Cybersecurity trends predictions

By Brian Pinnock

16 Jan 2020

The realities of the negative impact of modern cyber threats arguably hit home for South Africans in 2019 - more than any other year in memory.

Brian Pinnock, cybersecurity expert at Mimecast

The country fell victim to several high-profile breaches, including a successful ransomware attack on City Power's systems. And in July last year, South Africa experienced the single longest cyberattack seen globally by the Mimecast Threat Centre, with an unknown attacker launching a wide-ranging campaign on our financial services sector over an eight-day period.

Will 2020 hold more of the same, or will new and greater risks emerge?

Based on our work helping companies around the world build greater cyber resilience, we expect to see the following play out in the world of cybersecurity in the year ahead.

Moving from perimeter to pervasive email security

The world's number one business communication tool is also the most popular channel for attack by cybercriminals. And while email itself has remained fundamentally unchanged over the past 10, 20 years, email security has changed significantly.

In October, our CEO, Peter Bauer, outlined how organisations have to move from perimeter email security to pervasive email security. Email perimeter security is focused on keeping data and users safe by protecting them against phishing, malware, impersonation attacks and data loss. Additional measures are in place to limit the impact of a compromised user on the broader network.

However, as Bauer points out, organisations now have to consider threats that abuse trust outside of their own environments, and protect their brands and domains from being spoofed or hijacked by crooks who defraud their customers and partners.

This requires organisations to take an offensive approach to cybersecurity and leverage solutions that given them visibility outside of their purview. This enables them to hunt for – and take action against – threats where attackers present themselves fraudulently to customers using deception or impersonation. We believe 2020 is going to be the year where this becomes a vital component of any cyber resilience strategy.

A race for security maturity

A significant amount of the cyberattacks launched on businesses and consumers are fairly simple and one-dimensional, but they are effective because so many organisations still have limited security maturity.

This is unlikely to change in 2020. However, even in organisations with advanced security controls, most of those controls work independently of each other, leaving many vulnerable to more complex attacks.

We expect to see an escalation in complex attacks using multiple attack vectors that span several security controls – for example, email security and web security. Attackers will take advantage of limited threat sharing, low levels of automated orchestration, and a lack of bilateral threat sharing between different security controls to pry open the defences of organisations with relatively mature cybersecurity.

5G widens scope for cyberattacks

With the long-awaited spectrum allocation in progress, SA's mobile operators are keenly awaiting the rollout of next-generation 5G infrastructure. 5G is widely expected to become a foundational element of how people consume media and is a cornerstone of so-called smart cities.

However, it also provides cybercriminals with a welcome tool to gain access to higher volumes of valuable data. There will likely be an increase in the size and frequency of Distributed Denial-of-Service (DDoS) attacks, similar to the ones many of our local Internet Service Providers have experienced in recent months. It's also not unthinkable that we'll see a vast IoT botnet, comprised of a million devices, launch the biggest attack we've yet seen.

Blurring the lines

Cybercriminals have become very smart. Instead of targeting victims with a single email containing a malicious URL or attachment, they now target users on social media, email, and directly on their mobile device via SMS (SMishing) or voice (vishing).

By constantly inundating users with sophisticated attacks, cybercriminals make it increasingly difficult to distinguish what's real and what's fake, leaving many vulnerable.

Educating the vulnerable

Unsurprisingly, the rising sophistication of cyberattacks has left many vulnerable to exploitation, especially less digitally-literate groups such as older generations. Expect to see a renewed focus on educating consumers about safe online habits and to help them identify and avoid potentially risky behaviour.

This won't be limited to banks and other service providers educating their customers. There will likely be increased investment in awareness training within organisations, to equip employees with the skills and knowledge to prevent risky behaviour. This is essential, considering the risks to businesses of malicious files moving from one infected user to the next.

AI vs AI

This year will see artificial intelligence being put to broad use – for good and for bad. Organisations will start using advanced AI to help uncover trends and insights in their alerts and to better orchestrate and refine their overall security landscape. They will need to closely monitor their AI tool's effectiveness and accuracy and refine as needed.

At the same time, attackers will use AI to do reconnaissance of target networks, identify vulnerabilities and develop better malware. Considering the amount of publicly available information on, for example, social media, attackers are also likely to use AI to find information that could be used for targeted phishing attacks.

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...