PES UNIVERSITY

Digital Forensics
UE19CS336

Assignment Case Study -
Coronavirus now possibly largest ever cyber security threat

Name : Suhan B Revankar
SRN : PES2UG19CS412
Section : G Section

Abstract

The Coronavirus (COVID-19) pandemic has led to biggest number of employees globally bound to work remotely. The people working from home required awareness and knowledge of phishing scams, the fastest growing type of cybercrime, many of which are now playing on fears of the Coronavirus. Employees from organizations of all sizes and types now have minimal cybersecurity resources, if any, compared to what is normally available to them. Organisations are required to ensure any endpoint that an employee is using are fully protected. As the Absolute 2019 Global Endpoint Security Trend Report showed, 42 per cent of endpoints are unprotected at any given time. As the home-working becomes the new normal, criminals are seeking to capitalise on the widespread panic – and succeeding, alas.

New coronavirus-themed phishing scams are leveraging fear, hooking vulnerable people and taking advantage of workplace disruption. Therefore, the people working from home should immediately get educated about their cyber privacy and cybersecurity failing which the global cybercrime damage may costs as much as double by the end of this year.

Impact of COVID-19 on Digital working & Cybersecurity

The coronavirus pandemic has created new challenges for businesses as they adapt to an operating model in which working from home has become the 'new normal'. Companies are accelerating their digital transformation, and cybersecurity is now a major concern. The reputational, operational, legal and compliance implications could be considerable if cybersecurity risks are neglected.

The restrictions imposed by governments in response to the coronavirus pandemic have encouraged employees to work from home, and even 'stay at home'. As a consequence, technology has become even more important in both our working and personal lives. Despite this rise of technology need, it is noticable that many organisations still do not provide a 'cyber-safe' remote-working environment. Where business meetings have traditionally been held in-person, most now take place virtually.

Cyberattacks on video conferencing services

An example of criminals exploiting the cybersecurity weaknesses in remote working has been the series of cyberattacks on video conferencing services. Between February 2020 and May 2020 more than half a million people were affected by breaches in which the personal data of video conferencing services users (e.g., name, passwords, email addresses) was stolen and sold on the dark web. To execute this attack, some hackers used a tool called 'OpenBullet'.

Hackers also use credential stuffing techniques to gain access to employees' credentials and the stolen data is then sold to other cyber criminals. One of the consequences is a serious disruption to businesses that rely heavily on

videoconferencing platforms. Credential stuffing is a form of cyberattack whereby hackers use previously-stolen combinations of username and password to gain access to other accounts. This is possible because it is very common for individuals to use the same username/password combination across multiple accounts.

The changing nature of cyberattacks during Covid-19 pandemic

It appears that many hackers are upping their game, and to capitalize on the new shift by companies to remote working, they have developed new malware to attack and infiltrate systems.

Some of the new attacks use a form of machine learning that adapts to its environment and remains undetected. As an example, phishing attacks are becoming more sophisticated and using different channels such as SMS and voice (vishing). Moreover, news about vaccine developments is used for phishing campaigns. Ransomware attacks are also becoming more sophisticated.

For example: hackers are combining data leakage attacks with ransomware to persuade victims to pay the ransom.

This upsurge in sophisticated cyberattacks calls for new 'cutting edge' detection mechanisms to meet the threat, such as 'user and entity behavior analysis' . This analyzes the normal conduct of users, and applies this knowledge to detect instances where anomalous deviations from normal patterns occur.

Are businesses prepared for the new cybersecurity risks?

Remote working has created challenges for many small and medium-sized companies: they have not been sufficiently prepared for the upsurge in sophisticated cyberattacks, and much progress is needed to raise cybersecurity awareness. Before the pandemic, some companies were opposed to allowing remote working and especially when it came to accessing confidential data (e.g. banking client personal data). In only a short period of time, companies had to increase their capacity and capabilities for remote working. Unfortunately, cybersecurity was not always a key priority in the fast deployment of remote working capabilities.

