (LDAP) in verschlüsselter Form. Kennwörter werden übrigens nicht verschlüsselt oder in „Echtdaten“ übertragen, sondern nur als Hash gespeichert.

Ein kleiner Sonderfall sind die „Azure Active Directory Domain Services“ (Azure ADDS). Microsoft bietet unter dem Namen „Azure“ (Neuer Name „Entra“) Dienste aus der Cloud an. Dazu gehört auch das Azure ADDS. Entweder kann man sich diese Dienste exklusiv anmieten, um keine eigene Infrastruktur zu betreiben, oder man nutzt diese Dienste als zusätzlichen AD-Server außerhalb der Firmeninfrastruktur, um über den SSO

auch außerhalb des eigenen Netzwerkes Authentifizierungs-Anfragen bestätigt zu bekommen. Azure ADDS und das lokale AD unterscheiden sich in einigen Dingen, auf die wir hier aber nicht eingehen.

Außer den erwähnten Diensten gibt es für die Erweiterung der Single-Sign-On-Fähigkeit von Microsoft den „Active Directory Federation Service“ (ADFS), aber auch von Fremdherstellern diverse Tools und Verfahren, um mit einem Kennwort Zugriff auf alle notwendigen Services zu bekommen.

> Das Active Directory ermöglicht über ein Kennwort den Zugriff auf eine Vielzahl von Diensten und Daten. Daher ist dieses Kennwort bzw. der Zugang dazu besonders zu schützen.

3. Benutzer-Typen

Um die Verwaltung der Benutzer zu strukturieren und möglichst einfach zu gestalten, macht es Sinn, sich Gedanken zu machen, WELCHE Benutzertypen denn verwaltet werden. Diese sollten kategorisiert und mit einem eindeutigen Merkmal versehen werden, um die Einteilung leicht zu erkennen. Das kann der Anmelde-Name (sehr praktisch, da für alle sofort sichtbar) oder bestimmte Gruppenzugehörigkeiten sein oder auch Eintragungen in bestimmte Felder im AD z.B. in ein erweitertes Attribut.
Folgende Benutzer-Typen kommen in der Praxis am häufigsten vor. Als Unterscheidungsmerkmal nutzen wir in der Anmeldekennung ein Präfix. Dazu hängen wir zwei Buchstaben für den Benutzer-Typ und einen Bindestrich vor die eigentliche Kennung. (Achtung bei Namen, die bereits so ein Muster beinhalten, wie z.B. die Firma „AL-CAPONE“)

Typ	Beschreibung	Kürzel	Beispiel Anmeldekennung	Ablauf-Datum	Info
Interner Mitarbeiter unbefristet	Eine Person mit unbefristeter Festanstellung	-keines- oder IN-	MAXMUSTER IN-MAXMUSTER	Nein	
Interner Mitarbeiter befristet	Eine Person mit befristeter Anstellung (auch Praktikanten, Azubis, …)	BE-	BE-MAXMUSTER	Ja	
Externer Mitarbeiter	Namentlich bekannter externer Mitarbeiter (Projekt, Dauerhaft, …)	EX-	EX-MAXMUSTER	Ja	
Dienstleister	Wechselnde Personen eines Dienstleisters (z.B. für Wartung)	DL-	DL-MEYERGMBH	Ja	
Service-Account	Kennungen die für Ausführung von Diensten oder Jobs verantwortlich sind	SV-	SV-CHECKAD	Nein	
Administrator-Account	Kennungen für IT-Betrieb, die nur für administrative Tätigkeiten genutzt werden	AM-	AM-MAXMUSER	Ja	
Test-Account	Kennungen für kurzfristige Tests	TE-	TE-MAXMUSTER	Ja	
Gruppen-Account	Kennungen für mehrere Personen (Sammelaccounts)	GR-	GR-MARKETING	Ja	
Kontakte	Kennungen für Kontakte und nicht-personifizierte Mail-Kennungen	KT-	KT-WEBSHOP	Nein	

Dazu kommen sicherlich, je nach Umgebung oder Anforderung noch weitere Anmelde-Typen dazu.
Generell dürfen nur personenbezogene Kennungen ohne Befristung kein Ablaufdatum besitzen. Ausnahme sind Kennungen, bei denen das Passwort nicht bekannt ist (Service-Accounts). Kennungen, die von mehreren Personen benutzt werden (Gruppen-Accounts), sollten unbedingt vermieden werden. Ist dies nicht möglich, so muss durch einen organisatorischen Prozess sichergestellt werden, dass das Kennwort der Gruppe geändert wird, wenn Personen, denen das Kennwort bekannt ist, die Gruppe verlassen. Dies funktioniert in der Praxis jedoch erfahrungsgemäß eher nicht.

