BIZCOMMUNITY

Inside the mind of the attacker: How cybercriminals think when they enter organisations

Hackers want in. They want into the business, its data and its details because cybercrime is a multi-billion-dollar business and there is plenty of profit in phishing, stolen data and ransomware.

Anna Collard, SVP content strategy and evangelist at KnowBe4 Africa | image supplied

They dig into your business and they use every loophole and vulnerability they can find, whether that is your systems or your people. Their approaches follow several standard steps, although these can change depending on the target or the goal. After all, as Anna Collard, SVP content strategy and evangelist at KnowBe4 Africa, points out:

“Cybercriminals do have several steps they usually follow, although these can happen in a different order or some can be skipped along the way, these are the most common ways in which they approach a business,” she says.

“They start out with reconnaissance where they are trying to learn more about their target – including what hardware and software you run, your email addresses, employee names and other details that could give them an edge when it comes to planning a successful attack.”

Once they have the information, they then plan their attack. They could use root access found through automated malware that can be introduced into the system via a USB key, human error or a vulnerability. It is easier than most people realise to be tricked into downloading and executing a malicious programme that instals itself and delivers the goods.

Users and companies can minimise this risk by ensuring all their internet-facing and security systems are up to date and by constantly checking any downloads, apps and end-points for malware.

“If you want to defend against cyber-attacks, you need to think like a malicious hacker and know the tools and techniques that they use so you can defend against them,” says Collard. “The first thing is to stop worrying so much about what the hackers want and more about how they are going to get it. Using the house analogy, this is equivalent to making sure the doors are locked, there are bars on the windows and there is not an easy access point in the basement.”

The next step is to think about the type of attack vector that is most likely to be used against your organisation and then put measures in place to protect against them.

While this is still a measure of guesswork and should not be the only defensive part of your posture, it does help you to build a more robust security approach. This is a data-driven defensive stance – it uses information and insights to assess the most likely types of attack so you are protected against them.

“You need to ensure that you build a combination of defences,” says Collard. “This is overlapping policies, technical defences, training and other types of security that allow you to create more of a security mesh around your business. It also ensures you do not end up overlooking a critical part of your business and accidentally leaving a vulnerability wide open.”

Training is absolutely essential. Employees need to know that they are actually one of the company’s most attacked targets and how to protect against this. They need to know how to detect phishing attempts, how to avoid making obvious mistakes and how to dodge not-so-obvious mistakes.

Why cybersecurity needs to tighten up as cryptocurrencies plummet

Dan Thornton 22 Jun 2022

If people are on high alert and aware of how a simple mistake can cost them and their company, they will then move from being a liability to an integral part of the organisation’s security defences.

“Cybercriminals are always going to be trying new methods, new viruses, new threats, that is their job,” says Collard. “Companies need to make detecting and protecting against these attacks part of their job – part of their employee’s job

. That way, security shifts from being something people perceive as a pain or as a tedious box-ticking exercise to a habit, to a fundamental part of the office culture. And that awareness and vigilance will put the organisation in the best possible place when it comes to security.”