ProfCheck

أخطر موظف لديكم قدّم استقالته بالفعل

هذه النافذة، بين الإشعار واليوم الأخير، هي أعلى فترات الخطر في دورة التوظيف كلها. وهي لا تقتصر على سرقة مثيرة. تبدو أيضاً هكذا: نسخ قائمة عملاء للاستخدام الشخصي. إرسال مستندات تسعير إلى البريد الشخصي للاحتفاظ بنماذج عمل. تصوير منهجيات كتبها الموظف بنفسه، ولذلك هو واثق أنها ملكه. وأحياناً بلا نية سيئة على الإطلاق: حساب سحابي بقي مفتوحاً شهوراً بعد المغادرة، لأن أحداً لم يعرف بوجوده.

وهكذا تُغلق هذه النافذة. ست خطوات:

1. يوم الإشعار هو يوم الإبلاغ. إشعار الاستقالة يصل إلى مسؤول الأمن وإلى قسم تقنية المعلومات في اليوم نفسه. لا في نهاية الأسبوع، ولا بعد تحديد تاريخ المغادرة.

2. رسم خريطة الصلاحيات فوراً. ما الأنظمة وقواعد البيانات والمجلدات التي يملك الموظف صلاحية الوصول إليها، وأي منها حساس بوجه خاص في ضوء الجهة التي ينتقل إليها.

3. تقليص تدريجي. كل ما لا يلزم لتسليم المهام يُغلق الآن، لا في اليوم الأخير.

4. مراقبة النافذة. تنزيلات بحجم غير معتاد، وإرسال ملفات إلى بريد شخصي، وتوصيل أجهزة تخزين محمولة. في فترة النافذة هذه ليست ريبة، بل هي نقطة الضعف الأكثر شهرة.

5. مهام اليوم الأخير. قائمة مغلقة بالحسابات الواجب فصلها، بما فيها الأنظمة السحابية والمزودون الخارجيون غير المرتبطين بنظام إدارة المستخدمين المركزي. وهم الذين يُنسون دائماً.

6. مقابلة إنهاء خدمة منظمة. تذكير بالتزامات السرية والملكية الفكرية، وحديث صريح عن الوجهة التالية. ليس من باب الريبة، بل من باب إدارة المخاطر.

قسم التوظيف يعرف بدقة متى يدخل الموظف إلى المؤسسة. السؤال هو: من يمسك اللحظة التي يخرج فيها.