BRITISH COLUMBIA OCIO | Office of the Chief Information Officer

Security News Digest

May 15th, 2018

May is Password Protection Month

Take our monthly quiz and test your knowledge

This week's stories:

---

1) Regulate IoT devices for security, says BlackBerry CSO

https://www.itworldcanada.com/article/regulate-iot-devices-for-security-says-blackberry-ciso/405119

Another senior tech industry official has joined the call for government regulation of Internet of Things devices.

The call came last week from BlackBerry CSO Alex Manea at the second annual Urban Security and Resilience Conference in Toronto.

"I think there needs to be better government regulations around IoT," Manea said during a keynote speech.

"So one of the things I would like to see from an IoT regulatory standpoint is have a set of regulations that every device that connects to Internet has support, accepts and can load software updates. Because the reality is every piece of software is going to have vulnerabilities."

"What worries me in my mind is IoT fundamentally changes the threat model in terms of security." While hacking a desktop computer or a smart phone is unlikely to threaten a person's safety, manipulating an IoT device remotely could be a safety issue.

Researchers have already shown improperly secured vehicles can be hacked, he pointed out. He also noted the huge Murai botnet was assembled from unsecured IoT devices such as home routers and video surveillance cameras to launch massive distributed denial of service attacks.

Click link above to read more

2) Cyber Security Today: Malware on Facebook, a scam aimed at Apple users and a teacher's mistake

https://www.itworldcanada.com/article/cyber-security-today-malware-on-facebook-a-scam-aimed-at-apple-users-and-a-teachers-mistake/405106

Many of you know about being careful not to click on suspicious links in your email. The same warning applies to text messages and social media. Security vendor Radware has found a new campaign for spreading malware through Facebook. A message suggests a video worth seeing, which takes the unsuspecting victim to a fake YouTube page. The user is then asked to install a Chrome browser extension to play the video. That extension is malware that steals their Facebook login credentials and can be used for fraud. Radware believes this campaign has been going on since at least March and has infected more than 100,000 users in over 100 countries.

As some of our listeners know, the tough new European Union privacy regulation known as GDPR comes into effect May 25th. To make sure they comply, companies are emailing people on their lists to confirm they want to continue receiving messages. Scammers are taking advantage of this. They're sending email with messages asking people to update their privacy settings or confirm a new privacy policy. All the user has to do is click on the provided link – which is either malicious or takes them to a phony site. Trend Micro says the latest scam is an email entitled "Update your payment details," which tells users their Apple accounts have been suspended because of unusual activity. It asks them to click a link to update their payment details. The real goal is to trick Apple users to giving up their IDs and passwords.

Click link above to read more

3) Sizing Up the Impact of Synthetic Identity Fraud

https://www.databreachtoday.com/interviews/sizing-up-impact-synthetic-identity-fraud-i-3982

With recent data breaches and the associated flood of PII onto the dark web, synthetic identity fraud is easier to commit than ever. Credit card losses due to this fraud exceeded $800 million in the U.S. last year, says Julie Conroy, a research director at Aite Group. Perhaps more shocking is just how much of the fraud is going undetected, flying under the radar as credit write-offs.

"One of the challenging aspects of this is often it doesn't get recognized as fraud and gets written off as a credit loss; so understanding the scope of the problem has been a challenge," Conroy says in an interview with Information Security Media Group about Aite's latest research. "A number of institutions are starting to see fundamental shifts to things like their credit delinquency curves that are only explainable by synthetic identity fraud."

Click link above to read more

4) Crypto Fight: US Lawmakers Seek Freedom From Backdoors

https://www.bankinfosecurity.com/crypto-fight-us-lawmakers-seek-freedom-from-backdoors-a-11000

A bipartisan group of U.S. lawmakers reintroduced legislation in the House of Representatives on Thursday that would stop the government from forcing software vendors to intentionally weaken their products for surveillance purposes.

