CMSGu2020-02

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on cybersecurity in a work from home era

CERT-MU

National Computer Board

Mauritius

Version 1.0

April 2020

Issue No. 2

Table of Contents

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

The purpose of this guideline is to present to employers and employees various security measures that they can employ to secure their organisations in order to ensure a reliable and smooth delivery of their daily work and services.

1.2 Audience

The targeted audience for this document includes all employers and employees working from home during and after the coronavirus lockdown.

1.3 Document Structure

This document is organized into the following sections:

Section 1 gives an outline of the document's content, the targeted audience and the document's structure.

Section 2 presents a background on the current condition that the coronavirus has compelled employees and employers to adopt.

Section 3 outlines free cyber security products and services that are made available during the Covid-19 crisis

Section 4 depicts what measures organisations can take to ensure an enhanced cybersecurity posture.

Section 5 concludes the document

2.0 Background

As the world reacts to the Coronavirus (COVID-19) pandemic, businesses and governments are becoming progressively more reliant on technology to support citizens and workers forced to self-isolate or quarantine so as to mitigate the spread of the virus. Globally, 50% of employees are working from home for at least 2.5 days per week.

The virus has caused an unexpected level of social and economic disruption in modern times. Remote working and collaboration tools have become essential tools, with new demands placed on networks and datacentre infrastructure. The crisis is expected to be with us for a while according to worldwide statistics. Thus, organisations and their employees will be forced to make tough decisions rapidly, and enabling a remote workforce is one of those decisions. Moreover, some countries such as Mauritius are also working on making legal provisions as regards working from home.

Apart from the pressure this transition exercises on IT teams, network architectures and even equipment suppliers, there are real cybersecurity challenges organisations need to consider. As corporate networks extend beyond the firewall, security remains an ever-present concern, especially as cybercriminals look for opportunities to exploit fears over the pandemic. For every organisation involved in dealing with the crisis, digital systems have become an absolute lifeline. For health services for instance, the way they use technology can more than ever be the difference between life and death.

It is therefore critical to ensure that employees working remotely have the right technology to operate and are covered by adequate cyber security software. This includes all endpoint devices being used for corporate work such as laptops, mobiles and tablets, and ensuring software updates. It is also tremendously important to ensure that employees do not click on e-mails from unknown sources, which could be a phishing attack that is intended to implant malware and causing havoc to internal networks.

3.0 Free cyber security products and services during the COVID-19 crisis

To help maintain security in the face of this global office migration, many cyber security suppliers and service providers are introducing special offers for new and existing customers, extending introductory offers, and in many cases offering their products free of charge. Below are some of the latest offers that are currently available:

3.1 Kaspersky

Following on from previously announced offers for healthcare organisations, Kaspersky is offering six-month free trials of its extended Kaspersky Security for Microsoft Office 365.

The new version widens protection for remote worker collaboration by covering SharePoint Online and enabling secure file sharing within Microsoft Teams, which comes in addition to previously available protection for Exchange Online and OneDrive, shielding inboxes from phishing emails, blocking malware from spreading across a distributed company, and detecting and quarantining any malicious files that may be inadvertently shared.

According to the head of business-to-business (B2B) product marketing at Kaspersky, Sergey Martsynkyan, companies that are moving to cloud services and using communication tools, such as Microsoft Teams, must keep their data protected and meet the requirements of secure collaboration and messaging for their employees. To help companies meet these needs, they have expanded protection for Microsoft Office 365 to cover all associated applications. This gives customers the assurance that the entire cloud service is secured by default and that potential threats do not affect employees’ working practices.

3.2 Qualys

Qualys, a supplier of cloud-based security and compliance services, is offering 60 days of free access to its cloud-based remote endpoint protection solution for existing customers, with new customers prioritised based on sign-up date.

