CERTES BLOG

DO WE NO LONGER CARE ABOUT DATA BREACHES?

HAVE DATA BREACHES BECOME COMMON PLACE?

CERTES NETWORKS Blog Post
September 2019

Data breaches comprised of large volumes of sensitive information being compromised, stolen, or held for ransom, not only seem commonplace today but the repercussions may not be widely understood by the broader public. And, as I talk to the average person on the street, most are not even aware that large data breaches have happened compromising their personal data and potential financial security.

The year 2019 was a landmark year for data breaches experiencing over 3,800 breaches, which is a 50% greater increase over the last four years, according to a report published by Risk Based Security.

Despite cybersecurity concerns, 89% of breaches are the result of outside attacks and primarily due to the failure of organizations to properly handle or secure information resulting in over 3.2 billion records being exposed as of August 2019.

Risk Based Security also points to the dangers of placing sensitive data in the hands of third parties, naming the American Medical Collection Agency (AMCA) breach, in which "hackers infiltrated AMCA's network and pilfered over 22 million debtors' records including data such as names, addresses, dates of birth, Social Security numbers and financial details" as a critical event. "These breaches can be more difficult to manage given the multiple parties involved and can also have more damaging consequences for the individuals whose data is exposed in the event," the report said, noting that the breach has severe consequences for AMCA, as the company "was forced into filing for bankruptcy protection a mere 2 weeks after news of the breach made headlines."

Moreover, ransomware attacks on businesses are up 365% in 2019 with cybercriminals targeting businesses instead of consumers hoping for the “big payout.”

"Cybercriminals are searching for higher returns on their investment, and they can reap serious benefits from ransoming organizations over individuals, who might yield, at best, a few personal files that could be used for extortion or identity theft," the report stated. "Encrypting sensitive proprietary data on any number of endpoints allows cybercriminals to put forth much larger ransom demands while gaining an exponentially higher chance of getting paid.”

(Continued on Page 2)

HAVE DATA BREACHES BECOME COMMON PLACE?

(CONTINUED)

As breaches, ransomware, phishing attacks and the like become all too common, there can be no more motivation than these recurring events to protect and encrypt data. With all of the cybersecurity technology and tools available today, why are these attacks becoming more prevalent and frequent? Are cybercriminals becoming more sophisticated or are they simply banking on the fact that most organizations think their data is safe when indeed it is not?

Any network can be hacked, but encrypting sensitive data, defining strong policies between applications and end-users, and enforcing these policies through enhanced visibility, lessens the likelihood that in the event of a breach, it can either be detected much earlier and/or the data hackers breach will be unreadable and useless.

Contact Certes Networks

300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108

Tel: 1(888) 833-1142
Fax: 1(412) 262-2574

info@certesnetworks.com
sales@certesnetworks.com

We offer an encryption solution that is simple, scalable and uncomplicated.