BIZCOMMUNITY

Here's how hackers break into the business environment and how it can be avoided

By Anna Collard

11 Jun 2021

Organisations have to invest in comprehensive in-depth phishing plans, leveraging policies, technical tools and awareness training to ensure that they're not vulnerable to attack. And this attack is absolutely guaranteed.

Anna Collard, SVP content strategy & evangelist at KnowBe4 Africa

In 2020, phishing statistics were staggering, Verizon revealed that 22% of data breaches were as a result of a successful phishing endeavour, and the FBI received a record number of phishing complaints and concerns. These statistics underscore the absolute importance of building a secure and stable human firewall, a ring of trained employees who understand the risks, recognise the warning signs and know the rules of security.

There are around ten ways in which hackers and malware can break into the business environment: unpatched software, zero-day vulnerabilities, social engineering, authentication attack, human error, insider attacks, third-party compromise, physical attacks such as theft, misconfiguration of systems, and eavesdropping or network sniffing. Out of all these attack vectors, the most common are social engineering and unpatched software. The former is responsible for the majority of data breaches since 2009.

How not to be phished

The best way to address this is by blending a layer of best practice policies that include basic information such as: ‘Don't click on anything you haven’t expected,’ or ‘Never give your password to someone over email’. These are solid policies that help people to become more secure.

An acceptable use policy is the first and most important step, this is the generalised security document that covers the basic security hygiene factors. It needs to be signed and reviewed by every employee when they join and signed again annually thereafter. This should be bolstered by a phishing mitigation policy that drives consistent phishing training and management.

4 security vulnerabilities found in Microsoft Office

10 Jun 2021

There should be a simulated phishing test at least every month, month, or preferably even more frequent with possible consequences for people who fail the tests consistently. You need to expose every new employee to what phishing is, how to mitigate it and how to fight it. The phishing policy should cover the fact that there is regular testing of knowledge and phishing simulations, as well as clear definitions around what phishing and social engineering are.

The goal is to create a culture of acceptance. A culture where suspected phishing attacks are reported and where people are encouraged to play a role in building this human firewall. People need to know that they are part of the solution, not penalised for being part of the problem. Yes, there should be consequences for consistent failure to recognise a phish, but only from the perspective of increased training and, for those that don't take it seriously, conversations with management to reinforce the message.

Invest in technical defences

Then you need to invest in your technical defences, the firewalls and security configurations and anti-virus software and phish filtering tools. The defences prevent the risks from reaching the desktop in the first place. However, even with robust technical defences and rigorous policies in place, there are always going to risks that slide on.

This puts training in the spotlight. You need to train your employees, business leaders, and C-Suite to ensure that they are capable of detecting the risks, and not falling foul of the intelligent webs of deception. This includes everything from emails to SMS messages to phone calls. These are all socially engineered to trigger people into making the wrong decisions and revealing critical information that can put the business, and them, at risk.

Brands continue losing customer loyalty to cybercriminals, report reveals

Duane Nicol 1 Jun 2021

The combination of technical network defences, multi-factor authentication, the use of intelligent tools such as behaviour and threat monitoring, phishing simulations, and training engagement – these all come together to form a robust defence against the phishing phenomenon and building your human firewall.

ABOUT ANNA COLLARD

Anna Collard is the senior vice president of content strategy and tech evangelist at KnowBe4 Africa

- #BizTrends2022: Discriminatory AI and disinformation powered by deep fakes - 10 Jan 2022
- 5 important lessons to learn from the REvil ransomware attack - 13 Jul 2021
- Here's how hackers break into the business environment and how it can be avoided - 11 Jun 2021
- PoPI Act readiness: 6 things to do - 12 Apr 2021
- Top IT security threats in 2021 - 20 Jan 2021

View my profile and articles...