PRODATIS®

The eBusiness Solution Company.

Ausscheidende Mitarbeiter: Das müssen Sie prüfen

Ehemalige Beschäftigte können gewollt oder ungewollt zu einem großen Datenrisiko werden. Nur ein durchdachtes Verfahren für Kolleginnen und Kollegen, die aus dem Unternehmen ausscheiden, kann hier gegensteuern. Prüfen Sie deshalb diese Verarbeitungstätigkeit Ihres Unternehmens oder Ihrer Behörde.

Ausscheidende Mitarbeiter: Wo ist das Problem?
Ausscheidende Beschäftigte sind ein Risiko für personenbezogene Daten ebenso wie für Geschäftsgeheimnisse.

Ehemalige Mitarbeiterinnen und Mitarbeiter dürfen keine Berechtigungen und Rollen behalten, die ihnen ermöglichen, weiterhin auf Daten zuzugreifen (Angriffsrisiko „unbefugte Zugriffe“ durch fehlerhafte Berechtigungssysteme und veraltete Rollenkonzepte).

In der Praxis geschieht allerdings genau das. Das IT-Unternehmen Ivanti hat 400 IT-Profis zu On- und Offboarding-Prozessen in Unternehmen befragt, also zur Integration und zum Ausscheiden von Mitarbeiterinnen und Mitarbeitern.

Die Ergebnisse zeigen einen deutlichen Handlungsbedarf:

- Die größte Herausforderung für die Datensicherheit besteht darin, dass On- & Offboarding Prozesse von Mitarbeitern nicht klar definiert sind (24 Prozent).
- Ein weiterer Aspekt sind die internen Mitarbeiterwechsel. Hier vertraut mehr als die Hälfte der Befragten darauf, dass die IT unnötige Zugriffsrechte entfernt.

Verlassen Mitarbeiter Unternehmen komplett, muss vor allem die IT-Abteilung die Ärmel hochkrempeln. So kosten Unternehmensaustritte 26 Prozent der befragten IT-Mitarbeiter mehr als eine Woche Arbeitszeit.

Selbst dann kann nur knapp die Hälfte aller IT-Experten relativ sicher sagen, dass die Ex-Kollegen über keine Zugriffsrechte mehr verfügen.

Abgesehen davon gab die Hälfte aller Umfrageteilnehmer an, dass sie jemanden kennen, der noch Zugang zu den Anwendungen und Daten eines ehemaligen Arbeitgebers hat.

Ausscheidende Mitarbeiter: Was sind die größten Risiken?
Als Risiken durch ausscheidende Mitarbeiter nannten die Befragten:

- Verlust sensibler Daten (38 Prozent)
- Cybersicherheits-Hacks über ein nicht verwaltetes Konto (26%)
- Einschleusen von Schadsoftware und Datendiebstahl (24%)

Viele Unternehmen fürchten, dass gerade in so knapp besetzten Bereichen wie der IT Beschäftigte kündigen. Denn das verschärft die Personalknappheit und wichtiges Wissen geht verloren. Damit gerät auch die Produktivität anderer Bereiche in Gefahr.

Nicht zuletzt besteht das Risiko, dass ehemalige Arbeitnehmer zu Wettbewerbern gehen, ihr Know-how über das Unternehmen zu Geld machen oder sogar selbst zu Angreifern und Industriespionen werden. Das legt die Ivanti-Umfrage nahe.

Wo setzen Sie mit der Datenschutzkontrolle an?
Aus Sicht des Datenschutzes ist es deshalb wichtig, die Datenschutzkontrolle bei Verfahren rund um ausscheidende Mitarbeiter sehr genau zu nehmen und hier auch aktuelle Entwicklungen zu berücksichtigen.

Prüfen Sie diese Verarbeitungstätigkeit daher nicht nur regelmäßig. Bringen Sie sie auch fortlaufend auf einen aktuellen Stand.

Berechtigungs- und Rollenkonzept anpassen
Neue Technologien wie Cloud Computing bringen eine ganze Reihe möglicher Risiken mit sich, wenn Arbeitnehmer ihren Abschied nehmen. Ziel muss es immer sein, dass aus dem Kollegenverlust nicht noch ein Datenverlust wird, aus dem eigenen Angestellten nicht plötzlich ein potenzieller Angreifer.

