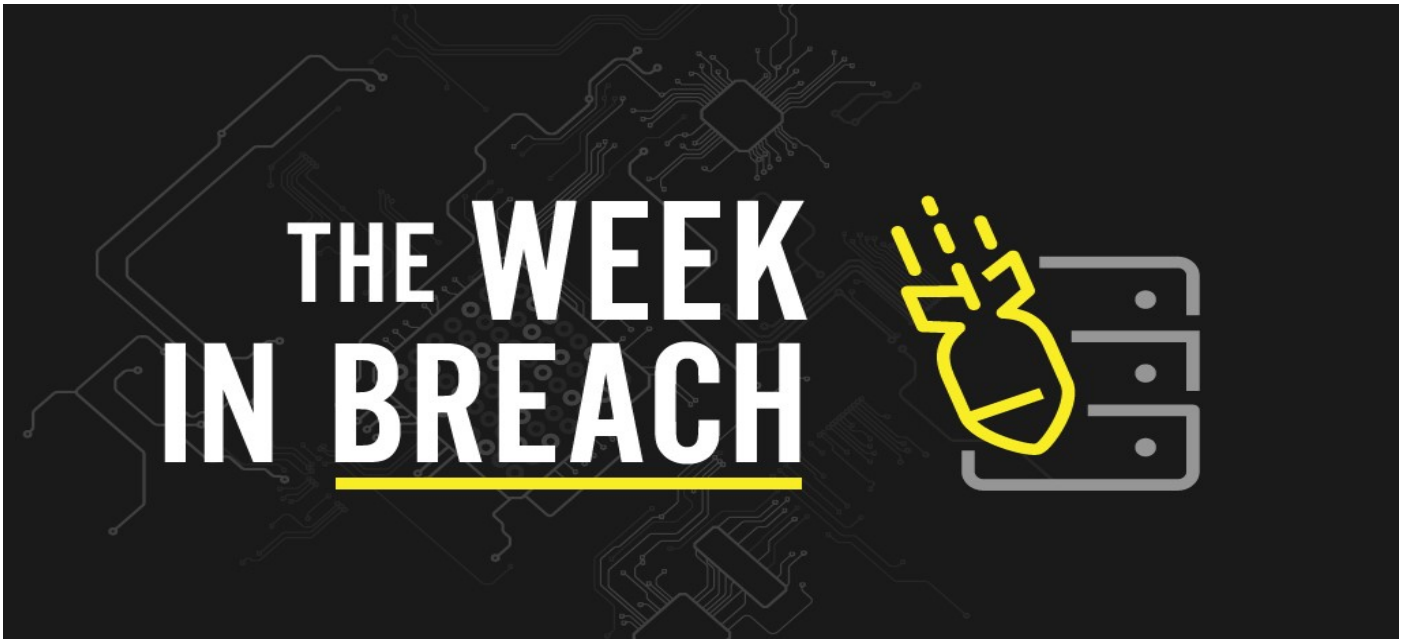
THE WEEK IN BREACH NEWS: 04/28/21 – 05/04/21

DenBe Computer Consulting
Connecting Business

May 5, 2021 by Dennis Jock

This Week in Breach News:

It's a very public-sector-oriented Week in Breach. Ransomware woes have made a home in five North American locales.



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***

Metropolitan Police Department of the District of Columbia

https://www.washingtonpost.com/local/public-safety/hacking-group-that-targeted-dc-police-briefly-posts-internal-police-files/2021/04/29/db18c98c-a8f2-11eb-8c1a-56f0cb4ff3b5_story.html

Exploit: Ransomware

Metropolitan Police Department of the District of Columbia: Law Enforcement Agency

Risk to Business: 1.717 = Severe

The Babuk Locker ransomware gang snatched data from the DC Metropolitan Police. The sample the cybercrime group posted, included 576 pages of personnel files including full names, Social Security numbers, phone numbers, financial and housing records, job histories and polygraph assessments for current and former officers. That data was briefly visible on the gang's site, but taken down after a short period. No word on whether the gang was paid or the exact contents of the stolen files. In total, the Babuk Locker gang claims it downloaded more than 250 GB of data from DC Police servers.

