THE WEEK IN BREACH NEWS: 11/25/20 – 12/01/20

DenBe Computer Consulting
Connecting Business

December 2, 2020 by Dennis Jock

This Week in Breach News: Baltimore County Public Schools learn a lesson about ransomware, healthcare targets worldwide take security hits, learn to spot and stop phishing with intel from our cybercriminal secret files, and see how business email compromise scams are taking a new turn.

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***

Baltimore County Public Schools

https://www.bizjournals.com/baltimore/news/2020/11/25/ransomware-attack-baltimore-county-public-schools.html

Exploit: Ransomware

Baltimore County Public Schools: School System

Risk to Business: **1.222 = Extreme**

Ransomware attacks on school systems around the country have grown exponentially, and that lesson was driven home for Baltimore County Public Schools last week. A ransomware attack forced the system to shut down completely for three days, disrupting online learning for K – 12 students. The district has 115,000 students.

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

Customers Impacted: Approximately 115,000 students and 7,300 teachers

How it Could Affect Your Customers' Business: Ransomware can unleash extreme devastation, going beyond stealing data to shutting down an organization's operations completely.

Belden

https://www.securityweek.com/belden-discloses-data-breach-affecting-employee-business-information

Exploit: Unauthorized Database Access

Belden: Signal Transmission Solutions Manufacturer

Risk to Business: 1.992 = Severe

An unauthorized user gained access to at least one database full of employee and client information. The company noted in a statement that attackers apparently accessed a “limited number” of Belden’s file servers, but the firm said the breach did not have any impact on production in manufacturing plants, quality control, or shipping.

Individual Risk: 1.990 = Severe

The company went on to state that filched employee information may have included names, birthdates, government-issued identification numbers (for example, social security / national insurance), bank account information of North American employees on the Belden payroll, home addresses, and email addresses. potentially compromised information for business partners includes bank account data and tax ID numbers.

Customers Impacted: Unknown

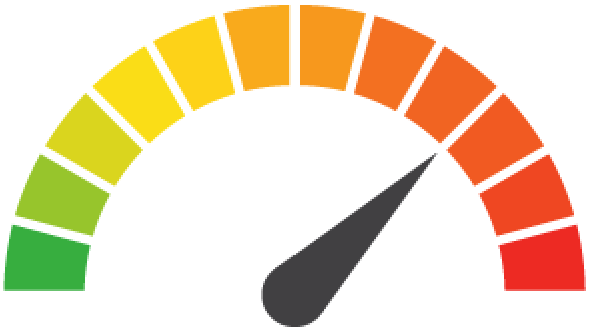
How it Could Affect Your Customers’ Business: Password compromise is often the culprit behind an intrusion like this, and that’s a matter that needs to be taken seriously in order to prevent this kind of drama.

Spotify

https://blog.malwarebytes.com/reports/2020/11/spotify-resets-some-user-logins-after-hacker-database-found-floating-online/

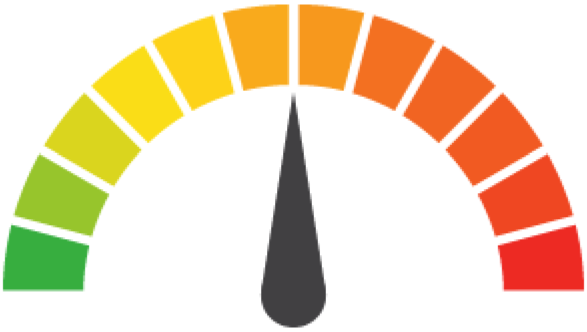
Exploit: Credential Stuffing

Spotify: Digital Music Streaming Service



Risk to Business: 1.992 = Severe

Spotify ended up with egg on its face last week after security researchers uncovered an unsecured Elasticsearch database containing more than 380 million records. The exposed data contained login credentials and other information belonging to Spotify users. The researchers in concert with Spotify investigators determined that whoever owned the database had probably obtained the login credentials from an external site and used them on Spotify accounts in a credential stuffing operation.



Individual Risk: 2.801 = Moderate

The data that was exposed includes customers' usernames and passwords for Spotify, as well as email addresses and countries of residence. Information like this could be used to fuel spear phishing attempts. Spotify users should reset their passwords.

Customers Impacted: 80,000

How it Could Affect Your Customers' Business: Credential stuffing is a threat that becomes more serious every day as new dumps of passwords hit the Dark Web. If you're not watching for potential trouble, you're leaving your business open to disaster.

