Devolutions

Départ d'employés : votre entreprise a-t-elle une stratégie?

UN RISQUE SUR LE PLAN DU RECRUTEMENT ET DE LA RÉTENTION

Il y a à peine quelques décennies, la majorité des gens passaient leur carrière entière à travailler pour une seule entreprise, en commençant par le bas et en gravissant les échelons jusqu'à la retraite. Les choses ont bien changé!

Aujourd'hui, le travailleur moyen effectuera environ 12 changements d'emploi au cours de sa carrière. Des millions d'employés prévoient d'ailleurs changer d'emploi après la pandémie, un phénomène que les experts en ressources humaines qualifient comme étant le prochain « tsunami » du roulement de personnel. Cette grande migration représente non seulement un risque sur le plan du recrutement et de la rétention, mais aussi pour la sécurité.

1 ex-employé sur 4 peut encore accéder à ses anciens comptes

Selon une enquête récente, 25 % des travailleurs ont déclaré avoir encore accès à leurs comptes d'anciens emplois, y compris les anciens responsables informatiques et gestionnaires qui possédaient « les clés du royaume » (c'est-à-dire l'accès à des comptes privilégiés).

Évidemment, la plupart de ces anciens employés ne sont pas devenus des voyous ayant l'intention de voler des données, de faire des ravages ou de mener des activités illégales. Mais que se passe-t-il si ces individus sont attaqués par des pirates qui, au cours de leur espionnage, découvrent ces anciens comptes et leurs identifiants associés? Les conséquences pourraient être graves, voire catastrophiques. Selon le rapport 2021 d'IBM Security, les violations de données coûtent désormais 4,24 millions de dollars par incident en moyenne aux entreprises, soit le coût le plus élevé depuis les 17 années d'existence du rapport.

La solution : une stratégie de départ des employés

Pour plusieurs entreprises, lorsqu'un employé quitte (volontairement ou involontairement), on se concentre avant tout sur la récupération des actifs. Par exemple, l'employé est invité à rendre son ordinateur portable, son téléphone, les fichiers de ses clients, sa carte d'accès au bâtiment, etc. Récupérer les actifs est, de toute évidence, une partie essentielle du processus de départ, mais il y a plus encore à considérer.

Dans toute bonne stratégie de départ des employés, il est aussi extrêmement important d'appliquer un processus de suppression des accès. Celui-ci devrait inclure les éléments suivants :

1. Changer immédiatement le mot de passe de l'employé

La première (et la plus importante) étape consiste à changer le mot de passe de l'employé. De cette façon, il (ou une tierce personne avec sa permission) ne pourra plus accéder à son(ses) ancien(s) compte(s).

2. Désactiver l'accès à tous les comptes

Deux options existent pour retirer les accès des employés : supprimer un compte ou verrouiller un compte. La suppression d'un compte est à privilégier parce qu'elle élimine toute possibilité d'un accès futur. Par contre, dans certaines situations, il peut être nécessaire de conserver un compte s'il contient des données précieuses comme des fichiers importants, de la correspondance, etc. Dans ce cas, les responsables doivent verrouiller le compte jusqu'à ce que les données soient archivées ailleurs en toute sécurité (après quoi, le compte peut être supprimé).

3. Modifier les mots de passe des comptes privilégiés partagés

Le rapport de Thycotic sur l'évolution de la gestion des accès privilégiés a révélé que plus de 50 % des mots de passe des comptes privilégiés des entreprises ne sont jamais supprimés. C'est une énorme vulnérabilité

qui signifie que les anciens employés (ou les pirates qui les attaquent) peuvent toujours accéder aux comptes partagés. Pour combler cette lacune, les entreprises doivent modifier les identifiants de tout compte privilégié partagé avec un ancien employé. Parmi ces comptes, on retrouve tous ceux qui offrent des droits d'utilisateur élevés, ainsi que :

- Les comptes d'administrateur de domaine
- Les comptes d'administrateur local
- Les comptes d'accès d'urgence
- Les comptes d'application
- Les comptes système
- Les comptes de service de domaine

Comment Devolutions peut vous aider?

Devolutions aide les entreprises à mieux gérer leur stratégie de départ des employés :

- Remote Desktop Manager et Devolutions Server offrent aux entreprises une traçabilité complète de tous les comptes employés dans un emplacement centralisé. Ainsi, dès qu'un employé quitte, les comptes qui doivent être supprimés et/ou verrouillés sont clairement affichés.
- Devolutions Server et Password Hub Business disposent d'une fonction d'injection d'identifiants intégrée, ce qui permet aux employés d'accéder aux comptes (y compris les comptes privilégiés), sans jamais voir les mots de passe. Lorsqu'un employé quitte l'entreprise, il n'y a aucun risque qu'il puisse accéder au(x) ancien(s) compte(s), puisqu'il n'a jamais connu le mot de passe en question. Pour en savoir plus sur les avantages de l'injection des identifiants, c'est ici.
- Avec Password Hub Business, il n'est plus nécessaire de courir après un ancien employé pour obtenir les identifiants de son coffre d'utilisateur (c'est-à-dire le mot de passe et les données confidentielles auxquels lui seul avait accès). Au lieu de ça, le personnel informatique autorisé peut accéder au coffre d'utilisateur de tout employé, actuel ou ancien. Pour en savoir plus, c'est ici.

Le mot de la fin

Il n'y a rien de vraiment nouveau à propos des départs d'employés. Par contre, ce qui va changer, et on peut déjà en observer les signes, c'est le nombre impressionnant de personnes, tous secteurs confondus, qui vont changer d'emploi au cours des mois et années à venir.

Les entreprises qui disposent d'une bonne stratégie de départ des employés, encadrée par des outils efficaces, vont réduire leur exposition aux fuites et aux violations de données tout en augmentant leurs chances de survivre au « tsunami » du roulement de personnel.