ProfCheck

The Most Dangerous Employee Has Already Handed In a Resignation Letter

This window, between the notice and the last day, is the highest-risk period in the entire employment cycle. And it is not only about dramatic theft. It also looks like this: copying a client list for personal use. Sending pricing documents to a private email address to keep work samples. Photographing methodologies the employee wrote themselves and therefore assumes are theirs. And sometimes with no bad intent at all: a cloud account left open for months after the departure, because nobody knew it existed.

Here is how to close it. Six steps:

1. The day of notice is the day of reporting. A resignation letter reaches the security officer and IT the same day. Not at the end of the week, not once a date has been set.

2. Immediate access mapping. Which systems, databases and folders the employee can reach, and which of them are especially sensitive given where they are going.

3. Gradual reduction. Anything not required for the handover is closed now, not on the last day.

4. Monitoring the window. Unusually large downloads, transfers to a private email address, connection of portable devices. During the window this is not suspicion, it is the best-known point of exposure.

5. Tasks for the last day. A closed list of accounts to shut down, including cloud systems and external vendors that are not connected to central user management. Those are the ones always forgotten.

6. A proper exit conversation. A reminder of confidentiality and intellectual property obligations, and an open discussion about where the person is heading next. Not out of suspicion, out of risk management.

Recruitment knows exactly when an employee joins the organization. The question is who owns the moment they leave.