Covid-19: SMEs Cybersecurity Challenges

OU PHANNARITH | TWITTER: @PHANNARITH

Agenda

- What’s Happening
- Cyber threat during COVID-19
- The Way to go

What’s happening?

❑ Create a new environment for Small and Medium Enterprise (SMEs)

❑ Internet connection becoming overwhelming, as a primary source of communicaiton for both both government and private sectors.

❑ Mindset and work culture have to transform in order to adapt during this downturn

Cyber Threats

- The more we are connected, the more vulnerable we are
- Tokopedia, the largest online store of Indonesia has been hacked with 15 millions records of users stolen and put into darkweb marketplace
- Health institution and medical agencies were also under attack. For example, in UK have been hit with ransomware, while in Mongolia were hit with digital coronavirus malware.

Cyber Threats …

❑ Manipulate the psychology of an individual has become one of the top attack vectors through social engineering

❑ It raise up 60 percent worldwide targeting indivdiuals and businesses

❑ The attackers leverage the COVID-19 situation through anxiety, using scare tactics and urgent calls to action including relief packages, help desk impersonations, safety measures, outbreak cases, donation scams, fake products, test of emergency notification systems, confidential information on COVID-19, Virtual Private Network connection, and more.

Cyber Threats …

- ❑ End-points security is another concerns.
- ❑ It will open-up a new vector of attack on cooperation credentials, sensitive data, and intellectual property.
- ❑ An average, there are around 10 internet connected devices for each home
- ❑ We rarely carry out security checks for PCs, Laptops, Smart-Phone, security camera (CCTVs)

Cyber Threats …

❑ Due to urgent change working environments, most of SMEs choose communication platforms based on ease and convenience, not on security and privacy

❑ Additional costs and sophisticated equipment required to be installed with technical expertise, also the important consideration

❑ Video conferencing app/software become a new playground for attacker

Cyber Threats …

❑ Most of the incidents fall into the hands of user who are using technology.

❑ Less vulnerability on video conferencing itself

❑ Users are not equipped with basic cybersecurity hygiene and up-to-date information

Cyber Threats …

❑ MSMEs that need to ensure that their company systems and data are securely protected with technical measures and procedures, during the sudden spike of remote connections.

❑ The lack of cybersecurity policies such as remote access, back-up, access control, monitoring, in addition to technical measures including software licenses, antiviruses, firewalls, and patching will open doors for attackers to penetrate systems easier than ever before.

Conclusion

The COVID-19 pandemic is playing a crucial role in accelerating digital transformation in both the government and private sector. Overcoming these unprecedented challenges can act as a digital exercise for all of us to be resilient in these types of extreme situations.

Cybersecurity should be the top priority for all MSMEs during this forced shift towards digital platforms. Transitioning out of this pandemic, a new normal for both work and life will continue to evolve, based on the utilization of digital technologies.