PECB

When Recognition Matters

PROJECTED CYBER-ATTACKS IN 2018

A MATTER OF 'WHEN', NOT 'IF'?

While governments point fingers at each other for failing to detect, prevent and/or effectively respond to attacks, the cyber-crimes are generating far-reaching impacts. The rise in cyber-attacks, as a result of the growth and development of the internet, has created problems for almost every industry worldwide, affecting the US, UK, EU and Russia the most.

Based on the most recent reports, cyber-attacks are going to be more destructive in 2018. The continued pressure placed upon organizations to operate with an online presence brings the risk of encountering myriad cyber threats. Information Security and IT teams, therefore, will witness many rapidly evolving threats, and many new, advanced extortionist methods. Richard Ford, a chief scientist at Forcepoint stated that "this has been a tough year, and 2018 is going to be a tougher year", in terms of cyber-attacks. He claims that the increased digital footprint will further continue to endanger the survival of the organizations because of the lack of awareness and shortfall in technical expertise. Referring to Ford, due to the necessity to keep pace with continually evolving technology, one can expect that the year 2018 will witness a significant rise in phishing emails and email compromise.

WHAT CAN WE EXPECT IN 2018?

1. More supply chain attacks

   These attacks are very advanced and are performed by employing means and tools that are too complex to be detected and responded to. The number of supply chain attacks is expected to increase in 2018, both from the point of discovery and actual attacks.

2. Increase of high-end mobile malware.

   According to a report by Kaspersky Lab, the total number of mobile malwares is higher than it is reported due to the shortcomings in telemetry. This report estimated that in 2018, there will be more high-end APT malwares successfully exposed, due to the increase in these types of attacks and the use of more sophisticated technologies to detect them.

3. Crisis in e-commerce identity

   In the past few years, we had an increase in the large-scale breaches of personally identifiable information (PII). Equifax, which took place in 2017, is the example that best illustrates PII breaches, where approximately 145, 5 million Americans were affected and had their personal information exposed. This type of attack is expected to increase in 2018 with targets being some of the most prominent and large companies in the world.

4. Increased router and modem hacks

   Routers and modems, in either homes or companies, tend to be vulnerable to attacks. We are aware that they are everywhere, they are very important for our daily basis operations, and they tend to run parts of software that is unpatched and left vulnerable. The number of attacks is expected to vastly increase in 2018.

HOW TO PREPARE YOUR ORGANIZATIONS FOR 2018

Enterprises need to prepare today to recover from or prevent potential cyber fraud in the future. But, how do we detect and/or prevent these cyber-attackers that seek to profit by targeting businesses and deceiving victims into providing access to vulnerabilities?

There are a few key steps companies and IT Security teams can take:

- Assess the capabilities of your staff, infrastructure, and processes to ensure they are prepared when threats are present
- Conduct an IT Risk Assessment
- Ensure that staff receives training and is aware of the cyber-threats
- Secure your network
- Secure your websites
- Conduct a Business Impact Analysis in regards to data security
- Create a proper contingency and disaster recovery plan for different cyber-attack scenarios

Once the organization has promoted awareness on specific causes of cyber-attacks, it has conducted proper staff training sessions, and it has established infrastructure to support the organization's network, the cybersecurity program should be prepared for responding to potential threats emerging during 2018. Information Security and IT Security teams, however, should constantly seek to identify and employ other protective countermeasures. At the end of the day, hackers don't play by a set of rules; thus, it is only through a spreading of awareness on the need to secure the networks that aggregate security across all businesses. Enterprises should at a minimum, perform an annual assessment with a group of ethical hackers to closely simulate a real attack. Doing this assessment, business owners are provided with feedback in how to shape and develop their responses to the ever-changing threats of cyber attackers.

PECB provides training and certification services for ISO/IEC 27032 Cybersecurity which prepares you for these types of attacks. For more information, please visit: https://pecb.com/en/education-and-certification-for-individuals/iso-iec-27032

Author: Ardian Berisha is the Portfolio Marketing Manager for Information Security Management at PECB. He is in charge of conducting market research while developing and providing information related to ISM standards. If you have any questions, please do not hesitate to contact him: marketing.ism@pecb.com.

Co - Author: Albion Bikliqi is the PECB's Information Security Manager. He is the key person or the process owner for all the activities pertaining to protecting the confidentiality and integrity of any related business data that is of great significance to the organization. While carrying out these ongoing activities, he ensures that the organization's rules and regulations are being adhered to. If you have any questions, please do not hesitate to contact him: information.security@pecb.com.