Der digitalen Souveränität verpflichtet.

Risikobasierte Checklisten

für die Entlassung eines IT-Admins

Vorwort

Es kann unterschiedliche Gründe geben, warum Mitarbeiter Unternehmen verlassen. Bei Mitarbeitern mit Zugriff auf sensible Daten, besonders IT-Admins, ist besonders bei nicht einvernehmlicher Trennung oder Unternehmensschädigung besondere Sorgfalt erforderlich.

Grundlegende Schritte sind immer sinnvoll und müssen entsprechend geplant werden. (☑)

Bei nicht einvernehmlicher Trennung oder sogar fristloser Kündigung können Zusatzmaßnahmen sinnvoll und angebracht sein. Die Prüfung der Angemessenheit mit zusätzlichen Elementen aus ☑ und ggf. ☑ ist hier wichtig, sowie eine risikobasierte Vorgehensweise.

Bei Fragen unterstützen die Sicherheitsexperten der IS4IT Sie gerne.
advisory@is4it.de Tel.: +49 89 63898480

	Art der Trennung / Risiko
☑	Einvernehmliche Trennung im Konsens. *Geringes Risiko, MA bleibt bis zum Ende tätig.*
☑	Nicht-einvernehmliche-Trennung (Betriebsbedingte Kündigungen, schlechte Arbeitsleistung, Fehlverhalten...) *Mittleres Risiko, MA wird beurlaubt, Prozess aktiv überwacht.*
☑	**Sonderfall: außerordentliche Kündigung/ fristlose Kündigung** *Hohes Risiko, zusätzliche Sonder-/Notmaßnahmen.*

1. Vorbereitende organisatorische Maßnahmen

	Aktion		
1	Vertrauenswürdigen Administrator für Prüfschritte hinzuziehen. Bei höherem Risiko zwei vertrauenswürdige Personen, damit deren Arbeiten im 4-Augen-Prinzip durchgeführt werden können.	☑	☑
2	Abklären, welche Applikationen die betroffene Person direkt bis ins Fachliche hinein betreut hat und inwieweit die Fachlichkeit von Vertretern, ggf. auch durch externe Unterstützung, übernommen werden kann.	☑	☑
3	Risikoprofil für diese Applikationen erstelle. (Auswirkungen auf den Geschäftsbetrieb)		☑
4	Sicherstellen, dass ein Spezialist für das besondere Themengebiet der betroffenen Person verfügbar ist.	☑	☑
5	Feststellen, welche alternativen Wege es für die kritischen abhängigen Geschäftsprozesse geben könnte. (Ersatz-Tätigkeiten bei Ausfall der Applikation)	☑	☑
6	Sicherstellen, dass zu allen relevanten von der betroffenen Person betreuten Systeme weitere administrative Zugänge für verbleibende IT-Administratoren bestehen.	☑	☑
7	Bei Bedarf externe Unterstützung hinzuziehen, zum Beispiel Sicherheitsberater oder Anwalt.		☑
8	Kommunikationsstrategie für verbundene Unternehmen, externe Partner, Administratoren und Rest der Mitarbeiter vorbereiten		☑
9	Kommunikation des Zutrittsverbotes planen, bei Bedarf Sicherheit/Werkschutz für eine angemessene Zeit nach Entlassung buchen. (ca. 2-3 Wochen)		☑
10	Ggf. Personen planen, die den frisch Entlassenen begleiten und den Arbeitsplatz sichern und z.B. IT-Equipment für spätere Forensik gerichtsverwertbar sicherstellen.		☑
11	Zeitlicher Ablauf zwischen Maßnahmen planen. Wichtig: Bei Risiko erst Zugänge sperren, dann informieren.	☑	☑