This will let security teams audit and build up-to-date inventories of their remote endpoint hardware and apps, get a real-time view of critical vulnerabilities and risky applications, remotely patch systems without using the limited bandwidth available on VPN gateways, and better realise visibility in device hygiene by tracking common misconfigurations that may leave them exposed.

It will initially support patching for Microsoft Windows 7 environments and above. Patching for Macs, and malware detection and protection that will be available at a later stage.

According to the Chairman and CEO of Qualys, Philippe Courtot, they are able to offer a real solution that will allow companies to ensure the security of both corporate and personal computers during these critical times Thanks to their cloud-based implementation, this offer will enable companies to assess in real-time their security and compliance posture and remotely patch employees' devices with the click of a button.

3.3 AppGate

AppGate, a supplier of software-defined perimeter (SDP) security, claims its product has multiple benefits over a traditional virtual private network (VPN), alleviating network choke points for remote workers accessing their business resources, and solving the problem of the inherent lack of security that stems from over privileged access.

The firm is offering a free 90-day pilot of its SDP product for enterprises affected by the coronavirus. It said the product can be set up quickly, scales cost-effectively to thousands of remote workers, integrates seamlessly with existing network hardware, and provides a simple experience for office workers who are working from home for the first time.

3.4 Click Armor

The security awareness platform Click Armor has launched a free coronavirus-edition of its "Can I Be Phished?" assessment tool for remote workers to test their mettle when it comes to identifying phishing attacks, coronavirus-related disinformation, and other security threats.

The online tool uses gamification to test and improve basic security skills, challenging players to pick out suspicious emails such as fake HR policy updates, fake health advisories and alerts, and fake news.

According to the CEO, Scott Wright, people are often surprised how easily they are fooled by the game’s realistic scenarios. They learn to be more careful in looking for real clues and risky elements. In under five minutes, individuals can learn practical tips they can use to protect themselves and their employers.

3.5 DomainTools

The threat intelligence specialist DomainTools has compiled a constantly updated coronavirus threat list to help enterprises make better decisions about the risks to their businesses posed by the pandemic.

It uses a keyword search-based list to include domains that the firm has judged to be high-risk, which are displayed in context alongside information such as their date of creation, and a proprietary risk score.

Jackie Abrams, DomainTools vice-president of product, said that the scoring mechanism, which draws on data points from more than 330 million active internet domains, predicts how likely a domain is to be malicious. It is based on two algorithms that analyse a target’s proximity to other bad domains and how closely its intrinsic properties resemble other bad domains.

DomainTools’ coronavirus list can be accessed via its website, and has grown from only 3,000 domains on 1 March 2020 to more than 57,000 by 22 March, showing how quickly cyber criminals have weaponised the pandemic.

3.6 Spirion

Data security and privacy specialist Spirion is also offering security teams a 60-day free licence for essential data discovery functionality in its Sensitive Data Manager software.

The offer includes a limited version of its console server software and agent software for examining Windows 7 and 10 endpoints, alongside four hours of professional services to install, configure and fine-tune new installations.

Meanwhile, remote employees can take advantage of a free version of its Data Discovery Agent to uncover personal information held on their home computers, such as National ID numbers, credit card and bank account details, driver's licence numbers, and passwords, enabling remote workers to take steps to better secure their personal data.

According to the firm's president and CEO, Spirion was established to protect personal data, and at no time in their company's history has data become more vulnerable and more targeted than it is right now. The sensitive data threat surface for almost every organisation, public or private, has grown exponentially in just the past 10 days as dedicated workers do their jobs from home. The team is committed to working alongside any organisation that is concerned with protecting sensitive data that belongs to its customers, employees, partners, and communities.

3.7 Varonis

Varonis has set up a COVID-19 Cyber Task Force to ease its customers and free up security teams to focus on availability for their remote workforces.

Based on resource availability, some of the zero-cost options will include assistance from Varonis' incident response team should the worst happen, free consultations with experts via Zoom, health checks on existing customer installations, incident alert tuning, daily and weekly security reports and reviews, and additional monitoring with free evaluation licences for customer VPNs, Office 365 installations, and DNS and proxy servers. Potential new customers can also take advantage of free evaluation licences.

4.0 How organisations can ensure a secure remote workforce

Organisations need to take serious actions to keep their systems, data and networks secure. Below is a list of steps that organisations can follow to lock down their systems for increased cybersecurity:

4.1 Implement Secure Configurations

New devices and software usually have default configurations such as predefined passwords. Since these are a part of the set-up for user convenience, it is not safe to leave this setting ‘as is’. A system that is not configured properly could allow attackers to gain access to critical and confidential information, or simply block your access to the device. Thus, it is important to secure configurations by:

- Creating and maintaining an asset register, that includes both software and hardware
- Changing the default password and avoid using weak passwords
- Removing all unnecessary user accounts and user privileges
- Removing all unnecessary software
- Regular vulnerability scans
- Using two-factor authentication before enabling users to access sensitive data

4.2 Use strong passwords

On top of having secure configurations for new devices and software, it is important that you and your employees leverage strong, complicated passwords that are not easy to guess, e.g. a combination of alphanumeric characters, upper and lower cases and special characters (@LphaB3t). Today there are hacking applications that can be plugged into a computer, and in about four minutes will run through the most common 10,000 passwords used, trying each of them. Many users having access to critical data have the password of “password,” or “password1”.

4.3 Deploy an up-to-date antivirus solution on all machines

Having an up-to-date antivirus software deployed on all of your desktops and servers is vital to organisational cyber security. An unprotected computer is an easy target for motivated attackers. Hence, do not make it easy on them, instead invest in a good antivirus software and ensure it is regularly updated by your IT staff. Most of these software has scan options that will scan all files to ensure no malware or other harmful files exist your computer.

Moreover, it is recommended that your employees conduct regular virus scans of their machines. The antivirus solution can also be set to scan incoming attachments and online downloads prior to these being allowed onto the local network to ensure they do not contain malicious content.

4.4 Download and apply latest updates and patches

Ensure all software being used by employees working remotely have the latest updates and are patched accordingly. Automatic updates can be turned on in the general computer settings areas of all laptops/PC computers and this will ensure that the computer itself checks for the most up to date operating software for installed applications on a daily basis.

4.5 Back up your data

Ensure critical business data is backed up, stored and easily recoverable (run tests to ensure the backup works as plan prior to closure). Using external or cloud based service providers is the safest practice as it ensures that your back up data is kept in a location separate to your business operation.

4.6 Manage user accounts and their access

Certain employees are only granted access in an organisation to a range of systems for performing their jobs. If their roles keep changing, they require permissions according to their respective roles. However, the permissions that are no longer necessary or relevant, often do not get revoked.

This also gets complicated with cloud computing, since most of the permissions are granular. However, for users who already have permissions but no longer require them, there is a principle of least privilege concept, that helps the chances of attack to surface things that are potential threats or may compromise any credentials.

4.7 Have a security policy that includes remote working

Organisations need to have a current security policy that includes remote working. Strong security policies may already exist, but it is important to review them and ensure they are adequate as your organisation transitions to having more people working from home than in an office. Security policies need to include remote working access management, the use of personal devices, and updated data privacy considerations for employee access to documents and other information. It is also important to factor in an increase in the use of shadow IT and cloud technology.

4.8 Focus more on data privacy and intrusions when using Wi-Fi networks

Sensitive data may be accessed through unsafe Wi-Fi networks. Employees working from home may access sensitive business data through home Wi-Fi networks that will not have the same security controls such as firewalls used in traditional offices. More connectivity will be happening from remote locations, which will require greater focus on data privacy, and hunting for intrusions from a greater number of entry points.

