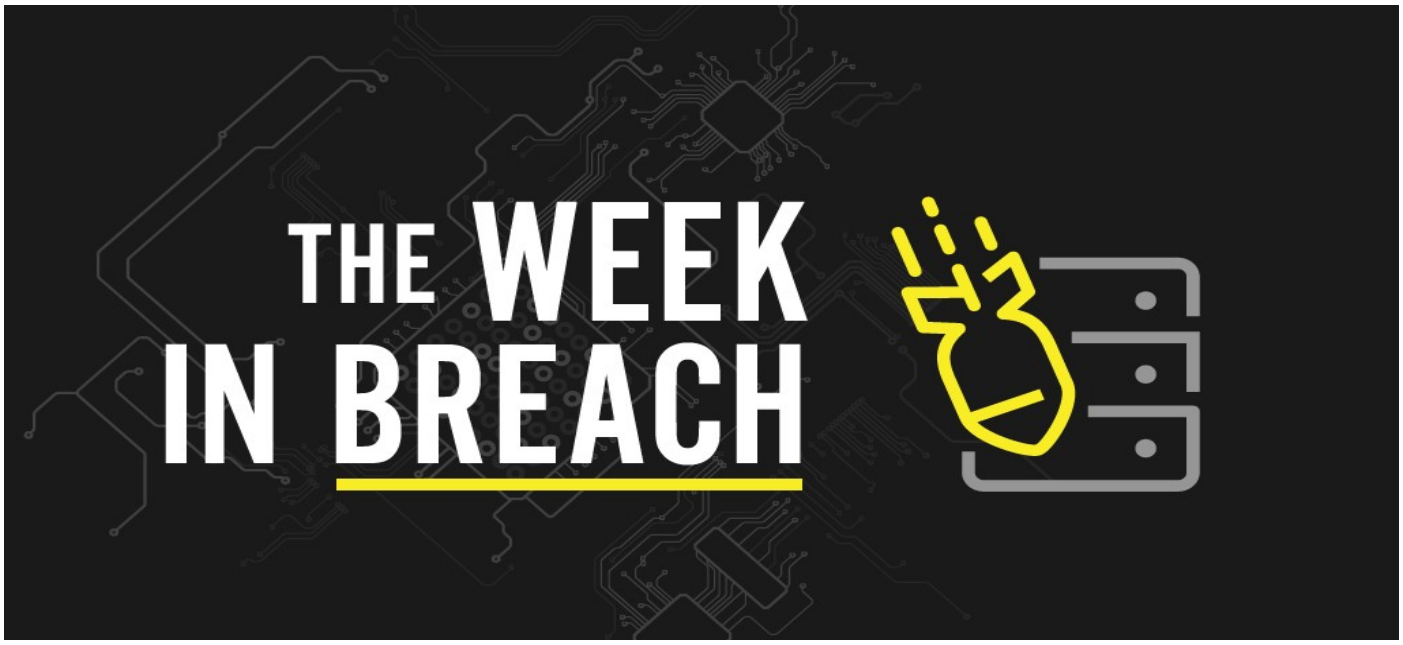
THE WEEK IN BREACH NEWS: 06/16/21— 6/22/21

DenBe Computer Consulting
Connecting Business

June 24, 2021 by Dennis Jock

Misconfiguration is the name of the game this week, as errors abound Carnival leaked data again (and Wegman's joined them), nation-state cybercrime hits South Korea and insights into leading MSPs from the MSP Benchmark Report.



If your business isn't using our ***Dark Web Monitoring Services*** please call us for a free scan and to discuss setting up this cutting edge monitoring service for you!

Not ready to talk yet? Visit our website to get your ***FREE Dark Web Scan.*** You will get a free, no obligation scan sent to your inbox within 24hrs. ***Visit today: www.denbeconsulting.com***

United States: Cognyte

https://beta.darkreading.com/attacks-breaches/cyber-analytics-database-exposed-5-billion-records-online

Exploit: Unsecured Database

Cognyte: Data Analytics Firm

Risk to Business: **1.802 = Severe**

Data analytics company Cognyte warns folks about data exposure from third-party sources, and it had to send one out for itself this week. Researchers discovered an unsecured database operated by Cognyte that left some 5 billion records collected from a range of data incidents exposed online. The stored data is part of Cognyte's cyber intelligence service, which is used to alert customers to third-party data exposures. The incident is under investigation.

Individual Impact: No sensitive personal or financial information for clients has been declared compromised in this incident and the investigation is ongoing.

Customers Impacted: Unknown

How It Could Affect Your Business: Proprietary like this is catnip for hackers. It's both useful for committing future cybercrime and quickly saleable in the busy dark web data markets.

United States - Invenergy LLC

https://www.infosecurity-magazine.com/news/revil-claims-responsibility-for/

Exploit: Ransomware

Invenergy LLC: Energy Company

Risk to Business: 1.916 = Severe

REvil has claimed responsibility for a recent cyberattack on renewable energy company Invenergy. The gang claims to have compromised the company's computer systems and exfiltrated four terabytes of data. Among the information allegedly taken by REvil are contracts and project data. In a bizarre twist, REvil also claims to have obtained "very personal and spicy" information regarding Invenergy's chief executive officer, Michael Polsky.

Individual Impact: No sensitive personal or financial information has been declared compromised in this incident and the investigation is ongoing.

