INSIGHT

In Germany, Another Cyber Weapons Test?

Author: Samuel S. Visner, Senior Vice President and General Manager, Cybersecurity, ICF International

While last year's Sony hack garnered global attention, another, more ominous cyber attack took place at a steel mill in Germany. As described by numerous news outlets, the annual report of the country's Federal Office for Information Security detailed the attack, which appeared to interfere with the computer-based industrial control system for a blast furnace at the mill. The furnace was reportedly rendered impossible to shut down normally, resulting in substantial, and possibly irreparable, damage. Just as in the Sony case, a real threat was demonstrated. The difference in Germany was the ability to reach and control a physical asset, not just gain access to information.

In the past, industrial control systems were considered protected by air gapping and even by the very specialized nature of their purpose. Many such systems were proprietary, and by definition, the range of threats was narrow. In an interconnected world (the Internet of Things), the set of players with the means and motives to do harm is broadening. A short list of possible culprits for events like the one reported in Germany includes foreign intelligence agencies, criminals, activists, and competitors.

In reality, the act is almost more important than the perpetrator. The operational sophistication of the German attack displays targeted intent, thorough planning, sufficient resources, and effective reconnaissance. The attacker was disciplined, persistent, and deliberate.

So, was this another weapons test? Certainly, it appears the attacker was testing and validating the ability to control a physical asset through interconnected systems. Equally certain: We should expect more attacks of this kind. A cyber attack on a German steel mill could be considered a relatively low-risk data-gathering exercise. Had a similar attack happened within U.S. infrastructure, the threat of retribution would be much higher.

For companies with industrial control systems as part of their operations networks, knowing this threat is credible presents a window of opportunity. Control systems must be protected like every other IT system—with robust network monitoring, threat detection, and incident response—especially in machine-to-machine systems.

We tend to worry more about data theft than data integrity, but a cyber attack on a physical asset demonstrates why monitoring is so critical and must be continuous. Spotting outlier data on a report after the fact is not good enough. In the real world, consequences happen too quickly.

We need to be prepared for most incidents like the one in Germany and, when the occur, learn everything we can from them. Our learning curve must be faster than that of the perpetrators if we are to achieve the level of security our society requires.

About ICF International

ICF International (NASDAQ:ICFI) provides professional services and technology solutions that deliver beneficial impact in areas critical to the world's future. ICF is fluent in the language of change, whether driven by markets, technology, or policy. Since 1969, we have combined a passion for our work with deep industry expertise to tackle our clients' most important challenges. We partner with clients around the globe—advising, executing, innovating—to help them define and achieve success. Our more than 5,000 employees serve government and commercial clients from more than 70 offices worldwide. ICF's website is www.icfi.com.