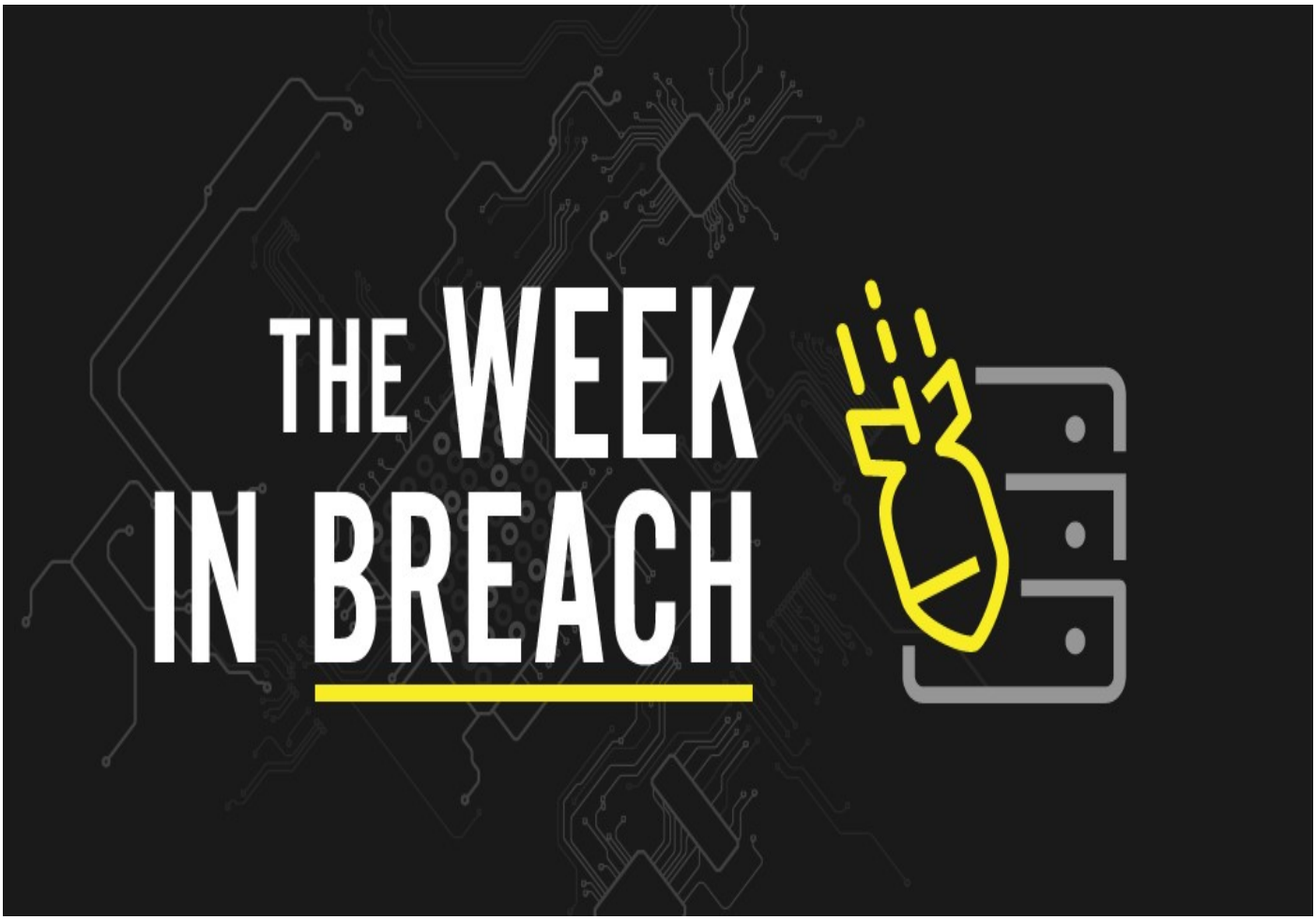
THE WEEK IN BREACH NEWS: 03/15/23 - 03/21/23