Customers Impacted: Unknown

How it Could Affect Your Business: Ransomware attacks against strategic targets are hot right now as ransomware gangs try to score a big payday fast from targets that can't afford downtime.

United States – CVS

https://www.zdnet.com/article/billions-of-records-belonging-to-cvs-health-exposed-online/#ftag=RSSbaffb68

Exploit: Third-Party Threat (Misconfiguration)

CVS: Drug Store Chain

Risk to Business: 1.416= Extreme

CVS is in hot water after researchers discovered a trove of over one billion records online that were connected to the US healthcare and pharmaceutical giant. The unsecured databasewas extimated to be 204GB in size. According to reports, the databases contained an astonishing assortment of sensitive data like event and configuration data, visitor IDs, session IDs, device access information and details on how the logging system operated from the backend. Search records exposed also included queries for medications, COVID-19 vaccines and a variety of CVS products, referencing both CVS Health and CVS.com.

Individual Impact: There has not yet been confirmation that sensitive personal or financial information has been compromised in this incident but the investigation is ongoing.

Customers Impacted: Unknown

How it Could Affect Your Business: Every company needs to make it a priority to be certain that their contractors and partners are handling and storing sensitive data correctly. Poor cyber hygiene at a service provider can become an expensive disaster fast.

United States - Wegman's

https://www.bleepingcomputer.com/news/security/us-supermarket-chain-wegmans-notifies-customers-of-data-breach/

Exploit: Third-Party Threat (Misconfiguration)

Wegman's: Grocery Store Chain

Risk to Business: 2.227 = Severe

East Coast gourmet grocer Wegmans issued a release announcing that a service provider had failed to correctly configure two of its databases, exposing a large quantity of customer data. According to Wegmans, the databases that the contractor maintained contained customer identity and shopping habit information as well as an assortment of client PII. The company says the issue is resolved.

Risk to Business: 2.776 = Moderate

The release says that customer information exposed in the data breach included names, addresses, phone numbers, birth dates, Shoppers Club numbers, Wegmans.com account e-mail addresses and passwords. No Social Security, financial or medical information was stolen and only salted password hashes were stored in the databases maintained by the negligent contractor.

Customers Impacted: Unknown

How it Could Affect Your Business: Clients expect a high level of information security from companies that they trust with their personal information and excuses about errors by contractors aren't going to get businesses off the hook if there's trouble.

United States - Carnival Cruise Line

https://www.scmagazine.com/home/email-security/carnival-discloses-new-data-breach-on-email-accounts/

Exploit: Hacking

Carnival Cruise Lines: Cruise Ship Operator

Risk to Business: 1.651= Severe

Perennially cybersecurity challenged cruise line Carnival issued a breach disclosure on Thursday confirming hackers attacked email accounts and gained access to data about its customers and employees. The company said that the data snatched was collected during the travel booking process, through the course of employment or from providing services to the company, including COVID or other safety testing.

Risk to Business: 1.802= Severe

The passenger data accessed included names, addresses, phone numbers, passport numbers, dates of birth, health information, and, in some limited instances, additional personal information like social security or national identification numbers. No clear information was provided about the employee information that was exposed.

Customers Impacted: Unknown

How it Could Affect Your Business: This is the third major cybersecurity blunder for Carnival in just one year, and that is likely to create a great deal of mistrust with consumers just as the travel industry is getting back on it's feet.

United Kingdom - Cake Box

https://www.bleepingcomputer.com/news/security/eggfree-cake-box-suffer-data-breach-exposing-credit-card-numbers/

Exploit: Hacking

Cake Box: Bakery Chain

Risk to Business: 1.661 = Severe

UK celebration cake chain Cake Box isn't celebrating this week. The company has disclosed a data breach after threat actors hacked their website and obtained credit card numbers. According to the release, the breach occurred way back in April 2020 and they're just informing consumers. Payment skimming malware is to blame. Experts suspect that this breach is the result of a Magecart attack.

Individual Risk 2.802 = Severe

When customers made purchases on the site while it was infected malicious scripts sent the first name and surname, email address, postal address, and payment card information including the three-digit CVV code to a remote server controlled by the attackers. This is an ancient breach in terms of the time it took for consumers to be informed, and the damage has definitely already been done.

Customers Impacted: Unknown

How it Could Affect Your Business: There is no excuse for waiting more than a year to inform customers that their data has been stolen, especially financial data like credit card numbers. This incident will shake consumer confidence in the brand.

South Korea - Korea Atomic Energy Research Institute (KAERI)

https://www.theregister.com/2021/06/21/south_koreas_nuclear_think_tank/

Exploit: Nation-State Cybercrime

Korea Atomic Energy Research Institute (KAERI): Government Agency

Risk to Business: 1.633 = Severe

South Korean officials have admitted that the government nuclear think tank Korea Atomic Energy Research Institute (KAERI) was hacked by nation-state threat actors in May 2021 after the incident was brought to light by reporters. The Korean media is accusing the agency of perpetrating a cover-up. According to experts, the North Korean Kimusky cybercrime gang is to blame. This group often uses phishing to mimic websites like Gmail, Outlook, Telegram and more. The group then installs Android and Windows backdoor "AppleSeed" to collect information and frequently makes use of ransomware. The extent of the data theft is unknown.

Individual Impact: No sensitive personal or financial information has been confirmed as compromised in this incident.

Customers Impacted: Unknown

How it Could Affect Your Business: Nation-state threat actors frequently use phishing and ransomware to get the job done, and no matter how big or small, no organization is safe.