Title: Securing corporate cyber frontiers while employees work from home
Author: Truc Van
Link: https://www.vir.com.vn/securing-corporate-cyber-frontiers-while-employees-work-from-home-76354.html

Securing corporate cyber frontiers while employees work from home

The rise of cyber threats in the midst of the coronavirus pandemic is a headache for both businesses and individuals.

Cloud video conferencing platform Zoom has gained huge numbers of users this year but its security remains controversial, with cybersecurity firm Cyble discovering that half a million Zoom accounts being given away on the dark web since early April at a price of 0.2 US cents each.

This is not the first time Zoom's security has been compromised. At the end of March, a security breach allowed trolls to see images from meetings without a username or password. Additionally, online criminals can easily break into Zoom meetings to interrupt, steal information and data, and share disturbing content. Despite the security concerns, Zoom is still gathering momentum as people are working from home in increasing numbers to curb the spread of the virus. Pho Duc Giang, director of PwC Vietnam Cybersecurity Ltd., told VIR that the pandemic gives cybercriminals more opportunities to take advantage and facilitate campaigns.

"By working from home, firms connect remotely to corporate networks or check out and take home the company's digital assets. If these practices are not properly authorised, protected, and monitored, businesses expose a much wider attack surface," Giang said.

Additionally, cybercriminals can now use the coronavirus theme to lure internet users into opening attachments or clicking on links to phishing websites and malware.

According to Giang, there are many advanced persistent threat groups which are actively targeting critical infrastructure and government entities, with the most heavily-used technique being injecting malicious macros into Word and Excel-based documents.

Title: Securing corporate cyber frontiers while employees work from home
Author: Truc Van
Link: https://www.vir.com.vn/securing-corporate-cyber-frontiers-while-employees-work-from-home-76354.html

In Vietnam, the Department of Cybersecurity and Hi-tech Crime under the Ministry of Public Security has reported similar attacks via email. Specifically, hackers have sent emails purported to be from the prime minister which contains false news about the pandemic in a Word document.

Once users download and open the document, the code will be activated and the computer is then under the control of hackers. As per the Global Check Point Threat Index, there is a significant surge in website domains registered in relation to COVID-19, of which at least 50 per cent are more malicious than others. Google also reported that they have blocked more than 18 million malware and phishing emails a day.

Tarun Sawney, senior director of The Software Alliance affirmed these trends, *"Particularly with the current health crisis, cybercriminals send fake news emails about the virus or links which contain malware or ransomware. Hackers can also use fake virus tracking apps to lock phones until a ransom is paid."*

He said that companies are also at risk of cyberattacks while employees are working from home. *"Three-quarters of Vietnamese companies are using unlicensed software so they are even more vulnerable to cybersecurity threats,"* he added. *"With employees outside their organisations' networks and no longer using devices under the control of the IT department, several new opportunities have opened up for attackers."*

Major General Nguyen Minh Chinh, director of the Department of Cybersecurity and High-tech Crime, said *"Businesses, organisations, and individuals both in Vietnam and throughout the ASEAN are facing more sophisticated attacks every day, and the destabilisation caused by the COVID-19 crisis has made many of them even more vulnerable. It is vital that they become more aware of the risks and protect their data – not just for their own sake, but for the public as well as the safety and security of the country."*

Meanwhile, Giang from PwC Vietnam Cybersecurity pointed out three key areas for companies to reduce cyber risks. He recommended that at the minimum, enterprises should establish a process to grant, authorise, and monitor remote access – for example, enabling two-factor authentication and encrypting communication channels, using the latest software patches, and carrying out security configuration reviews.

Additionally, cyber awareness training is important. Staff with more working time at home should get continual updates on the threats of social engineering, external phishing attacks, and other precautions.

"Lastly, for business resilience, it is important that the IT team or specialised cyber team is prepared to address any cyber incident responses," Giang added. *"For example, they need to make sure there is sufficient staff on hand, provide timely internal communications, and action IT disaster recovery practices."*

He noted that organisations can consider automated technology to assist in early detection and proactive alerts of cyberattacks.

A web security report from Vietnam's technology startup company CyStack Security revealed that Vietnam ranked as 11 in the world and third in Southeast Asia in the number of websites attacked by hackers, with 9,300 in 2019.

Cybersecurity is no longer just something for the IT department to worry about and in this time of crisis, it will be more imperative than ever for companies to employ safe and secure digital practices. Their survival through these difficult times could depend on it.

By Truc Van