> Vermeiden Sie die Anlage von Kennungen, deren Passwörter mehr als einer Person bekannt sind. Die Verwaltung dieser Kennungen lässt sich oft nicht sicher gestalten.

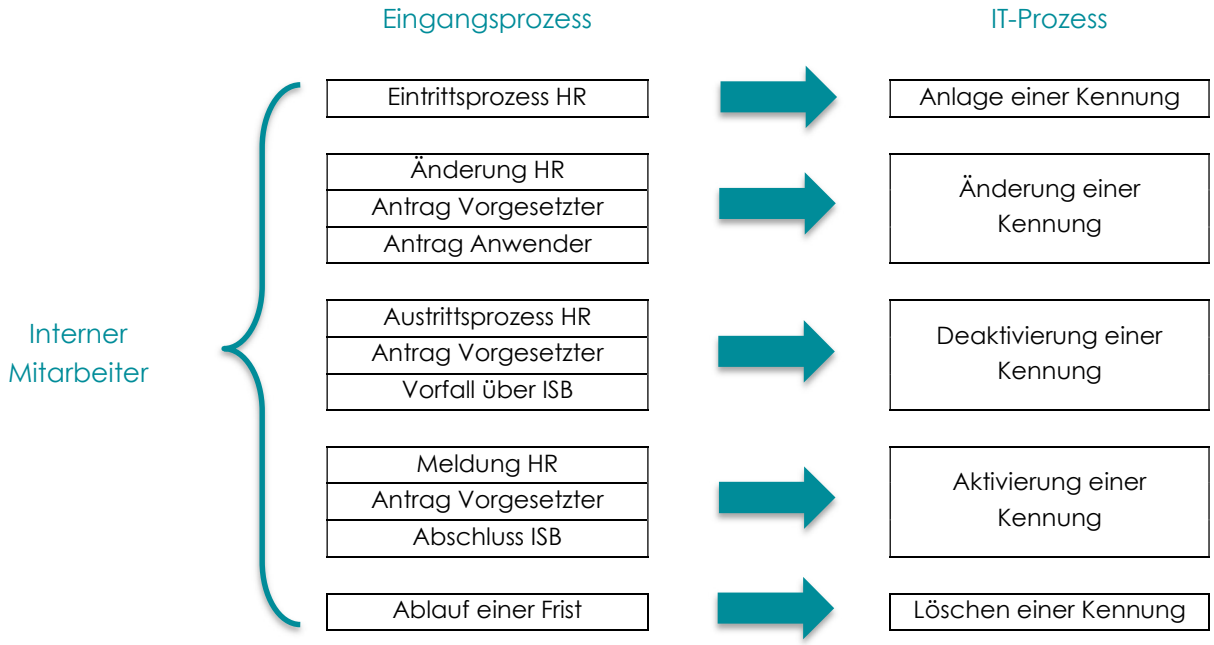
4. Benutzer-Prozesse

Verschieden Arten von Zugangs-Kennungen hängen oft an unterschiedlichen Prozessen oder Workflows. Z.B. ist der Einstellungsprozess für einen Mitarbeiter ein anderer als die Beantragung einer Test-Kennung. Diese Prozesse müssen detektiert werden und an die IT-Prozesse angebunden werden. Nur so ergibt sich ein funktionierendes Konstrukt.

