Unsplash © Miłosz Klinowski

The true cost of phishing attacks

It is becoming increasingly difficult to ignore the rising number of cyber attacks over the last few years. New working environments have further accelerated the risk landscape for small to medium size businesses across all different markets.

As the threat landscape broadens, so do those who are under threat. News coverage often only scratches the surface on the attacks and tries to answer immediate questions in terms of who, what, where, how. But, the true costs of online attacks are felt deeply by the businesses attacked as they are left to consider the preventative measures they could have taken to limit the chances of a breach.

Home intrusion

The threat landscape is increasingly evolving and expanding with the increase of employees choosing to work remotely. In particular, phishing attacks have grown exponentially since the shift to remote work. According to *Microsoft's New Future of Work Report*, 80% of security professionals have experienced increased security threats since shifting to remote work. 62% of these professionals noted that phishing attacks have increased more than any other type of threat.

Phishing attacks aim to steal user information, such as credit card numbers and

login information. They occur when an attacker deceives a victim into opening an email, instant message, or text message by disguising themselves as a reliable source. The theft of such data, however, has an impact beyond the targeted individual, and enables the hacker to access corporate systems from home set-ups.

The surge in phishing attacks can be attributed to the fact that more employees are now working from unprotected home network systems. Malicious actors are able to infiltrate these home networks more easily, as they lack the level of protection that is typically available in office environments.

The business impact

Whether it's an employee using work devices that lack adequate security software, or company data being exposed through open networks outside of the office, SMBs are facing greater security risks than ever before.

The financial cost of such attacks can have catastrophic impacts on a business. According to *IBM*'s 2021 report on the cost of a data breach, phishing-related attacks are the second most costly breach, costing firms an average of $4.65M.

Furthermore, if a company is hacked and its customer data is leaked, this could have huge reputational consequences for the business. For example, last year *T-Mobile paid $350M* to settle a class-action lawsuit after the company faced a serious data breach.

Dark Web monitoring

More often than not, the data that is gathered during a phishing attack is sold on the dark web for other cybercriminals to use at their will. Furthermore, many companies may find that, once they are subjected to a phishing attack, they are then inundated with wave after wave of malicious emails. This is because these same malicious actors publish the vulnerable email addresses for other criminals to harness in the future.

While educating your staff on cybersecurity is the best first defence against such attacks, SMBs must now be prepared for when their data inevitably ends up on the dark web. Investing in dark web monitoring services will allow organisations to uncover if their data has been uploaded to the dark web.

This security service works by searching the dark web marketplaces for company or personal information. If any company or personal data is detected, the service notifies the IT administrators, allowing them to take appropriate

action in order to mitigate the threat.

There has been a dramatic shift in the way people are being attacked online, and SMBs must now adapt to protect themselves against the new wave of cyberthreats. In the face of this incessant online threat potential, it’s imperative that small and medium sized businesses adopt dark web monitoring to protect against any possibly ruinous threat.

Kevin Drinkall Director of GTM Strategy for EMEA at *Zyxel Networks*

Article by KEVIN DRINKALL