ProfCheck

最も危険な従業員は、すでに退職届を提出しています

退職の申し出から最終出社日までのこの期間は、雇用サイクル全体で最もリスクが高い時期です。そしてそれは、劇的な情報窃取だけを指すわけではありません。実際にはこのような形で現れます：個人利用のための顧客リストのコピー。作品サンプルを手元に残すための、価格資料の私用メールへの転送。自分が書いたものだから自分のものだと思い込んでいる、社内方法論の撮影。さらに、悪意がまったくない場合もあります：誰もその存在を知らなかったために、退職から数か月経ってもクラウドアカウントが有効なまま残っている、というケースです。

この期間を閉じる方法は次のとおりです。6つのステップ：

1 申し出の日が報告の日です。退職の申し出は、その日のうちにセキュリティ責任者と情報システム部門に届きます。週明けでもなく、退職日を確定してからでもありません。

2 直ちにアクセス権を洗い出します。その従業員がどのシステム、データベース、フォルダにアクセスできるのか。そして転職先を踏まえたとき、そのうち何が特に機微なのかを確認します。

3 段階的に権限を絞ります。引き継ぎに不要なものは、最終日ではなく今すぐ閉じます。

4 この期間を監視します。異常な規模のダウンロード、私用メールへの転送、外部記憶デバイスの接続。この期間にこれを見るのは疑いではなく、最もよく知られた弱点への対処です。

5 最終日のタスクを決めます。停止すべきアカウントの確定リストを用意します。中央のユーザー管理に接続されていないクラウドサービスや外部ベンダーも含めてください。忘れられるのは、いつもそれらです。

6 退職面談をきちんと行います。秘密保持義務と知的財産に関する取り決めを改めて確認し、次の勤務先についても率直に話します。疑いからではなく、リスク管理としてです。

採用部門は、従業員がいつ組織に入ってきたかを正確に把握しています。問題は、その従業員が組織を出ていく瞬間を、誰が受け持っているのかです。