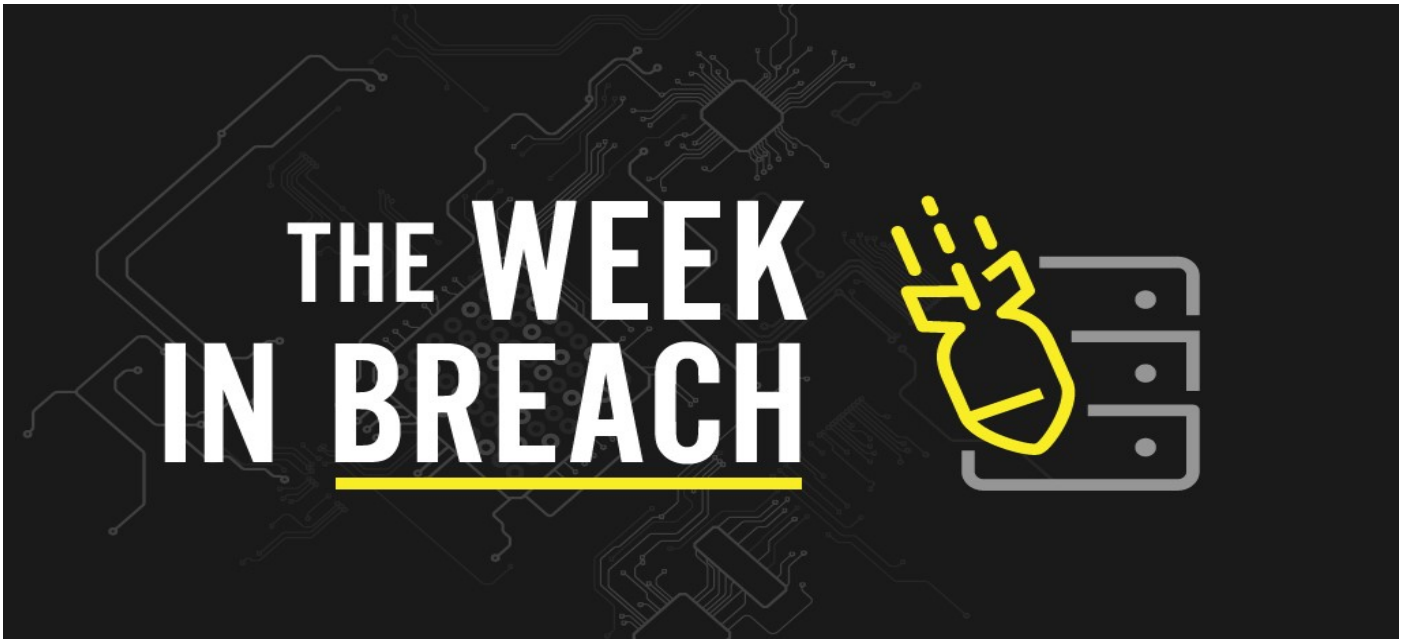
THE WEEK IN BREACH NEWS: 04/07/21 – 04/13/21

DenBe Computer Consulting
Connecting Business

April 14, 2021 by Dennis Jock

This Week in Breach News:

Cybercriminals leak the PII of millions of professionals in a new LinkedIn breach, an unwelcome visit by nation-state hackers exposes data at BlueCross BlueShield DC.



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***

CareFirst BlueCross BlueShield Community Health Plan District of Columbia (CHPDC)

https://thehill.com/policy/cybersecurity/547250-major-dc-insurance-provider-hacked-by-foreign-cybercriminals

Exploit: Nation-State Hacking

CareFirst BlueCross BlueShield Community Health Plan District of Columbia (CHPDC): Insurer

Risk to Business: 1.761 = Severe

CareFirst BlueCross BlueShield's Community Health Plan District of Columbia (CHPDC) has announced a data breach carried out by what it described as a "foreign cybercriminal" group. The insurer confirmed that sensitive information about members was snatched and that they've notified authorities including the FBI and the Office of the Attorney General for the District of Columbia.

