Checkliste für die Sicherheit beim Mitarbeiter-Offboarding

Eine gemeinsame Anstrengung von HR, IT und Sicherheit

Austretende Mitarbeiter stellen eines der größten Risiken für Insider-Bedrohungen dar. Daher ist es entscheidend, dass jedes Unternehmen den Sicherheitsaspekt im Offboarding-Prozess integriert. Diese Checkliste kann Ihnen dabei helfen.

Bleiben Sie im Einklang – HR, IT und Sicherheit müssen ab dem Moment der Kündigung oder des Rücktritts als Einheit agieren. Das bedeutet, dass alle gleichzeitig benachrichtigt werden und automatisch einen gemeinsamen Offboarding-Prozess starten.

Den Rückspiegel prüfen - Die 90 Tage vor dem Verlassen eines Unternehmens sind ein kritisches Zeitfenster für verdächtige Datenaktivitäten. Incydr führt eine automatische historische Analyse für die Dateiaktivität jedes ausscheidenden Mitarbeiters oder Auftragnehmers durch, damit Sie ungewöhnliches Verhalten rechtzeitig erkennen können.

Zugriff entziehen, Verantwortlichkeiten übertragen – Wenn die Person, die das Unternehmen verlässt, ein Systemadministrator, App-Inhaber oder für Lieferantenbeziehungen verantwortlich ist, stellen Sie sicher, dass deren Zugriff entfernt und die Zuständigkeiten vor dem Ausscheiden übertragen werden.

Liste erstellen, dreimal prüfen – Erstellen Sie eine Liste aller Apps, Systeme, Geräte, Werkzeuge, Ressourcen, Schlüsselanhänger, Zugangscodes und alles andere, auf das austretende Mitarbeiter Zugriff haben – fragen Sie ihren Vorgesetzten nach etwaigen unbekannten Spuren.

Vor dem Ausstieg befragen – Mitarbeiterfeedback einholen und klare Erwartungen nach dem Beschäftigungsverhältnis festlegen. Warum verlassen sie das Unternehmen? Gibt es eine Wettbewerbsklausel oder eine Abwerbeklausel? Verstehen sie alle relevanten Richtlinien zur akzeptablen Nutzung?

Forensisch werden – Validieren Sie die Austrittsbefragungen Ihrer Mitarbeiter mit einer risikobasierten Analyse ihrer Rolle, Dienstzeit, Cyberverhalten, Austrittsgründe und Datenzugriffe. Wenn sie als hohes Risiko eingestuft werden, verfolgen Sie ein strengeres Offboarding-Programm.

Das Offboarding selbst – Denken Sie daran, das Datenverhalten während des gesamten Offboarding-Prozesses zu überwachen (wiederum mit etwas wie derIncydr-Watchlist für austretende Mitarbeiter). Nur weil in den letzten 90 Tagen nichs Auffälliges gemeldet wurde, schützt das nicht vor letzten verdächtigen Aktivitäten.

An ihrem letzten Tag

Alles zurückholen – Stellen Sie sicher, dass alle Firmeneigentümer (insbesondere Geräte und Ausweise) gesammelt und den richtigen Teams zurückgegeben werden.

Abschalten – Beginnen Sie den Prozess zur Abschaltung des Systemzugriffs, sobald derMitarbeiter das Unternehmen verlässt.

www.mimecast.com | ©2025 Mimecast | All Rights Reserved | DE07450