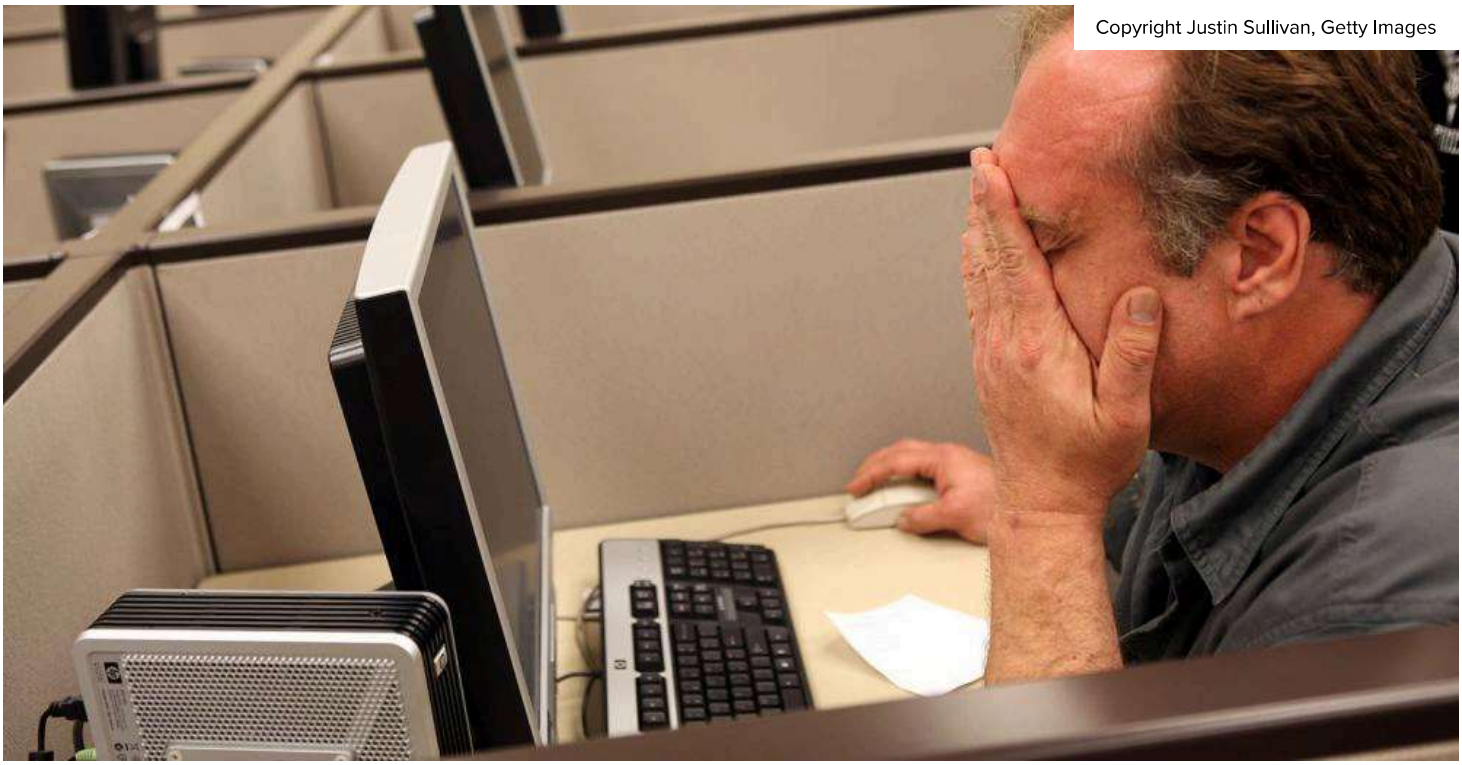
WealthManagement.com



TECHNOLOGY

Cyber Attacks May Make Financial Industry "WannaCry"

The financial services industry is a huge target for cyber criminals — more than any other industry.

Stacey Robinson | May 24, 2017

Large-scale cybersecurity breaches are in the news on a weekly and even daily basis in 2017. The WannaCry ransomware attack that sent millions of malicious emails and infected hundreds of thousands of computers globally, the Google Docs phishing scheme that spread rapidly, granting access to a malicious third party under the guise of a shared document and dozens of other smaller attacks have affected organizations across industries and put cybersecurity on everyone's minds.

