Hacker Lexicon: What Counts as a Nation's Critical Infrastructure?

Author: Kim Zetter.Kim Zetter Security
WIRED | 2016-02-16

As the US government contemplates the recent hack of Ukraine's power grid, which is only the second hack of this kind against critical infrastructure since the Stuxnet attack against Iran's nuclear program was discovered in 2010, the implications for the US power grid are clear.

"[E]very bit of this is doable in the US grid," Robert M. Lee, a former Cyber Warfare Operations Officer for the US Air Force and co-founder of Dragos Security, a critical infrastructure security company, told WIRED about the hack.

Critical infrastructure is in the spotlight more than ever in the wake of Stuxnet, as it's become clear that many important systems used to keep society operating and healthy—water plants, power-generation plants, oil refineries—have vulnerable systems that, in some cases, are accessible to hackers over the Internet.

But just what is considered critical infrastructure these days?

TL;DR: Critical infrastructure is any system or facility that has high importance to the safety and operation of the country. The government has identified sixteen industries that meet this criteria, a categorization that includes not only water and power plants but also, to the surprise of many, Hollywood motion picture studios like Sony.

In broad terms, critical infrastructure refers to any system of high importance to the safety and operation of the country. Most people assume this applies to power plants, water treatment facilities and other utilities–such as what was hacked in both the Stuxnet attack the Ukrainian attack. But in truth, the government's definition encompasses a wide swath of industries and facilities.

The U.S. government has actually defined sixteen sectors of critical infrastructure that are important to the functioning of the country and therefore could be at risk of sabotage. Broadly categorized, the industries include: chemical, communications, commercial facilities, critical manufacturing, dams, defense industrial sector, emergency services response and recovery, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors and materials, transportation systems, water and wastewater systems.

On the surface, most of these don't seem controversial. But many people were surprised to learn after the Sony hack in 2014 that the government considered the entertainment company to be critical infrastructure, since motion picture production studios fall into the same protected category as commercial facilities like hotels, amusement parks, convention centers and sports stadiums. Not everyone agrees with the government's assessment.

"This strikes me as faintly ludicrous," Paul Rosenzweig, former deputy assistant secretary for policy in the Department of Homeland Security, wrote after learning that Sony was considered critical infrastructure. "America will not collapse if Hollywood is dark. If everything is critical, then nothing truly is critical."

If everything is critical, then nothing truly is critical. Paul Rosenzweig

The definition of critical infrastructure is important, because although many of the facilities that fall under this definition are owned by private parties, the government has committed to protecting CI from attack. “The common defense of privately-owned critical infrastructures from armed attack or from physical intrusion or sabotage by foreign military forces or international terrorists is a core responsibility of the Federal government,” the president’s cybersecurity report stated in 2009. This includes attacks conducted in the digital realm.

We got a hint of how important the government considers its role in protecting critical infrastructure to be when President Obama signed an executive order in 2015 allowing the government to levy economic sanctions against individuals overseas who engage in destructive cyberattacks or commercial espionage.

Sanctions can be levied only for significant attacks that meet a certain threshold of harm. They must, for example, directly hurt the “national security, foreign policy, economic health or financial stability of the United States,” according to the president’s announcement. But the damage threshold could be met by the disruption of computer networks through widespread DDoS attacks, or through the theft of financial data, trade secrets or intellectual property in a way that harms the nation’s economic stability. The sanctions can, of course, only be applied when the government is able to attribute the attacks to a specific nation or entity, but they wouldn’t be applicable only to parties engaging directly in the cyberattacks and theft. The order also allows the government to apply sanctions against individuals and entities who knowingly use and receive data stolen in such attacks. This could apply, for example, to a company that hires hackers to steal data from a competitor to gain a market advantage or purchases stolen data after the fact.

What all of this means with regard to pre-emptive protection for critical infrastructure facilities is unclear. Since most critical infrastructure is in the hands of the private sector, the government cannot impose itself on these industries or mandate that they take certain security measures. There is an exception to this—the handful of industries that are government regulated, such as the financial, health and nuclear industries. All the government can do for other industries that are not regulated is advise best practices, share threat intelligence with them, and provide forensic and recovery assistance after an attack. The government can also use its intelligence powers to spot attacks that are in the works and ward them off, though the nature and limits to what the government can do in this regard are still murky.

This doesn’t mean that companies can’t take steps on their own to protect the critical infrastructure we all rely on. The hackers who got into power distribution centers in Ukraine last December and turned off the lights to more than 230,000 customers were able to do this because there were few barriers in place to prevent them from jumping from the Internet-facing corporate networks of the distribution centers to the critical production networks where workers controlled the power grid. As Lee told WIRED after the attack, US systems are just as vulnerable to the same kind of attack.

Go Back to Top. Skip To: Start of Article.

read:http://www.wired.com/2016/02/hacker-lexicon-what-counts-as-a-nations-critical-infrastructure/