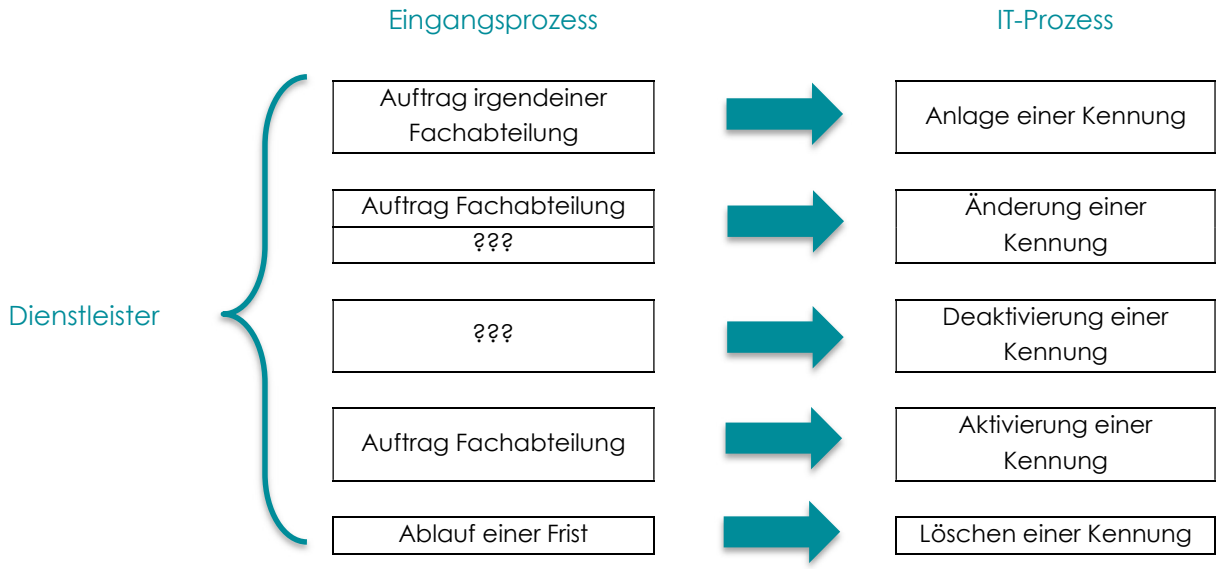
Generell gibt es vier grundlegende IT-Prozesse für Kennungen:

- Anlage einer Kennung
- Änderung einer Kennung
- Deaktivierung einer Kennung
- Löschung einer Kennung

Der einfachste Prozess, der in jedem Unternehmen funktioniert, ist die Anlage einer Kennung. Wenn dieser ins Stocken kommt, eskaliert die Situation oft sehr schnell. Die nicht erfolgte Löschung einer Kennung eskaliert dagegen eher selten, birgt aber ein deutlich höheres Sicherheitsrisiko.
Um überhaupt die Schnittstellenprozesse zu verstehen, macht es Sinn, die Abhängigkeiten mit den Eingangsprozessen darzustellen.
Schauen wir uns bei der Verwaltung von internen Mitarbeitern an, welche Eingangsprozessen die IT-Prozesse nach sich ziehen. Die Eingangsprozesse sind üblicherweise HR-Prozesse, können jedoch auch ganz andere Prozesse sein. Beispielsweise kann ein Sicherheitsvorfall die Deaktivierung eines Zugangs nach sich ziehen. Nachfolgende Tabelle ist nur ein Beispiel, das keinen Anspruch auf Richtigkeit oder Vollständigkeit beansprucht und in jedem Unternehmen ganz anders aussehen kann.



Betrachten wir die identischen IT-Prozesse für externe Dienstleisters, so finden sich völlig andere Eingangsprozesse.



Hier fallen zwei Dinge auf.
Zum einen sind die Prozesse nicht mehr so eindeutig und kommen aus diversen Bereichen und zum anderen fehlt der eine oder andere definierte Prozess, bzw. es gibt keinen Sachzwang. Das heißt, wenn die Fachabteilung es versäumt, die Änderung oder Beendigung eines Dienstleister-Vertrages an die IT-Abteilung zu melden, bleibt die Kennung bestehen. Das passiert in der Praxis leider sehr häufig.

> Alle Prozesse, die zur Anlage, Änderung oder Löschung einer Kennung führen, müssen bekannt sein und/oder festgelegt und bekannt gemacht werden. Nur so lassen sich Zugangs-Kennungen sicher verwalten und die IT-Prozesse automatisieren.

5. Automatisierungs-Ansätze

Die Automatisierung der IT-Prozesse bringt mehrere Vorteile mit sich:

- Deutlich schnellere Umsetzung von Anträgen und Veränderungen
- Einsparung von Personal
- Erhöhung der Informationssicherheit

Außer der bisher erwähnten IT-Prozesse zur Anlage, Änderung und Löschung von Zugangskennungen ist es wichtig, Kontroll-Prozesse einzuführen. Diese Kontrollen sollen unter anderem Folgendes erkennen und darauf reagieren:

- Inkonsistenzen
- menschliche Eingabe-Fehler
- Fehlverhalten, Umgehen von Vorgaben
- Mangel in Eingangsprozessen
- Angriffe und Sicherheitsvorfälle

Wir setzen uns nachfolgend mit einigen Szenarien und Beispielen auseinander. Ob und was Sie in welchem Umfang und wie automatisieren, hängt immer von Ihrer Umgebung ab.

