BDO NEWS

December 2020

www.bdo.com.hk

TECHNOLOGY UPDATES
December 2020 Issue

CONTENTS

- Critical vulnerable issues found in products of a famous home router-manufacturing company in Asian countries
- Spearphishing attack spoofs Microsoft.com to target 200m Office 365 users
- Google patches critical Wi-Fi bugs in Android phones
- Warning after 75,000 'deleted' files found on used USB drives
- 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.

Critical vulnerable issues found in products of a famous home router-manufacturing company in Asian countries

Recently security researchers found that number of remotely exploitable root command injection flaw found in VPN routers from a famous wireless routers manufacturer D-Link. The vulnerabilities lead millions of home and business networks open to cyberattacks even if they are secured with a strong password.

Discovered by researchers at Digital Defense, the three security issues were disclosed to D-Link on 11 August 2020, which, if exploited, could allow remote attackers to execute commands on vulnerable networking devices via tailored made requests and even launch denial-of-service attacks.

The Taiwanese networking equipment manufacturer confirmed the above issues in an advisory on 1 December and provide security patch to address the above issues.

What is home network security? Why security of home network is important during the time of COVID-19?

Home network security is defined as the protection of a home network including different devices, ie computers, smartphones, WiFi-enabled cameras, and most importantly your home router. As COVID-19 turns working from home into the new normal, adapting and keeping a focus on cyber security in all settings of home network is critical.

However, many people think that because it is 'just' their home network and too small to matter, a feeling that security rules for home networks 'don't apply to me'. Whilst the notion is untrue. Cyber-attacks can take place in homes and businesses. Every network can be vulnerable and being hacked.

We have seen business experiencing security threats coming from home network during work-from-home policy. The longer your organisation waits without doing further actions, the bigger the risk becomes of a potentially costly attack. Don't wait and do security assessment and better protect your network.

Read more from the source:
https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10195

Spearphishing attack spoofs Microsoft.com to target 200m Office 365 users

A cyberattack is spoofing Microsoft.com to target more than 200 million Microsoft Office 365 users including financial services, healthcare, manufacturing and utility providers. According to the security report published on 7 December 2020, researchers at Ironscales discovered the campaign targeting several thousand mailboxes at nearly 100 of the email security firm's customers. Other industries targeted includes telecommunication and insurance companies.

The attack is particularly deceiving because it deploys an exact domain spoofing technique, "which occurs when an email is sent from a fraudulent domain that is an exact match to the spoofed brand's domain," Ovadia wrote. This means even though users who check sender addresses to ensure an email is legitimate could be fooled, the searcher said.

The attack is comprised of a realistic-looking email that attempts to persuade users to take advantage of a relatively new Office 365 capability that allows them to reclaim emails that have been accidentally marked as spam or phishing messages, according to the report. The messages come from sender 'Microsoft Outlook'.

What is cybersecurity awareness training?

Security awareness training gives employees knowledge to keep your organisation sensitive data safe. The best security awareness training applies phishing simulations and other practical exercises to teach users how to safeguard against cyber threats like phishing, spear phishing, ransomware, malware, social engineering, and more.

Why the awareness training is important for email security?

Email solution alone does not provide your organisation with perfect protection from cyber-attacks. Security awareness training enable employees to avoid falling victim to cyber threats. It also cultivates a security mind-set and culture that prioritises the protection of your organisation's data.

Since cybersecurity awareness training is important to help your employees recognise and handle phishing, ransomware, CEO fraud and other types of attack, the longer your organisation did not perform regular training, the bigger the cyber risk becomes of a potentially costly attack.

Read more from the sources:
https://ironscales.com/blog/Microsoft-O365-Fails-to-Block-Spoofed-Emails/

https://threatpost.com/spearphishing-attack-spoofs-microsoft-office-365/162001/

Google patches critical Wi-Fi bugs in Android phones

According to the latest statistics provided by statcounter, the most widely used operating system in November 2020 of the world is Android. Whilst there are number of reasons why Google Android is so popular in smartphone market, the security threat of mobile phone is always a topic in different media.

On 7 December 2020, Google has patched a critical security vulnerability in system component related to Wi-Fi and audio hardware under Android system. It is possible for a remote attacker using a specially crafted file to execute arbitrary code within the context of a privileged process and trigger critical Wi-Fi bug in which the hardware provider Qualcomm rated this issue as 9.8 out of 10 in severity, using the standard CVSS score.

What is mobile device security? Why it is important to organisation?

Mobile device security is the protection of smartphones, tablets, and laptops from threats associated with wireless computing. It has become increasingly important in mobile computing. Of particular concern is the security of personal and business data now stored on smartphones especially many employees working from home in recent days.

More and more of businesses use smartphones to communicate, plan and organise their work. Within companies, these technologies are causing profound changes in the organisation of information systems and therefore they have become the source of new risks. Indeed, smartphones collect and compile an increasing amount of sensitive information to which access must be controlled to protect the privacy of the user and the intellectual property of the company.

Whilst organisation can adopt security countermeasures when using smartphones, from security in different layers of software to the dissemination of information to end users, there are good practices to be observed at all levels, from design to use,

through the development of operating systems, software layers, and downloadable apps. The longer your organisation waits without doing further actions, the bigger the risk becomes of a potentially costly attack. Don't wait and enhance mobile security controls and better protect your network.

Read more from the sources:

https://gs.statcounter.com/os-market-share/mobile/worldwide

https://source.android.com/security/bulletin/2020-12-01#asterisk

Warning after 75,000 'deleted' files found on used USB drives

USB drives are a great way of transferring and backing up files. However, there are many data security threats introduced by the improper USB drive management.

In July 2020, a research paper published by Abertay University and discovered that about 75,000 files after buying 100 of the drives on an internet auction site. Whilst some USB drives contained files named 'passwords' and images with embedded location data, All but two of the drives appeared empty, but the team said it had been 'worryingly easy' to retrieve data. The researchers also finalised that many of the files extracted were determined to be of 'high sensitivity'.

What are major challengers of using USB drives?

The large storage capacity of USB flash drives relative to their small size and low cost means that using them for data storage without adequate operational and logical controls may pose a serious threat to information confidentiality and integrity.

Moreover, USB drives is always used to transfer files between computers, which may be on different networks, in different offices, or owned by different people. This has made USB flash drives a leading form of information system infection. When a piece of malware gets onto a USB flash drive, it may infect the devices.

Why security control is important of USB drives?

There are many security controls to manage USB drives. While many enterprises have strict management policies toward USB drives and some companies ban them outright to minimise risk, others seem unaware of the risks these devices pose to system security.

We have seen security threats introduced by USB drives. The fewer health checks performed with IT devices, the bigger the risk becomes of a potentially costly attack. Don't wait, do IT security health check to protect your critical infrastructure to sustain business operations.

Read more from the sources:

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3631441

https://www.bbc.com/news/uk-scotland-tayside-central-54779322

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