ARTICLE

How CISOs can prepare their organizations for the new normal

By Rishikesh Kamat
Vice President - Products & Services
NTT Global Data Centers and
Cloud Infrastructure, India
(erstwhile NTT-Netmagic)

Even as the world prepares itself for a new normal impacted by Covid 19, the impact on enterprise security has been huge. Consider these facts. A recent survey conducted by software firm, Hiver, revealed that 60% of respondent companies in India were targeted by email-related security threats every week. Security firm, McAfee, has stated in a report that over the first 13 weeks of the Covid 19 crisis, the number of bogus websites centered around Covid 19 increased from 1600 to over 39,000.

Researchers from Palo Alto's Unit 42 team found that of the 1.2 million newly registered domain containing information related to Covid-19 between March and April 2020, close to 86,600 domains were malicious in nature.

As work priorities have changed, there is a scramble among CISOs to ensure robust security and make the necessary changes in security priorities and strategies. We recommend some best practices for this new world:

Securing remote employees

The International Information Systems Security Certification Consortium also known as (ICS)2, estimates that 23% of organizations have seen an increase in cybersecurity incidents since they have asked their employees to transition to remote work. Secure remote access hence becomes an important priority. Traditionally,VPNs have been the choice, however given the scale of WFH in the new normal, combined with the required granularity to control access, CISOs should evaluate a cloud based implementation of a zero trust framework. Similarly, virtual desktops can be provided for accessing company data and applications. This ensures that all applications or data is stored on company servers and cannot be downloaded to a home computer. A further level of security can be added by using two-factor or multi-factor authentication. Given the uncertainty about employment, it is also important for organizations to ensure that all access is monitored proactively and specifically privileged IDs are controlled through a PIM or PAM solution.

Preventing third party application installation

A recent survey from security firm, CyberArk has found that work-from-home habits– including password re-use and letting family members use corporate devices – are putting critical business systems and sensitive data at risk. The survey found that 77% of remote employees were using unmanaged, insecure "BYOD" devices to access corporate systems. Firms should ensure that their employees use pre-approved laptops with the required security solutions and applications installed on them. This prevents unauthorized installation of applications, thereby reducing risks. Companies must also advise employees on the software, hardware and platforms they can use to connect and share with colleagues.

Ensuring awareness and enforcement of security policies

Many data breaches happen due to old or weak passwords. As part of their security policy, organizations must enforce rules that ensure that employees keep updating their passwords on a regular basis. Attacks can also happen via cleverly designed phishing mails. Hence, employees must be advised and cautioned against clicking on suspicious emails. There is increasing evidence that such emails once clicked provide hackers a gateway to invade the networks of organizations. Employees must also be encouraged to avoid any communication on unsecured communication channels or social media. Employees must also be educated to configure their home Wi-Fi settings for ensuring robust security (for example, WPA2).

The importance of patching and updating

As history has shown us, even a single unpatched device can give a hacker an opportunity to gain access to your corporate network. The security policy must be designed to ensure that employees constantly keep on patching their software updates. As software updates can cause a huge strain on VPN networks in large organizations, they must be planned in such a way that it does not cause any further stress on existing bandwidth and networks. Organizations can address the problem of patch management by using remote cloud-based automated patch management solutions or MDM solutions to push updates to remote devices.

Keep backing up data

A recent report by security firm, Kaspersky states that DDoS attacks in Q1 2020 have doubled in comparison to the final quarter of 2019. Ransomware attacks have also gone up exponentially. Hence, data received and stored from multiple employees across the globe must be constantly backed up either on the cloud or on secondary storage solutions. This is especially crucial for data recovery if your organization gets hit by a ransomware attack.