Liberty cyberattack underscores high threat level for SA businesses

By Colin Thornton

4 Jul 2018

With breaking news of major South African insurer Liberty Holdings falling victim to a cyberattack, local companies have to heed the warning and pay more attention to their internal systems and processes - which includes employee training and awareness.

© raw pixel

The Liberty attack, which appears to be an inside job, is just one of many examples of the large-scale cyber threats that every company now faces.

According to reports, Liberty refused a ransom demand after hackers breached its IT infrastructure and accessed emails.

Worryingly, ransom-type attacks on businesses are becoming all too common. The findings of a 2017 survey by endpoint security provider, Sophos, titled *The state of endpoint security today*, found that for South Africa, the median total cost of a ransomware attack was around R1.7m "including ransom, downtime, manpower, device cost, network cost, and lost opportunities."

Looking at Liberty: How big is the human factor in the cybercrime epidemic?

Nicol Mullins 19 Jun 2018

Sadly, despite the frequent and large-scale nature of cyberattacks on businesses of all sizes and across sectors, local business owners and managers continue to take a flawed approach to cybersecurity.

> *Instead of turning their attention to internal systems and processes, employee training, testing and awareness programmes, businesses continue to rely on perimeter defense – the use of firewalls, anti-virus software, etc.*

Arguably, this represents an outdated way of thinking about security – one that, as the name suggests, ensures that you secure the perimeter of your network. In fact, the most common IT security test within the enterprise today is called a

'penetration test', and involves trying to break through this perimeter.

Yet it has emerged, through many studies and reports, that by far the greatest (and most common) threats emerge from the inside of the network. For example, having compiled the 2016 Cybersecurity Intelligence Index, IBM revealed that insiders carried out 60% of all attacks. As an HBR.org article explained, of these attacks, "three-quarters involved malicious intent, and one-quarter involved inadvertent actors…."

Liberty refused hacking ransom demand

18 Jun 2018

Furthermore, according to historical claim data analysed by the London-based consultancy Willis Towers Watson, employee negligence or malicious acts accounted for two-thirds of cyber breaches. A mere 18% were directly driven by an external threat, and extortion accounted for just 2%.

Significantly, the research revealed that about 90% of all cyber claims stemmed from some type of human error or behaviour.

Attacking the weakest link

Take phishing, for example, a form of attack that has been around for many years and continues to plague businesses. A scammer will send an email or emails to people which look authentic, but that contain links to sites that attempt to get usernames, passwords or other personal information. Armed with this information, scammers will attempt to gain access to bank accounts, emails or a businesses' network.

The recent attack on local comedy and entertainment agency Goliath and Goliath was a classic case. According to reports, hackers intercepted agency invoices and then changed banking details. The money that was 'mistakenly' paid over to the hackers ranged between R60,000 and R130,000.

In addition to phishing, social engineering has become a common and highly successful way of hacking into private data and accounts, and it is a method that requires little to no IT skills.

This is how to avoid cyberattacks during the Fifa World Cup in Russia

12 Jun 2018

Added to this, scammers in the UK and USA have taken to loading memory sticks with malicious software and then leaving them in parking lots or public places. Naturally, someone sees it lying there, and thinks they've scored a free memory stick - only to unwittingly infect their computer or business network when they plug it in.

All of these methods involve a user within the network unknowingly sharing confidential information…or actually activating software that could let cybercriminals in.

Zero trust security

Given the fact that hackers are clearly exploiting the human factor (human fallibility) within businesses, it is clearly time for a new approach to cybersecurity.

> *"One approach that is increasingly gaining traction, relies on the concept of Zero Trust. In a 'Zero Trust' environment, the user's authority is never taken for granted. So, even if someone is inside the network, there should be alternate ways of checking their authenticity."*
>
> This can include requiring another password, checking the source IP address (does it originate in China, for instance?), or checking the machine ID.

Hands-on employee training and testing

While the Zero Trust concept will very likely grow in prominence within the IT security community, most local companies will not have the resources to immediately implement the changes in IT infrastructure that such an approach requires.

As a result, it is critical that other methods are urgently implemented – and without doubt, the most effective method is simple employee training, paired with regular performance testing.

The wrong technology in the wrong environment can actually increase risk

Marius Coetzee 31 May 2018

Today, business owners and managers should initiate regular workshops and training sessions that explain the various threats to employees - and that provide tools and strategies to help them to recognise scams. Importantly, scams and hacking methods are evolving all the time – so effective training and awareness programmes should be updated regularly, and implemented regularly.

A critical part of this training involves performing tests in which employees are sent fake phishing emails, for example, and then monitored to see whether the training is, in fact, having an impact. Such tests should be performed regularly, on an annual, or ideally bi-annual basis.

Importantly, in addition to ramping up employee training, companies must ensure that they are regularly backing up all of their data, and that their backup processes are robust and frequent in nature.

Even if businesses have impeccable IT security in place, it is arguably just a matter of time before the business is hacked – so it is critical to ensure that robust backup and disaster recovery systems are firmly in place.

ABOUT COLIN THORNTON

Colin founded Dial a Nerd in 1998 as a consumer IT support company and in 2002 the business- focused division was founded. Supporting SME's is now its primary focus. In 2015 his company, merged with Turrito Networks who provided niche internet services outside of the local network. These two companies have created an end-to-end IT and Communication solution for SME's. Colin has subsequently become the managing director of Turrito. Contact him at info@dialanerd.co.za

- Understanding SA's 5G reality - 4 Apr 2019

- Why your business needs a cloud architect - 21 Feb 2019
- Privacy vs Profit: Will 2019 be the year of consumer paranoia? - 26 Nov 2018
- Why SMEs should be looking at cyber insurance - 28 Sep 2018
- Why your future digital ID should harness blockchain technology - 23 Aug 2018

View my profile and articles...