Nexia SJ Tanzania

Are you ready for the new challenges facing businesses in 2019?

Modern Threat landscape - Why is Security more important now for your organization?

The Modern Threat landscape exposes businesses to both physical and digital information security threats. It is more important now to run a business in a secure way particularly in a world of Cyber attacks; with threats becoming more complex and cyber attackers more persistent, small and medium-sized companies are increasingly becoming target of cybercrime, however banking is the leading risk sector.

Cyber criminals have been targeting Tanzania for some time now and according to a 2016 report published by SERIANU Tanzania Limited on cyber security, Tanzania has lost approximately $85 million to cyber criminals. Therefore organizations in Tanzania must step up their investment in cyber security, to counter the growing threat of cyber attacks!

Cyberattacks resulting in cyber breaches should be considered as business risks by the CEOs and board members because of the impact it has on the organization's reputation and profitability.

Every year almost 1 percent of global GDP is lost to cybercrime as reported by McAfee and the Center for Strategic and International Studies. The cost of cybercrime is very high and may be as much as US $600 billion. Moreover, monetization of the stolen data is now easier because of the use of digital currencies and improvement in cybercrime black markets.

Organizations therefore must integrate IT security into leadership and business decisions in order to grow, streamline, and innovate as well as keep pace with the evolution of cyber threats.

The top security concerns for businesses in 2019, should be targeted phishing attacks against employees, advanced persistent threats, ransomware, denial-of-service attacks and the rapid increase of use of their own mobile devices by employees. Also threats from viruses, trojans, back doors to outright attacks from hackers as the majority of threats involve multiple exploits.

Although companies invest in technology to defend against external cyber threats, their biggest security vulnerability is internal: ***their employees***. Therefore the focus should be more on **insider threats.** Almost two thirds of cyber breaches are caused by employees' negligence or malfeasance, including losing of laptops, disclosure of information or actions of rogue employees.

For example, a hacker might use a **Phishing attack** to gain information about a network and break into a network: AI-generated "phishing" e-mails can be used to trick people into handing over passwords and other sensitive data as hackers are now able to throw highly realistic fake video and audio into the mix, either to reinforce instructions in a phishing e-mail or as a standalone tactic.

Shadow IT is the unsanctioned use by employees of rogue Software as a Service (SaaS) applications like Google Apps, Dropbox, Salesforce, Cisco WebEx, Concur, GoToMeeting and other cloud services, and it is a very serious and growing threat to IT compliance and cyber security.

Additionally, shadow IT usage is not confined to SaaS applications. Also in some cases employees or groups may set up their own cloud servers to process and store organization's data leading to compliance violations and data breaches.

Therefore, it is important to train the employees on cyber-risks and security.

Malware of all types is a huge problem. It is becoming more difficult to counter, as cyber-attackers are getting more skilled at developing software that can avoid traditional detection and employ more sophisticated malware.

Cryptojacking, or "Cryptomining malware" affects endpoints, mobile devices, and servers. It steals resources from victims using both invasive methods of initial access, and drive-by scripts on websites. Therefore **EDR/MDR** (endpoint detection and response/managed detection and response) tool will be another big advance in 2019.

For example, the recent incident at Marriot: EDR could have mitigated the recent Marriott security breach, which was just discovered. Someone was in their network stealing data for 4 years and no one discovered it. Scary. I'm sure they had anti-virus, firewalls and alike in place.

Therefore **Data security** will continue to be a major threat for businesses of all sizes.

Data privacy/protection will be big in 2019 particularly with implementation of General Data Protection Regulation (GDPR) with effect from May 2018.

The **General Data Protection Regulation (GDPR)** is a set of new rules of data privacy that requires businesses to protect the personal data and privacy of EU citizens for transactions that occur within EU member states. The exportation of personal data outside the EU is also regulated under GDPR. For example, If your company does any kind of business with companies or customers residing in the EU, you're obligated to comply with this regulation. Non-compliance with this new regulation could result in heavy fines.

The first fines in Europe happened in last quarter of 2018 for organizations that failed to comply with GDPR and therefore we believe that the budgets for technological solutions will in the next couple of years increase drastically.

Automation and **business intelligence** is a new form of high-quality automation. Machine learning will play a critical role in gathering intelligence and will begin making more of their own decisions as well as execute changes themselves to minimize an organization's cyber-risk, based on this intelligence.

Nexia SJ Tanzania

How to better defend against cyber-theft

While cyber attacks continue to grow ever year, many medium and large corporations do not devote sufficient resources to cyber risk management.

All businesses can become better prepared and more adept at protecting against cyber-crime which continues to surge every year. Cyber-defenders will have to prepare themselves for the new threats, too. Here are some actions concerning cyber security that can be taken to become more security-conscious:

- Conduct a **security audit**. Learn how secure your network and other security systems are, where vulnerabilities exist and how to resolve them.
- Ensure you have a proper backup system.
- Assess your system threats.
- Put a prevention system in place to defend against intruders.

It will pay to increase spending on cyber-security protection, developing qualified cyber security policy and, perhaps use a consultant to check resilience to cyber risks.

For any queries please contact our Cyber Security Team on:

Nexia SJ Tanzania

info@nexiasj.co.tz

+255713444254