If it **becomes law, the Secure Data Act of 2018** would likely **end the passionate "going dark" debate,** which has pitted law enforcement against the technology industry.

Many top law enforcement officials contend that the increasing use of encryption in software products has made it difficult or impossible to access information that investigators require to better protect the public.

The introduction of the legislation marks the third attempt by lawmakers in the past four years to gain traction for such a law. The same bill was introduced in the Senate in 2014 and the House in 2015.

Click link above to read more

---

5) Nuance Communications Breach Affected 45,000 Patients

https://www.databreachtoday.com/nuance-communications-breach-affected-45000-patients-a-11002

Nuance Communications, which specializes in speech recognition software, says an unauthorized third party accessed one of its medical transcription platforms, exposing 45,000 individuals' records.

So far, it appears only one of its customers, the San Francisco Department of Health, has reached out to affected patients.

The data breach occurred in December 2017, and Nuance - based in Burlington, Massachusetts - says in a Thursday filing with the U.S. Securities and Exchange Commission that it promptly shut down the platform while it investigated.

Nuance says it has notified all affected customers and moved them onto its eScription transcription platform. The software is designed to convert dictation by clinicians into documents.

"We also notified law enforcement authorities and have cooperated in their investigation into the matter," Nuance writes. "The law enforcement investigation resulted in the identification of the third party, and the accessed reports have been recovered."

Click link above to read more

---

6) Chili's Speed Question: To Notify or Not to Notify Quickly?

https://www.bankinfosecurity.com/blogs/chilis-speed-question-to-notify-or-to-notify-quickly-p-2628

This appears to have been the question facing Chili's Grill & Bar, which says it confirmed on Friday that some of its corporate-owned locations had **suffered a data breach resulting of some customers' credit and debit card data, as well as cardholder names, being exposed.**

Click link above to read more

---

7) Real-Time Payment Networks Face Off Against Fraudsters

https://www.bankinfosecurity.com/interviews/real-time-payment-networks-face-off-against-fraudsters-i-3979

Leading the latest edition of the ISMG Security Report: How real-time payment networks are battling attempts by fraudsters to compromise them in near real time. Also, attackers exploit legitimate websites to more stealthily distribute "Gandcrab" crypto-locking ransomware.

Click link above to read more

---

8) Protecting the Industrial Internet of Things

https://www.databreachtoday.com/protecting-industrial-internet-things-a-10997

The industrial internet of things presents a significant new risk paradigm, says Asif Effendi of GE Oil and Gas, who offers threat mitigation tips.

Click link above to read more

---

9) PANDA Banker malware used in several campaigns aimed at banks

https://securityaffairs.co/wordpress/72497/malware/panda-banker-campaigns-2018.html

Researchers at security firm F5 recently detected several campaigns leveraging the Panda Banker malware to target financial institution, the largest one aimed the banks in the US.

Click link above to read more

10) Critical Flaws in PGP and S/MIME Tools

https://securityaffairs.co/wordpress/72487/hacking/pgp-s-mime-tools-flaws.html

Researchers found critical vulnerabilities in PGP and S/MIME Tools, immediately disable and/or uninstall tools that automatically decrypt PGP-encrypted email.

Click link above to read more

11) GDPR: What you need to know about the EU's 'Right to Erasure' of personal information

http://itincanadaonline.ca/index.php/security/2378-gdpr-what-you-need-to-know-about-the-eu-s-right-to-erasure-of-personal-information

There are fewer than ninety days left until the European Union's General Data Protection Regulation (commonly referred to as GDPR), which governs the collection, use, storage and disclosure of any personal data of individuals in the EU, comes into effect. Canadian-based organizations who conduct business with the EU – or even have an online presence to market their products to customers in the EU – must make sure their current procedures for handling personal data of people based in the EU are aligned with the GDPR's requirements.

According to a recent survey by Sage, 91 per cent of businesses in Canada are either not very familiar with the GDPR or haven't heard of it at all. A further 83 per cent of businesses are not aware of how….

Click link above to read more

****