Offboarding ohne Restzugriffe: Tokens, Apps und geteilte Geheimnisse

PRUEFEN. BELEGEN. NACHHALTEN.

Für einen autorisierten Austritt in einer Entra-/M365-Umgebung mit weiteren SaaS- und Entwicklungsdiensten. Richtwert: 90 Minuten für eine vorbereitete Person und ausgewählte kritische Anwendungen; Wartezeiten, Datensicherung und Sonderfälle zusätzlich. Aufbewahrung und Übergabe vor Löschung klären.

Pruefbereich / Team:

Datum:

- [ ] **01 / Identitäten und alternative Zugänge der Person dienstübergreifend erfassen, einschließlich lokaler SaaS-Konten, VPN, SSH-Schlüssel und persönlicher API-Tokens.**

  Nachweis: Abgeglichenes Austrittsinventar mit je einem verantwortlichen Dienstbetreiber; offene unbekannte Zugänge markiert.

- [ ] **02 / Zum vereinbarten Zeitpunkt Anmeldung in den zuständigen Identitätsquellen sperren und die erfolgreiche Übernahme in abhängige Verzeichnisse prüfen.**

  Nachweis: Sperrzeitpunkte, Synchronisationsstatus und abgewiesene frische Anmeldung des freigegebenen Testkontos.

- [ ] **03 / Entra-Sitzungen widerrufen und je kritischer Anwendung eigene Sitzungen beziehungsweise lokale Konten gesondert beenden.**

  Nachweis: Widerrufsprotokolle und dienstbezogene Restgültigkeitsprüfung; Access-Token- und Cookie-Verhalten dokumentiert.

- [ ] **04 / Rollen, Gruppen, direkte Freigaben und delegierte Zugriffsrechte entfernen; anonyme Freigabelinks separat auf Weitergabe und Erforderlichkeit prüfen.**

  Nachweis: Vorher-nachher-Export und wirksame Zugriffsentscheidung auf benannten Testressourcen.

- [ ] **05 / App-Eigentümerschaft und erteilte Einwilligungen prüfen; weiter benötigte Anwendungen übergeben und unnötige Grants gezielt entziehen.**

  Nachweis: App-Liste mit neuem Eigentümer; delegierte Grants, App-only-Berechtigungen und andere Ressourcenzuweisungen getrennt bewertet.

/ MAURISEC.DE

FIELD NOTES / CHECKLIST 15

- [ ] **06 / Geteilte Geheimnisse mit Kenntnis der Person risikobasiert ersetzen und den alten Wert im Zielsystem unwirksam machen.**

  Nachweis: Rotations- und Widerrufsnachweis ohne Geheimnisinhalt; Abhängigkeiten und erfolgreicher Dienstbetrieb geprüft.

- [ ] **07 / Betriebliche Daten, Automationen und Geräte kontrolliert übergeben; notwendige Aufbewahrung vor Konto- oder Lizenzlöschung sichern.**

  Nachweis: Abgenommene Zuständigkeiten, Datenzugang der Nachfolge und dokumentierter Umgang mit Geräten und gespeicherten Kopien.

- [ ] **08 / Nach dem dienstbezogenen Widerrufsfenster erneut nach Zugriffen suchen und Restfälle mit Frist und Eigentümer offenhalten.**

  Nachweis: Zeitbezogene Auswertung erfolgreicher und verweigerter Zugriffe; Abschluss erst nach Prüfung der kritischen Anwendungen.

GEGENPROBE / AUTORISIERTE TESTUMGEBUNG

Mit einem eigens dafür angelegten Testkonto vor dem Übungsaustritt eine Sitzung in einer benannten Testanwendung öffnen. Nach Sperre und Entra-Widerruf dieselbe harmlose Testressource über diese bestehende Sitzung abrufen. Bestehen: Der separat vorgesehene App-Widerruf beendet den Zugriff innerhalb des dokumentierten Zielzeitraums; eine fortbestehende Sitzung wird als Restzugriff erfasst.

GRENZEN UND VORAUSSETZUNGEN

Kontosperre, Passwortwechsel und Session-Widerruf sind unterschiedliche Maßnahmen. Entra kann ein von der Anwendung ausgestelltes Sitzungscookie nicht direkt widerrufen; CAE gilt nur für unterstützte Kombinationen. App-only-Zugriffe hängen nicht vom ausgeschiedenen Benutzer ab. Bereits heruntergeladene Daten lassen sich durch Kontosperre nicht zurückholen.

PRIMAERQUELLEN / STAND 09.11.2026

Microsoft Learn: Revoke user access
learn.microsoft.com

Microsoft Learn: Remove a former employee and secure data
learn.microsoft.com

Microsoft Learn: Review permissions granted to enterprise applications
learn.microsoft.com

OWASP NHI1:2025: Improper Offboarding
owasp.github.io

OWASP: Secrets Management Cheat Sheet
cheatsheetseries.owasp.org