THE WEEK IN BREACH NEWS: 03/03/21 – 03/09/21

DenBe Computer Consulting
Connecting Business

March 10, 2021 by Dennis Jock

This Week in Breach News:

Nation-state actors sliding in through a Microsoft flaw.

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

Qualys

https://www.bleepingcomputer.com/news/security/cybersecurity-firm-qualys-is-the-latest-victim-of-accellion-hacks/

Exploit: Third Party Breach (Ransomware)

Qualys: Cybersecurity & Cloud Development

Risk to Business: 1.412 = Extreme

Qualys is the latest victim to have suffered a data breach after a zero-day vulnerability in their Accellion FTA server was exploited to steal hosted files. The Clop ransomware gang posted screenshots of files allegedly belonging to the cybersecurity firm including purchase orders, invoices, tax documents and scan reports.

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: It’s especially damaging for a cybersecurity company to fall victim to something like ransomware. Unfortunately, this problem came through a third-party partner, but potential customers may see a cybersecurity firm that can’t protect itself.

PrismHR

https://www.bleepingcomputer.com/news/security/payroll-giant-prismhr-outage-likely-caused-by-ransomware-attack/

Exploit: Ransomware

PrismHR: Payroll Services

Risk to Business: 2.212 = Severe

A suspected ransomware attack has brought trouble to payroll giant Prism HR and its clients. PrismHR’s platform is experiencing a service outage as a result, which has led to smaller accountants, and their clients, to lose access to PrismHR’s customer portals.

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

Customers Impacted: Unknown

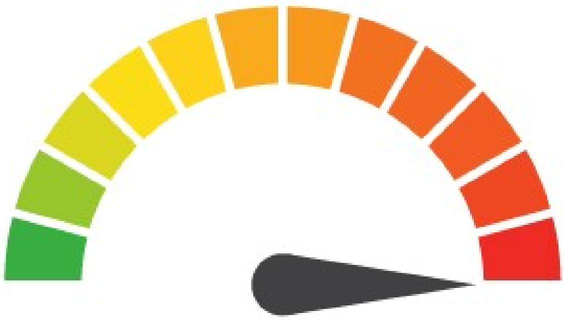
How it Could Affect Your Business: Ransomware can strike anytime, anywhere and companies of any size are vulnerable. Smart companies take proper precautions like increased security awareness training.

Microsoft

https://www.nytimes.com/2021/03/06/technology/microsoft-hack-china.html

Exploit: Nation-State Hacking

Qualys: Software Developer



Risk to Business: 1.227 = Extreme

Microsoft is reporting a that suspected Chinese nation-state actors have exploited a flaw in Exchange that has given them some access to data or email accounts. The company estimates that 30,000 or so customers were affected. This flaw impacts a broad range of customers, from small businesses to local and state governments and some military contractors. The hackers were able to steal emails and install malware to continue surveillance of their targets. Patches are available and should be installed immediately.

Individual Impact: No sensitive personal or financial information was announced as part of this incident from Microsoft directly, but organizations around the world will be conducting assessments with potentially wide-ranging fallouts.

Customers Impacted: Unknown

How it Could Affect Your Business: This is a tremendous problem for businesses of every size, and something that will be lingering for years for impacted organizations.

CallX

https://www.infosecurity-magazine.com/news/telemarketing-biz-exposes-114000/

Exploit: Unsecured Server

CallX: Telemarketing Firm

Risk to Business: 1.727 = Severe

An unsecured AWS S3 bucket has been leaking information gathered by CallX, whose analytics services are utilized by a wide array of companies including LendingTree, Liberty Mutual Insurance and Vivint to improve their media buying and inbound marketing. Discovered by researchers, 114,000 files were left publicly accessibly in the leaky bucket. Most of these were audio recordings of phone conversations between CallX clients and their customers, which were being tracked by the firm's marketing software. An additional 2000 transcripts of text chats were also viewable.

Individual Risk: 1.447 = Extreme

Personally identifiable information (PII) contained in these files included full names, home addresses, phone numbers and call details. The leaked data can be used to launch spear phishing attacks and other fraud.

Customers Impacted: Unknown

How it Could Affect Your Business: Information like this makes its way quickly to the bustling data markets and dumps on the dark web, seeding future trouble.