BIZCOMMUNITY

What the new year holds for cybersecurity

By Brian Pinnock

6 Jan 2021

The year 2020 has been one of the most challenging years in recent memory, both in terms of the effects of the coronavirus pandemic on societies and economies around the world, and the impact of a dramatic rise in cybercrime.

Brian Pinnock, cybersecurity expert at Mimecast

As the virus spread and countries around the world implemented lockdowns, cybercriminals sprang into action and launched attacks on businesses, consumers and critical infrastructure at an unprecedented scale. In the first 100 days of coronavirus, Mimecast researchers detected huge increases in spam attacks - up 46%, impersonation attacks - up 75% - and malware, which spiked by 385%.

The continued disruption caused by the pandemic and the 'new normal' of remote work will likely create fertile ground for an array of cyberattacks in 2021. I chatted to a few of my colleagues about what they think the future holds and here are the cyber risks that we believe businesses and consumers will face in 2021:

Protecting public sector systems in the cloud

The adoption of cloud services among South African public sector organisations is gaining momentum and is enabling greater agility. But it also introduces new risks. In 2021, public sector ICT leaders will seek growing levels of support from technology and cybersecurity partners to build greater cyber resilience in an effort to protect systems and infrastructure from cyberattacks.

As more systems move to the cloud, new strategies will be needed to ensure high levels of security and compliance to public sector policy while maintaining data sovereignty. Cloud adoption will help the public sector with productivity and the increased ability to deliver services. But downtime due to an outage or a cyberattack could lead to widespread disruption of critical national infrastructure if these departments are all dependent on a single cloud provider.

Ransomware will be used to sow chaos

Nearly half - 45% - of South African respondents in Mimecast's State of Email Security 2020 report said ransomware attacks had impacted their organisation. Common consequences of successful attacks included data loss, downtime, financial loss and damage to the reputation of the affected organisation, impacting their customers' trust.

It is likely that we will see at least one major new ransomware strain that will compromise global networks in 2021. The objective won't be money, but anarchy, as DoppelPaymer proved in 2020 when an attack on a German hospital prevented a dying lady from getting to hospital in time. Some have even labelled this is the first officially recorded death due to cyberattack.

All eyes will be on the world's pharmaceutical companies and researchers as they roll out Covid-19 vaccines. We've already seen cybercriminals turning their attention here and this is only likely to continue, with the intention to cause widespread disruption. Mimecast's Threat Intelligence Centre predicts it is also a near-certainty that cybercriminals will continue to target supply chain operations, with attacks focused particularly against the transportation, storage and delivery networks needed for an effective mass vaccination response.

Remote workers become prime targets

With many people likely to continue working from home in 2021, an increase in cyberattacks exploiting consumer-grade home networking vulnerabilities is inevitable.

Such attacks will negatively affect businesses that have not yet adapted their network security posture to align with the new hybrid work scenarios. Data breaches involving insiders will increase due to continued remote work. It's also likely that cyberattacks will increase at a greater pace for smaller businesses than for large organisations, who are likely to increase their uptake of cyber insurance in the belief that this will mitigate all risk.

Renewed focus on cybersecurity awareness training

Employee awareness of cyber risks will be in the spotlight in 2021, and organisations will likely enhance their cybersecurity awareness training efforts to strengthen their 'human firewall'.

In Mimecast's State of Email Security 2020 report, 99% of South African organisations offered security awareness training.

However, there are questions about the effectiveness of some training. In a recent global study by Mimecast, employees were asked about their use of work devices for personal activities during the pandemic. It found that half of South African respondents admitted to opening emails they considered suspicious.

Security teams are likely to launch live phishing simulations and other real-life, de-weaponised campaigns to stress-test

employees' ability to identify and avoid risky behaviour.

Reported breaches skyrocket due to POPIA

Starting in July, South Africans should also expect to see headlines proclaiming a massive increase in data breaches. These breaches are likely already happening but will suddenly be made public in line with the POPI Act's breach notification obligations. It is also when we will possibly start seeing the first regulatory fines being issued due to significant data breaches.

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...