Security News Digest
Information Security Branch

British Columbia OCIO Office of the Chief Information Officer

May 14, 2024

Theme of the month: Cloud Authentication
(look for the ✪)

Challenge yourself with our Cloud Authentication Quiz!

What you can do to improve your authentication processes:

All Users	Technical Users	Business Owners
Use authenticator apps that have a high level of trust, like the B.C. Services Card app and the B.C. Wallet app.	Develop services that take advantage of authentication apps that have a high level of trust.	Ensure your security teams have opportunities and funding to continuously educate themselves about emerging authentication technologies and best practices to implement them.

Check out our **Cloud Security Thought Paper** to learn more.

This past week's stories:

🍁 **'Sophisticated' cyberattacks involving B.C. gov't networks found**
🍁 **State actor blamed for cyberattack on B.C. government systems**
✪ **The fundamentals of cloud security stress testing**
MorLock ransomware attacking organizations to steal business data
Hackers using weaponized shortcut files to deploy CHM malware
Microsoft to make security a top priority, above all
Cybersecurity issue disrupts operations at Ascension health care network
Dell hacked – 49 million customers data affected
Pupils miss classes as school cyber attacks rise
Cybersecurity in a race to unmask a new wave of AI-borne deepfakes
CISA warns of Black Basta ransomware attacking 500+ industries

Severe vulnerabilities in Cinterion cellular modems pose risks to various industries

---

'Sophisticated' cyberattacks involving B.C. gov't networks found

B.C.'s premier said Wednesday that the government has recently identified "sophisticated cybersecurity incidents" involving government networks.

https://www.cbc.ca/news/canada/british-columbia/bc-premier-cyberattacks-sophisticated-1.7198501

Click above link to read more.

Back to top

State actor blamed for cyberattack on B.C. government systems

The head of B.C.'s public service has announced that there is a high degree of confidence a state or state-sponsored actor attempted to breach government systems in a cyberattack.

https://www.cbc.ca/news/canada/british-columbia/bc-government-cyberattack-state-actor-1.7200735

Click above link to read more.

Back to top

The fundamentals of cloud security stress testing

“Defenders think in lists, attackers think in graphs," said John Lambert from Microsoft, distilling the fundamental difference in mindset between those who defend IT systems and those who try to compromise them.

https://thehackernews.com/2024/05/the-fundamentals-of-cloud-security.html

Click above link to read more.

Back to top

MorLock ransomware attacking organizations to steal business data

A new group known as MorLock ransomware has intensified its attacks on Russian businesses, causing disruptions and financial losses.

https://cybersecuritynews.com/morlock-ransomware-attacking-organizations/

Click above link to read more.

Back to top

Hackers using weaponized shortcut files to deploy CHM malware

Hackers exploit the weaponized shortcut files due to their ability to execute malicious code without knowing the user being targeted.

https://cybersecuritynews.com/weaponized-shortcut-chm-malware/

Click above link to read more.

Back to top

Microsoft to make security a top priority, above all

Microsoft has announced a major shift in its operational priorities, placing security at the forefront of its agenda, above all other considerations.

https://cybersecuritynews.com/microsoft-to-make-security/

Click above link to read more.

Back to top

Cybersecurity issue disrupts operations at Ascension health care network

Ascension, a major health care network in the U.S., said a suspected cybersecurity issue disrupted its “clinical operations” on Wednesday.

https://wgno.com/news/nmw/cybersecurity-issue-disrupts-operations-at-ascension-health-care-network/

Click above link to read more.

Back to top

Dell hacked – 49 million customers data affected

Dell Technologies is investigating a data breach incident involving a company portal containing limited customer information related to purchases, the computer technology company announced Friday.

https://cybersecuritynews.com/dell-hacked/

Click above link to read more.

Back to top

Pupils miss classes as school cyber attacks rise

Cancelled lessons and snaking lunchtime queues are among the ways pupils are being affected by an increasing number of cyber attacks on schools.

https://www.bbc.com/news/articles/c2vwz4exq4xo

Click above link to read more.

Back to top

Cybersecurity in a race to unmask a new wave of AI-borne deepfakes

Everyone's talking about deepfakes, but the majority of AI-generated synthetic media circulating today will seem quaint in comparison to the sophistication and volume of what's about to come.

https://www.darkreading.com/threat-intelligence/cybersecurity-in-a-race-to-unmask-a-new-wave-of-ai-borne-deepfakes

Click above link to read more.

Back to top

CISA warns of Black Basta ransomware attacking 500+ industries

Threat actors use black Basta ransomware because of its powerful abilities and inconspicuous moves.

https://cybersecuritynews.com/cisa-black-basta-ransomware-industries/

Click above link to read more.

Back to top

Severe vulnerabilities in Cinterion cellular modems pose risks to various industries

Cybersecurity researchers have disclosed multiple security flaws in Cinterion cellular modems that could be potentially exploited by threat actors to access sensitive information and achieve code execution.

https://thehackernews.com/2024/05/severe-vulnerabilities-in-cinterion.html

Click above link to read more.

Back to top

Click unsubscribe to stop receiving the Digest.

****
****

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:

https://www.gov.bc.ca/informationsecurity

OCIOSecurity@gov.bc.ca

The information presented or referred to in SND is owned by third parties and protected by copyright law, as well as any terms of use associated with the sites on which the information is provided. The recipient is responsible for making itself aware of and abiding by all applicable laws, policies and agreements associated with this information.

We attempt to provide accurate Internet links to the information sources referenced. We are not responsible for broken or inaccurate Internet links to sites owned or operated by third parties, nor for the content, accuracy, performance or availability of any such third-party sites or any information contained on them.

Security News Digest
Information Security Branch
BRITISH COLUMBIA OCIO Office of the Chief Information Officer