Iran new york electric grid

Iran new york electric grid

Russia hit critical electricity transmission facilities linked to nuclear power plants ...

Iran wants to avoid a shooting war following the United States' assassination of a top military leader, making domestic cyberattacks "almost a foregone conclusion," according to one expert.

As tensions between the United States and Iran rise, observers say the Middle Eastern nation is likely considering a reprisal attack on critical domestic infrastructure -- putting the utility sector square in the "crosshairs" of an international conflict.

The United States military last week killed Iran Maj. Gen. Qasem Soleimani with a drone strike, heightening tensions in the region. Cybersecurity experts say Iran wants to avoid a "shooting war" and over the years has developed its cyber capabilities to the point where an attack on several sectors is possible.

"The two most likely types of responses are an overseas terrorist attack or a domestic cyberattack. I think a domestic cyberattack is the most likely of all scenarios," Jamil Jaffer, vice president for strategy and partnerships at IronNet Cybersecurity, told Utility Dive.

Jaffer said Iran has for years been probing and studying several sectors, including the electric sector, oil and gas, financial services, healthcare and government.

"We know Iran has the capabilities to deliver destructive attacks. They have a strong set of capabilities," Jaffer said. "They are now very much a top-tier threat."

Iran"s capabilities are not equal to the U.S. or Russia but are more along the lines of North Korea, according to experts. And the country has a history of taking action.

In 2016, Iran executed a cyberattack on a New York dam. Before that, in 2014, the nation levied a cyberattack on the Las Vegas Sands casino.

"There is ample evidence to suggest that Iranian-sponsored actors have invested considerable time and effort over the past several years to infiltrate the computer systems that control the critical infrastructure of the United States and its allies," PAS Global COO Mark Carrigan said in an email. "At some time these actors may leverage a successful infiltration to launch a cyber attack."

Richard Henderson, head of global threat intelligence at cybersecurity firm Lastline, said it is "almost a foregone conclusion that we will now see retaliatory cyber attacks on U.S. assets by Iran."

Iran new york electric grid

Industrial control systems (ICS) which help manage the electric grid"s flow of power were identified as a potential weakness in a September assessment from the U.S. Government Accountability Office. An ICS attack was the cause of a major 2015 blackout in Ukraine, and experts say growing digital networks will exacerbate that risk.

Contact us for free full report

Web: https://www.kary.com.pl/contact-us/
Email: energystorage2000@gmail.com
WhatsApp: 8613816583346