BDO NEWS

August 2020

www.bdo.com.hk

TECHNOLOGY UPDATES
August 2020 Issue

CONTENTS

- Threats of ransomware surges during pandemic COVID-19
- Cybersecurity risks of work from home under the third wave of coronavirus infections in HK
- To step up vigilance against rising COVID-19-themed phishing attacks
- 'Embarrassed' Twitter reveals 130 accounts were hacked under COVID-19
- How can BDO help?

Innovation and technology are drivers for organisation growth and the key to enhance competitiveness of different industries. Just as technology rapidly evolves, so does the sector. In every monthly issue of our 'Technology Updates', it will include the latest updates from cybersecurity, emerging technology & data privacy.

Threats of ransomware surges during pandemic COVID-19

The COVID-19 crisis has escalated the risk of malicious cyber attacks as organisations large and small increase their reliance on remote working and online services. Honda, a Japanese public multinational conglomerate corporation primarily known as a manufacturer of automobiles, motorcycles, and power equipment, was hit by a cyber attack and some production disrupted in June 2020.

Although production resumed at most of the plants later, its main plant in Ohio, as well as those in Turkey, India and Brazil remain suspended as the ransomware disputed the company's production systems.

The ransomware suspected of hitting Honda mentioned an in-house domain according to Takashi Yoshikawa of Mitsui Bussan Secure Directions, a unit of trading house Mitsui & Co.

What is ransomware?

Ransomware is malicious software that prevents or restricts a user from accessing a computer system by freezing the computer's screen or encrypting the computer files unless a ransom is paid. Crypto-ransomware, one of the most common ransomware in recent years, encrypts computer files on infected systems and even the files stored on external storage devices or the same network. Users are then demanded to pay a

ransom in hope of obtaining a decryption key. Crypto-ransomware can infect computers via emails, websites or malicious online advertisements.

Screenshots of a computer with 'WannaCry' ransomware infection:

Why ransomware is dangerous especially during the pandemic crisis?

Undoubtedly, COVID-19 has led to a sharp increase in cyberattacks worldwide. Cyber criminals have been quick to exploit the current weak situation and are targeting service providers in different industries as well as businesses in the manufacturing and even public authorities. According to a study conducted by VMware Carbon Black, several malicious attacks campaigns designed to exploit public fears around COVID-19 and reported ransomware attacks jumped by 148% in a single month—from February to March 2020.

What makes ransomware especially dangerous is how an infection can spread across a network of computers and mobile devices. After accessing a network, ransomware fraudsters can also steal sensitive data to use as leverage to force ransom payment or raise the price.

Whether you decide to pay the ransom or not, your first action should be disconnecting your computer from the network and external drives: you don't want ransomware to spread to other devices or cloud services. Users should always be vigilant when using computers. In addition to the installation of anti-virus software and firewalls, users should also adopt good IT security practices to prevent from ransomware.

Read more from the sources:

https://www.reuters.com/article/us-honda-cyber/honda-hit-by-cyber-attack-some-production-disrupted-idUSKBN23G1CI

https://www.carbonblack.com/blog/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted/

Cybersecurity risks of work from home under the third wave of coronavirus infections in HK

In July 2020, Hong Kong's third wave of coronavirus infections shows little sign of easing, the government has stepped up the fight against coronavirus and requested civil servants working from home (WFH). Whilst WFH is a work arrangement in which employees do not commute or travel (eg by bus, bicycle or car, etc) to a central place of work, such as an office building, warehouse, or store, many companies have mandated employees work from home to let their employees keep social distance in the time of the pandemic. Working from home went from being a secondary approach to a mainstream capability for businesses of all sizes.

Although WFH is not a new approach, the potential cyber-risks has been ignored sometimes. A study of WFH conducted by IBM in June 2020, there are more than two thousand U.S. adults who are newly working from home due to COVID-19 joined the study. Researchers found that 53% of employees are using their personal laptops and computers for business operations while WFH. However, those computers and laptops have not yet been enforced by security controls deployed by companies and believe users browse social media and other high-risk web sites by the same computer in their leisure times.

Why personal computers of WFH become weakness link of cybersecurity?

Ranging from participating in after-hours meetings with clients/team members to accessing a distributed workforce to supporting company business operations, users working from home may access companies' critical systems as well as handle sensitive information of customers under their personal computer.

Personal computers are always lacking in IT security governance. For example, weak or even no password in personal computer, default settings of services, insufficient security hardening of a personal computer and insufficient protection and lack of encryption for sensitive customer data under personal computer and no up-to-date security patches deploy to home computers.

As a result, the unprepared personal computer will create an opportunity for cybercriminals and thereafter introduce security loopholes. According to a study, researchers from Shodan reported a 41% increase in the number of remote desktop protocol (RDP) endpoints exposed online, since the beginning of the COVID-19 pandemic.

We urge companies to raise their awareness of the risks relating to remote access services, and immediately

implement necessary security measures and conduct security assessments to ensure that these services are used safely.

