THE WEEK IN BREACH NEWS: 02/10/21 – 02/16/21

DenBe Computer Consulting
Connecting Business

February 17, 2021 by Dennis Jock

This Week in Breach News:

A Florida municipal water plant breach raises alarm.

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***

Chess.com

https://www.hackread.com/vulnerability-chess-com-50-million-user-records-accessed/

Exploit: Security Vunerability

Chess.com: Gaming and Resource Site

Risk to Business: 2.211 = Severe

Security researchers found a critical bunch of vulnerabilities in chess.com's API. The flaws could have been exploited to access any account on the site. They could also be used to gain full access to the site through its administrator panel. The website quickly fixed the problem after they were informed. There's no current evidence that it was accessed by bad actors before it was patched.

Customers Impacted: 50 Million

How it Could Affect Your Business: Security vulnerabilities can lead companies down dangerous paths and expose them to unexpected risks. Building a strong security culture helps make sure everyone is on the same page when it comes to data protection.

Oldsmar Water Treatment Plant

https://threatpost.com/florida-water-plant-hack-credentials-breach/163919/

Exploit: Credential Compromise

Oldsmar Water Treatment: Municipal Water System Plant

Risk to Business: 2.022 = Severe

In an attack that made national headlines, bad actors are suspected of using stolen credentials to access operational systems at a Florida wastewater treatment plant. The attackers likely used remote access software to enter the operations system with the intent of changing the level of sodium hydroxide, more commonly known as lye, in the water from 100 parts per million to 11,100 parts per million. Other systems detected the chemical change and stopped it before anyone was hurt. Officials suspect that the compromised credentials may have been part of a huge 2017 data dump.

Individual Impact: No sensitive personal or financial information was announced as part of this incident, but the investigation is ongoing.

Customers Impacted: Unknown

How it Could Affect Your Business: Recycled, reused, and weak passwords can cause trouble for years, and that’s especially dangerous when they give access to critical infrastructure like this.

Syracuse University

http://dailyorange.com/2021/02/names-social-security-numbers-of-syracuse-university-students-exposed-in-data-breach/

Exploit: Unauthorized Access to Email

Syracuse University: Institution of Higher Learning

Risk to Business: 2.379 = Severe

An unknown party gained unauthorized access to an employee's email account at Syracuse University. The university launched an investigation with a third party firm that determined in early January that emails and attachments in the account that had been improperly accessed did contain names and Social Security numbers of students, and those affected who have been informed by letter.

Individual Risk: 1.347 = Severe

Impacted students may have had names and Social Security numbers exposed. officials aren't clear on how much data was stolen or who may have taken it. Students should be alert to potential identity theft or spear phishing attempts.

Customers Impacted: 10,000

How it Could Affect Your Business: Data like this is a currency on the Dark Web, and it can hang around for years acting as fuel for future cybercrime like phishing.

Nebraska Medicine

https://apnews.com/article/technology-data-privacy-nebraska-94d8a76d2b772a3014773023c989d71a

Exploit: Malware

Nebraska Medicine: Health System

Risk to Business: 1.663 = Severe

Nebraska Medicine and the University of Nebraska Medical Center have begun notifying patients and employees whose personal information may have been compromised in a breach in late 2020. Bad actors gained access to Nebraska Medicine and UNMC's shared network using unnamed malware. The breach led to the interruption of some services including the postponement of patient appointments and required staff in the system's hospitals and clinics to chart by hand.

Individual Risk: 2.101 = Severe

Nebraska Medicine officials say that the incident did not result in unauthorized access to the health system's shared electronic medical record application. However, an unspecified number of records that
included information such as names, addresses, health insurance data, Social Security numbers and clinical information was compromised. Patients and employees should carefully watch for identity theft, spear phishing or fraud attempts using this data.

Customers Impacted: Unknown

How it Could Affect Your Business: Ransomware isn't the only kid on the block when it comes to causing a data breach – many types of malware are available for bad actors to use, and they can do devastating damage without the ransom.