New York Law Journal

SERVING THE BENCH AND BAR SINCE 1888

WWW.NYLJ.COM

An ALM Publication

VOLUME 258—NO. 83

MONDAY, OCTOBER 30, 2017

Outside Counsel

Expert Analysis

Vulnerability Management: A Holistic View

By
Anthony J. Ferrante

When the Petya cyberattack was launched in June of this year, just on the heels of the massive WannaCry ransomware outbreak, thousands of computers across the globe were hit, disrupting worldwide business. The campaign, which a NATO cybersecurity group said was likely launched by a state actor, left companies around the world reeling. International companies confirmed that even months after the attack, their systems were not completely recovered. Systems at TNT Express, a Dutch shipping company, may never be fully restored, according to statements from its parent company FedEx.

These attacks were capable of such damage because they took advantage of known vulnerabilities to impair, or even destroy, networks. From this, we have learned that our ability to protect our networks requires a complete understanding of the vulnerability ecosystem. To understand this concept, we have to first define vulnerability as distinct from risk or threat. The term vulnerability refers to security flaws in a system that permit an attack to be successful. Complementarily, a patch is a piece of software designed to update a computer program or its supporting data, to fix or improve it; this most often including fixing security vulnerabilities.

It is generally agreed that both of the attacks mentioned above used the "EternalBlue" vulnerability in Microsoft's Windows operating system. This vulnerability works by exploiting the Microsoft Server Message Block 1.0, a network file sharing protocol, and allows applications on a computer to read and write to files and request services that are on the same network. Microsoft issued its patch for the flaw on March 14, before either attack. Theoretically, customers who properly installed this patch when issued were protected against these attacks.

The vulnerability became broadly known when the Shadow Brokers, a hacker group, published several leaks containing hacking tools claimed to be from the National Security Agency (NSA). The exposure of these sophisticated exploits revealed previously undisclosed vulnerabilities in enterprise firewalls, anti-virus products and Microsoft products. While Microsoft developed a timely patch to address this specific vulnerability, adoption of the patch was not universal, thus many networks around the globe were left susceptible to attack. The imperfect adoption of patching also demonstrated that networks are often only as strong as their weakest link—in the Petya attack, ransomware was able to laterally infect patched machines within networks once it gained entry through a single unpatched computer.

> We have learned that our ability to protect our networks requires a complete understanding of the vulnerability ecosystem.

At a high level, business leaders must plan for continuous improvement as part of their information technology investment, as well as restorative measures when improvements are not adequate to restore business operations. Business leaders should also recognize that many modern workplace conveniences are increasing the vulnerability exposure of their business networks. For example, often the devices or equipment of remote employees are not maintained as securely as devices that remain on-site at the business. Further, third-party

ANTHONY J. FERRANTE *is a senior managing director at FTI Consulting and is based in Washington, D.C. in the global risk and investigations practice (GRIP) of the forensic and litigation consulting segment.*

systems, like infrastructure providers for the business, can also increase vulnerabilities by exposing your network to broad, lateral access for a supposedly trusted purpose.

Improved network security also demands the implementation of proactive vulnerability assessments. These assessments should include ranking and prioritizing the sensitivity of various systems within the network, auditing existing security tools, performing vulnerability scans, and remediating based on the findings of the assessment. When known vulnerabilities arise, it is critical to protect against them quickly and aggressively. Assessment results can also help frame risks in context of industry-specific issues, in a way that is meaningful to key stakeholders within the organization, to ensure ongoing support for cybersecurity initiatives from organizational decision makers.

While these attacks have underscored the importance of remaining on the cutting edge of possible threats, the darker side of the story is the briefly referenced origin of the vulnerability and its exposure around the world—the purported exploitation of the vulnerability by the NSA, and the exposure of this by the Shadow Brokers hacking group. This aspect of these incidents has renewed attention on cybersecurity amongst lawmakers, and new legislation has been introduced by Congress to purportedly increase transparency in the U.S. government's process for disclosing flawed or vulnerable code that may be found in a commercial product or system.

As currently organized, the federal government researches and identifies "zero-day vulnerabilities," which are vulnerabilities in commercial technologies that are unknown to vendors. The government must then decide whether the vulnerability should be disclosed to the vendor so it can be patched or privately retained to support law enforcement, intelligence gathering and exploitation activities. The process of deciding how to move forward once a vulnerability is discovered is known as the Vulnerabilities Equities Process, or VEP.

The VEP was introduced in 2010 by the Obama Administration and requires government agencies to work together to weigh the costs and benefits of vulnerability disclosure; the proposed legislation introduced in recent months indicates that Congress finds the current process inadequate, as evidenced by changes recommended in the FY18 Intelligence Authorization Act and the Protecting our Ability To Counter Hacking (PATCH) Act. The Intelligence Authorization Act seeks to review the disclosure process, while the PATCH Act seeks to formalize the VEP, replacing current processes with a Vulnerability Equities Review Board comprised of leaders from government agencies who would set defined parameters for zero-day disclosures.

During my time at the National Security Council at the White House, I led the implementation of the United States' VEP program. This responsibility offered me a close look at how the United States achieves the balance between helping businesses protect against known cyber weaknesses and protecting national security opportunities. The current structure of the process and its existing mechanisms provide much needed flexibility for coordinating communications and actions around exposed vulnerabilities. The time and expense of transferring the current VEP to a new interagency body with a handful of new guidelines will likely not produce clear benefits, either for corporations looking for government support in protecting against vulnerabilities or for the government's management of the vulnerabilities it retains.

I do believe that there is room for improvement, particularly in providing more transparency around VEP intelligence and decision making. Striking the right balance between government capability and broader privacy and security is a delicate task. The current Administration's cybersecurity coordinator, Rob Joyce, has indicated in recent interviews that he intends to be more transparent about the program, which should resolve much of the confusion that has surrounded the process. With improved transparency, the current vulnerability disclosure process can continue to be an effective enabler for cybersecurity collaboration and communication between the public and private sectors.

Regardless of how vulnerability-related legislation evolves this year and in coming years, what remains critical for organizations is to take stock of their internal vulnerabilities and address them proactively. The fact that the U.S. Congress is discussing cyber vulnerabilities demonstrates the significance of this issue. There is no single set of actions that will solve the problem and ensure secure and resilient networks, but improving our understanding of the vulnerabilities that weaken our systems only enhances our ability to effectively mitigate them.