May 14th, 2019

Try our May quiz - Security By The Numbers

This week's stories:

Cost of security breaches to Canadian firms studied averaged over $9 million a year: Report

https://www.itworldcanada.com/article/cost-of-security-breaches-to-canadian-firms-studied-averaged-over-9-million-a-year-report/417893

The price of security incidents in organizations in 11 countries jumped an average of 12 per cent last year, if a new study is representative.

According to the annual Accenture Cost of Cybercrime survey, the average cost of investigating and remediating breaches of security controls to the 355 organizations surveyed was US$13 million in 2018, compared to US$11.7 million in 2017.

Click link above to read more

Serious vulnerabilities found in WhatsApp, Cisco devices

https://www.itworldcanada.com/article/serious-vulnerabilities-found-in-whatsapp-cisco-devices/417985

Infosec pros are advised to patch vulnerabilities in two major products, one that could open end users to having their communications hacked, the other that could open the network to intrusion:

Facebook says it has issued fixes for several versions of WhatsApp — including Business versions for Android and iOS — after discovering a buffer overflow problem that could allow a remote attacker to install spyware.

Click link above to read more

Amazon's Echo for kids accused of saving information — even when asked to forget

https://globalnews.ca/news/5258513/amazon-echo-dot-kids-saving-information/?utm_source=%40globalnews&utm_medium=Twitter

Amazon has come under fire once again over privacy practices related to its Alexa voice assistant software.

On Thursday, privacy advocates in the U.S. said the kids' version of Amazon's Alexa won't forget what children tell it — even after parents try to delete the conversations.

Click link above to read more

Customers respond to Docker Hub security breach

https://searchmicroservices.techtarget.com/news/252462771/Customers-respond-to-Docker-Hub-security-breach?%20220multi-cloud

Under the lights of its annual conference, Docker took time away from its latest enterprise container platform updates to discuss the recent data breach, and despite reassurances some customers are on guard.

Click link above to read more.

Hackers Access Over 461,000 Accounts in Uniqlo Data Breach

https://www.bleepingcomputer.com/news/security/hackers-access-over-461-000-accounts-in-uniqlo-data-breach/

Fast Retailing, the company behind multiple Japanese retail brands, announced that the UNIQLO Japan and GU Japan online stores have been hacked and third parties accessed 461,091 customer accounts following a credential stuffing attack.

As detailed in the official statement issued Fast Retailing following the security breach, the credential stuffing attack which led to the data breach took place between April 23 and May 10, 2019, with the number of compromised accounts possibly being higher seeing that the investigation has not yet concluded.

Click link above to read more

Linksys Smart Wi-Fi Routers Leak Info of Connected Devices

https://www.bleepingcomputer.com/news/security/linksys-smart-wi-fi-routers-leak-info-of-connected-devices/

More than 25,000 Linksys Smart Wi-Fi routers are currently impacted by an information disclosure vulnerability which allows remote and unauthenticated access to a vast array of sensitive device information.

This issue is very similar to a Linksys SMART WiFi firmware security issue from 2014 tracked as CVE-2014-8244 which allowed "remote attackers to obtain sensitive information or modify data via a JNAP action in a JNAP/ HTTP request."

Click link above to read more

U.S. Govt Issues Microsoft Office 365 Security Best Practices

https://www.bleepingcomputer.com/news/security/us-govt-issues-microsoft-office-365-security-best-practices/

The Cybersecurity and Infrastructure Security Agency (CISA) issued a set of best practices designed to help organizations to mitigate risks and vulnerabilities associated with migrating their email services to Microsoft Office 365.

CISA's AR19-133A analysis report was published after it was discovered that a number of misconfigurations lowered the overall security of organizations which adopted Microsoft Office 365 as their default email provider.

Click link above to read more

Nigerian BEC Scammers Shifting to RATs As Tool of Choice

https://www.bleepingcomputer.com/news/security/nigerian-bec-scammers-shifting-to-rats-as-tool-of-choice/

Scammers running business email compromise (BEC) fraud have grown in number, attack more often, and turn to remote access trojans as the preferred malware type to accompany their raids.

Although the FBI's Internet Crime Complaint Center (IC3) developed a Recovery Asset Team has made a difference in reducing losses caused by BEC scams, now there are more fraudsters than ever.

Click link above to read more

Sensitive Information of Millions of Panama Citizens Leaked

https://www.bleepingcomputer.com/news/security/sensitive-information-of-millions-of-panama-citizens-leaked/

An unprotected Elasticsearch cluster exposed 3,427,396 records containing sensitive personal information on Panama citizens with "patient" labels, together with another 468,086 records labeled as "test patients".

As Security Discovery researcher Bob Diachenko discovered during his investigation, the data was leaked because the Elasticsearch cluster storing it was not properly configured, allowing anyone with an Internet connection to access it using a web browser.

Click link above to read more

Cybersecurity skills shortage still the root cause of rising security incidents

https://www.helpnetsecurity.com/2019/05/14/cybersecurity-skills-shortage-causes-security-incidents/

The cybersecurity skills shortage is worsening for the third year in a row and has impacted nearly three quarters (74 percent) of organizations, as revealed in the third annual global study of cybersecurity professionals by the Information Systems Security Association (ISSA) and independent industry analyst firm Enterprise Strategy Group (ESG).

Click link above to read more

The Security News Digest (SND) is a collection of articles published by others that have been compiled by the Information Security Branch (ISB) from various sources. The intention of the SND is simply to make its recipients aware of recent articles pertaining to information security in order to increase their knowledge of information security issues. The views and opinions displayed in these articles are strictly those of the articles' writers and editors and are not intended to reflect the views or opinions of the ISB. Readers are expected to conduct their own assessment on the validity and objectivity of each article and to apply their own judgment when using or referring to this information. The ISB is not responsible for the manner in which the information presented is used or interpreted by its recipients.

For previous issues of Security News Digest, visit the current month archive page at:

http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-news-digest

To learn more about information security issues and best practices, visit us at:

Information Security Awareness Team - Information Security Branch

Office of the Chief Information Officer,

Ministry of Citizens' Services

4000 Seymour Place, Victoria, BC V8X 4S8

https:www.gov.bc.ca/informationsecurity

OCIOSecurity@gov.bc.ca