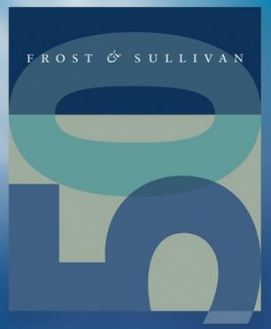
Cyber Security Predictions for 2017 —an Asia-Pacific Perspective

Cyber Security Practice, Asia-Pacific



March 2017

FROST & SULLIVAN

1 Business Email Compromise (BEC) attacks will overtake Ransomware and Advanced Persistent Threat (APT) attacks.

BEC generally happens when email accounts of key executives are compromised and involves payments made to fraudulent bank accounts. In Singapore alone, about S$19 million has been lost through BECs between January and September 2016. When compared to the same period last year, there has been an increase of 20% in the number of such cases. Police investigations revealed that the scam usually involves businesses with overseas dealings, with email as the main form of communication in the dealings. As a BEC is relatively easier to execute and evade cyber defense tools better than other popular attack vectors, such as ransomware and APTs, it can potentially be the main cyber threat in Asia.

2 DDoS attacks might cause the Internet to be down for an entire day in a country.

Distributed Denial of Service (DDoS) volumetric attacks hit over 1 Tbps of traffic and shut down several popular online services in 2016. Gvernment authorities grapple with ensuring strict security regulations and manufacturers continue to deliver insecure IoT devices to the market; however, when coupled with the fact that internal volumetric attacks to DNS servers for service providers are not well defended, cyber attackers will most likely attempt to exploit the vulnerability to the next level and bring down the Internet in a country for at least a day.

3 Greater enforcement expected for Internet of Things devices to meet cyber security standards.

As authorities become increasingly concerned about the threats unsecured IoT devices will pose to the community, it will be illegal for these manufacturers to sell their products in countries that demand these devices comply with security standards. The recent Mirai botnets exploiting the vulnerabilities of IP cameras are an example of how manufacturers did not include a security process of changing default passwords when connecting the devices to the Internet.

4 The healthcare sector will have more stringent regulations towards ensuring uptime of computer systems handling critical operations.

Globally, ransomware attacks on computer systems of healthcare providers in 2016 infected computer systems and disrupted operations; in some cases, patients in need of immediate attention had to be diverted to other hospitals. While major healthcare providers in Asia had initiatives to comply with security standards (e.g., HIPAA), their use of legacy security tools to meet minimal compliance standards could not keep up with the new types of cyber attacks. These days, stolen personal healthcare records are worth more in the dark web than credit card information and medical machines are increasingly connected to the Internet, which pose a possible safety risk to patients.

The healthcare industry needs a good ‘cyber health check’ before it is too late.

5 New technologies such as Blockchain may be used to enhance trust between stakeholders and facilitate exchange of threat intelligence among industries.

The setting up of more Information Sharing and Analysis Centers (ISAC) will act as platforms for both private and private sector participants to share threat intelligence. However, participants are wary of exposing their weak security posture when contributing intelligence due to a successful attack, and there are issues of untrusted sources that may contribute the wrong intelligence. Blockchain may emerge as the technology to facilitate the exchange, as it authenticates the trusted party to contribute, obfuscates the contributor's detail with anonymity, and offers a tamper-proof system that prevents unauthorized alteration of any data shared.

6 More adoption of technologies that focus on threat actors and “hunting” for their next attack.

Traditionally, enterprise security teams have adopted a ‘wait and see’ posture, and try to build their defenses to mitigate the possible threats they are aware of. However, more enterprises are working toward trying to know what the attackers are innovating in terms of cyber attack techniques, their next moves, and build their defenses to counter the new attack vectors.

7 More enterprises will offer bug bounty programs, which are seen as a measure to deter talents from taking up black hat hacking.

The idea is simple yet effective. Pay the attackers for finding and reporting major vulnerabilities in enterprise and/or developed applications. Enterprises will be able to strengthen their security defenses by using the crowdsourcing model and encouraging potential hackers to discover more and do more of the good rather than the bad.

8 More drones will be used to facilitate cyber attacks.

A group of researchers from iTrust, a Center for Research in Cyber Security at the Singapore University of Technology and Design, demonstrated that it is possible to launch a cyber attack using a drone and a smartphone. In the future, it is expected that drones will be an easy way to scan for unsecured wireless traffic as a way of performing war-driving attacks. While more applications are developed for drones in commercial use, inevitably cyber criminals will think of new techniques to launch a cyber attack. Other possible types of attacks include delivering GPS-jamming signals to a vessel or dropping USB drives containing malware to air-gapped critical infrastructures.

FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies? Contact Us: Start the Discussion

www.frost.com