BIZCOMMUNITY

6 cybersecurity trends to watch in 2020

By Charl Ueckermann

15 Jan 2020

The cybersecurity threat landscape is always shifting, making it easy for businesses to become vulnerable to emerging threats.

Charl Ueckermann, CEO at AVeS Cyber Security

Here are six top trends business executives should look out for in 2020.

1. The cyber skills gap will keep on widening

The gap between cybercriminals' skills to create and deploy threats and the manpower within organisations to detect and deal with those threats is widening.

Cybercriminals, global and local, are becoming more sophisticated and innovative in their methods and companies not responding to this ever-evolving threat landscape can lag behind. Predictive security tools as well as using near real-

time threat intelligence feeds from strategic vendors and sources will become increasingly important. So too are prioritising developing specialist IT security skills locally.

If the right skills are not available or can't be developed in-house, companies can consider outsourcing cybersecurity to third-party experts. Cybersecurity skills are predicted to remain scarce in the near future and organisations can help to narrow the cyber skills gap by implementing youth training programmes with creative problem-solving training, as cybercriminals get more innovative by the day.

2. Cloud misconfiguration will be a growing risk to confidential data in the cloud

The growing shift to the cloud for delivering better accessibility to company apps and resources presents security challenges that require specific capabilities and skills.

Although there are built-in security capabilities in many cloud offerings that are innovative and creative, these are not plug-and-play features yet and have to be activated and configured to suit the organisation's unique requirements.

Companies adopting cloud solutions without proper data security and governance in place will be easy targets to cybercriminals in the coming decade. Greater focus must be placed on ensuring that best practice cloud security architectures are adopted, cloud solutions are appropriately configured, access to data in the cloud is well-managed, and that proactive monitoring takes place on an ongoing basis.

3. Cyber incident response will rely more on predictive models

With more cyber touchpoints and data being communicated at an ever-faster rate, the average time available to respond to cyber incidents is going to decrease significantly, placing unprecedented pressure on cyber experts to detect indicators of attack very quickly.

This means that traditional approaches for responding to incidents, after-the-fact, will need to adapt to more predictive models where potential cyber risks are identified before they become a real incident. Companies can also break down their data silos to create unified dashboards and correlate different data sets into single platforms to identify and mitigate risks early.

4. Social engineering will continue to be a pressing problem

Social engineering will continue to be one of the top cybersecurity concerns in 2020, as attacks become more sophisticated and targeted, bypassing traditional security controls and requiring more human scrutiny than before.

The repercussions of successful attacks can be sinister, from financial fraud and data theft, to identify theft. Phishing is the biggest but not the only conduit for socially engineered cyber-attacks. Fake websites where people are tricked

into entering confidential information, social media and instant messaging platforms are also on the list.

Companies can implement a multi-pronged approach to protect data and users against social engineering attacks. This includes robust technologies that can detect phishing messages on any digital platform.

Employees also need to be educated about what social engineering and phishing is, how attacks happen and what they should avoid if they want to maintain ownership of their personal information. Watch out for Voice Deepfakes that will become the new phishing bait, where voice messages are received that sound just like employees but are not.

5. Data itself will become the security perimeter

As more companies empower employees to work remotely and on-the-go, data is becoming the security perimeter. The right security strategies and tools should be implemented to protect assets and data anywhere, whether inside or far from the organisation's traditionally protected network. This includes the plethora of devices and apps that employees use to do their jobs.

Companies can use smart security layers to protect business and client data proactively, even in the most outlying spaces and on an array of devices, including smartphones. Coupled with this, security awareness training is imperative to ensure that users understand the risks of using unsecured devices, open Wi-Fi hotspots, and unauthorised apps and tools.

6. There will be a shift to business risk-driven cyber security

Companies will start to move away from product-driven security with numerous vendors, towards risk-driven security with fewer strategic partners. This will help to ensure that cyber security is tailored to the company’s risk profile and risk appetite, and complements the business strategy.

In the past, too many security tools with an array of vendors complicated cyber security efforts by being costly and time-intensive to manage. As businesses will operate in a more "digitally-enabled by default" environment and invest in more intangible assets, cyber security will become a business imperative.

IT teams will have to address the following three business challenges to get their IT budgets approved: realise the benefits, optimise the risks, and optimise the resources.

ABOUT CHARL UECKERMANN

Charl Ueckermann currently serves as chief executive officer at AVeS Cyber Security and assists organisations with strategic IT solutions. He has more than 25 years' in-depth experience in the IT industry, specialising in banking, government, automotive, manufacturing and telecom industry verticals. He has a proven track record in IT and business strategy in the SMB and enterprise markets.

- #BizTrends2020: 6 cybersecurity trends to watch in 2020 - 15 Jan 2020
- Don't spend another cent on cybersecurity until real risks have been assessed - 6 Apr 2018
- Tips for C-level employees when managing IT security risks - 2 Feb 2018

View my profile and articles...