GLOBAL BEST PRACTICE DELIVERED LOCALLY...!

SENACA EA

SAFETY AND SECURITY SERVICES

EVOLVING SECURITY THREATS FOR 2021

If COVID-19 has taught us anything, it is that there is a very real need to anticipate threats, to develop scenarios for handling them and to test our response before they destroy our businesses. From January to December this has been a lesson we have learnt every day. As data breaches increase, new technologies emerge, and the geopolitical landscape becomes more complex, business leaders need to **rethink cyber**. Increasingly they need to view it as one that, if left unguarded, can wreak significant damage.

From the developing stories that have been happening over the months amidst the Pandemic, the top threats identified to be most prevalent for 2021 are stated as below.

Cybercrime: We have seen an increase in cybercrime targeting the **COVID-19** "**opportunity".** Not restricted to ransomware attacks on hospitals and banks, this has also seen targeting of **remote workers** who are accessing **corporate systems.** Setting up **fraudulent charities**, **fraudulent loans, extortion** along with an increase in traditional **phishing** and **malware** are all on the increase. The changing threat landscape requires risk management and security practitioners to pay close attention to how exposures change over the coming months and the circumstances that influence the level of protection.

Insider Threats are Real: The insider threat is one of the greatest drivers of security risks that organizations face as a malicious insider utilizes credentials to gain access to a given organization's critical assets. Many organizations are challenged to detect internal acts, often due to limited access controls and the ability to detect unusual

activity once someone is already inside their network. The threat from malicious insider activity is an increasing concern, especially for financial institutions, and will continue to be so in 2021.

The Digital Generation Becomes the Scammer's Dream: The next generation of employees will enter the workplace, introducing new information security concerns to organizations. Their attitudes toward sharing information will fall short of the requirements for good information security. Reckless attitudes to sharing information online will set new norms for security and privacy, undermining awareness activities; attackers will use sophisticated social engineering techniques to manipulate individuals into giving up their employer's critical information assets.

Edge Computing Pushes Security to the Brink: Edge computing will be an attractive architectural choice for organizations; however, it will also become a key target for attackers. It will create numerous points of failure and will lose many benefits of traditional security solutions. Organizations will lose the visibility, security and analysis capabilities associated with cloud service providers; attackers will exploit blind spots, targeting devices on the periphery of the network environment, causing significant downtime.

Rushed Digital Transformations Destroy Trust: Organizations will undertake evermore complex digital transformations deploying AI, blockchain or robotics expecting them to seamlessly integrate with underlying systems. Those that get it wrong will have their data compromised. Consumers and dependent supply chains will lose trust in organizations that do not integrate systems and services effectively; new vulnerabilities and attack vectors will be introduced, attracting opportunistic attackers.

What we generally think as a Security Company is that attackers will continue to be presented with the tools and opportunities to target and exploit those who are unprepared. The coming year will once again be volatile, but targets will be predictable. The organizations that see security as a strategic business issue, one in which people throughout the enterprise have a role to play, will be the organizations that prosper going forward.

Did you enjoy this article?

Please follow us and like our social media pages: FACEBOOK, INSTAGRAM, LINKEDIN, TWITTER.