Breach Exposes at Least 58 Million Accounts, Includes Names, Jobs, and More:

Summary:

Poorly secured databases belonging to the data storage and data hosting company Modern Business solutions were breached, leaking millions of records. Modern Business Solutions are using the open sources database software mongoDB which they did not secure properly. This major breach is exposing names , IP addresses, Birth dates, Gender, addresses, email addresses, vehicle data, and occupations of at least 58 million users but could be upwards to 260 million accounts according to Risk Based Security. According to Risk Based Security there have been over 2928 publicly disclosed data breaches this year, which adds up to about 2.2 billion records.

My thoughts:

There was a promoted comment on the bottom of this article from a user by the name of Jackattak that reads, “...I wonder how current the data was? Would be nice to know which businesses use Modern Business Solution so we could ascertain this information on our own...” I totally agree, the information about how current is the breached data, and what other business are affected by this data breach would be nice to know. According to the article they have released 34000 users out of the known 59 million users were informed via Have I Been Pwned? Which is a percentage of 0.0006% of users being informed and isn't good enough in my opinion. I know you must give the investigators time to assess the damages dealt but users have the right to know if their information has been compromised let alone stolen. I wish companies would do better at informing their affected users about breaches. I would be more inclined to forgive a company that informed me as soon as possible about a breach that may or has affected me because it gives me a chance to take the needed precautions like changing passwords, setting multi step authentication, and taking further precautions to protect myself. We all know the majority of people dont take simple precautions to protect themselves. The article states it pretty great, “a stark reminder of why it is usually a good idea to omit or falsify as much requested data as possible when registering with both online and offline services. It is also a good idea to use a password manager…” Those two suggestions are great suggestions.

The data breach was discovered by someone posting the exfiltrated data on three filesharing sites. There was an initial 58.8 million records posted, but the exposed records are expected to be up in the 260 million range of personal compromised data. The expected vulnerability is due to mis configurations of Modern Business Solution’s databases. The funny thing is the databases vulnerability wasn't a zero day, but a known vulnerability. I found an article warning about MongoDB misconfiguration security issues posted back on December 21nd of 2015. That is almost a year for Modern Business Solutions to discover the problem and fix the leak. Businesses need to be uptodate on current vulnerabilities and events. Especially with software that you are currently using within your business. It is better to learn from others mistakes rather than your own. According to databreach.net the breached data was put up for sale for 200 dollars; Also Modern Buiness solutions have taken down their contact information from their site. Like Professor Pogue said in his post not a big surprise. To me every single breach we have addressed in this class is the same story, just a different company. I am starting to see Professors point he made in his Webinar about how we aren't going to see further change without major events correlating with those changes. 2,928 publicly disclosed data breaches within the past year, wow…. I mean they state in the article that is 2.2 Billion records exposed. I have a feeling that these breaches are not going to stop any time soon.

References:

<https://www.riskbasedsecurity.com/2016/10/modern-business-solutions-stumbles-over-a-modern-business-problem-58m-records-dumped-from-an-unsecured-database/>

<https://www.databreaches.net/modern-business-solutions-leaky-bucket-provided-a-field-day-for-downloaders/>

<https://securityintelligence.com/news/mongodb-databases-may-be-exposed-by-security-misconfigurations/>