THE WEEK IN BREACH NEWS: 12/16/20 – 12/22/20

DenBe Computer Consulting
Connecting Business

December 23, 2020 by Dennis Jock

This Week in Breach News: The fallout of last week's massive nation-state hacking incident continues for Microsoft, Cisco & more organizations (and it isn't letting up), plus yet another Spotify breach.

The Week in Breach News: Top Threats This Week

- **Top Source Hits:** ID Theft Forum
- **Top Compromise Type:** Domain
- **Top Industry:** Education & Research
- **Top Employee Count:** 501+

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!

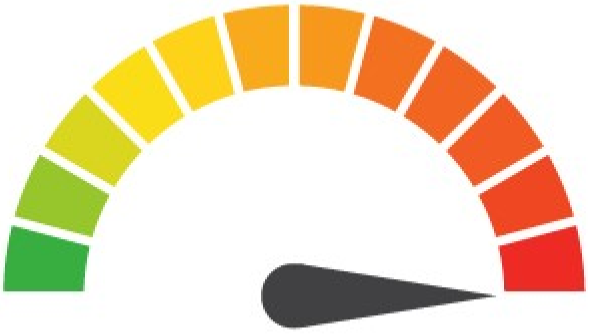
Not ready to talk yet? Visit our website to get your ***FREE Dark Web Scan*****.** You will get a free, no obligation scan sent to your inbox within 24hrs. ***Visit today: www.denbeconsulting.com***

Microsoft

https://portswigger.net/daily-swig/microsoft-falls-prey-to-solarwinds-supply-chain-cyber-attacks

Exploit: Hacking (Nation-State)

Company Name: Type



Risk to Business: **1.402 = Extreme**

Another chapter in the SolarWinds Nation-State Hack opened when Microsoft disclosed that it had been hacked as well. The same suspected Russian hacking activity that rocked the world last week hit the software giant as well. This Microsoft compromise appears to have a direct path back to the infected updates to SolarWinds' Orion. The company notes that it has "not found evidence of access to production services or customer data", but that's in dispute.

Individual Risk:

No personal or consumer information was reported as impacted in this incident at this time but the incident is still under investigation.

Customers Impacted: Unknown

How it Could Affect Your Business: Nation-state hacking is a risk that can only grow, and that has to be part of every business' risk calculus. Putting overlapping protection in place can help your clients resist these attacks.

Cisco

https://www.crn.com/news/security/cisco-hacked-through-solarwinds-as-tech-casualties-mount

Exploit: Hacking (Nation-State)

Cisco: Technology Developer

Risk to Business: 1.411 = Extreme

Cisco also took a hit in last week's disaster, but it appears to have been very small. The company has so far reported that the SolarWinds Orion software update was only impacting a small number of computers in its' test environments. Cisco says that no customer systems or data were impacted from their end. that's in dispute.

Individual Risk:

No personal or consumer information was reported as impacted in this incident.

Customers Impacted: Unknown

How it Could Affect Your Business: Nation-state hacking is a risk that can only grow, and that has to be part of every business' risk calculus. Putting overlapping protection in place can help your business resist these attacks.

Spotify

http://techgenix.com/spotify-data-breach/

Exploit: Accidental Data Exposure

Risk to Business: 2.223 = Severe

In their 3rd breach of the year, Spotify has announced that starting in April 2020, some user information was inadvertently exposed to third-party partners that shouldn't have been able to access it. The leak was discovered and closed in November 2020.

Individual Risk: 2.212 = Severe

The leaked information may have included email address, display name, password, gender, and date of

Customers Impacted: Unknown

How it Could Affect Your Business: This kind of data inevitably makes its way to the Dark Web, providing fodder for cybercriminals to exploit to fuel future cyberattacks.

City of Independence, MO

https://fox4kc.com/news/customers-frustrated-after-independence-utility-payment-system-goes-offline-following-cyber-attack/

Exploit: Ransomware

City of Independence, MO: Municipal Government

Risk to Business: **2.017 = Severe**

Energy customers in the city of Independence, Missouri were unable to pay their utility bills after a ransomware attack spurred the city’s IT team to take all city systems offline in response to a ransomware incident. The municipal government is still conducting investigation and remediation. Citizens can currently only pay utility bills in person.

Customers Impacted: 54,000

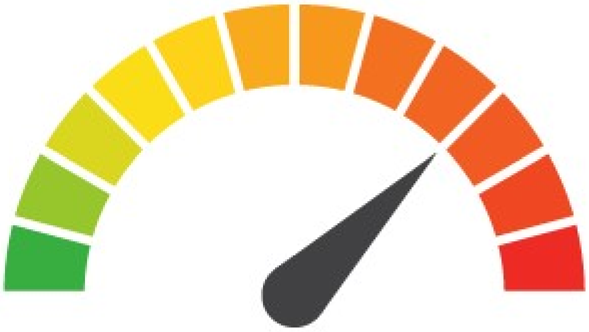
How it Could Affect Your Business: More municipalities are finding themselves in the crosshairs of cybercriminals looking to make a quick profit than ever.

Sonoma Valley Hospital

https://www.infosecurity-magazine.com/news/svh-notifies-67k-patients-of-data/

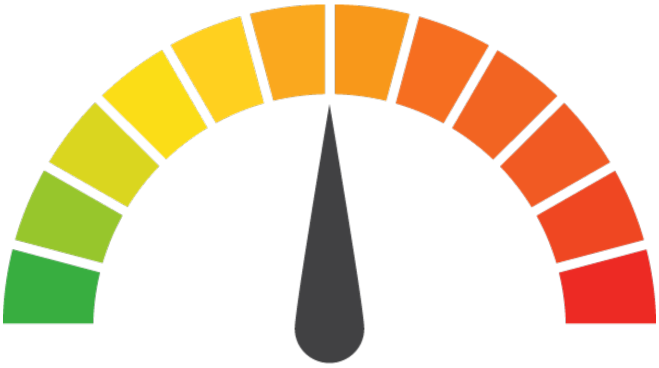
Exploit: Hacking (Nation State)

Sonoma Valley Hospital: Medical Center



Risk to Business: **1.809 = Severe**

In their 3rd breach of the year, Spotify has announced that starting in April 2020, some user information was inadvertently exposed to third-party partners that shouldn't have been able to access it. The leak was discovered and closed in November 2020.



Individual Risk: **2.667 Moderate**

It's unclear to what extent customer data was impacted, but it is possible that some personally identifying information and treatment data was accessed or copied by the intruders. The investigation is ongoing, but people who have been treated at this facility should be alert for spearphishing attempts.

Customers Impacted: 67,000

How it Could Affect Your Business: Ransomware is a huge threat to every organization right now, and it has been so widely deployed in the healthcare sector that CISA released guidance on risk avoidance.