Individual Risk: 1.603 = Severe

In a written notification to customers, CHPDC noted that the stolen information may have included names, addresses, phone numbers, dates of birth, Medicaid identification numbers, and other medical information. The company is offering free two-year credit and identity theft monitoring and a website with more information on help for consumers.

Customers Impacted: Unknown

How it Could Affect Your Business: Nation-state cyberattack risks aren't just a problem for government and military targets anymore. These clever cybercriminals will exploit any opening fast.

Office Depot

https://www.websiteplanet.com/blog/office-depot-leak-report/

Exploit: Unsecured Database

Office Depot: Business Supply Retailer

Risk to Business: 1.803 = Severe

Security researchers discovered a non-password-protected Elasticsearch database belonging to Office Depot that contained just under a million records. The exposed records were labeled as "Production" and contained customer information, file logs and other internal records for European customers, primarily in Germany. The company has addressed the issue.

Individual Risk: 2.267 = Severe

The exposed data includes names, phone numbers, physical addresses (home and/or office), @members.ebay addresses, and hashed passwords. The leak also exposed Marketplace logs and order history, exposing the customers' past purchases and costs from European customer records.

Customers Impacted: 533 Million

How it Could Affect Your Business: Cybercriminals will benefit from this trove. Data like this is transacted every day on the dark web, providing ample ammunition for future cyberattacks and fraud.

LinkedIn

https://cybernews.com/news/stolen-data-of-500-million-linkedin-users-being-sold-online-2-million-leaked-as-proof-2/

Exploit: Hacking

LinkedIn: Social Media Network

Risk to Business: 1.612 = Severe

Bad actors have dropped notice that they've obtained an archive containing data purportedly scraped from 500 million LinkedIn profiles. A sample of data was posted on a popular hacker forum, with another 2 million records leaked as proof of the haul. More than 780,000 email addresses are associated with this leak. The initial listing contained 4 archives, but after LinkedIn denied the data breach, threat actors updated their ad to include 6 additional archives that allegedly include 327 million scraped LinkedIn profiles, putting the overall number of scraped profiles at 827 million including potential duplicates.

Individual Risk: 2.309 = Severe

This mass of leaked files contains PII about LinkedIn users including LinkedIn IDs, full names, email addresses, phone numbers, genders, links to LinkedIn profiles, links to other social media profiles, professional titles and other work-related data.

Customers Impacted: Unknown

How it Could Affect Your Business: Following hard on the heels of last week's Facebook breach social media risks are multiplying fast and growing serious for businesses.

Personal Touch Holding Corp. (PTHC)

https://www.prnewswire.com/news-releases/personal-touch-holding-corp-identifies-and-addresses-data-security-breach-301256229.html

Exploit: Hacking

Personal Touch Holding Corp. (PTHC): Home Healthcare Provider

Risk to Business: 1.241 = Extreme

The Clop ransomware gang had a banner week. UMB is one of at least 6 US colleges that they've hit successfully in the past week after gaining access to systems at data transfer and processing behemoth Accellion in late 2020. At UMB, the gang snatched an assortment of student and staff data including federal tax documents, requests for tuition remission paperwork, applications for the Board of Nursing, passports, ID data and tax summary documents.

Individual Risk: 1.412 = Extreme

Exposed patient information may include medical treatment information, insurance card and health plan benefit numbers, medical record numbers, first and last name, address, telephone numbers, date of birth, Social Security number, and financial information, including check copies, credit card numbers, and bank account information. Leaked Member information may include Medicaid ID number, ID number, provider name, clinical/medical information, first and last name, address, telephone number, date of birth, Social Security numbers, and credit card numbers and/or banking information if members paid their Medicaid surplus through credit card or check.

Customers Impacted: Unknown

How it Could Affect Your Business: This breach isn't just going to cost a fortune to fix now – it's also likely to incur a hefty regulatory penalty from state and federal authorities.