"From hackers to ransomware, governments byte back on cyberattacks"

Colin M. Battersby | Thursday, January 30, 2020

Vigilance in the cybersecurity world is only as strong as its weakest link, which is why the mere thought of anyone within any organization unwittingly clicking on an executable file in an email is enough to keep any low-key IT person awake at night.

The same trepidation holds true for those overseeing elections.

A person would have to have been buried underneath a mountain of discarded Commodore 64 computers for the past three years not to have known about Russia's purported role in attempting to influence the 2016 election, which was outlined in Robert Mueller's 448-page report to the U.S. Congress.

The coordinated meddling effort not only involved a sweeping disinformation campaign, but drilled down with hacks into the voter databases.

In Illinois, 76,000 registered voters' information — addresses, partial Social Security numbers, dates of birth and driver's license numbers — was compromised in a June 2016 data breach, according to a Chicago Times report.

Florida election computers were targeted through a Russian-engineered spearphishing scam, which involved the email appearing to be from a regular vendor, but containing a malicious Trojan virus. Hackers were able to gain access to at least one of that state's county election systems, according to a New York Times report.

Russian intruders reportedly made similar attempts on voting systems in all 50 states in 2016, national security experts said.

“The desire to interfere with our elections appears to be fairly well-established by other countries,” said Colin Battersby, data private security lawyer with the Bloomfield Hills-based firm McDonald Hopkins. Battersby specializes in counseling companies that have been victims of data breaches. Colin Battersby of McDonald Hopkins

“How they’ve done that appears to be an open question to a certain extent … So when there is a technically driven way of collecting votes, there is a possibility of messing with that,” Battersby added. “We’re talking about some issues of significance here. We’re not just talking about personal data anymore; we’re talking about the proper functioning of the country.”

Click here to read the full article from Corp!

Colin M. Battersby