4.9 Plan for bring your own device (BYOD) devices

Organisations have to plan for BYOD devices connecting to their internal network. Employees working from home may use personal devices to carry out business functions, especially if they cannot get access to a business-supplied device as supply chains may slow down. Personal devices will need to have the same level of security as a company-owned device, and you will also need to consider the privacy implications of employee-owned devices connecting to a business network.

4.10 Secure your cloud

No matter what cloud provider or service you use, make sure you do a complete review and analysis of their security practices. If they cannot easily and quickly tell you how your data is secured, odds are it is not secure. Also, for any accounts used to access your organisations data, make sure you have strong passwords and only access it via a computer you own or trust. If you access your cloud on an infected machine, there is a real potential for a hacker to learn your password and use it later on without your knowledge.

4.11 Protect your banking information

Make sure that all financial data, accounts, and records are kept secure and segregated from the rest of your business' general shared drives. If financial transactions are conducted electronically, ensure they are done over an encrypted connection and that your employees never email account numbers, credit card information, or sensitive financial documents.

4.12 Have crisis management and incident response plans in place

Crisis management and incident response plans need to be executable by a remote workforce. A cyber incident that occurs when an organisation is operating outside of normal conditions has a greater potential to get out of control. Effective remote collaboration tools including out-of-band conference bridges, messaging platforms and productivity applications can allow a distributed team to create a "virtual war room" from where response efforts can be managed. If your organisation's plans rely on physical access or flying in technicians for specific tasks (e.g., reimaging or replacing compromised machines), it may be wise to explore alternate methods or local resources.

4.13 Review security protection strategy

It is important for testers and development teams to analyse the security protection strategy to make the most of their security testing efforts.

Penetration testing services can have excellent results and can help organisations prevent future security attacks. With the help of experts, small to medium companies can easily and conveniently manage their cyber-security concerns. With more demanding testing approaches, these experts bring in their experience and expertise at a common point to achieve business goals and protect the business from any data breach or cyber threats.

4.14 Ongoing cyber awareness and training for employees

In the current environment it is increasingly important to ensure your staff are security aware and take the right measures to protect themselves, the company and your customers. Many international organisations as well as CERT-MU have already warned about ongoing coronavirus-themed phishing attacks and scam campaigns. Continuous end-user education and communication are vital and remote workers should be given the assurance that they can contact

IT in a timely manner for advice. Organisations should also consider employing more stringent email security measures.

It is now more than ever a good time to remind employees:

- about the heightened risk that will unfortunately arise from coronavirus-related scams
- to keep their laptops within their physical control, and their screens hidden from others
- never to provide login credentials in response to an email request
- not to use less secure devices, such as the family computer, to obtain or store work information
- not to use personal email accounts to transmit work information
- not to transmit or store work information on their personal cloud storage accounts unless their companies specifically allow that practice
- not to leave written corporate materials in shared or unsecured locations
- even when at home, log off when not using network
- to use strong passwords and ensure they are required to regularly change them
- to refrain from using public Wi-Fi for work related activity
- to use two factor authentication for financial payments as invoice fraud schemes are on the rise.

Furthermore, ensure your staff know how to spot common phishing attacks as these are already on the rise in the remote environment. Actions such as those outlined below can assist:

- hovering the mouse over the email senders address to verify that it has been sent from a genuine location
- only opening attachments from trusted senders
- ask for a second opinion from a manager in times of doubt before responding to emails.

5.0 Conclusion

With restrictions on individual movement being in force in countries affected by the coronavirus pandemic, staff are routinely working from home and need the right tools to support them. The COVID-19 crisis is not likely to disappear in the next few days or weeks. Hence, organisations will have to take decisions regarding remote working for a longer period. There are many risks involved in accomplishing this too quickly, however, the security of your networks, devices and data should not be among those risks. Hence, appropriated security measures will have to be implemented and adapted to the current situation.

References

- https://www.computerweekly.com
- https://www.expresscomputer.in
- https://www.crombielockwood.co.nz
- https://www.itweb.co.za
- https://www.industryweek.com
- https://www.myob.com