Are You On Top Of Your Patch Management?

cyber security regulatory

Summary: Software vulnerabilities cause severe headaches for IT personnel. The number of vulnerabilities has almost tripled from just under 6,500 in 2015 to more than 18,300 in 2020. Is your IT team ready for this exponential explosion? We discuss why it is vital to address these software issues and provide you with three steps to help keep your institution and customers safer.

The world is increasingly connected. In fact, 35B internet-connected devices are forecasted for this year, growing to 75B in 2025. That means more cyber risk. Since October is cyber security awareness month, we wanted to provide you with some key ways to stay on top of your patch management to keep your institution and customers cyber safe.

With the exponential rate that new vulnerabilities in software are uncovered, community financial institutions (CFIs) are increasingly under the gun to ensure their internal and customer-facing software is properly "patched" as soon as possible. According to IT security provider, Kaspersky, exploiting unpatched vulnerabilities is one of the top three ways that cybercriminals worm their way into corporate networks. The other two use brute force to figure out passwords and send phishing emails.

However, even for large institutions, patching known and emerging security gaps is a challenge. Many are identified on a daily basis and can affect various types of workstations, servers, mobile software, and applications that a CFI might use regularly. Case in point: In March of this year, Microsoft issued several updates to its pervasive Windows 10 platform. This update in turn contained vulnerabilities that not only might have made it easier for cyber thieves to sneak onto their systems, but also prompted internal PCs and servers to crash. This sudden event prevented some employees from being able to view their emails on Outlook or print documents.

The recent Win10 update was just one incident out of hundreds that happens every day, as software companies release and update fixes for dozens of common software platforms and applications used by financial institutions. Indeed, the number of common vulnerabilities and exposures (CVEs) identified annually by Trend Micro has nearly tripled from just under 6,500 in 2015 to more than 18,300 in 2020.

Given the relatively small amount of resources that CFIs typically have to commit to IT security overall, it may seem near impossible for them to stay ahead of a massive, proactive exercise like patching vulnerabilities as they emerge. However, there are steps that can help.

Review (and revise) patch management. Like most things in IT (and life), a failure to plan is a plan for failure. Hence, as part of its regular IT planning, CFIs should routinely revisit and update information useful to patch management. This includes defining which staff handle which roles when it comes to tracking and issuing patches to employees or customers. Make sure they have clear guidance on the steps they need to take and the timeline for rolling out a fix or update. At the same time, CFIs should make sure they have an accurate, up-to-date understanding of all their IT software and applications, and where they reside to smooth the process of patching.

Test patches first with a small group. Just like IT departments might pilot a new application with a limited audience to start, experts including regulatory bodies such as the Federal Financial Institutions Examination Council, agree that financial institutions would be more effective if they started testing patches that are released with a small group of users (if only for a day or two), before releasing them to the entire employee or customer base. In the best-case scenario, this test group would include those using various types of devices or platforms to see how the patch works out in different settings.

Consider employing an automated patch management software. In this increasingly complex world of remote and hybrid workforces, a CFI may find the easiest route to success is employing the use of a "patch management" service. This allows CFIs to automatically monitor potential vulnerabilities as they are publicly identified and install patches across different platforms. Such third-party options limit the need for extra IT personnel, which are difficult to find these days.

Patch management is more and more important these days. Making sure that your institution and your customers are safe from cyber thieves, who take advantage of vulnerabilities, can be daunting. Following the three above steps can mitigate this cyber risk.

IMPROVED EFFICIENCY WITH CHECK IMAGING FOR CANADIAN CASH LETTERS

PCBB's enhanced cash letter service for Canadian checks can help your institution minimize its credit exposure, increase operational efficiency, and deliver faster fraud notification. Learn more about our check imaging for Canadian cash letters.

ECONOMY & RATES

Rates As Of: 10/05/2021 06:15AM (GMT-0700)

Treasury	Yields	MTD Chg	YTD Chg
3M	0.04	0.00	-0.05
6M	0.06	0.01	-0.03
1Y	0.09	0.01	-0.02
2Y	0.29	0.01	0.17
5Y	0.97	0.01	0.61
10Y	1.51	0.02	0.59
30Y	2.07	0.02	0.42
FF Market	**FF Disc**		**IORB**
0.08	0.25		0.15
SOFR	**Prime**		**OBFR**
0.05	3.25		0.07