/ MAURISEC.DE

FIELD NOTES / CHECKLIST 05

Identity Incident: eindämmen, Spuren sichern, Zugriff prüfen

PRUEFEN. BELEGEN. NACHHALTEN.

Für autorisierte Reaktion auf einen vermuteten kompromittierten Entra-/Microsoft-365-Benutzer. Maßnahmen mit Vorfallleitung und Betriebsverantwortlichen abstimmen; Beweissicherung und erforderliche Eindämmung parallel planen. Quellenstand: 09.11.2026.

Pruefbereich / Team:

Datum:

- [ ] **01 / Betroffenes Konto, Zeitpunkt, Meldeweg und vermutete Folgezugriffe erfassen; Hypothesen von bestätigten Befunden trennen.**

  Nachweis: Fall-ID, Zeitleiste, Quellen und dokumentierte Unsicherheiten.

- [ ] **02 / Anmelde-, Audit- und relevante Ressourcenprotokolle rechtzeitig exportieren und nachvollziehbar sichern.**

  Nachweis: Zeitfenster, Korrelations-IDs, Exportzeit und geschützter Ablageort.

- [ ] **03 / Konto bei bestätigtem Verdacht möglichst sperren; notwendige Ausnahmen ausdrücklich entscheiden und überwachen.**

  Nachweis: Zeitpunkt und Verantwortlichkeit der Eindämmung; dokumentierter Alternativplan bei notwendiger Verfügbarkeit.

- [ ] **04 / Anmeldesitzungen und Refresh-Token widerrufen; Wirksamkeit je betroffener Anwendung überprüfen.**

  Nachweis: Ausgeführte Aktion und neue Zugriffsversuche im relevanten Ressourcenprotokoll.

- [ ] **05 / Passwort und registrierte Authentifizierungsmethoden prüfen; kompromittierte Mittel kontrolliert ersetzen.**

  Nachweis: Änderungsereignisse und sichere Wiederherstellung mit der betroffenen Person.

/ MAURISEC.DE

FIELD NOTES / CHECKLIST 05

- [ ] **06 / Neu erteilte App-Zustimmungen und Anwendungsberechtigungen untersuchen und unzulässige Freigaben entziehen.**

  Nachweis: Berechtigungsbestand, Audit-Ereignisse und überprüfter Entzug.

- [ ] **07 / Posteingangsregeln, externe Weiterleitung, Delegierungen und auffällige Mailaktivität auf Persistenz prüfen.**

  Nachweis: Vorher-Nachher-Bestand und Begründung für entfernte oder erhaltene Einstellungen.

- [ ] **08 / Anwendungseigene Sitzungen und gegebenenfalls direkt verwaltete Konten zusätzlich beenden beziehungsweise sperren.**

  Nachweis: Bestätigung der jeweiligen Anwendungsverantwortlichen und geprüfte Zugriffsverweigerung.

- [ ] **09 / Wiederfreigabe erst nach Ursachenprüfung, notwendiger Bereinigung und dokumentierter Nachkontrolle entscheiden.**

  Nachweis: Freigabe, verbleibende Risiken, Überwachungszeitraum und nächste Maßnahmen.

GEGENPROBE / AUTORISIERTE TESTUMGEBUNG

Mit einem ausschließlich dafür bestimmten Testkonto eine Sitzung widerrufen und die Restgültigkeit in der jeweiligen Testanwendung prüfen.

GRENZEN UND VORAUSSETZUNGEN

Ein Passwortwechsel oder revokeSignInSessions macht nicht jedes bereits ausgegebene Access-Token sofort ungültig. Ohne unterstützte kontinuierliche Zugriffsauswertung oder zusätzliche Ressourcenkontrollen kann Zugriff bis zum Ablauf bestehen. Auch CAE ist ressourcen- und clientabhängig; Ereignisverteilung benötigt Zeit. App-eigene Sitzungen und lokal gespeicherte Daten sind eigenständig zu behandeln. Keine Log-Treffer beweisen keinen ausbleibenden Datenabfluss.

PRIMAERQUELLEN / STAND 09.11.2026

Microsoft Learn: Revoke user access in an emergency
learn.microsoft.com

Microsoft Learn: Continuous access evaluation
learn.microsoft.com

Microsoft Learn: Respond to a compromised cloud email account
learn.microsoft.com

Microsoft Learn: Review application permissions
learn.microsoft.com