Read more from the sources:
http://filecache.mediaroom.com/mr5mr_ibmnews/186506/IBM_Security_Work_From_Home_Study.pdf

https://securityaffairs.co/wordpress/102495/hacking/covid-19rdp-bruteforce-attacks.html

To step up vigilance against rising COVID-19-themed phishing attacks

With the global 2019 Coronavirus Disease (COVID-19) pandemic intensifying, different types of cyber-attacks in the name of the disease have increased dramatically. Cybercriminals are taking advantage of the fear and uncertainty surrounding the coronavirus pandemic as well as the increased time spent online during social-distancing to trick people into releasing sensitive information. There has been a huge rise in COVID-19 themed phishing scams where criminals send emails that appear to come from hospitals or government agencies to trick people into downloading an attachment or giving them personally-identifying information. The World Health Organisation recently warned of criminals sending emails posing as the WHO for such purposes as well.

Which content do COVID-19 themed phishing emails look like?

According to BBC news, varies type of phishing attacks targeted different individuals and/or industries based on COVID-19-themed are found:

- Click here for a cure – email purported to be from a mysterious doctor claiming to have details about a vaccine being covered up by the Chinese and UK governments
- A little measure that saves – email pretended to represent the World Health Organization claim that attached document details how recipients can prevent the disease's spread
- The virus is now airborne – an email with a link and encourage login fake Microsoft web portal
- Donate here to help the fight – an email asks for donations to develop a vaccine and redirect fake web site
- COVID-19 tax refund – an email with a click for 'access your funds now', it would take them to a fake government webpage, encouraging them to input all their financial and tax information

Phishing remains cybercriminals' method-of-choice to infect users' computers. Corporate employees are particularly vulnerable since they are heavily targeted as an easy entry into sensitive data. Cybercriminals use social engineering to trick their victims into launching malicious files on their computers, opening a link to an infected website for private data. We urge companies should strengthen IT security awareness of their employees especially in the time of the pandemic.

Read more from the sources:
https://www.bbc.com/news/technology-51838468

https://www.who.int/about/communications/cyber-security

'Embarrassed' Twitter reveals 130 accounts were hacked under COVID-19

Criminals would attack our facilities during such a time when we are all working tirelessly and collectively to fight the COVID-19 pandemic. Twitter, a social media giant in the world providing microblogging and social networking service on which users post and interact with messages known as 'tweets' was hacked on 17 July 2020.

The company says the hack that compromised the accounts of some of its most high-profile users targeted 130 people. The hackers were able to reset the passwords of 45 of those accounts.

"We're embarrassed, we're disappointed, and more than anything, we're sorry. We know that we must work to regain your trust, and we will support all efforts to bring the perpetrators to justice," Twitter said in the blog post.

The hackers manipulated a small number of employees and used their credentials to access internal tools. The former employees further explained to Reuters that Twitter had gotten better about logging the activity of its employees after previous mishaps, including searches of records by an employee accused of spying for the Saudi Arabian government. After a rogue employee deleted President Donald Trump's account two years ago, the company limited access to national leaders' accounts to a much smaller number of people. Obviously, security controls from unauthorised access should be improved.

What is unauthorised access?

Unauthorised access is when someone gains access to a website, program, server, service, or other system using someone else's account or other methods. For example, if someone kept guessing a password or username for an account that was not theirs until they gained access, it is considered unauthorised access. By gaining unauthorised access to organisational systems or user accounts, attackers can steal or destroy private data and/or compromise systems for illegitimate and criminal activity.

How can we prevent unauthorised access?

Some system administrators set up alerts to let them know when there is an unauthorised access attempt, so that they may investigate the reason. These alerts can help stop hackers from gaining access to a secure or confidential system. Many secure systems may also lock an account that has had too many failed login attempts. Meanwhile, you can also enforce the authentication process by implementing two-factor authentication. Eg even though a strong password was compromised, access will not be granted until the user input an one-time password, a SMS, sent to an authorised mobile device.

Read more from the sources:

https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.html

https://www.reuters.com/article/us-twitter-cyber-access-exclusive/exclusive-more-than-1000-people-at-twitter-had-ability-to-aid-hack-of-accounts-idUSKCN24O34E

How can BDO help?

The BDO Risk Advisory Services (RAS) team is formed by a group of dedicated IT professionals. We are well equipped, qualified, experienced and well-prepared to assist your board or management to perform IT security assessments, data protection reviews, vulnerability assessments as well as penetration tests or any other IT matters relating to regulatory requirements. Please do not hesitate to contact us and talk to our consultants. We are pleased to provide further insight or assistance if needed.

BDO'S SUPPORT AND ASSISTANCE

25th Floor, Wing On Centre
111 Connaught Road Central
Hong Kong
Tel: +852 2218 8288
Fax: +852 2815 2239
info@bdo.com.hk

RICKY CHENG
Director and Head of Risk Advisory
Tel: +852 2218 8266
rickycheng@bdo.com.hk