U.S. Government Cybersecurity Ranks 16th Out of 18 Industry Sectors

Tags: NEWS & INDUSTRY Risk Management

7-8 minutes

The U.S. state and federal government's cybersecurity standing is ranked 16th of 18 industry sectors in a new report. This is a very small improvement on last year's comparable position, which was 18th out of 18; but it still paints a grim picture of public sector readiness to fight cybercrime and cyber espionage.

The 2017 U.S. State and Federal Government Cybersecurity report (PDF) was just published by SecurityScorecard, a firm that seeks to help business manage third- and fourth-party risk (the supply chain). It does this by collecting and analyzing subject data through its own data engine, ThreatMarket -- which uses 10 categories such as web applications, network security, DNS health, patching cadence and what it calls 'hacker chatter'.

SecurityScorecard is based in New York. It was founded in 2013, and raised $12.5 in Series A funding led by Sequoia Capital in 2015. Its stated mission is "to empower every organization with collaborative security intelligence."

For this report, SecurityScorecard analyzed more than 500 state and local government agencies, and compared the results, as a

group, to 17 other industry sectors. Although there has been a slight improvement over last year's results, government organizations are particularly weak in network security (13th), application security (11th), leaked credentials (12th), patching cadence (16th), endpoint security (17th), IP reputation (16th), and hacker chatter (18th).

Government is, however, performing well in three of the 10 categories: DNS health (2nd), social engineering (3rd), and cubit score (2nd). The cubit score is a measure of exposed administrative portals and subdomains. Nevertheless, the only two sectors performing worse than government overall are Telecommunications and Education. Surprisingly, perhaps, regulation doesn't put the heavily regulated industries at the top of the chart: transportation, healthcare and energy are all among the poorest performing industries, while financial services only ranks at fifth position.

Within the 500 government offices analyzed, the Federal Reserve, the Secret Service and the IRS are all -- reassuringly -- within the top ten performing agencies. In fact, among the larger organizations, the top four agencies are the IRS, the Congressional Budget Office, the Federal Trade Commission and the Defense Logistics Agency.

The report does not specify the poorest performing agencies -- in fact, the report rarely specifies individual agencies, more usually saying only 'federal agency', or 'county (or city) in [state]'.

Commenting on the report, Sam Kassoumeh, COO and co-founder at SecurityScorecard, said, "On an almost daily basis, the institutions that underpin the nation's election system, military,

finances, emergency response, transportation, and many more, are under constant attack from nation-states, criminal organizations, and hacktivists. Government agencies provide mission-critical services that, until they are compromised, most people take for granted. This report is designed to educate elected officials, agency leadership, as well as government security professionals about the state of security in the government sector."

In reality, however, reports like this can only provide indicators of overall security -- this one relies on the interpretation of external factors without being able to analyze the internal security. For example, in the leaked credentials category, Government ranks 12th out of 18. "SecurityScorecard," says the report, "maps the information [from password dumps] back to the companies who own the data or associated email accounts that are connected to the leaked information. By doing so, SecurityScorecard is able to assess the likelihood that an organization will succumb to a security incident due to the leaked information."

But it doesn't know the internal processes and controls of the organization concerned -- whether, for example, all passwords have been changed since the leak, or whether new multi-factor and behavioral authentication controls have been introduced.

Similarly, an organization's susceptibility to social engineering (here government scores well at 3rd out of the 18 sectors) is measured by monitoring social media practices to see how easy it would be to build an employee profile that can be phished or spear-phished. But this doesn't measure the existence or effectiveness of the organization's internal awareness training, nor any anti-spam or anti-phishing controls. A more accurate way to measure social engineering susceptibility would be to measure employees'

phishing clicks through simulated phishing attacks -- which SecurityScorecard cannot do.

This doesn't mean that the report has no value. It does -- but it should, perhaps, be taken with a pinch of salt. "I personally like this type of reporting and feel we need more such metrics," comments Martin Zinaich, the information security officer at the City of Tampa. "However, the efficacy of such is mixed."

He gives the example of a local TV station running the Qualys SSL scanner against a number of local governments. "One entity scored an F," he said. "So, the TV station ran a number of stories about them failing -- which of course caused political havoc."

The reality was different. "That failing score was based on support for an outdated cipher. Now SSL ciphers negotiate to the highest level both sides support. To have a material breach someone would have had to have an outdated browser and then a third party would have to perform a man-in-the-middle attack on that outdated connection. The reward of which would have probably been seeing a water bill." The danger comes in drawing black and white conclusions from insufficient data.

Zinaich believes it is all part of what he calls the "Security Theatre". At one level, the SecurityScorecard report is a sales pitch marketing the SecurityScorecard third-party risk service. But on another level, it also provides some genuine indicators of security posture that are valid provided they are treated as indicators rather than statements of fact. It is worth noting, for example, that rival third-party risk management company, BitSight, rated the federal government as "the second highest performing sector" out of six sectors in September 2015.

Kevin Townsend is a Senior Contributor at SecurityWeek. He has been writing about high tech issues since before the birth of Microsoft. For the last 15 years he has specialized in information security; and has had many thousands of articles published in dozens of different magazines – from The Times and the Financial Times to current and long-gone computer magazines.

Previous Columns by Kevin Townsend: