The importance of cybersecurity in the post-COVID-19 world

3 August 2020

By Sony Anthony, Partner, Cyber Security, IT Advisory-Risk Consulting, KPMG in India

(5 mins read)

The weakest link in cybersecurity, it's often said, is humans. Individuals are increasingly the targets of two types of attacks: 1) **social engineering** seeks to circumvent an existing process and exposes an individual's lack of security awareness. 2) **logical engineering** targets a system or technology and exposes obsolete/vulnerable software/misconfigurations.

The new normal of remote working has put the focus firmly on cybersecurity, trust and protecting data. COVID-19 has forced the hand of businesses in several sectors by requiring them to confront their digital preparedness in tackling cyber threats head on.

Changes in the work environment

In the pre COVID-19 era, most employees worked from offices, where the local area network (LAN) as well as the desktops/laptops were adequately secured. Sophisticated technologies could protect against cyber-attacks that originated primarily from the internet and targeted the enterprise network. Enterprise protection technologies secure the employees' systems from targeted phishing campaigns that lure them into clicking on unknown links and attachments. Offices also offer an additional layer of security in the sense that employees can check in with their colleague in the neighbouring cubicle or their manager and alert the IT security team if they notice any suspicious emails or links.

In the post COVID-19 era, only support staff personnel or those who need direct system/hardware access e.g.: research labs, direct console, specific printing machines in banking environment, etc., are working from office. The rest of the workforce is operating from home, and connected to more vulnerable networks when compared to the ones at the office.

Security challenges of work from home

While organisations are offering secure virtual private network (VPN) access to employees, the first point of interface for the employee's laptop or desktop is typically a broadband network, mobile hotspot or shared wireless network. Employees are connecting via home wireless routers, which have rudimentary security for encryption of traffic. Some of these devices have default passwords for administration that are left unchanged by the home user. There are several security challenges associated with connecting to home networks, including:

1. These wireless routers are a shared asset with the family and/or neighbours. The data traffic flow is not controlled, and covers a wide range of activities including personal email and educational needs

2. Employees in the age group of 22 to 28 in cities lean towards shared accommodation to address travel and costs of living. They usually have flat mates who also are working from home and have weak protection on their laptops

3. A corporate user on the home network can access unfiltered internet, personal email and drives unlike in the past, where the user was governed by the IT security team and is now a COVID-19 specific phishing theme target

4. A home user clicking on an unsuspecting link or redirected to a malicious website could end up loading malicious codes into the browser of the corporate user's laptop which gets executed unsuspectingly in the background and proceeds to compromise the enterprise network

5. This malicious code could also extract valid corporate credentials when the home user logs into the enterprise portal or VPN via keylogging or tab-nabbing, thereby compromising the security of the entire organisation

6. There are also heightened risks of IP theft and leakages, especially for work-from-home users operating for organisations in research and development.

There are about 10 COVID-19 phishing themes that are actively targeting corporate work-from-home users. The most prominent phishing theme is related to how employees can claim an additional benefit related to work from home. This specific theme does not compromise the system or technology, instead spoofs the origin of a government email address with an excel attachment claiming to help compute work from home expenses that can be claimed for a tax exemption in the light of COVID-19. The targeted user simply opens the attachment and a malicious code is injected within the system.

A more sophisticated COVID-19 theme is to target system and network administrators who are working from home. This attack requires a deeper understanding of the target to be successful. Professional database sources are scoured for profiles of people who have significant technical privileges at the organisation

Guarding against cyberattacks

An organisation's IT security team could put in place additional focus on detection technologies for traffic originating from the home user. Additionally, analytical technologies like 'user behaviour' needs could be adopted at the earliest. It would be beneficial to incorporate and adopt enhanced tele-worker policies for the organisation as well as the teleworker.

The corporate user's current security awareness levels are limited to only password sharing/complexity, clean desktop and locked cabinets. In the wake of COVID-19 based attacks, the home user needs to be informed on accounts, sessions, remote maintenance, software updates, security of home network routers and integration of home-based printers, gaming consoles and IOT devices, among other aspects.

It would be advisable to educate the home user on incident understanding and handling thereby supporting the IT teams with a time sensitive response and enhancing the capability of recovery in the wake of any unprecedented attack. Organisations need to conduct Red Team exercises that simulate attacks via social

engineering and compromise technology to understand the organisation’s capability to detect, respond and recover in time.

In conclusion

In the post-COVID-19 world, cyber attackers are increasingly seeking to exploit vulnerabilities in an organisation’s security infrastructure that the shift to remote working has exposed. It is time for cybersecurity leaders to re-visit their security measures and focus on deploying new processes and technologies to fortify their digital architecture going forward.