The financial services industry is a huge target for cybercriminals — more than any other industry — and the risk has evolved from financial theft and fraud to more complex and serious consequences like theft of intellectual property, business disruption and reputation damage (Deloitte) .

In other words, hackers are not just stealing lists of Social Security numbers anymore, but rather executing serious breaches with more far-reaching consequences. Even large firms may struggle to keep up with the evolving cybersecurity threats and the situation is particularly challenging for mid- and small-tier firms. As recent events like WannaCry show, malicious cybercriminals are only getting quicker and more sophisticated.

Cybercriminals Exploit Financial Services Firms' Vulnerabilities

At financial services firms, cyberattacks exploit flaws in security programs that allow threat actors to gain access. Among the most common attack targets are endpoints, such as laptops, tablets and smartphones. Endpoints are particularly vulnerable because they require both robust security protocols and effective education for the firms' employees, who act as the last line of defense.

Attackers use weaponized email attachments and links to attack sites in order to compromise credentials and establish a foothold on the endpoint. The 2016 Data Breach Investigations Report (DBIR) from Verizon points out that it only takes minutes to compromise a host and collect a set of valid credentials, and in most cases, data exfiltration is underway just days after compromise.

Additionally, the DBIR uncovers some surprising figures about common security vulnerabilities. In 2015, the top 10 unpatched vulnerabilities accounted for 85 percent of successful exploit traffic. Furthermore, of those top 10 unpatched vulnerabilities that were exploited, only two of the patches were from 2015, and all of the remaining eight patches were published in or before 2003. The SEC's Office of Compliance Inspections and Examinations found recently that while nearly all firms surveyed had regular system maintenance processes in place, including the installation of patches to address vulnerabilities, 10 percent of broker/dealers and 4 percent of investment management firms had not updated a significant number of critical, high-risk security patches. Given these statistics, it's unsurprising that attackers find success.

The WannaCry attacks that started on May 12, 2017 exploited the EternalBlue vulnerability. Microsoft had released a critical patch for EternalBlue on March 14 — almost two full months prior to the attacks. “Frankly, if you wait two months to apply a critical Microsoft patch, you’re doing something wrong,” said Kasper Lindgaard of Flexera Software . “This time, we even had a warning in April that this could very likely happen, so businesses need to wake up and start taking these types of threats and risks seriously. There is simply no excuse.”

Why Are Endpoints Especially Vulnerable

Endpoints are a primary target for several reasons: 1) they are not being patched consistently or fully, 2) policy configuration may be ineffective, 3) they directly interact with attack sites and are often exposed to untrusted networks such as public hotspots and ineffectively secured home/home-office networks and 4) a portion of end users will inevitably open malicious attachments and click links to attack sites.

Compromising an endpoint gives the attacker a lot of bang for their buck, since they provide easy access to additional data and systems. One of the most effective ways to exploit endpoint security vulnerability is via phishing, a form of social engineering that commonly targets financial services companies. Per the DBIR, 30 percent of phishing emails were opened and 12 percent clicked on the malicious attachment or link, thereby enabling the attack. Clearly, we still have a long way to go in educating employees on security risks associated with emails and social engineering.

Successful endpoint security is a complex endeavor, requiring an extensive framework and consistent attention. It requires quality and maturity in areas such as OS hardening, the principle of least privilege and patching. Particular consideration should be paid to advanced security solutions around application whitelisting, exploit detection and prevention, device blocking, firewalls, web filtering and malware prevention.

While attackers will continue to use phishing as an attack vector in order to capitalize on human error, it’s certainly possible — and these days, essential — to develop and implement a robust security framework that accounts for all vulnerabilities.

From simple patch maintenance programs to in-depth user awareness and education, the best approach to preventing a breach involves difficult and too expensive for criminals to infiltrate your organization. Consistently adapting and improving security controls and countermeasures drives up the cost and risk for cybercriminals, while in turn makes companies better and more effective at spotting and stopping attacks sooner.

While recent global attacks are unfortunate, they may be the wakeup call that some financial services firms need in order to put stricter protocols in place.

Stacey Robinson, CISSP, is Chief Technology Officer at Mediant.