Ein erster wichtiger Schritt ist, den ausgeschiedenen Mitarbeiter bei Projekten, Abteilungen oder sogar im ganzen Unternehmen im Berechtigungs- und Rollenkonzept zu berücksichtigen:

- Es darf auf keinen Fall möglich sein, dass ein ehemaliger Beschäftigter noch Passwörter für die IT-Systeme des früheren Arbeitgebers hat und sie dann zum Beispiel via Fernzugriff einsetzt.
- Ebenso darf es nicht passieren, dass sich Ex-Kollegen eigene Hintertüren anlegen. Damit sind neue und zusätzliche Benutzerzugänge gemeint, die aktiv und nutzbar bleiben, auch nachdem das Unternehmen das Hauptkonto deaktiviert und gelöscht hat.

Mobile Endgeräte, Clouds und Social Media nicht vergessen
Besonders leicht kann es passieren, dass neue Technologien im Prozess „Ausscheidende Mitarbeiter" unter den Tisch fallen.

Das etablierte Verfahren, das abläuft, wenn ein Mitarbeiter ausscheidet, ist meist ein erprobter Laufzettel. Dieser Laufzettel ist aber womöglich seit Jahren unverändert, obwohl in den letzten Monaten und Jahren

- mobile Endgeräte,
- mobile Apps,
- BYOD (Bring Your Own Device),
- Cloud-Services und
- soziale Netzwerke

zur betrieblichen Nutzung eingeführt wurden.

Ausscheidende Mitarbeiter: Was müssen Sie prüfen?
Kontrollieren Sie als Datenschutzbeauftragte oder Datenschutzbeauftragter den Laufzettel. Berücksichtigt der Laufzettel die folgenden kritischen Punkte, die allesamt zu ungewolltem Datenverlust und zu möglichen unerlaubten Datenzugriffen führen können?

Mobile Endgeräte / mobile Apps / BYOD:

- Manchmal überlassen Unternehmen ihren ehemaligen Arbeitnehmern das nicht mehr ganz aktuelle Smartphone. Darauf aber könnten sich noch betrieb-

liche Daten befinden. Sie müssen gesichert und auf dem Gerät sicher gelöscht werden, bevor der Ex-Mitarbeiter es bekommt.
- War es dem Kollegen erlaubt, ein privates Gerät zu nutzen, oder wurde das vielleicht geduldet, können sich darauf ebenfalls betriebliche Daten befinden. Die IT muss sie sichern und lokal löschen.
- Es kann zudem sein, dass sich betriebliche Apps mit Zugang zu betrieblichen Netzwerken oder Clouds auf den privaten Endgeräten befinden. Typisches Beispiel ist eine E-Mail-App für den betrieblichen Mail-Dienst. Diese Apps müssen entfernt werden, wenn der Beschäftigte das Unternehmen verlässt.

Cloud Computing:
- Sorgen Sie dafür, dass die IT die Zugänge für betriebliche Cloud-Services deaktiviert und nach der Sicherung die Cloud-Daten löscht, wie dies für lokale und Netzwerk-basierte Dienste der Fall ist.
- Waren bei mobilen Kollegen Cloud-Speicherdienste für den Austausch von Daten im Einsatz, müssen auch diese gesichert, geleert und deaktiviert werden.
- Hat der Verantwortliche einen privaten Cloud-Dienst für den Datentransfer geduldet, müssen auch hier die betrieblichen Daten entfernt werden.

Soziale Netzwerke:
- Genau wie bei Netzwerk- und Cloud-Dienstenmuss die IT die betrieblichen Zugänge der ausscheidenden Mitarbeiter deaktivieren und nach der Sicherung entfernen.
- Durfte der Mitarbeiter seine (privaten) Zugangsdaten zu sozialen Netzwerken auch für betriebliche Logins nutzen (Social Sign-in), muss diese Berechtigung entfernt werden.

Nutzen Sie die Arbeitshilfe, um zu prüfen, ob die Verarbeitungstätigkeit in Ihrem Unternehmen oder in der Behörde bereits neue Technologien und Datenrisiken berücksichtigt.

Download:
Checkliste: Verarbeitungstätigkeit Ausscheidende Mitarbeiter

Quelle:
www.datenschutz-praxis.de