DenBe Computer Consulting
Connecting Business

March 22nd 2023 by Dennis Jock



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***

AT&T
https://www.bleepingcomputer.com/news/security/atandt-alerts-9-million-customers-of-data-breach-after-vendor-hack/

Exploit: Supply Chain Attack

AT&T: Communications Conglomerate

Risk to Business: 1.802 = Severe

AT&T is notifying roughly 9 million customers that some of their information was exposed after a marketing vendor was hacked in January 2023. The company did not name the vendor, and they were quick to reassure customers that financial data and Social Security numbers were not involved. Impacted customers have been informed that some or all of their Customer Proprietary Network Information (CPNI) has been exposed, including customer first names, wireless account numbers, wireless phone numbers and email addresses. The company said that a small percentage of customers also had additional data exposed including their rate plan name, past due amount, monthly payment amount, minutes used and various other monthly charges. AT&T said that the data was several years old but didn't specify a time period.

How It Could Affect Your Business: Supply chain risk is spinning out of control for businesses, and IT professionals need to be ready to mitigate it fast.

DC Health Link
https://wtop.com/dc/2023/03/dc-health-link-responds-to-data-breach-saying-investigation-in-the-works/

Exploit: Hacking

DC Health Link: Health Insurance Marketplace

Risk to Business: 1.702 = Severe

The U.S. Federal Bureau of Investigation (FBI) is investigating a cyberattack on DC Health Link that Left some information exposed for more than 56,000 people including members of Congress. The health insurance marketplace became aware it had been hacked last Wednesday. People whose information was leaked include small business owners, uninsured District residents and lawmakers, including members of Congress and their staff. The data stolen includes names, Social Security numbers, dates of birth, health plan information and other personal information, including home addresses, phone numbers, email addresses, ethnicity and citizenship status.

How It Could Affect Your Business: This kind of information security disaster will be a big, expensive and painful mess to clean up.

Cerebral
https://www.bleepingcomputer.com/news/security/mental-health-provider-cerebral-alerts-31m-people-of-data-breach/

Exploit: Human Error

Cerebral: Telehealth Provider

Risk to Business: 1.267 = Extreme

Mental health platform Cerebral is informing 3.8 million customers that it has experienced a data breach. The company recently admitted that it had been using invisible pixel trackers from Google, Meta (Facebook), TikTok and other third parties on its online services since October 12, 2019. Those pixels had data logging features, resulting in the exposure of sensitive medical information of people who used the provider's platform to third parties without the customer's knowledge. Exposed patient information includes a client's full name, phone number, email address, date of birth, IP address, client ID number, demographic information, self-assessment responses and associated health information, subscription plan type, appointment dates, treatment details, clinical data, and health insurance and pharmacy benefit information. Social Security numbers, credit card information, and bank account information have not been impacted.

How It Could Affect Your Customers' Business: This debacle is a disaster for Cerebral and will end up costing the company a fortune after regulators get finished with it.

Group 1001 Insurance
https://www.cybersecuritydive.com/news/insurance-holding-1001-restored-ransomware/644330/

Exploit: Ransomware

Group 1001: Financial Services Company

Risk to Business: 2.779 = Moderate

New York-based financial services and insurance holding company Group 1001 has announced that it was the victim of a ransomware attack that impacted some of its member companies. The February 9, 2023, attack snarled operations for several member companies, including Delaware Life Insurance, Delaware Life Insurance Company of New York, Clear Spring Life and Annuity, Clear Spring Property and Casualty and Clear Spring Health. The company said that it did not pay a ransom but offered no specifics about the attacker, noting that they've brought in a third-party forensics team to investigate this incident along with the FBI. The Gainbridge subsidiary of Group 1001 was not affected. Operations have since been restored. People who were impacted are being informed by mail.

How It Could Affect Your Customers' Business: Ransomware attacks against financial industry targets like this have proliferated in the past three years.