For example, some companies do not check that personal devices are equipped with standard security protections before their employees access corporate data, relying on virtual private network (VPN) technologies to do a job that they are not by default designed for. There are ways that companies can implement security measures without being intrusive. For example, host checking is a technology that validates individual requirements on personal devices before allowing access to corporate applications. When vulnerabilities in VPNs are discovered and patches are produced to deal with them, it is important to apply the patches in a timely manner, where possible.

Examples of how companies and employees can increase cybersecurity

Employees working from home and using their personal computer (and even those using a corporate-owned device) should implement essential cyber hygiene practices. These include:

- Antivirus protection: Employees should be provided with a license to antivirus and malware software for use on their personal computers. Although this does not provide failsafe protection, it eliminates many low-level attacks.
- Cybersecurity awareness: Staff should be briefed on best practices and procedures to regulate the sending of emails or other content to private email addresses and/or cloud storage.
- Phishing awareness: Employees should be vigilant when receiving emails and should check the authenticity of the sender's address.
- Home network security: Employees should ensure that their home Wi-Fi is protected by a strong password.
- Use a VPN: Virtual private networks add a further layer of protection to internet use from home. They cannot on their own be relied upon to prevent cyberattacks, but they can be a useful barrier against cyberattack. There are some basic cybersecurity strategies that businesses can adopt.
- Identify weak spots: All IT systems have weaknesses. Companies should run tests to identify them and patch the most critical vulnerabilities as soon as possible. This can take the form of vulnerability scanning, or various type of penetration testing exercises. Additionally hardening of components of the technical infrastructure should be performed.
- Frequent reviews: Companies should regularly evaluate cybersecurity risk exposure and determine whether existing controls are robust enough. Any new forms of cyberattack that have appeared recently should be considered during these reviews.
- Renew business continuity and crisis plans: Business lines Managers need to keep their business continuity plans updated and consider cyberattack scenarios.

More advanced measures that can be taken include:

- Apply new technology and tools: Companies can use advanced tools such as host checking (a tool to check the security posture of an endpoint before authorizing access to corporate information systems) to reinforce the security of remote working.
- Intelligence techniques: Businesses should encourage proactive use of cyber threat intelligence to identify relevant indicators of attacks (IOC) and address known attacks.
- Risk management: Businesses can apply governance, risk and compliance (GRC) solutions for improved risk management. GRC solutions provide a detailed view of

the company's risk exposure and help link together the various risk disciplines (e.g. cybersecurity, operational risks, business continuity).

- Prepare for attacks: In these high-risk times, companies are advised to carry out frequent cyber crisis simulation exercises to prepare their response to a cyberattack.
- Zero Trust: CISOs and CIOs should consider implementing a zero trust approach to cybersecurity. This is a security model where only authenticated and authorized users and devices are permitted access to applications and data. It challenges the concept of "access granted by default".

Conclusion

Cybersecurity is on the agenda of most executive committee meetings, but should perhaps be given extra attention in view of the growing threats during the pandemic. In the midst of the second wave of the coronavirus and concerns about a potential third wave, companies should be proactive in addressing the threats, and plan ways of preventing successful cyberattacks rather than responding when they occur. However although prevention measures are important, there is also a need for cyberattack detection, response and recovery capabilities.

This pandemic has taught us that preparation is key to successfully limiting the risks related to cyberattacks. The ability to quickly react to unforeseen events helps reduce the impact of a cyberattack. Companies that already benefited from secure remote working capabilities will be better prepared to face the continuous increase of cyber threats. Companies that were caught off guard will have to quickly assess their exposure to cyber threats and prioritize initiatives to address their cybersecurity gaps with recommended practice. In addition, corporate owned devices should be the standard for companies allowing remote access to confidential and sensitive data. When it is acceptable to access corporate data from a personal device, cyber risks should also be assessed and actions should be taken to limit cyber threats exposure. **The reality is that companies need to change their outlook from 'if' they get attacked, to 'when', and recognize that the fallout from breaches of data privacy or ransomware can be financially devastating**. It should also be remembered that financial gain is not the only motive behind cyberattacks. 'Hacktivism' and its aim of damaging business reputations is an additional threat.

There are ways to reduce the likelihood and impact of a cyberattack, but it requires focused action and planning. Companies need to make their remote working practices resilient to cyberattacks and enhance their development and application of security measures.

*****