Van Ness Feldman LLP
vnf.com

Escalated Tension with Iran Heightens Cybersecurity Threat Despite Military De-Escalation

JANUARY 08, 2020

Gwen Keyes Fleming, Lilly Scott, Darsh Singh, T.C. Richmond, and Tracy Tolk

The recent conflict between the United States and Iran has heightened America's long-time concern of an imminent, potentially lethal Iranian cyber-attack on critical infrastructure in America. The team at Van Ness Feldman (VNF) is closely monitoring this evolving situation and its potential implications for our clients. Below, is the latest information including the United States Government's analysis on the current standing of these threats as of January 8, 2020.

CISA Alert

The U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) issued Alert (AA20-006A) in light of "Iran's historic use of cyber offensive activities to retaliate against perceived harm." In general, CISA's Alert recommends two courses of action in the face of potential threats from Iranian actors: vulnerability mitigation and incident preparation. The Alert specifically instructs organizations to increase awareness and vigilance, confirm reporting processes and exercise organizational response plans to prepare for a potential cyber incident. CISA also suggests ensuring facilities are appropriately staffed with well-trained security personnel who are privy to the tactics of Iranian cyber-attacks. Lastly, CISA recommends disabling unnecessary computer ports, monitoring network and email traffic, patching externally facing equipment, and ensuring that backups are up to date.

Iranian Threat Profile

CISA asserts that Iranian cyber actors continually improve their offensive cyber capabilities. These actors are also increasingly willing to engage in destructive, kinetic, and even lethal cyber-attacks. In the recent past, such threats have included disruptive cyber operations against strategic targets, including energy and telecommunications organizations. There has also been an increased interest in industrial control systems (such as SCADA) and operational technology (OT). Refer to CISA's Alert and the Agency's "Increased Geopolitical Tensions and Threats" publication for specific Iranian advanced persistent threats to the nation's cybersecurity.

Imminence of an Iranian Cyber-attack

While CISA urges vigilance and heightened prudence as it pertains to cybersecurity, DHS has been clear that there is "no information indicating a specific, credible threat to the Homeland." Nevertheless, the same National Terrorism Advisory System Bulletin publication (dated January 4, 2020) warns that Iran maintains a robust cyber program. This program can carry out attacks with varying degrees of disruption against U.S. critical infrastructure. The bulletin further states that "an attack in the homeland may come with little to no warning." There is also a concern that homegrown violent extremists could capitalize on the situation to launch individual attacks. With the ongoing tension, it is unlikely that the imminence of an Iranian cyber-attack will dissipate in the near term.

Van Ness Feldman LLP
vnf.com

Implications

It is vital for businesses, especially those deemed critical infrastructure, to stay apprised of new developments on these matters. Given that the Alert calls for organizations to take heightened preventative measures, it is imperative that critical infrastructure entities revisit their cybersecurity protocols and practices and adjust them accordingly. A deeper understanding of the organizational vulnerabilities in relation to this particular threat will be imperative. VNF's cybersecurity team is prepared to advise clients on the impact of CISA's Alert on their business practices and help clients navigate the implementation of heightened protocols. With the status of this threat changing at a rapid pace, we are closely monitoring developments related to cybersecurity and geopolitical activity to help protect our clients' interests.

FOR MORE INFORMATION

For more information or to learn how VNF can help you bolster your cybersecurity, please contact any member of our cybersecurity team in Seattle (206) 623-9372 or Washington, D.C. (202) 298-1800.

Follow us on Twitter @VanNessFeldman