Top Ten Cybersecurity Predictions for 2019

By Ian Kilpatrick, EVP Cyber Security, Nuvias Group

1. **Increase in crime, espionage and sabotage by rogue nation-states**
   With the ongoing failure of significant national, international or UN level response and repercussion, nation-state sponsored espionage, cyber-crime and sabotage will continue to expand. Most organisations are simply not structured to defend against such attacks, which will succeed in penetrating defences. Cybersecurity teams will need to rely on breach detection techniques.

2. **GDPR - the pain still to come**
   The GDPR deadline has come and gone, with many organisations breathing a sigh of relief that it was fairly painless. They've put security processes in progress and can say that they are en route to a secure situation – so everything is OK?

   We are still awaiting the first big GDPR penalty. When it arrives, organisations are suddenly going to start looking seriously at what they really need to do. So GDPR will still have a big impact in 2019

3. **Cloud insecurity – it's your head on the block**
   Cloud insecurity grew in 2018 and, unfortunately, will grow even further in 2019. Increasing amounts of data are being deployed from disparate parts of organisations, with more and more of that data ending up unsecured.

   Despite the continual publicity around repeated breaches, the majority of organisations do not have good housekeeping deployed and enforced across their whole data estate in the cloud.

4. **Single factor passwords – the dark ages**
   Single-factor passwords are one of the simplest possible keys to the kingdom and are the key tool for attack vectors, from novice hackers right the way up to nation-state players. And yet they still remain the go-to security protection for the majority of organisations, despite the low cost and ease of deployment of multi-factor authentication solutions. Sadly, password theft and password-based breaches will persist as a daily occurrence in 2019.

5. **Malware - protect or fail**
   Ransomware, crypto mining, banking Trojans and VPN filters are some of the key malware challenges that will continue to threaten businesses and consumers in 2019.

   Increasing sophistication will be seen in some areas such as ransomware, alongside new malware approaches and increased volumes of malware in other areas. Traditional AV will not provide sufficient protection. Solutions that have a direct malware focus are essential for organisations, alongside tracking of network activity (in and out of the network).

6. **Cyber hygiene growth**
   The shift of attack vectors, from the network to the user, means many organisations are now recognising, perhaps belatedly, that their users are their weakest link.

   Alongside greater awareness of the insider threat from malicious current and ex-staff, there is a growing recognition that staff cyber awareness and training is a crucial step in securing this vulnerable area. The response from organisations in 2019 will include cyber education, coupled with testing, measuring, and monitoring of staff cyber behaviour. Increasingly, Entity and User Behaviour Analytics (EUBA) systems will be adopted, alongside training programs and automated testing, such as simulated phishing and social engineering attacks.

7. **IOT – an increasing challenge**
   2019 will significantly demonstrate an upward trend in the security challenges raised by IoT. The technology is being increasingly deployed by organisations, with minimal thought by many as to the security risks and potential consequences.

Because some IoT deployments are well away from the main network areas, they have slipped in under the radar. IoT will continue to be deployed, creating insecurity in areas that were previously secure. For the greatest percentage of IoT deployments, it is incredibly difficult or impossible to backfit security.

8. **Growing risks with shadow IT systems and bad housekeeping**
   Shadow IT systems continue to proliferate, as do the number of applications and access points into systems, including legacy applications. In the case of shadow IT systems, these are indefensible as they are; and in the case of increasing applications and access points, if they relate to old or abandoned applications, they are difficult to identify and defend. There has been both an increased awareness of the opportunity for attack via this route, and an increase in the number of attacks, which will accelerate in 2019.

9. **DDoS - usually unseen, but still a nightmare**
   DDoS is the dirty secret for many organisations, and attacks will continue to grow in 2019, alongside the cost of defending against them. The cost of launching an attack is often shockingly low, and the rewards are quick – the victim pays for it to go away. Additionally, cryptocurrencies have aided the money transfer in this scenario. Yet the cost for the victim is much higher than the ransom, as it involves system analysis, reconstruction and, naturally, defending against the next attack.

10. **Cybersecurity in the boardroom**
    A decade or two late for some organisations, cybersecurity is now considered a key business risk by the board. 2019 will see this trend accelerate as boards demand clarity and understanding in this area. The financial, reputational and indeed C- Suite employment risks of cyber breach will continue to drive board focus on cybersecurity up the agenda.

Bio of author

Ian Kilpatrick, EVP (Executive Vice-President) Cyber Security for Nuvias Group
A leading and influential figure in the IT channel, Ian now heads up the Nuvias Cyber Security Practice. He has overall responsibility for cyber security strategy, as well as being a Nuvias board member. Ian brings many years of channel experience, particularly in security, to Nuvias. He was a founder member of the award-winning Wick Hill Group in the 1970s and thanks to his enthusiasm, motivational abilities and drive, led the company through its successful growth and development, to become a leading, international, value-added distributor, focused on security. Wick Hill was acquired by Nuvias in July 2015.

Ian is a thought leader, with a strong vision of the future in IT, focussing on business needs and benefits, rather than just technology. He is a much published author and a regular speaker at IT events. Before Wick Hill, Ian qualified as an accountant, was financial controller for a Fortune 50 company, and was a partner in a management consultancy.

ENDS

For further press information, please contact Orietta Sutherberry at Nuvias on +44 (0)7741 149367, email orietta.sutherberry@nuvias.com or Annabelle Brown, PR Consultant on +44 (0)191 237 3067, email pr@nuvias.com