Why HR is at risk from cyberattacks

Human Resources professionals (HRs) are a common, high risk target for cyberattacks - simply because they are easily accessible. They are the "front of house" for businesses, with the contact details often available on the company website. While this is to make them easy to reach for current and future employees, and anyone else who chooses to do so.

© stokkete – 123RF.com

They are also high-value contacts because HRs are the guards of company information. They have access to and protect company intellectual property and employee personal information. And this data is highly valuable to cyber attackers. Here are three main ways in which HR professionals are vulnerable to attack:

- **Incoming mail:** Cybercriminals penetrate the corporate security perimeters by sending an employee an email containing a malicious attachment or link. Opening this link can release a virus, which can download personal files.
- **Access to personal data:** HRs have access to all personnel data held by a company. By compromising a HR employee's mailbox, access is opened.
- **Email hijacking:** Here, a senior staff member's mail account is hacked. It sends out emails to colleagues requesting fund transfers or the forward of confidential information.

7 steps to keep your SME cyber safe

24 Mar 2021

Kaspersky and B2B International also researched employees' role in a business's fight against cybercrime. "We've found that just over half of businesses (52%) believe they are at risk from within. Their staff, whether intentionally or through their carelessness or lack of knowledge, are putting the businesses they work for at risk," explains Lehan van den Heever, enterprise cyber security advisor, Kaspersky. "This is why staff training is essential in raising awareness among personnel and motivating them to pay attention to cyberthreats and countermeasures — even if it's not part of their specific job responsibilities."

Think cybersecurity is expensive? Just wait until there's a breach...

Lukas van der Merwe 18 Dec 2020

To minimise the likelihood of intruders penetrating an HR department, van den Heever recommends the following tips:

- Employee-focused security measures such as employee engagement and training on cyberattacks.
- Identify compromised file formats that come through, looking like resumes and work samples.
- Install updates and ensure that anti-virus protection is always on.
- Isolate HR computers on a separate subnet. If one computer is compromised, the threat cannot spread.
- Store personal data on a different server, not on HR machines.
- Update software on HR computers regularly and maintain a strict and easy-to-follow password policy.