BIZCOMMUNITY

Continued explosion of cyberattacks

By John Mc Loughlin

13 Jan 2023

If the last two to three years has shown us anything, it is that the world can change almost overnight. Gone are the days of small and incremental changes, we live in a time of massive change without warning.

J2 Software CEO John Mc Loughlin | image supplied

This has proven to be the same in the world of cybercrime and cyberattacks. The rapid change of the way we work and live has fuelled a gigantic wave of attacks from around the world. The attackers do not worry about your industry, they do not care about how good you and your business are, they care only about profit.

The trend for 2023 is going to be the continued explosion of attacks and if you have not implemented a cyber resilience programme, then 2023 will be your year. The year your business is compromised and held to ransom. What's that? It won't happen to you? You have nothing worth stealing?

One of my favourite phrases is that there are two kinds of businesses out there: "Those who have been breached and those who do not know they have been breached."

Which one are you?

There is little argument that cyber threats are now the biggest risk to the modern business. The attacks continue to grow in volume and sophistication. New vulnerabilities are exploited before they are patched and the cyber gangs move faster than vendors. Even when there is a patch, most businesses have no formal program to implement these into their environments.

The modern business is failing to keep up – with the difficulties encountered in simply running the business, rising costs and uncertainty most do not even know that the vulnerability is there or that there is already a bad apple sitting within their digital environment.

Every single day we find compromised and leaked information, compromised accounts and this is across every industry and in businesses of all sizes. Do not think that you are too small or too big to be affected.

We constantly identify organisations that have open and accessible platforms and do zero monitoring to identify anomalies and detect compromise. This is the same as having an intruder in your home, but you do not see them because you do not bother to turn on the lights. Without basic controls and ongoing management gaining access to your world is simple, all we need is one detail.

The attackers walk right in through the front door because you leave it open. Businesses of all sizes are at fault using default passwords or not fixing a previously known breach. Access to critical systems is easy when you have the information. All you need to do is log in – not hack. Less than 28% of businesses force the use of MFA and almost none set adequate access controls. If it is one click for you to access your data, then it is also that simple for the criminals.

Once they have your email system – they own all your information. Perimeter and gateway security is vital but if you don't see what is happening internally you could be bleeding without seeing the wound. An internal bleed can also be fatal.

The question then comes up, where do I focus my attention in 2023?

Do I lockdown the firewall? Focus on patching? Monitor activity? Do we ensure modern malware detection? How about intrusion detection?

The simple answer is yes – do all of those. Then do more. You need visibility to give you the capability to identify problems when they occur and destroy the threat before you bleed out. We are hyper connected and it is pointless to throw money at different solutions if they are not part of a combined cyber resilience program.

In the cyber war, we cannot focus on only one area of the assault. Understand that you are not untouchable. Nobody is. Stopping attacks is impossible – but you can reduce cyber risk with a structured cyber resilience program that gives you defence in depth and provides the ability to detect when an attack starts. If you can be alerted at the start of the attack you can take action before it is too late.

Using ongoing and consistent monitoring, vulnerability analysis and mapping real usage will let you know where you need to apply the bandages. Identify, neutralise, remediate and then investigate. Then start all over again. The number of threats will continue to increase - visibility and agility is the only way. Or keep doing things the way you have always done it. Then you can be assured that 2023 will be your year.

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...