Brinker Capital

Ideas. Discipline. Outcomes.™

A tale of two billboards

Jim O'Hara, CISM, CISSP, CEH, Information Security Officer

Imagine a plush community of beautiful, sprawling estates where each property is protected by a high-end security system. Now imagine two enormous billboards along the nearby interstate. Once per month, the first billboard displays a list of newly discovered flaws in the community's security systems. The second describes methods to repair the same flaws. Which billboard would be more closely watched? Who would be watching it?

By now it's common knowledge that the Equifax breach was a direct result of the company's failure to properly maintain a webserver. What's less talked about is the fact that the exploited Apache Struts flaw had been published and rated "Critical" by security authorities well in advance of the breach. Even less discussed is Equifax's admission to knowing of the vulnerability at the time of breach, but not applying the associated patch, which had been available for months.

Software patching is essentially the 2-billboard scenario described above:

- **Billboard #1:** The Common Vulnerabilities and Exposures (CVEs) database. Maintained by the Cyber Security FFRDC, and funded by the Department of Homeland Security, the CVEs database is an ever-updated list of all known software vulnerabilities.
- **Billboard #2:** A collection of patches and other mitigating controls issued by software providers and security authorities, designed to mitigate the vulnerabilities listed on Billboard #1.

The primary shortcoming of this system is the vulnerability information on Billboard #1 is almost always newer than the remediation information on Billboard #2. While most software providers strive to release patches concurrently with the publication of the corresponding CVE,

this is not always possible. This occasionally creates a period of time when hackers can use the CVE data to attack vulnerable systems. In fact, Verizon's 2015 Data Breach Investigation Report found that half of published CVEs are used to successfully compromise some systems within two weeks. Hackers are keeping a close eye on the CVE database, and working quickly to weaponize new information it provides. So, for users and IT departments, it's an unwinnable race, right? Not so fast.

The same Verizon study also found that 99.9% of system compromises occurred more than a year after the associated CVEs and corresponding patches were made public. So, while the hackers may be fast, there is plenty of blame left for the victims - 99.9%, in fact. Going back to our community of beautiful, sprawling estates, this suggests that even if home owners are bothering to read Billboard #2, many are not acting on the information it contains. Equifax.

The key to keeping systems protected is a strong patch management program. Responsible organizations put in place policies, procedures and systems necessary to ensure vulnerabilities are quickly identified and thoroughly mitigated. Despite a strong patch management process, however, it remains possible that an attacker may find and exploit a vulnerability not yet listed in the CVEs database. This is known as a "Zero Day" attack. In order to mitigate Zero Day attacks, organizations must utilize a layered defense-in-depth strategy, which would include implementation of controls such as malware detection software, next generation firewalls, intrusion detection/prevention systems (IDPS), and data loss protection (DLP) technologies.

What can individual advisors and clients do?

- **Ensure your operating system and software are configured to update automatically.** Waiting for an update to install can be frustrating, but it's nothing compared to the sinking feeling you'll experience if your system is compromised. As a bonus, you'll no longer see those annoying reminders in the task bar.
- **Consider installing malware detection software on your computer.** This would be in addition to any anti-virus solutions already installed. There are many free and low-cost malware detection and eradication options available. Research the tool before installing to ensure it is legitimate and properly supported.
- **Encrypt critical and sensitive data.** Password protecting spreadsheets, Word documents, and PDFs containing sensitive data will greatly reduce the impact of a Zero Day attack on your computer. The attack may compromise your system, but it won't be able to decrypt your protected files. This could spare you many uncomfortable phone calls.

Brinker Capital

Brinker Capital is a privately held investment management firm. The company was founded in 1987 based on the idea of providing a multi-asset class, institutional-quality investment approach to individual investors. Brinker Capital's highly strategic, disciplined approach is the key to helping advisors and their clients achieve better outcomes for the past 30 years. With a focus on wealth creation and management, Brinker Capital serves financial advisors and their clients by providing the highest quality investment manager due diligence, asset allocation, portfolio construction and client communication services.