Russian hackers infiltrated utility control rooms, DHS says

Dive Brief:

- Russian hackers infiltrated the control rooms of multiple electric utilities over the past year, gaining the ability to cause blackouts and grid disruptions, officials from the Department of Homeland Security said on a Monday web briefing.

- Hackers were able to breach isolated, "air-gapped" utility networks thought to be secure, officials said, and "got to the point where they could throw switches" on the grid to disrupt power flows. The attacks claimed "hundreds of victims," more than the dozens DHS has previously acknowledged.

- The hackers accessed utility networks by compromising vendor companies who do business with the utilities, officials said. The attacks began in 2016, continued through last year and are ongoing.

Dive Insight:

Electric utilities are under constant attack from both independent and state-affiliated hackers, which have infiltrated power control systems in the U.S. and even disrupted the delivery of electricity in places like Ukraine.

The DHS briefing on Monday, however, is the latest indication of the scope of the cyber threats against the U.S. utility sector, revealing new information on the effectiveness of the hackers.

Infiltrators exploited the relationship between utilities and their private vendors that supply critical software and communications technologies to run the grid, administration officials said. The hackers used relatively common techniques — like spearfishing emails — to steal credentials from these companies and gain access to utility networks thought to be secure.
Once in a utility system, hackers began collecting information on how the company operates its grid, from the configuration of its networks to what grid equipment is utilized in different situations. The goal, officials said, is for hackers to "learn how to take the normal and make it abnormal." Some utilities may not know they have been compromised, officials said, because hackers commonly stole the information of actual vendor employees to access utility systems. But the attacks are ongoing, they emphasized, and the latest round could preview an increase in hacking activity as attackers learn how to automate their operations.

Not all cybersecurity experts agreed on the severity of the threat, as first reported in the Wall Street Journal. "Messaging in the WSJ article around “throwing switches” and causing “blackouts” is misleading on the impact of the targeting that took place," Robert Lee, CEO of cybersecurity firm Dragos, said in an emailed statement. "What was observed is incredibly concerning but images of imminent blackouts are not representative of what happened which was more akin to reconnaissance into sensitive networks."

The DHS and other federal agencies have been warning against cyberthreats to the utility system since 2014, but the discussion has taken on a new dimension in the Trump administration, as the White House argues that keeping uneconomic coal and nuclear plants online is necessary to guard against potential disruptions to the interstate pipeline system that serves natural gas plants.

Critics, including sitting members of the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC), say the pipelines are no more vulnerable than other power equipment. The latest round of attacks could bolster that argument, as they targeted utility control systems that operate all types of grid infrastructure.

Instead of subsidizing older plants, FERC and NERC have pushed utilities and their vendors to boost their reporting of cyberthreats on their systems. Just this month, FERC directed NERC to expand the criteria under which utilities must report an attack to federal authorities, including attempted breaches of reliability protocol in addition to successful attacks.

FERC Chairman Kevin McIntyre said the modified standard "will improve awareness of existing and future cyber security threats."

Utility companies themselves are also acutely aware of the hacking threat, with sector executives naming cybersecurity as a top concern in Utility Dive's last two annual sector surveys. In 2018, 81% of more than 600 utility professionals listed cybersecurity as either important or very important — a jump from 72% the year before — and the vast majority of companies have taken some steps in recent years to beef up cyber security.