CSO

FEATURE

Hostile nations have breached U.S. infrastructure. But don't panic

For years, government officials and security experts have warned that the security of the nation's critical infrastructure is drastically porous – vulnerable to cyberattacks that could take down the entire energy grid. Those warnings have been tempered recently, but the possibility remains

By Taylor Armerding | Follow
CSO | Nov 5, 2015 8:18 AM PT

Don't worry too much. But don't be too happy either.

That seems to be the mixed message to Americans who rely on the nation's critical infrastructure for just about everything that defines modern life: Lights, heat, air conditioning, clean water, transportation, appliances, TV, the expanding Internet of Things (IoT) and, of course, social media.

There has been ongoing, sometimes fierce, debate for more than a decade about the likelihood of a cyberattack taking down the grid and other industrial control systems (ICS), not just for a few days or weeks, but for months or even a year or more.

Obviously, nothing of that scale has hit the nation yet. But the topic hit front pages and major TV news shows recently because retired ABC TV "Nightline" anchor Ted Koppel is now on tour promoting his new book, "Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath," in which he contends that not only is the nation's critical infrastructure vulnerable to cyberattacks, but that multiple hostile nation states have already breached those systems and that the U.S. has no plan in place to cope with a catastrophic attack. He told TV interviewers that he and his wife are concerned enough that, "we decided we were going to buy enough freeze-dried food for all of our kids and their kids."

Koppel began to research the subject after hearing multiple warnings from top government officials and private sector security experts about those vulnerabilities.

The 15 worst data security breaches of the 21st century

The warnings go back years, coming from people like former Secretary of Defense Leon Panetta, who said in 2012 that a major cyberattack could amount to a “cyber Pearl Harbor.” Panetta also said at the time that the U.S. was at “a pre-9/11 moment.”

James Lewis, director and senior fellow of the Technology and Public Policy Program at the Center for Strategic and International Studies (CSIS), told CBS’s “60 Minutes” in November 2009, that if major electrical generators went down, it would require three or four months just to order replacements.

“It's not like if we break one, we can go down to the hardware store and get a replacement,” he said.

Other officials say there is no reason to panic. Director of National Intelligence James Clapper, in a "statement for the record" less than two months ago before the House Permanent Select Committee on Intelligence, said he believes the chances of a “Cyber Armageddon” are remote.

But, he acknowledged ICS vulnerabilities to what sounded like death by a thousand cuts. “We foresee an ongoing series of low-to-moderate level cyber attacks from a variety of sources over time, which will impose cumulative costs on U.S. economic competitiveness and national security,” he said.

And he essentially admitted that U.S. infrastructure has been breached. “… foreign actors are reconnoitering and developing access to US critical infrastructure systems, which might be quickly exploited for disruption if an adversary’s intent became hostile,” he said.

Clapper named hostile nation states including Russia, China, Iran and North Korea, but especially Russia, which he said has developed the capability to remotely hack at least three ICS vendors, “so that customers downloaded malicious software designed to facilitate exploitation directly from the vendors’ websites,” he said.

Meanwhile, ICS-CERT (Industrial Control Systems Computer Emergency Readiness Team) reported in March that it had received reports of 245 ICS incidents in 2014, more than half of which were advanced persistent threats (APT).

And USA Today reported in September that cyber attackers had successfully breached the U.S. Department of Energy (DoE) 159 times between October 2010 and October 2014.

The bottom line, according to a range of experts, is that while Clapper is probably correct that a catastrophic attack is unlikely, it is very much possible.

As Chris Petersen, CTO and cofounder of LogRhythm, put it, "nation states like Russia know that to actually do something harmful would be considered an act of war by the U.S.

Chris Petersen, CTO and cofounder, LogRhythm

"However, just as Russia paraded mobile ballistic missiles during the Cold War, they are equally as interested in parading their cyber capabilities," he said, adding that most hostile nation states want their enemies to know about their capabilities, but would only use them in a worst-case situation – the cyber equivalent of a balance of terror.

Petersen and others have also said in the past that nation states like China and Russia want to get inside U.S. ICS less for destructive purposes and more for espionage and political leverage, as a deterrent against U.S. policies they find objectionable.

Alan Berman, president of DRI International, noted that "having access and doing damage are two very different consequences," of cyber intrusions.

