Kaspersky Lab reveals cyberrevenge from ex-employee

Parting with employees is part of business. But in some cases it can be painful. Aside from fraying the nerves of managers, disgruntled ex-employees can also cause reputational and financial harm while trying to settle the score.

We look at what such resentment can lead to and how to guard against cyberrevenge.

++ The $200,000 password ++

One potent example of post-employment trouble comes from the online American College of Education. Management there didn't hit it off with system administrator Triano Williams, who worked for the company remotely.

In 2016, the employee filed a racial discrimination complaint against the organization. A short while later, he was offered a relocation to Indianapolis to work in the local office. Williams refused; teleworking was one of his key conditions. As a result, he was dismissed. Although he received a severance package, the IT expert was discontent. He concluded that the whole story about relocating had been concocted because of his complaint. To take revenge on the school, he changed its Google account password, depriving former colleagues of access to e-mail and study materials for more than 2,000 students.

Williams argued that the password was automatically saved on his work laptop, which he returned shortly after being fired. However, according to the college, the former administrator wiped the device before returning it.

The institution asked Google to restore access to the account, but it turned out the profile was registered to Williams' personal account, not the company. The ex-employee's lawyer hinted that his client might be able to remember the lost password in exchange for $200,000 and a positive recommendation from the company.

++ Exhibitory attack ++

Another example involves more active measures post-employment. Richard Neale, cofounder and former IT director of information security company Esselar, departed on bad terms and spent six months plotting his revenge.

To discredit his former colleagues, he waited for the day when Esselar was due to demonstrate its services to a major client, insurance company Aviva. On the eve of the presentation, Neale hacked the mobile phones of about 900 Aviva employees and deleted all information from the devices.

After the incident, Aviva broke off relations with Esselar and demanded £70,000 in compensation. But the total reputational losses and potential harm were estimated at £500,000 by Neale's former partners. According to the company, his actions were so damaging that Esselar considered a rebrand.

++ A quick and very costly data wipe ++

Also dangerous are employees who only suspect that dismissal might be coming. Mary Lupe Cooley, an assistant director at an architectural firm, saw a newspaper ad seeking someone for her position with her boss's number listed in the contact details.

Assuming she was about to be fired, Cooley deleted project data stretching back seven years, causing damage estimated at $2.5 million. As for the ad, it was for a vacancy at the company of her boss's spouse.

++ How to avoid falling victim to cyberrevenge ++

To prevent ex-employees from harming your IT infrastructure, keep a close eye on their rights and permissions from day one. Here are a few rules for companies that want to stay secure:

• Keep a log of employees' IT rights, plus accounts and resources to which they have access. Grant additional rights only if you are absolutely sure that the employee needs them. And immediately log this information.
• Regularly review and revise the lists of rights. Remember to revoke obsolete permissions.
• Register corporate resources only to corporate addresses. No matter what the advantages of setting up a personal account may be, or how reliable the employee may seem, keep in mind that you have a business relationship that sooner or later will run its course. Domain names, social media accounts, and website control dashboards are ultimately company assets, and it is short-sighted to relinquish their control to staff.
• Block all access rights and accounts of ex-employees as soon as possible, ideally as soon as you inform them of their dismissal.
• Do not openly discuss possible staff layoffs and restructuring, and when listing an ad to fill a specific position, remember that it may be seen far beyond the applicant pool.
• Try to maintain good relations with all employees and a friendly atmosphere in the workplace. Cyberattacks against a former employer are often driven not by greed, but by bruised feelings.