beazley

Article

The cat and mouse game of cyber security

July 11, 2023

Cybersecurity experts have been locked in a battle with hackers for decades. It is a technological arms race. Every evolution of security technology and techniques is tested and probed for new weaknesses. New innovations which provide benefits to societies can also enhance cyber gangs' armouries. When a silver bullet is purported to be found, thus far, hackers have always found another route in. For cybersecurity, unfortunately, there is no such thing as a flawless defence, but there is defence in depth, and by understanding their exposures and monitoring their points of vulnerability that cannot be eliminated, businesses of all sizes can stop cybersecurity incidents in their tracks or minimize the damage they cause.

Every business is a target

Every organisation, from SMEs to multinationals, has become dependent on technology. Virtually every business is connected and, by extension, exposed to cyber security risks. Smaller businesses typically lack the resources to invest in cybersecurity teams and support compared to their larger peers. They are increasingly aware of this. Over a quarter of small businesses (28%) with annual revenues below US$1mn believe that is the top threat facing their business, they also feel more exposed than ever, with 25% now stating that they are unprepared to deal with the risk (2022: 19%)

However, this does not mean that they are doomed to become perennial victims for hackers. Smaller businesses have smaller attack surfaces. They tend to have fewer employees and points of entry, exposing them to fewer risks. Those that recognise that they are at risk and seek to take the steps within their means to mitigate it are vastly better protected than those who continue to believe that they are not big enough to be interesting to cyber criminals, or don't make enough money to be a target. They are, and they do. Whether it is their business or client data or their money that is of interest - every business, to some degree, is exposed.

HOW IS THE CYBER-CRIME THREAT FOR SMES EVOLVING?

“Cybercrime is organised crime and big business. The gangs are increasingly sophisticated and they tend to use SME businesses that hold personal information with value, such as medical practices, schools, retailers and accountants as training attacks for interns learning ‘their trade’.

Many SMEs are part of a supply chain that lead to large companies, so they can act as a gateway in a hack to more lucrative funds.” Jon Miller, CEO and Co-Founder of Halcyon AI

Big business, bigger risk landscape

Bigger businesses are typically more cognisant of the risks they face. They know more. They have security teams that understand what the threat landscape looks like. Our data shows that nearly three-quarters (72%) of businesses with an annual revenue over US$100mn felt prepared to deal with future cyber risks compared to only 59% of small businesses with annual revenues below US$1mn.

Large organisations also have extremely large attack surfaces, they must consider every risk. They have a larger workforce which means that they have more people who can be making bad decisions. Sometimes all that is required is one employee, making one mistake with their monitoring or one bug to go unpatched, and hackers can gain a foothold. Employees creating shadow IT systems, wherein they setup their own infrastructure to solve particular problems, outside of the wider systems, which are not secured in a consistent manner with the Group, becomes more of an issue as businesses become bigger and more diversified. When we see large organisations breached, it tends to be a partial breach. Because they're groups of companies, they have dispersed IT and infrastructure, and might have regional separation. While this has its drawbacks, it can stop the spread of any malware contagion.

However, a breach in Brazil can still affect a brand in Birmingham. The fact that a global brand’s IT security was only lacking in one branch will not feature in the headlines notifying the world that customer data has been compromised. While small businesses recognise their limitations and big businesses have to prepare for issues on multiple fronts, often it is those in the middle that are most exposed. They understand the risk to a certain degree but often assume the bare minimum action they have taken is adequate. Often, it is not.

Keeping alert to new risks, but don’t ignore the existing threats.

Staying abreast of the very real dangers which businesses face is a constant battle, and this is before the view of the risk landscape is skewed by often overblown reports of the impact of the latest new threat. An example of this is Deepfakes. While they are a risk to businesses and the technology is evolving, their inflated profile in the media is not commensurate with their risk. Arguably, this is the reverse of ransomware, where because the media has moved on from its focus during the ransomware pandemics of 2021-22, the assumption is that the threat has been nullified. In reality, for a Deepfake to be effective and allow for a financial transaction to be executed, there will be wider concerns within the business.

WHAT MEASURES SHOULD FIRMS TAKE TO COUNTER DEEPFAKES?

“If proper controls are in place around authorisation of payments, such as identity verification and approval flow, then Deepfake fraud attempts should not be successful.

There is a growing maturity around the need for appropriate payment protocols to prevent people acting on an email from the “CEO” asking them to make a payment to a random bank account on their behalf, but the issue does persist. Speaking directly to the person who purportedly has made the request is still the best approach.

Deepfake technology is evolving to allow for the faking of these conversations over the phone, but instances are currently rare. As this nascent technology evolves, then it is likely it will become more of a risk. So the cat and mouse game will continue,” Adam Harrison, Managing Director, Lodestone UK

beazley