THE WEEK IN BREACH NEWS: 01/06/21 – 01/12/21

DenBe Computer Consulting
Connecting Business

February 10, 2021 by Dennis Jock

This Week in Breach News:

Spotify is in the spotlight with yet another breach, third-party risk backfires on multiple organizations, short and long term planning for rising remote work risk.

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***

WestRock

https://www.securityweek.com/packaging-giant-westrock-says-ransomware-attack-impacted-ot-systems

Exploit: Ransomware

WestRock: Packaging Manufacturer

Risk to Business: 2.779 = Extreme

Packaging giant WestRock has experienced a ransomware attack that has impacted both its manufacturing and IT environments, severely impacting production. The company has noted in an announcement to shareholders that it expects that continued delays during the recovery and cleanup process are expected.

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: Ransomware can be especially devastating to manufacturing companies by not just impacting office business but halting production, leading to a cascade effect.

Washington State Auditor

https://sao.wa.gov/

Exploit: Third Party Data Breach

Washington State Auditor: Regional Government Regulator

Risk to Business: 1.379 = Severe

The unemployment claims data of more than 1 million people in Washington State has been reported as stolen in a hack of software used by the state auditor's office. The State announced the breach after receiving notice that it was involved through a third party service provider, Accellion, a software provider the auditor's office uses to transfer large computer files. the breach affects the personal information of people who filed for unemployment claims with the Washington Employment Security Department (ESD) between Jan. 1, 2020, and Dec. 10, 2020, and included a total of 1.6 million claims. Those claims represent at least 1.47 million individuals, according to data from the ESD website.

Individual Risk: 1.379 = Severe

The data breach involved claimants' names, Social Security numbers and/or driver's license or state identification number, bank information, and place of employment. The state auditor has set up a web page for people who think their personal information could have been exposed in the data breach. See https://sao.wa.gov/breach2021/.

Customers Impacted: 1.40 million or more people.

How it Could Affect Your Business: Data like this is sought-after by cybercriminals to power phishing operations. Unfortunately for these folks, it often hangs around for years on the Dark Web, acting as fuel for future cybercrime.

DriveSure

https://www.scmagazine.com/home/security-news/data-on-3-2-million-drivesure-users-exposed-on-hacking-forum/

Exploit: Hacking

DriveSure: Customer Retention Platform

Risk to Business: 2.211 = Severe

Hackers dropped data on 3.2 million DriveSure users on the Raidforums hacking boards late in January. One leaked folder totaled 22 gigabytes and included the company's MySQL databases, exposing 91 sensitive databases. The databases range from detailed dealership and inventory information, revenue data, reports, claims and client data. A second compromised folder contained 11,474 files in 105 folders and totals 5.93 GB, likely a repository of backup data.

Individual Risk: 2.325 = Severe

The information exposed included names, addresses, phone numbers, email addresses, IP addresses, car makes and models, VIN numbers, car service records and dealership records, damage claims and 93,063 bcrypt hashed passwords.

Customers Impacted: 3.2 million

How it Could Affect Your Business: Data isn't always stolen via ransomware – sometimes it's just old-fashioned hacking. That's one reason why it's essential to use a secure identity and access management solution to keep hackers locked out.

SN Servicing Company

https://www.scmagazine.com/home/security-news/mortgage-loan-servicing-company-discloses-ransomware-attack-to-multiple-states/

Exploit: Ransomware

SN Servicing Company: Mortgage Loan Services

Risk to Business: 2.022 = Severe

SN Servicing, the California-based servicing arm of Security National Master Holding Company, disclosed a data breach impacting clients in Vermont and California. The incident was also reported by the Egregor ransomware gang. SN Servicing says that it has engaged a third party team of investigators to determine the scope of the incident.

Individual Risk: 2.171 = Severe

The stolen data appears to be related to billing statements and fee notices to customers from 2018, including names, addresses, loan numbers, balance information, and billing information such as charges assessed, owed, or paid. Clients should be aware of potential spear phishing and identity theft risks.

Customers Impacted: Unknown

How it Could Affect Your Business: Ransomware is around every corner these days, and just one misclick on a phishing email can spell disaster.

Spotify

https://threatpost.com/spotify-credential-stuffing-cyberattack/163672/

Exploit: Credential Stuffing

Spotify: Streaming Music Service

Risk to Business: 1.668 = Severe

Spotify has returned for another appearance with a credential stuffing disaster eerily similar. This time, data for approximately 100k users appeared in an Elasticsearch instance spotted by researchers. This is distinctly different data than the load that researchers discovered in November 2020.

Individual Risk: 1.802 = Severe

No specifics were listed about the stolen data, but Spotify users should reset their account passwords and be on the lookout for spear phishing attempts.

Customers Impacted: 100k+

How it Could Affect Your Business: Protection against credential stuffing isn't something that a company like Spotify should struggle with, and suffering two credential stuffing incidents in one quarter shows a sloppy attitude toward security.