LSU Health New Orleans

https://www.infosecurity-magazine.com/news/louisiana-hospitals-report-data/

Exploit: Unauthorized Systems Access

LSU Health New Orleans: Medical System

Risk to Business: 1.802 = Severe

A major attack on another healthcare target, LSU Health New Orleans disclosed that an unauthorized intrusion into an employee email inbox occurred on September 15, 2020. The mailbox access was discovered and disabled on September 18, 2020, but not before sensitive information was potentially snatched about patients who received care at Lallie Kemp Regional Medical Center in Independence; Leonard J. Chabert Medical Center in Houma; W. O. Moss Regional Medical Center in Lake Charles; the former Earl K. Long Medical Center in Baton Rouge; Bogalusa Medical Center in Bogalusa; University Medical Center in Lafayette; and Interim LSU Hospital in New Orleans.

Individual Risk: 1.616 = Severe

Data exposed in the attack may have included patients' names, medical record numbers, account numbers, dates of birth, Social Security numbers, dates of service, types of services received, phone numbers and/or addresses, and insurance identification numbers. The type and amount of patient information compromised in the incident varied and a limited number of exposed emails may have contained a patient's bank account number and health information including a diagnosis. Patients treated by LSU health New Orleans should be alert to potential identity theft and spear phishing risks.

Customers Impacted: Unknown

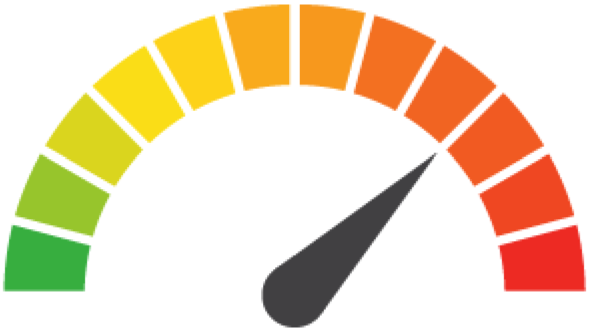
How it Could Affect Your Customers' Business: Controlling access to your company's systems and data is even more important when the data that you're storing is especially sensitive and its exposure could incur major penalties.

Sophos

https://www.zdnet.com/article/sophos-notifies-customers-of-data-exposure-after-database-misconfiguration/

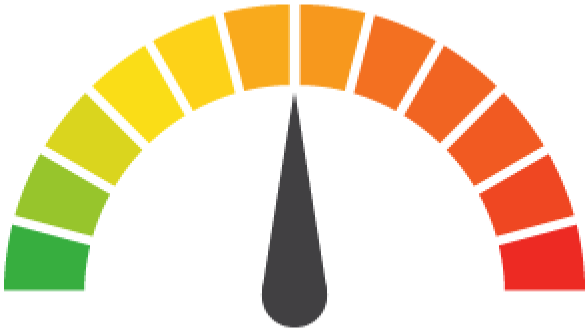
Exploit: Misconfiguration

Sophos: Cybersecurity Provider



Risk to Business: **2.336 = Severe**

A misconfigured database with access permission issues is to blame for the exposure of client data at Sophos. The company stated that the exposed database was used to store information on customers who have contacted Sophos Support. This is the second major security incident Sophos has dealt with this year.



Individual Risk: **2.772 = Moderate**

The database did not contain any sensitive information. Sophos disclosed that the exposed information included details such as customer first and last names, email addresses, and phone numbers. Clients should be alert to potential spear phishing risk using this data.

Customers Impacted: Unknown

How it Could Affect Your Customers' Business: No company can avoid occasional problems like this, whether they're caused by malfunctioning software or an employee misclick. Putting extra layers of security in place helps mitigate the damage of these troublesome security incidents.

US Fertility

https://securityaffairs.co/wordpress/111513/data-breach/ransomware-hits-us-fertility.html

Exploit: Ransomware

US Fertility: Specialty Medical Clinic Operator

Risk to Business: 2.229 = Severe

Ransomware disrupted operations at the largest provider of fertility services in the US after a number of servers and workstations became encrypted by ransomware. While US Fertility was able to restore operations quickly, the healthcare company determined that some patient data had been exfiltrated in the incident.

Individual Risk: 2.312 = Severe

Cybercriminals were able to steal an indeterminate number of files containing patient information including names, addresses, dates of birth, MPI numbers, and for some individuals Social Security numbers. Clients should be alert to the possibility of spear phishing and identity theft using this data.

Customers Impacted: Unknown

How it Could Affect Your Customers' Business: Ransomware is a huge threat to healthcare targets right now, as was disclosed in a recent CISA alert. Healthcare sector businesses need to be alert to the danger and using their resources wisely to combat it.