SECURITY OUTLOOK 2017

We asked IT security experts for their predictions for 2017. If you thought 2016 was bad, fasten your seat belts – next year is going to be even worse.

What kind of technology trends will impact security in 2017?

Matthew Gardiner, Senior Product Marketing Manager of Mimecast

Companies are now faced with an unprecedented mix of reward and risk as they migrate to the cloud with a vast majority of execs committed to their cloud transformations. Email is usually the first platform organizations move into the cloud. It's the business application that IT departments are most comfortable relegating to a third party to maintain. Yet it's also the ultimate Killer App, a vital conduit – and repository – for business-critical and strategic information. Whether cloud-based or on premises, email data is crucial for closing sales, negotiating, and brainstorming. It's no wonder that email has also emerged as the single biggest threat vector for attacks on corporate information and we believe that we will continue to see this continue in 2017.

Scott Manson, Cyber Security Leader for Middle East and Turkey, Cisco

The Internet of Things and other emerging technologies are going to require even more security. IoT in both the consumer and B2B market will continue to accelerate, connecting data, things, processes and people. Intelligent systems will grow rapidly in 2017, as more applications and products are made available. Wearable devices will continue to grow and mesh with healthcare and big data. Security in the IoT environment is

will naturally become more challenging and complicated.

Inadequate security will be a critical barrier to large-scale deployment of IoT systems and broad customer adoption of IoT applications. Simply extending existing IT security architectures to the IoT will not be sufficient. The IoT world requires new security approaches, creating fertile ground for innovative and disruptive thinking and solutions.

Azeem Aleem, Director, Advanced Cyber Defense Practice, EMEA, RSA

Another surging cybersecurity trend is attacks across industrial control systems. The shift from legacy systems towards process control networks with connectivity around enterprise and internet will create more extensive backdoors to exploit industrial control systems (ICS). Organizations will be oblivious to the device connectivity patterns inside and outside their ICS environment. Moreover, with attacks within ICS through cloud service providers progressing at a faster pace, calls for a dire need for intelligence correlations and reporting mechanisms through behavioral analytics around supervisory control and data acquisition (SCADA) attacks.

In addition, artificial intelligence, big data and analytics, augmented and virtual reality, smart mobility and drones are few of the many emerging technology trends that are most likely to impact cybersecurity in the coming year.

Ray Kafity, Vice President – META, Attivo Networks

Emerging technologies such as industrial IoT, big data, artificial intelligence, machine learning, and mobility are proving to be game changers, unleashing a deluge of disruption across industries. And with these technology trends making inroads into enterprise deployments, it is likely that they will impact security in the coming year.

Ghareeb Saad, Senior Security Researcher, Global Research & Analysis Team, Middle East, Turkey and Africa, Kaspersky Lab

There are a number of trends that we see. The main theme of 2017 is the growing ability of attackers to customize, hide, disguise or manipulate evidence and indicators – making it ever harder to spot and correctly identify them.

We predict espionage campaigns, which can also be a serious threat to businesses, will look to target primarily mobiles, benefiting from the fact that the security industry can struggle to gain full access to mobile operating systems for forensic analysis. As Internet of Things (IoT) device manufacturers continue to develop devices that are not necessarily protected, which can then cause wide-scale problems, there is a risk that vigilante hackers could take matters into their own hands and disable as many devices as possible.

Kamel Heus, Regional Manager - MEA, Centrify

The 'identity' is the new security perimeter as it is the common denominator for any activity involving access to critical resources. There will be an increase in adoption of multi-factor authentication for securing identities, as the password is no longer fit for purpose. We will also see organisations adopting the least-privilege model, where

people will access resources on a need to know basis – this is one of the most important recommendations in security, which organisations are lagging behind in implementing. We will also see an increased adoption of hybrid cloud, where businesses need to find new ways to manage who has access to what data. The latest Shamoon attack in Saudi shows the vulnerability surrounding privileged accounts credentials.

What changes do you foresee in the threat landscape next year?

Mohammed Abukhater, Regional Director for the Middle East and North Africa at FireEye

With the region becoming a hub for many key industries and seeing an increasing consolidation of wealth and assets, it's bound to capture the attention of malicious players. In 2017, we expect the number of politically and financially motivated attacks to increase. Nation-state attacks will not abate anytime soon and are only likely to increase in intensity with the current geopolitical climate in the region.

Ransomware will continue to be a menace to organizations in the GCC, being a more attractive and lucrative option for criminals with the proper skillsets and motivations. We expect to see credit and debit card fraud, illicit bank transfers, and ATM fraud.

Tareque Choudhury, Head of Security and BT Advise, Middle East and Africa, BT Global Services

The threat landscape is one that is constantly evolving. With some of the highest levels of financial assets, energy resources and lucrative real estate investments concentrated in the region, coupled with a move towards smart government and smart services, the GCC will increasingly find itself in the crosshairs of cyberattackers.

With every passing year, the adoption of the cloud by enterprises and the government alike is increasing. Likewise, IoT is gradually reaching a higher level of maturity. As mentioned before, these innovations have exponentially expanded the attack surface, putting strain on existing on cybersecurity resources.

Alain Penel, Regional Vice President – Middle East, Fortinet

Increasing attacks targeting IoT devices is probably the safest prediction for 2017. With over 20 billion IoT devices online by 2020, versus one billion PCs, the math is pretty easy. And we are in the middle of a perfect storm around IoT: A huge M2M (machine-to-machine) attack surface, growing to over 20 billion connected devices, built using highly vulnerable code, and distributed by vendors with literally no security strategy. And of course, most of these devices are headless, which means we can't add a security client or even effectively update their software or firmware.

The move to cloud-based computing, storage, processing, and even infrastructure is accelerating. Naturally, this expands the potential attack surface. The weakest link in cloud security, however, is not in its architecture. It lies in the millions of remote devices accessing cloud resources. Cloud security depends on controlling who is let into the network and how much they are trusted. In this next year we expect to see attacks designed to compromise this trust model by exploiting endpoint devices, resulting in client side attacks that can effectively target and breach cloud providers. Businesses were initially slow to adopt cloud-based strategies precisely because they were concerned about the security of an environment they didn't own or control. If the cloud-based environments and solutions they are now adopting are suddenly found to be untrustworthy, it could radically affect the current migration to the cloud and the resulting evolution of network infrastructures.