BIZCOMMUNITY

Data breaches becoming more common

By John Mc Loughlin

16 Oct 2020

Another day, another data breach. South African businesses are becoming more susceptible to cyberattacks and seem to be easy targets for criminals. Data breaches are now a common phenomenon with Nedbank, Momentum, Lombard Insurance, Experian and Stefanutti Stocks making headline news.

John Mc Loughlin, CEO at J2 Software

Who is the next victim to be made public? The truth is, this is not new, there has been an ongoing spike in cyberattacks that continues to grow from year to year, it is only recently that businesses are being exposed in the media.

These publicly known breaches are only the tip of the iceberg. Cyber criminals are successfully infiltrating and taking down systems on a daily basis. Until businesses take proper action, one can expect a continued increase of successful attacks.

All businesses are targets

Many small business assume they are too small to be attacked, but the truth is - businesses of all sizes are targets. A cyberattack on an SME will often have a devastating effect and possibly mean the end for them. More and more SME's are targeted because they are often easier to access because little or no attention is given to cybersecurity.

Gartner predicts by 2024, personal liability will fall directly onto many CEOs for failing to protect systems from cyber incidents. It believes that CEOs will no longer be able to plead ignorance or retreat behind insurance policies. The financial impact of cyber-physical security (CPS) attacks resulting in casualties to human life is predicted to reach over $50 billion by 2023.

Furthermore, poor advice and lack of understanding means that a small business will have a false sense of security with only the free anti-virus software between them and a cyberattack. Many SME's do business with larger business and this is another reason that the SME is a very valuable target for cybercriminals.

Account takeover is rife and the use of weak or reuse of passwords is a contributing factor. Once an attacker has the credentials, all they need to do is wait. They set rules, forward emails and add themselves to management groups - waiting for the right piece of information to target their victims.

We recently discovered in a pool of over 400 mailbox rules on Microsoft 365, there were four malicious rules configured that scrape for financial information and then forward the information out to a Gmail account. These rules were in place for some time at this company, and they were unaware. The rules were set using known user credentials and it was never checked.

Visibility of real and available sources of information provide visibility to combat the growth in cybercrime. We recommend that you get visibility across data, machines, applications and people to understand what is really happening across your environment.

Focusing on the network is simply not sufficient, this is evident with the spate of breaches in the news each day. Businesses must push towards a user-centric approach to security. The users are the ones accessing information and these are the places that the attacker will target. Your network is where your user is. Increased visibility is critical with the remote workforce and changing office landscapes.

It's a myth that cybersecurity is unaffordable - this misconception is driven by fear - the fact that some businesses are taking advantage of the lack of knowledge and fear to overcharge their customers. We prefer to remove the 'fluff' and get things done.

There is no value is deploying tech for the sake of tech and then not doing the basics. Covering the basics of cyber resilience will ensure that you can properly maintain, monitor and prevent cyberattacks. Using a combination of proven tools and services, cybersecurity is achievable whether you are a listed multi-national or a family run business that runs from the dining room.

Finally, partner with a reliable service provider to ensure increased visibility and report to stakeholders. Bolster your cyber defences by running a simple, comprehensive and effective cyber resilience program.

ABOUT JOHN MC LOUGHLIN

John Mc Loughlin is a visionary entrepreneur that has been involved in the setup and management of a number of start-up businesses. For the past seven years, he has been working towards changing the security landscape for SMEs in South Africa through his company, J2 Software, which provides solutions around reducing risk and improving compliance. John is an industry specialist and thought leader in the security space, and his particular areas of expertise lie in planning and strategising.

- #BizTrends2023: Continued explosion of cyberattacks - 13 Jan 2023
- Many faces of malware: Are you protected? - 2 Mar 2021
- Data breaches becoming more common - 16 Oct 2020
- I've been hacked! What do I do? - 21 Feb 2020
- The complex and challenging world of cyber risks - 11 Dec 2019

View my profile and articles...