Managing Security Risks in Today's Work-from-Home World

Steps to raise your organization's immunity against heightened cybersecurity risks

To battle the COVID-19 crisis, work-from-home is now the new norm for several organizations. In a recent survey (1), 85% of organizations reported the pandemic has triggered at least 50% of their workforces to shift to telework. This transition to the work-from-home operating model has heightened cybersecurity risks and security incidents for enterprises. In the last few weeks, Cisco Systems reported a 10-fold jump in help-desk requests from remote workforces for security issues alone (2).

The COVID-19 crisis brings multiple cybersecurity challenges

When most employees work from outside the corporate networks during a pandemic, hackers exploit the associated vulnerabilities. Using fear and doubt in the public mind as a vantage, they trick employees to making poor security decisions by accessing fraudulent websites and phishing emails.

Recently, there has been a significant uptick in successful phishing attempts. Since the end of February, COVID-19 related spear-phishing emails have surged by 667% (3). IBM's threat Intel platform (4) reported a new malware, named Emotet, was used to infect devices in certain countries. In this scam, phishing emails posing as if welfare providers were used to distributing Emotet.

There are also reports of state-sponsored attacks on healthcare facilities, relief agencies, financial services, etc. In Europe, a recent cyberattack in a healthcare facility forced an emergency evacuation of patients in critical condition along with a complete shutdown of the IT network (5).

Business leaders need to recognize these new security challenges and determine steps to protect their organizations in the new operating environment.

Cybersecurity needs to be front and center now more than ever

Based on the current risk factors and threat intelligence data, our security experts at Nivid Technologies recommend three key steps to enhance enterprise security in today's work-from-home world.

Security Awareness and Guidelines

The pandemic has forced many employees to work remotely who otherwise would be on-prem. These employees are finding their way out of using corporate tools and applications securely in their new work environments. Many of them are non-technical staff with limited IT expertise. This raises the need to educate employees on how to securely access and use electronic assets and applications from home. They need to be made aware of the new exploits and be vigilant about emails from unknown sources, or while releasing sensitive personal information, etc.

Cybersecurity guidelines can help to address the unique risks for employees working from home. For example, policies that reinforce personal data confidentiality guidelines as enshrined in regulations like the GDPR, limit the use of third-party collaboration tools to company-approved ones, ensure security updates are pushed in laptops even when those are not on-prem, etc.

Remote surveillance to detect cyber threats

While most employees use company-issued laptops when working-from-home, the use of other personal devices are also prevalent. This expands the attack surface. The importance of remote surveillance in such scenarios is more of an imperative. Remote monitoring and management of devices and connections can detect activities that could be potential cyber threats.

Augment cybersecurity capabilities with advanced tools and services

When the work patterns involve multiple variables, your existing security tools may not be adequate. It is prudent to evaluate and augment existing security capabilities with third-party solutions to mitigate new risks. For example, security analysts may benefit AI-enabled tools to tackle the surge in security events, your connectivity infrastructure may need an upgrade to securely manage and scale remote connections.

The surge in remote application volumes is stress testing your cybersecurity capabilities. Our next blog discusses a solution custom-designed to improve your organization's security posture with certainty.

End Notes

1. CNBC, “Phishing scams, spam spike as hackers use coronavirus to prey on remote workers, stressed IT systems”, March 2020
2. Reuters, “Mass move to work from home in coronavirus crisis creates opening for hackers: cyber experts”, March 2020
3. TechRepublic, “667% spike in email phishing attacks due to coronavirus fears”, March 2020
4. Capgemini Research Institute, “Reinventing Cybersecurity with Artificial Intelligence”, July 2019 report
5. ZDNet, “Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak”, March 2020