5.1 Vorbereitung

Hinter jeder Art von Automatisierung steckt irgendeine Art von Programmierung. Auch wenn von künstlicher Intelligenz gesprochen wird, steckt dahinter eine Programmierung. Die Kunst besteht vor allem darin, die vorhandenen Daten so aufzubereiten, dass das Ergebnis sehr komplex, sehr schnell und innovativ berechnet und dargestellt wird.

Für eine Programmierung, sei es eine API, eine individuelle Schnittstelle oder eine Programmfunktion einer vorhandenen Applikation, müssen vorab folgende Dinge eindeutig festgelegt bzw. strukturiert werden:

- Alle Typen von Kennungen müssen identifiziert und festgelegt werden
- Für alle Typen von Kennungen müssen alle notwendigen Attribute festgelegt werden
- Alle Typen von Kennungen müssen eine eindeutige Typ-Kennzeichnung haben
- Alle Prozesse und Regeln müssen eindeutig definiert werden
- Alle Eingangsprozesse und ggf. Ausgangsprozesse müssen identifiziert und wenn möglich vereinheitlicht werden

Beispielsweise muss festgelegt werden, nach welcher Zeit ein Zugang für einen Dienstleister abläuft. Dabei müssen sinnvolle Regeln, die die Informationssicherheit unterstützen, beachtet werden. So ist eine Ablaufzeit von 10 Jahren nicht sinnvoll. Besser ist es hier, jährlich eine Überprüfung durchzuführen, um dann ggf. die Laufzeit zu verlängern.

5.2 Vorhandene Programmfunktionen nutzen

Die simpelste Automatisierung, die bestimmt viele intuitiv nutzen, sind Funktionalitäten, die im Active Directory bereits hinterlegt sind. So lässt sich z.B. ein Ablaufdatum direkt bei der Kennung hinterlegen und nach Erreichen des Datums wird die Kennung automatisch gesperrt. Etwas mehr versteckt sind die Funktionen zur automatischen Kennwort-Erneuerung. Zum einen darf die Eigenschaft „läuft nie ab“ in der Kennung nicht aktiviert sein, zum anderen erfolgen die Einstellungen der Kennwort-Vergabe über sogenannte Gruppenrichtlinien (group policies oder auch GPOs). Dort werden Konfigurationen, wie z.B. „wie häufig muss ein Passwort geändert werden“ und „Komplexität der Kennwörter“ hinterlegt.
Wichtig hierbei ist die Vorbereitung (siehe vorheriges Kapitel) und die dazugehörige Festlegung von Parametern, die der gesamten Organisation bekannt sind und vom Management unterstützt werden. Jegliche Ausnahmen gefährden die Sicherheit und verursachen Mehraufwand.

Unabhängig von den Möglichkeiten im AD bieten manche Applikationen, wie z.B. HR-Systeme eine AD-Anbindung an. D.h. das HR-System steuert zum Teil die Verwaltung der AD-Kennungen. Im Normalfall handelt es sich dabei um die Kennungen der Mitarbeiter. Andere Zugänge können nicht verwaltet werden. Ebenso mangelt es oft an der Möglichkeit für unterschiedliche Benutzertypen unterschiedliche Basis-Eigenschaften festzulegen.

Weiterhin gibt es Systeme am Markt, die die Verwaltung der AD-Zugänge abnehmen und unterstützen. Somit lassen sich Benutzer leichter anlegen, suchen oder filtern, haben Schnittstellen zu weitern Systemen und erzeugen Reports, wer z.B. sein Passwort am häufigsten falsch eingegeben hat.
Automatisierungen finden sich eher seltener.