1 | 2 | NEXT ›

Insider: How a good CSO confronts inevitable bad news ›

View 1 Comment

CSO

FEATURE

Hostile nations have breached U.S. infrastructure. But don't panic

For years, government officials and security experts have warned that the security of the nation's critical infrastructure is drastically porous – vulnerable to cyberattacks that could take down the entire energy grid. Those warnings have been tempered recently, but the possibility remains

By Taylor Armerding | Follow
CSO | Nov 5, 2015 8:18 AM PT

He cited the cyber espionage campaign named Dragonfly (aka Energetic Bear), which security vendor Symantec reported in 2014 had targeted U.S. and European energy firms. The attacks bore the, "hallmarks of a state-sponsored operation," it said.

"It appears that their mission has been information gathering," Berman said.

Alan Berman, president, DRI International

But that mentality may not apply with less stable nation states like Iran and North Korea, or terrorist groups like ISIL, which seem to be more interested in apocalyptic conflicts than simply maintaining their own national security.

And Joe Weiss, managing partner at Applied Control Solutions, said it is not just Russia and China that have the capability to breach U.S. systems. "The Iranians are very good at this," he said.

What is more worrisome to Weiss and others is that not much has changed to improve security of ICS in the past decade, even with the increase and sophistication of attacks.

The large majority of ICS facilities have hard-coded passwords, which can't be changed without modifying the entire program.

That is because, as Udi Yavo, cofounder and CTO of enSilo, put it, those systems were, "designed under the assumption that they would never be connected to other systems, including the Internet,"

and therefore, designers didn't "bake in the relevant security measures."

Petersen agrees. Since those systems were, "largely isolated, not connected to the Internet, they weren't designed for security since nobody could get to them without physical access," he said. "That has all changed. ICS are now connected to corporate networks that are connected to the Internet, and are remotely accessible."

And patching the vulnerabilities is close to impossible. "They act as a sort of Band-Aid, not fixing the root cause of the problem," Yavo said.

Udi Yavo, cofounder and CTO, enSilo

Also, what Lewis said six years ago is still true – major generators cannot be replaced quickly. "We're talking about nine to 18 months," Weiss said.

That doesn't mean the immediate future is hopeless, however.

Berman said there are both public and private-sector groups working on improving detection and response to cyber intrusions.

The Industrial Control Systems Joint Working Group (ICSJWG) provides a vehicle for communicating and partnering across all critical infrastructure sectors between federal agencies and departments, as well as private asset owners and operators of industrial control systems," he said.

The goal is cooperation that will alert utilities to known efforts by hackers.

Yavo said the key is to "reduce the attack surface. That includes disengaging connectivity between the critical systems and the Internet, limiting VPN access, enforcing two-factor authentication, etc."

Petersen said there has to be much more focus on monitoring ICS. "We have to get eyes on these systems and make sure we understand when attacked, if they become compromised, corrupted, or disrupted," he said.

According to Weiss, that isn't happening. "We don't have cyber forensics or logging," he said. "You can count on one hand the systems that are being monitored."

Weiss added that the problem is not just that ICS are connected to the Internet. "You can't blame everything on that," he said, noting that the Iranian nuclear facilities damaged by the Stuxnet attack were not online.

"The other problem is that they are networked, with remote access," he said.

The most obvious way to improve ICS security, Petersen said, is simply to do the basics. USA Today reported that an audit of the DoE last year found that 41 servers and 14 workstations used default or easily guessed passwords.

“If organizations would just take a reasonably balanced approach, risk could be dramatically decreased,” Petersen said. “Protect the perimeter, control access, and practice good password hygiene.”

Yavo said the basics are valuable, but won’t make an organization bulletproof either. “It’s not just passwords,” he said. “There are endless ways for a threat actor to enter an organization, such as enticing the user to open a seemingly legitimate file, which in fact contains malicious code. It’s important to understand that a dedicated threat actor is precisely that – dedicated.”

Weiss said another incentive might be even more compelling – pressure from Wall Street.

“One of the major stock rating agencies is now looking at cyber security,” he said. “I talked with one of them a few weeks ago. You want it taken seriously? Have Moody’s start downgrading their stock.”

Taylor Armerding

PREVIOUS | 1 | 2

Insider: How a good CSO confronts inevitable bad news >

View 1 Comment