2. Vorbereitende technische Maßnahmen - Ablaufplan erstellen

	Aktion		
1	Externe Zugänge der betroffenen Person eruieren und Sperr-Möglichkeiten planen. (z.B. Citrix-Admin-Server, VPN-Zugänge, Direct-Access, dauerhafte Team-Viewer)	☑	☑
2	Alle (Enterprise) Domain-Admin-Gruppen überprüfen und die Sicherung betroffener Accounts planen.	☑	☑
3	Weitere privilegierte Gruppen im Active Directory, Cloud und weiteren privilegierten Systemzugriffen nach in Verbindung mit der betroffenen Person stehenden Accounts (auch technische) durchsuchen und diese dokumentieren, Sperrschritte planen.	☑	☑
4	Benutzer-Accounts in den betreuten Applikationen, insbesondere bei eigenem Benutzermanagement, dokumentieren, Kontosperrung oder Passwortwechsel planen. Passwortsafes und Dokumentation prüfen!	☑	☑
5	Benutzer-Accounts, die die betroffene Person verwaltet, dokumentieren, Sicherungsschritte planen (z.B. wg. möglicherweise angelegtem Zweitkonto oder Accountübernahme von Mitarbeiter in Elternzeit)		☑
6	Überprüfen und dokumentieren der möglicherweise bekannten generischen, nicht-personalisierten (administrativen) Konten, lokalen Benutzerkonten und technischen Accounts auf allen relevanten Systemen. Sicherungsschritte planen!	☑	☑
7	Überprüfen ob gehostete Applikationen (z.B. SAP) extern zugänglich sind und die zentrale Konto Sperrung den Zugriff verhindert. Ggf. Sicherungsschritte planen!	☑	☑
8	Prüfen und dokumentieren, welche privilegierten Zugriffe auf externe Dienste (DNS-Verwaltung, Cloud-Dienste, Einkauf) der betroffenen Person bekannt sein können. Sicherungsschritte planen!	☑	☑
9	Prüfen und dokumentieren, ob die betroffene Person Zugang zu firmeneigenen Social Media Accounts oder anderen Firmen-Kommunikationstools hat. Sicherungsschritte planen!	☑	☑
10	Zugriff auf Schlüssel und bekannte Aufbewahrungsorte prüfen und dokumentieren. Sicherungsschritte planen!		☑
11	Feststellen, welche relevante Zugangsdaten am Tag der Entlassung nicht geändert/deaktiviert werden können, ggf. Workaround zur Zugangsbeschränkung planen.		☑

3. Maßnahmen am Tag der Entlassung, Zugriff der betroffenen Person beenden

	Aktion		
1	Alle Accounts sperren, insbesondere auch lokale Accounts auf den Systemen	☑	☑
2	Externe Zugangsmöglichkeiten deaktivieren	☑	☑
3	Passworte der Standard-Accounts (z.B. „root/admin“) ändern, die der betroffenen Person bekannt sein könnten	☑	☑
4	Passworte der internen technischen Accounts ändern.		☑
5	Benutzer-Accounts im AD/EntraID/IAM, die durch die betroffene Person verwaltet wurden, deaktivieren oder ändern, sofern diese durch andere MA genutzt werden. Ggf. Account Daten ändern, MFA erneuern.		☑
6	Benutzer-Accounts in den betreuten Applikationen deaktivieren.	☑	☑
7	Passworte gemeinschaftlich genutzter Benutzerkonten ändern, auch für PasswortSafes.	☑	☑
8	Ggf. Zugangsdaten von extern erreichbaren Applikationen/ Diensten ändern.	☑	☑
9	Kommunikation gemäß Vorbereitung durchführen (immer Team-intern, bei Bedarf z.B. externe Partner informieren)		☑
10	(Elektronische) Schlösser/Schlüssel/Karten: Schlüssel und Zugangsberechtigung einziehen.	☑	☑
11	Bei Bedarf physische Schlüssel/Token einziehen – ggf. Schlösser tauschen	☑	☑
12	Sicherstellen, dass kritische Zugänge versperrt sind (ggf. Kontrolle durch Werkschutz)		☑
13	Bestätigung der Rückgabe aller Unternehmensschlüssel, Zugangstoken, Geräte und Unterlagen durch die betroffene Person (IS4IT kann bei Bedarf eine Vorlage liefern).	☑	☑
14	Firmeneigene Assets einziehen (Laptop / Mobiltelefon / Datenträger usw.)	☑	☑
15	Entlassenen schriftlich darauf hinweisen, dass er auf die Systeme von nun an nicht mehr zugreifen darf.	☑	☑
16	Person vom Werksgelände/Standort begleiten		☑
17	Die betroffene Person darf keinesfalls mehr an interne Computer oder andere Systeme.	☑	☑
18	Verhalten des Entlassenen beim Verlassen von Arbeitsplatz und Unternehmen beobachten, gegebenenfalls weitere Maßnahmen evaluieren.		☑

4. Maßnahmen ab dem Tag der Entlassung

	Aktion		
1	Direktive Ausgeben: Bei Kontaktaufnahme des Entlassenen und Fragen zu Unternehmensinformationen, Zugangsdaten oder Systemänderungen, sofort den benannten Verantwortlichen informieren.		☑
2	Weitere administrative Einheiten (z.B. SAP, Linux, Netzwerk, …) informieren	☑	☑
3	Monitoring verstärken, zumindest: ▪ bei Verwendung/Konfigurationsänderung von VPN-Zugängen ▪ Verwendung/Konfigurationsänderung des Citrix Admin-Terminal Servers ▪ Konfigurationsänderung im Active Directory ▪ Verlauf/Konfigurationsänderungen der Backup-Prozeduren ▪ Verwendung/Konfigurationsänderung der VMware Infrastructure Umgebung ▪ Verwendung/Konfigurationsänderung der administrativen Konten im Active Directory		☑
4	Ggf. Sicherheit/ Werksschutz für die nächsten zwei Wochen auch ganztags zumindest in kritischen Bereichen verstärken, z.B. Verteilerräume/ Rechenzentrum, Stromversorgung		☑
5	Umfrage bei allen verbliebenen IT-Administratoren, ob ▪ bisher unbekannte Zugänge (auch bei verbundenen Unternehmen) vorhanden sein könnten; Diese prüfen und ggf. absichern/beseitigen. ▪ welche administrativen Zugangsdaten der Entlassene im Kopf / im Besitz (Passwortmanager) haben könnte; diese Zugangsdaten ändern		☑
6	Sicherstellen, dass das Backup, auch ausgelagerte Backups und die internen Safes, außer Reichweite des Entlassenen sind und bleiben.		☑
7	Zugangsdaten, die aufgrund zu erwartender Schwierigkeiten nicht sofort geändert/deaktiviert werden konnten, nacheinander abarbeiten	☑	☑
8	Ggf. Überwachen von Social Media / Foren / Internetauftritte auf böswillige Einträge mit Bezug auf das Unternehmen.		☑
9	Liste der noch von betroffener Person abzugebenden Dingen verfolgen	☑	☑

5. Sonderfall: außerordentliche Kündigung / fristlose Kündigung

In Sonderfällen wie beispielsweise Mitarbeiterkriminalität, Spionage, Verdacht auf baldigen Angriff /Anschlag oder Schädigung des Unternehmens müssen kurzfristig folgende zusätzliche Ad-hoc-Maßnahmen mit Spezialisten vorbereitet werden:

☑	Ggf. ist dies ein Notfallstab-/Krisenstabsthema, besonders bei (drohenden) Schäden!
☑	Externe Unterstützung z.B. durch IT-Sicherheitsspezialisten oder Anwälte involvieren.
☑	Verwischen der Spuren verhindern. Dazu Quellen für forensische Untersuchung erheben. Die unerkannte Erstellung forensischer Kopien oder den Einzug des Gerätes am Tag zeitgleich zur Entlassung sicherstellen.
☑	Prüfung auf mögliche Mittäter durchführen.
☑	Ggf. Polizei oder zivile Ermittler einschalten und Vernehmung vorbereiten.
☑	Administrations-Team informieren, um weiteren Zugriff des Mitarbeiters zu verhindern.
☑	Vertrauensleute der Person erheben. Gespräche führen, um weiteren Zugriff des Mitarbeiters zu verhindern.
☑	Flurfunk vermeiden! Interne Kommunikation vorbereiten.
☑	Aktive Sicherheitsprüfung aller privilegierten Zugänge im Vier-Augenprinzip durchführen. Gibt es Hinweise auf weitere Zugriffsmöglichkeiten des Entlassen?
☑	Tägliche Sicherheitsüberwachung auf unerlaubte Zugriffe für z.B. 2-3 Wochen durchführen
☑	Bei Verdacht auf Hintertüren: Notfallplan zur Sicherung der Administration erstellen.

Bei Fragen unterstützen die Sicherheitsexperten der IS4IT Sie gerne.
advisory@is4it.de Tel.: +49 89 63898480