

SECURING U.S. UTILITIES

PUBLISHED
3 March 2018

CATEGORY
Terrorism

TERRORISM · MARCH 2018

Securing U.S. Utilities

Compared to many other industries – e.g., medical, retail, and finance for example – the energy industry is rather new to interconnectivity. As with other industries, as connectivity increases – think of push for a so-called smart grid – the security risks will, likewise, continue to grow. Unlike many other industries, utilities, as an especially critical part of a nation's infrastructure, are extremely valuable targets for cyberattacks – especially by perpetrators looking to either cripple a country/region or to make a political statement. By undertaking a phishing attack or through the exploitation of unknown or unpatched system vulnerabilities, perpetrators can remotely gain access to a utility's internal control network and, subsequently, lock local operators out and either sabotage or partially sabotage the utility itself or simply hold it hostage and shut off power to customers. On any scale, such attacks would be significant; however, if done on a larger scale, a state actor could potentially cripple an adversary. If done during a conflict, such an action could, potentially, be a determining factor in the outcome of conflict.

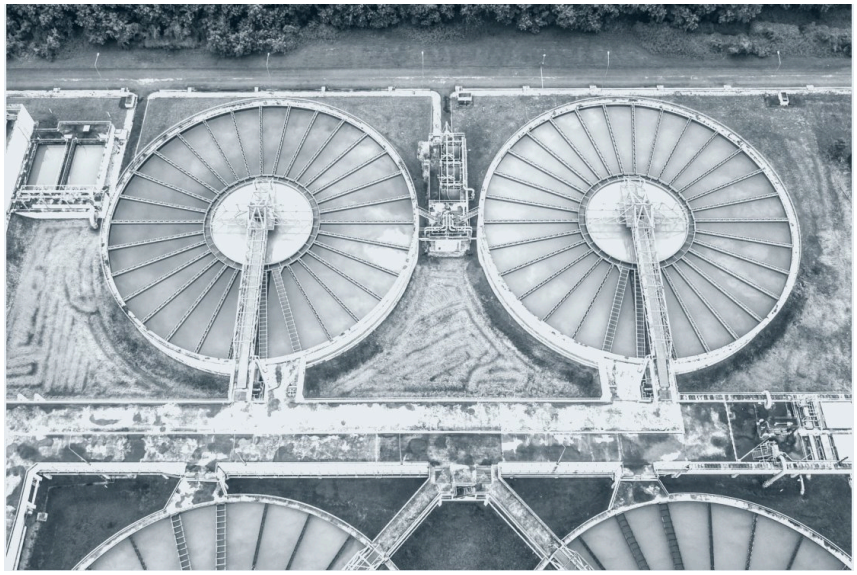
Such claims are not mere speculation; indeed, in December of 2016, an attack with a malware agent later named CrashOverride caused a massive disruption in the city of Kiev, Ukraine that shut down power to 1/5 of the populace for an hour. One year prior, in December of 2015, another attack occurred in Ukraine that hijacked the supervisory control system and locked the operators out of controlling the system. While not a utility, although illustrative of the potential damage that can be done through cyberattacks, in 2015, there was an attack that caused physical damage to a steel mill in Germany.

Security experts – in conjunction with public authorities and utility companies – have been working to increase preparedness amongst utility companies by working to ensure that adequate security systems and controls exist. For example, some utilities are using systems developed by cybersecurity firm Dragos to proactively monitor for threats and to, when necessary, alert personnel. As example, the utility Duke Energy created an incident and security team that is tasked with cybersecurity 24 hours a day, and, moreover, Duke collaborates regularly with emergency management and law enforcement officials. Some states have also implemented requirements that utilities implement risk assessment and mitigation programs to decrease the risks of significant damage from being caused by a successful attack. In New Jersey, for instance, such plans must also include training and recovery plans. In other states, Texas as an example, yearly security audits are conducted.

Officials expect that such threats and attacks will continue as their value as a political tool are demonstrated. As an example, in fiscal year 2014, it was found that 32% of reported cybersecurity incidents were related to the energy industry. Additionally, in 2017, it was found that Russian hackers were able to use stolen credentials to familiarize themselves with the control systems of American utility systems. While the threat will continue, it is, likewise, true that efforts by authorities and private parties will continue to assist utilities in preparing to mitigate such threats and to control the risk of damage being caused. It is increasingly evident that such attacks will become a vital tool for the exercise of military power in the coming years.

© 2018 ThreatRate Risk Management. All Rights Reserved

There is a projected shortage of 1.8 million cyber-professionals globally by 2022, according to a 2017 study by the Center for Cyber Safety and Education.



https://www.bna.com/utilities-prepare-increased-n73014481471/

Soundbite analytics

- 83% of surveyed security professionals stated they believe that attacks on critical infrastructure by nation-states will continue.
- 93% of those surveyed believe more attacks by nation-states are going to occur.
- 69% of those surveyed said their organizations have increased efforts to defend against nation-state attacks.
- Only 18% of surveyed organizations asserted that they were unprepared.

SOURCES

1 https://rtoinsider.com/naruc-dragos-cybersecurity-scada-86882/

2 https://forbes.com/sites/constancedouris/2018/01/16/as-cyber-threats-to-the-electric-grid-rise-utilities-regulators-seek-solutions/#36a617f1343e

3 https://schneider-electric.com/en/work/insights/cyber-security-how-utilities-can-reduce-threat.jsp

4 https://www.infosecurity-magazine.com/news/russian-hacking-campaign-on-us/

© 2018 ThreatRate Risk Management. All Rights Reserved



Risk intelligence that keeps you safe

ABOUT THREATRATE

ThreatRate helps you benchmark your risk management strategy against rapidly evolving global and local trends, with real-time, actionable analytics and insights.

For more information contact us at

info@threatrate.com

MEMBERS HAVE ACCESS TO

100+
risk-focused reports published annually

API
customised access option

Dashboards
customised dashboards and infographics

Experts
ThreatRate analysts with cross-industry depth

© 2018 ThreatRate Risk Management. All Rights Reserved

ThreatRate RISK MANAGEMENT