Defending Within: How to Protect Companies from Advanced Cyber-Security Threats

Many companies and organizations have set up defenses to keep hackers on the outside, protecting the information of their customers and clients. However, with increasingly sophisticated use of malware, some hackers can sit silently within a company’s information systems for years without being detected.

A new report from the Temple University Institute for Business and Information Technology (IBIT), at the Fox School of Business, examines advanced persistent threats to information assets by using the medieval analogy of barbarians inside the gate.

In December 2013, retail chain Target announced a security breach resulting in 40 million credit and debit card records being compromised. Other retail chains such as 7-Eleven and Carrefour have also suffered attacks, having 160 million credit and debit card numbers exposed. Hackers have also targeted Nasdaq and bank accounts at Citigroup and PNC.

“My goal with the article was to raise people’s awareness, which is the most powerful tool [for security enhancement],” said Gregory Senko, associate director of the Fox School’s Master of Science in Information Technology Auditing and Cyber-Security program. “I wanted to make people aware that there is a risk and they need the proper tools to know when they are being attacked.”

While working on a book, Security Intelligence – How Big Data and Machine Learning can tackle the increasingly complex world of Cyber Security, Senko realized that the rate of persistent polymorphic attacks is growing and that more vendors are developing tools intended to address these threats.

Symantec, a leading information security company, noted the escalated rate of reported Advanced Persistent Threats (APT). In November 2013, the number of reported APT attacks increased to about 118 from only 57 in November 2012. “We’re likely to see a big wave of aggressive attacks,” Senko said.

The Stuxnet virus in 2010-11 served as the first well-publicized appearance of a successful, state-sponsored act of modern cyber warfare. This virus inspired hackers to employ analytics, reverse engineering and code cannibalization to design malware that was able to circumvent traditional security arrangements that recognize threats as patterns
in digital transmissions. This allowed hackers to penetrate networks that seemed secure, operating stealthily over extended periods of time. These attacks are known as Advanced Persistent Threats.

Senko recommends four transformative steps to achieve even more robust enterprise security.

First, he urges companies to strengthen their fundamental security processes. This means spending money to pay for up-to-date perimeter security and employing well-educated security engineers and well-informed employees.

Second, Senko recommends companies to look at metrics used for performance management, issue identification and problem mitigation, from a more security-oriented perspective. According to the report, “this same data may yield opportunities to identify subtle changes in activity that underlie a persistent attack.”

Third, a culture must be created that promotes information security organizations to act proactively. Procedural and structural approaches to deal with day-to-day prevention need to be set in place, versus waiting to react to emergencies.

Finally, Senko suggests companies should invest in tools such as cloud-based, Big Data-driven offerings that allow for more enhanced network performance management and improved network management.

“Companies will find this preventive approach can be expensive. But they will end up dealing with the problem sooner or later. The question is: Will spending now avoid even greater spending later if they don’t take steps to protect themselves,” Senko said.

The ongoing IBIT Report series is based on rigorous, vendor-neutral academic research that provides actionable knowledge on topics relevant to industry partners. To download Senko’s full report, visit http://ibit.temple.edu/blog/2014/02/20/barbarians-inside-the-gate-dealing-with-advanced-persistent-threats/

—Alexis Wright-Whitley