5.3 APIs

APIs oder „Application Programming Interfaces" werden definierte Schnittstellen zu Applikationen genannt. Auch das Active Directory bietet eine Art von APIs. Jedes Windows-System bringt diese Schnittstellen mit. Zum einen lässt sich die integrierte „.NET" Umgebung nutzen, zum anderen bietet sich PowerShell als mächtiges Werkzeug an. Veraltete Techniken über VBS oder WMI sind natürlich noch möglich, aber davon ist deutlich abzuraten. Für PowerShell gibt es eine Vielzahl von Erweiterungen, so auch für die AD-Schnittstelle.
Wenn nun die am Prozess beteiligten Applikationen und Workflows ebenfalls eine nutzbare Schnittstelle mitbringen, lassen sich die beiden Systeme verknüpfen.
Nehmen wir als Beispiel folgendes an. Das HR-System erzeugt bei der Anlage eines neuen Mitarbeiters automatisch eine Export-Datei. Mit einer automatischen Überwachung des Exports und eines einfachen PowerShell-Skriptes kann nun ohne manuelles Zutun die Kennung im AD erzeugt werden.
Dabei muss der Workflow mit Abarbeitung der Anlage des AD-Objektes nicht enden. Ein Postprozess im Automatismus kann z.B. das Kennwort an eine bestimmte Stelle verschlüsselt übertragen oder ein Postfach angelegen oder Zugänge zu weiteren Systemen erzeugen. Zusätzlich lassen sich Dokumentationen oder Tickets erstellen (oder auch schließen).

Mittels einer geschickten Programmierung können eine Vielzahl der Standard-Prozesse zur Anlage, Änderung und Löschung automatisiert werden. Dabei werden Inkonsistenzen und Tippfehler vermieden, Workflows beschleunigt und insgesamt steigt die Benutzer-Zufriedenheit.

6. Automatisierungen zur Erhöhung der IT-Sicherheit

Ein weiterer großer Vorteil der Nutzung von Automatisierungen stellt eine Risikominimierung im Umgang von AD-Kennungen dar. Der Markt bietet nur sehr wenig standardisierte Produkte an, die dies leisten. Insbesondere werden „Events" oft nur dargestellt, es erfolgt aber keine Handlung und es ist ein manueller Eingriff bzw. Entscheidung notwendig. Nehmen wir als Beispiel die Eigenschaft „never expires", also dass ein Passwort niemals abläuft. Viele Produkte listen diese Kennungen auf, aber eine automatische Korrektur ist nicht möglich. D.h. ein IT-Administrator muss regelmäßig die Reports durchsehen und abarbeiten und Missstände manuell beheben.

Beispiel:
Eine Regelung heißt: „Alle internen Mitarbeiter müssen ihr Kennwort alle 90 Tage ändern“. Ein automatisiertes Skript überprüft regelmäßig alle Kennungen aller internen Mitarbeiter. Wenn eine Einstellung im Active Directory nicht korreliert, dann wird diese automatisch entsprechend der Regelung geändert. Wenn ein Kennwort länger als 90 Tage aktiv ist, wird eine Passwort-Änderung bei der nächsten Anmeldung erzwungen. Zusätzlich wird noch ein Protokoll geschrieben oder ein Ticket erzeugt, in der die Korrektur vermerkt wird.
Wie dieses Beispiel aufzeigt, ergeben sich jede Menge Möglichkeiten, um mittels Automatisierung eine Umgebung stabil und auf einem hohen Sicherheitsniveau zu halten. In der nachfolgenden Tabelle finden Sie weitere Beispiele, die mit beispielhaften Workflows oder Maßnahmen verknüpft sind, die daraus folgen. Die Liste erhebt kein Anspruch auf Vollständigkeit und soll nur als Inspiration dienen.

Automatisierung		Ausgabe, Workflow, Folge
Check, ob alle notwendigen Attribute bei einem Mitarbeiter eingepflegt worden sind (Vorname, Name, Telefon, Lokation, Gruppenzugehörigkeit, Berechtigungen)	→	Ticket-Erzeugung
Check, ob „never expired“ angekreuzt	→	Automatische Korrektur, Attribut ändern
Check, ob bei Dienstleister die Kennung ein Ablaufdatum hat und ob dieses jünger ist als 1 Jahr	→	Automatische Korrektur, Datum setzen, wenn fehlt bzw. Datum verkürzen, wenn länger als 1 Jahr
Check, ob Kennung innerhalb den nächsten 4 Wochen abläuft	→	Information Verantwortlicher, Anstoß Workflow zur Wiedergenehmigung
Check, ob eine Kennung länger als 90 Tage abgelaufen ist	→	Automatische Deaktivierung
Check, ob interner Mitarbeiter im Personalsystem vorhanden ist	→	Automatische Deaktivierung
Check, ob sich ein Mitarbeiter/Dienstleister in den letzten 100 Tagen angemeldet hat	→	Automatische Deaktivierung
Check, ob Kennung länger als 90 Tage deaktiviert	→	Automatische Löschung
Erkennung zu häufiger Anmeldeversuche	→	Automatische Sperrung und Ticket-Erzeugung
Erkennung ob an vielen unterschiedlichen Rechner angemeldet wurde		Ticket-Erzeugung
Erkennung Anmeldeversuche an nicht berechtigten Systemen	→	Ticket-Erzeugung
Check, ob sich die Gruppe der Administratoren verändert hat	→	Alarm auslösen, bzw. ID aus der Gruppe löschen
Check, wann Benutzer Kennwort zuletzt geändert haben	→	Kennwort-Änderung veranlassen, Ticket-Erzeugung
Passwort-Sicherheit (Länge) überprüfen	→	Kennwort-Änderung veranlassen, Ticket-Erzeugung

