BIZCOMMUNITY

Avoiding the high cost of poor cyber resilience

By Brian Pinnock

2 Oct 2018

Ransomware attacks are increasing, both in frequency and cost to businesses. They are expected to impact one business every 14 seconds by the end of 2019, up from every 40 seconds this year. This makes it hard to know how much an attack will cost businesses in downtime, lost revenue and ransom. But R1.7m is the average for a South African business.

Brian Pinnock is director of sales engineering at Mimecast

Globally, damages from ransomware attacks are expected to reach $11.5bn in 2019. That's up from $5bn in 2017 and $325m in 2015. These are massive increases every two years – and the trend is likely to continue. My point is that R1.7m might be a conservative estimate in a few months' time. Plus, the golden rule of cybersecurity is not to wonder if, but when you will be attacked. Honestly, assume you're already a target.

In the case of a ransomware attack, your organisation needs to be able to recover quickly so employees can carry on with their day 'business as usual'. This will help avoid losing valuable productivity, revenue, brand reputation – and, potentially, customers. And the best way to do that is by having a comprehensive cyber resilience for email plan in place.

A new study by Vanson Bourne and Mimecast found that ransomware attacks impacted 23% of South African businesses in the last year. The good news is that this was below the global average of 27%. The bad news? Fifteen percent of those businesses didn't know they had been attacked, well above the global average of 7%.

The longer an attack goes undetected, the bigger the financial and reputational damage, and the harder it is to recover. An alarming 73% of affected businesses experienced downtime of between two and seven days. And 45% took between one and two weeks to recover. Could your business survive if it came to a screaming halt for that long?

Keys to the kingdom

Ransomware is just one type of attack that businesses should be concerned about. Another way cybercriminals can access valuable information or money is through impersonation fraud. So, not only do criminals kidnap your king and demand money for his safe return; they sometimes also pretend to be your king – and it's hard to spot the imposter.

Impersonation fraud is one of the most common attack vectors used by cybercriminals to gain access to company information, with South African businesses seeing a 36% increase in this type of fraud. Typically, hackers masquerade as a high-ranking individual in the company. They send an email to someone, asking them to wire money or send them sensitive information. Because this person carries a lot of authority within the business, few people will object to the request.

In South Africa, the most attractive target for impersonation attacks sits in the legal department. In the UK, it’s human resources and, in the US, finance or sales. If you received an email from your head of compliance, asking for personal data about your customers, you'd probably give them the information. You might not notice that the email was fake until it was too late because hackers use sophisticated techniques such as URL spoofing and domain similarities, which most office workers are not trained to spot.

When sensitive information gets into the wrong hands, it creates all sorts of problems for the business. Reputational and financial damage is one thing. Running into compliance issues because someone unintentionally flouted the Protection of Personal Information Act is a whole other ballgame. And losing could mean fines and prison time – the European Union’s General Data Protection Regulation, which came into effect in May this year, can impose fines of up to R300 million on companies that fail to protect European citizens’ personal information.

Batten down the hatches

One in eight South African businesses conducts near-continuous training to help employees spot cyber-attacks. Twenty-one percent of respondents have monthly training sessions and 42% have quarterly sessions. But monthly or quarterly training is not enough and the information being shared usually isn’t absorbed properly. This is because training sessions are seen as inconvenient by staff and are often boring. For the best results, businesses should conduct security awareness training continuously. More importantly, training should be engaging and interesting.

Security awareness training is a crucial aspect of a cyber resilience strategy and needs to be entrenched in the culture of an organisation – especially since 31% of local businesses are not confident that their employees can spot and defend against impersonation fraud.

But training alone will not deter cybercriminals from trying to ‘kidnap your king’ – your critical data, systems and, of course, your money. And because email breaches account for 96% of security incidents, addressing this exposure should form the core of your cyber resilience strategy.

If you think your business is protected because you use Microsoft Office 365, I have bad news. In our latest Email Security Risk Assessment (ESRA) report, we found that incumbent email security systems missed and delivered 15,656 malware attachments to users’ mailboxes, a 25% increase quarter-on-quarter. The report also found an 80% increase in impersonation attacks in comparison to last quarter’s report, with 41,605 caught.

Traditional, defence-only security approaches that rely on disparate technologies are no longer enough and will leave you chasing your tail. The only way to get ahead of cybercriminals is through cyber resilience for email, which will help you secure, preserve and continue the flow of information via email, even during an attack.

A key component of any cyber resilience strategy is email and data archiving, which allows you to immediately recover all your data in the event of an attack. This ensures your data is always protected and accessible to users. It also prevents a data hostage situation and means you never have to pay a ransom to get your data back.

Having a solid cyber resilience for email strategy prepares you for every stage of attack: it puts the right security in place before an attack happens, provides you with the durability to continue with business as usual during an attack, and helps you recover your data after an attack.

A robust email security inspection system should be able to score emails for potential impersonation attacks and either block, quarantine or flag them as suspicious before they reach the recipient's inbox.

Essentially, they give you time to move the king to safety before the kidnappers arrive at your door. Who knows what arsenal they're carrying and if you can fight fire with fire? If you only act after they've arrived, it's probably already too late to save the king.

ABOUT BRIAN PINNOCK

Director of Sales Engineering at Mimecast

- #BizTrends2021: What the new year holds for cybersecurity - 6 Jan 2021
- #BizTrends2020: Cybersecurity trends predictions - 16 Jan 2020
- Control+Z your data - 29 Mar 2019
- #BizTrends2019: South African cybersecurity trends for 2019 - 21 Jan 2019
- #BlackFriday: Safe shopping starts with awareness - 22 Nov 2018

View my profile and articles...