BDO NEWS

February 2021

www.bdo.com.hk

TECHNOLOGY UPDATES
February 2021 Issue

CONTENTS

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.

Dairy Farm suffers ransomware attack

Asian retail chain operator Dairy Farm Group that operates numerous brands in Hong Kong and Asia market, including Wellcome, Giant, Cold Storage, Hero, 7-Eleven, Rose Pharmacy, GNC, Mannings, Ikea, Maxims, suffered a ransomware attack in January 2021 and hackers demanded $30 million in ransom.

Around 14 January 2021, Dairy Farm was attacked by the REvil ransomware operation. The ransomware group compromised Dairy Farm's network and encrypted devices. The allegedly attackers had access to information up until seven days after the attack.

What is Revil ransomware?

Revil is a private ransomware-as-a-service (RaaS) operation that recruits affiliates to distribute the ransomware for paid client. As part of this arrangement, the affiliates and ransomware developers split revenue generated from ransom payments. 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. What makes ransomware especially dangerous is 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 affected equipment from the network and external drives: you do not want ransomware to spread to other devices or cloud services. In long term, companies should get holistic cybersecurity maturity visibility across all of their IT infrastructure environments. As a result, companies can keep pace with the needs of the business while ensuring continuous security and compliance.

What is the recommended approach to address cybersecurity risks?

We recommend a threat-based cybersecurity approach to address cybersecurity risks and mitigate costly data breaches. Threat-based cybersecurity is forward-looking that it uses analysis of a company's unique threat profile to identify risky areas and protects against probable types of cyberattack. The threat-based approach includes proactive steps among which a comprehensive cybersecurity review is first and foremost.

A comprehensive cybersecurity review is important to company. The review result details a company's unique threat profile, upon which a threat-based cybersecurity approach can rely on to mitigate cybersecurity risks. The review can cover various domains, including email threat, network and endpoint threat, vulnerability assessment, penetration testing, red-team security assessment and security software tools assessment.

Read more from the source:
https://www.bleepingcomputer.com/news/security/pan-asian-retail-giant-dairy-farm-suffers-revil-ransomware-attack/

New attack could let remote hackers target devices on internal networks

Disconnecting devices from the internet is no longer a solid plan for protecting them from remote attackers. A new version of a known network-address translation (NAT) slipstreaming attack has been uncovered, which would allow remote attackers to reach multiple internal network devices, even if those devices do not access to the internet.

A new security research has demonstrated a technique that allows an attacker to bypass firewall protection and remotely access any IT devices like network printers, camera, on a victim machine.

Called NAT slipstreaming, the method involves sending the target a link to a malicious site (or a legitimate site loaded with malicious ads) that, when visited by victim will then open any TCP/UDP port and thereafter circumventing browser-based port restrictions.

Next, the victim's device has a Windows device vulnerable item EternalBlue, the attacker can access the victim device using NAT slipstreaming technique, from the internet, exploit the vulnerability, and take over the device.

"The only thing required for this attack to take place, is that the victim clicks on link, or visits a web page of which the attacker has implanted some JavaScript code," researchers noted.

What is malicious link?

Attackers embeds malicious links in the spear phishing e-mails for distribution to the target audience. On clicking the link, user's browser is directed to the malicious web server and download malicious codes in background. Whilst the antivirus software may not able to determine malicious link, IT security officers should consider compensation controls and additional security measures to address NAT slipstreaming attack.

We urge companies to raise awareness of the network communication risks, and promptly complete a comprehensive risk assessment and conduct a full vulnerability scan to ensure that its communication between different systems across the network are protected sufficiently.

Read more from the source:
https://thehackernews.com/2020/11/new-natfirewall-bypass-attack-lets.html

Accelerated cloud migration may leave business data insecure

The pandemic has accelerated digital transformation for 88% of global organisations. However, this increase in cloud adoption may leave business data insecure, Trend Micro reveals.

Accelerated cloud migration

"It's a very positive sign that a majority of organisations around the world are embracing digital transformation and adopting the cloud," said Mark Nunnikhoven, VP of cloud research for Trend Micro.

"But the survey findings also highlight the challenges remaining with understanding security in the cloud. Cloud adoption is not a one off process, but takes ongoing management and strategic configuration to make the best security decisions for your business."

Responsibility of data security & how we can secure cloud migration

The survey confirms a simple misconception that can lead to serious security consequences. While cloud infrastructure is secure, customers are responsible for securing their own data – which is the basis of the shared responsibility model for cloud.

Moreover, the research has found that misconfigurations are the number one risk to cloud environments, which can happen when companies don't know their part of the shared responsibility model.

Companies should consider cloud services as a more secure cloud infrastructure but it should not be taken as a service that

is available to production with 'out of the box' set up. For example, it is recommended to use proper manage key authentication files, and enabling cluster encryption for data warehouse encryption. However, as different cloud products require different secure settings, companies should conduct IT risk assessment before/after the cloud migration.

We have encountered business with cloud infrastructure with poorly configuration or misconfigurations that lend to data and business value loss. The longer your organisation waits without doing further actions, the bigger risk your company will suffer with these losses. Don't wait up and now is a good time to review and properly configure you company infrastructure set up.

Read more from the source:
https://www.helpnetsecurity.com/2020/12/16/accelerated-cloud-migration-business-data-insecure/

NeurIPS 2020 | Machine learning vs climate change

Organisers of NeurIPS 2020 (Conference on Neural Information Processing Systems) see machine learning as an invaluable tool in the fight against climate change.

Climate change is one of the greatest threats humans have ever faced, with increasingly severe consequences feared as sea levels rise, ecosystems falter, and natural disasters. Tackling climate change is a huge and complex challenge, where it's hoped that AI-powered efforts can play an equally huge and beneficial role.

Organisers of NeurIPS 2020 (Conference on Neural Information Processing Systems) see machine learning as an invaluable tool in the fight against climate change. A wide array of applications and techniques are already being explored, from smart electric grid design to satellite-tracking of greenhouse gas emissions and others.

What is machine learning (ML) and how it can help business and community?

Machine-learning algorithms use mathematical statistics to find specified patterns from massive amounts of data. And data in this context, encompasses a lot of things—numbers, words, images and so on. If it can be digitally stored, it can then be fed into a machine-learning algorithm and provide users with meaning insights.

Machine learning had been widely used for operation optimisation. Commercial buildings implement different algorithm such as time series forecast to forecast the future temperature in order to optimise the energy usage for buildings. Also, that is a win for both business and environment as the less energy consumption for building, the less damage to the planet.

It is crucial for the ML community to work with disciplinary experts to identify urgent problems and figure out where and how to use ML as tools to implement climate change strategies, says Jennifer Chayes, associate provost of the Division of Computing, Data Science, and Society, and dean of the School of Information at UC Berkeley.

AI and machine learning had been widely adopted in order to solve different issues from Financial to Environmental.

Read more from the source:
https://syncedreview.com/2020/12/14/neurips-2020-machine-learning-vs-climate-change/

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