Check, ob Mail-Zugang noch benutzt wird	→	Automatische Sperrung des Mail-Zugangs
Nutzung von administrativen Kennungen für nicht administrative Aufgaben	→	Ticket-Erzeugung, Info-Mail Erzeugung an Vorgesetzten

7. Zusammenfassung, Ausblick

Automatisierungen im Umfeld eines Active Directorys können Fehler vermeiden, Aufwände verringern und Sicherheitslücken erkennen. Bereits essenzielle Tools, wie Konsistenzprüfungen helfen auch in kleineren Umgebungen die Stabilität und Sicherheit zu erhöhen.

Ausgangspunkt für alle Aktivitäten sind

- **Klare und strukturierte Verwaltung**
- **Klare Definition von Regeln**

Für die meisten Prozesse ist es wichtig, sich die Management-Unterstützung zu sichern. Es müssen dabei die Risiken vorab aufgezeigt werden. Denn spätestens, wenn das Management Passwörter ändern muss und es dazu vorab keine Abstimmung gab, können Sie sicher sein, dass die erste Ausnahme geschaffen wird. Und Ausnahmen erhöhen generell die Arbeitslast und verringern die IT-Sicherheit.

> Automatisierungen können helfen, Fehler zu vermeiden, IT-Sicherheit zu erhöhen und Aufwände zu verringern. Diese sind nur auf einer strukturierten Basis möglich.

In einem weiteren Artikel werden wir beispielhafte Powershell-Scriptlets veröffentlichen, mit Hilfe derer Automatisierungen umgesetzt wurden.

Über advisio

Das Team der advisio GmbH besteht aus kompetenten Mitarbeitern, die langjährige Erfahrung im Informationssicherheits-Umfeld, im Datenschutz, bei Digitalisierung und weiteren Betriebsprozessen haben.

Der Aufbau eines Informationssicherheitsmanagement-Systems (ISMS), wie auch durch NIS2 gefordert, gehört zu unseren Kernkompetenzen. Business Impact Analysen, Risikoanalysen, Erstellung von Maßnahmenplänen, Schulungen und Notfallplanung werden auf Wunsch durch unsere Fach-Spezialisten durchgeführt. Dies nicht nur im Aufbau, sondern auch im Betrieb eines ISMS. Durch entsprechende Zertifizierungen können wir Sie bei Bedarf bis zur ISO-Zertifizierung nach 27001:2022 oder anderen Standards führen.

Über den Autor

Martin Zeyer ist Diplom Informatiker und Spezialist für Informationssicherheit und IT-Service Management.
Seit Anfang der 1990 Jahre beschäftigt Herr Zeyer sich mit Themen der Informationssicherheit und dem IT-Servicemanagement und begleitet namhafte Unternehmen verschiedener Branchen – u.a. Mercedes Benz, T-Systems International GmbH, SPIRIT/21 AG.
Den defacto Standard ITIL begleitet Martin Zeyer als Experte bereits seit frühen Versionen.
Bereits frühzeitig spezialisierte sich Herr Zeyer zudem auf Managementsysteme für Informationssicherheit nach verschiedenen Standards wie der internationalen Norm ISO/IEC 27001 und dem BSI-Grundschutz.
Über Jahre dozierte Herr Zeyer an der Hochschule für Wirtschaft und Umwelt Nürtingen-Geislingen (HfWU) zur Wirtschaftsinformatik.