WebsterBank®

The humble security patch:
A business-critical part of cyber hygiene

Despite a growing awareness, cyber threats show no signs of abating. In fact, just the opposite. Experts expect cybercrimes to cost the world **$10.5 trillion annually**[1] by 2025, up from $3 trillion USD in 2015.

As hackers grow more sophisticated, cutting-edge software solutions and cybersecurity services continue to evolve, providing more options to protect your company. Yet one critical tenet of diligent cyber hygiene too often goes ignored for more elaborate, expensive, large-scale, sweeping actions: the humble security patch.

What Is a Patch?

Patches are ad hoc, typically small, code updates that address security vulnerabilities, fix performance bugs, and enhance product features in software and operating systems. They're one of the most durable defenses against ransomware. But when not managed properly, they can leave your company exposed.

90% of common vulnerabilities could be exploited by attackers with limited technical skills.[2]

3 Weaknesses Weaponized Against Your Organization's Cyber Shield

1. **Unpatched vulnerabilities**
   As soon as a vulnerability is made public, systems are even more susceptible to attacks. The disclosed weakness raises the red flag to everyone, including hackers. Yet, studies show **36% of companies** were able to patch systems and applications within hours of new vulnerabilities being discovered, and a further 44% were able to do so within days.[3] However, a whopping **40% of companies** expect business-critical systems would be down for 2–15 days after a ransomware attack.[4]

2. **The atmospheric rise of open-source code usage**
   In recent years, third-party applications, software code libraries, and other open-source software (OSS) have proliferated in codebases. During the past five years, OSS development rose from approximately **35% to about 75%** of organizations' audited codebase.[5] OSS offers benefits like lower costs and faster development, but with the benefits come risks. Decentralized sourcing and extra integration points add complexity, making identifying and addressing vulnerabilities more unwieldy and disconnected.

continue >

3. **End-of-life software**
   Antiquated software is no longer evaluated for vulnerabilities or maintained with security upgrades. Yet, when it's embedded into enterprise environments and relied upon for day-to-day operations, implementing a replacement can require reconfiguring the whole system. In response, companies resist or delay sunsetting these platforms. Meanwhile, the window of opportunity for hackers grows.

5 Best Practices

Patch management, in tandem with access privilege management, employee training, and other risk mitigation measures, is a critical piece of a hardened ransomware defense. Yet their efficacy hedges upon a robust implementation approach.

1. **Establish a regular patch cycle**
   Routine, prompt updates will forever be the centerpiece of effective patch management. Establish an audit system to identify available patches and known vulnerabilities — be sure to include older exposures as well as emerging threats — to stay abreast of the latest releases. Rather than relying on employees, enable automatic software updates whenever possible. That way, if update notifications go ignored or dismissed, updates still happen.

2. **Do not use unsupported end-of-life software**
   There is no denying that sunsetting software or a system integral to your business is disruptive at best, and painful at worst. But delaying the shift to a new platform only prolongs the pain and increases your exposure. Plan ahead, blueprint dependencies within your technology infrastructure, get in front of the changes before they're announced — and when they are, appoint a dedicated task force to hit the ground running.

3. **Protect every endpoint**
   Think beyond the computer. Include workstations, laptops, servers, Internet of Things (IoT) devices, and any other connected devices in your patch management plan. Avoid pushing updates until a device is on a trusted network.

4. **Know your code — and its source**
   Establish formal vetting processes and appropriate safeguards before partnering with a third-party vendor. Once onboard, leverage a third-party software program to manage open-source code usage and track emerging threats.

5. **Ensure compliance with real-time reports**
   Track enterprise-wide performance to establish a baseline, identify opportunities for improvement, and celebrate wins.

Received a fraudulent or suspicious email that appears to be from Webster Bank?

Contact a Webster Relationship Manager or call 888-932-2256.

Want more information on protecting your company from cyber threats?
Connect with Webster Bank.

[1] Sources: Cybersecurity Almanac, 2022. [2] Redscan, 2021. [3] Osterman Research, 2021, Patching Cadence . [4] Cybersecurity Dive, 2022. [5] McKinsey, 2022.

The opinions and views herein are for informational purposes only and are not intended to provide specific advice or recommendations. Please consult professional advisors with regard to your situation.