Risk to Business: 2.166 = Severe

Current and former employees of the Metro Police may be in danger for spear phishing, identity theft or blackmail and should remain alert for fraud attempts.

Customers Impacted: Unknown

How it Could Affect Your Business: Data theft like this is the bread and butter of cybercrime. This data is especially desirable because it contains information about law enforcement. When storing this kind of information, ensuring that you're using multifactor authentication is essential as is antiphishing security to guard against ransomware.

Illinois Office of the Attorney General

https://therecord.media/ransomware-gang-leaks-court-and-prisoner-files-from-illinois-attorney-general-office/

Exploit: Ransomware

Illinois Office of the Attorney General: State Government Agency

Risk to Business: 1.807= Severe

The DopplePaymer ransomware gang has leaked a large collection of files from the Illinois Office of the Attorney General after the agency declined to pay the ransom that they gang demaded. The cybercrimnals released information from court cases orchestrated by the Illinois OAG, including some private documents that do not appear in public records. the data also contains personally identifiable information about state prisoners, notes of their grievances, and case information.

Risk to Business: 2.177= Severe

In the documents posted so far there is some personal data for prisoners, but the full extent of the breach is not clear. formerly incarcerated people may be at risk of blackmail or spear phishing.

Customers Impacted: Unknown

How it Could Affect Your Business: More than 50% of businesses were impacted by ransomware in the last 12 months. by taking sensible precautions like antiphishing software, secure identity and access management and updated security awareness training, companies can avoid this menace.

Pennsylvania Department of Health

https://6abc.com/covid-19-contact-tracing-coronavirus-pennsylvania-pa-data-breach-insight-global/10560542/

Exploit: Third Party Data Breach

Pennsylvania Department of Health: State Government Agency

Risk to Business: 1.803= Severe

The Pennsylvania Department of Health received an unpleasant shock when it learned that the third-party firm it had employed to process contact tracing data had made data handling mistakes, potentially opening thousands of residents of the Keystone State up to trouble. The contractor, Atlanta-based Insight Global reported that several employees violated security protocols to create unauthorized documents outside of the secure data system that the state's contract required using the data collected.

Risk to Business: 2.277= Severe

Some of the records in question associated names with phone numbers, emails, genders, ages, sexual orientations and COVID-19 diagnoses and exposure status. They did not include financial account information, addresses or Social Security numbers. A daytime hotline is available for anyone concerned they might have been involved at 855-535-1787. Free credit monitoring and identity protection services will be offered.

Customers Impacted: 72,000

How it Could Affect Your Business: No business is an island. That's why it pays to take precautions against potential intrusions and data theft that results from a service provider's cybersecurity failure.

Wyoming Department of Health

https://www.infosecurity-magazine.com/news/data-breach-impacts-1-in-4/

Exploit: Unsecured Database

Wyoming Department of Health: State Government Agency

Risk to Business: 2.303 = Severe

Wyoming's Department of Health (WDH) has announced the accidental exposure of personal health information belonging to more than a quarter of the state's population on GitHub.com. The data breach occurred when an estimated 53 files containing laboratory test results were mishandled by a worker. Data in the leaked files included test results for flu and COVID-19 performed for Wyoming. One file containing breath alcohol test results was also exposed.

Risk to Business: 2.676 = Severe

Along with the test results were patients' names, ID numbers, addresses, dates of birth and dates of when tests had been carried out. WDH has begun the process of notifying impacted individuals and victims will be offered a year of free identity theft protection.

Customers Impacted: 164,021 Wyoming residents and others

How it Could Affect Your Business: Taking care of business includes taking care of training to prevent slip-ups like this that will ultimately cost the state million after remediation and fines.