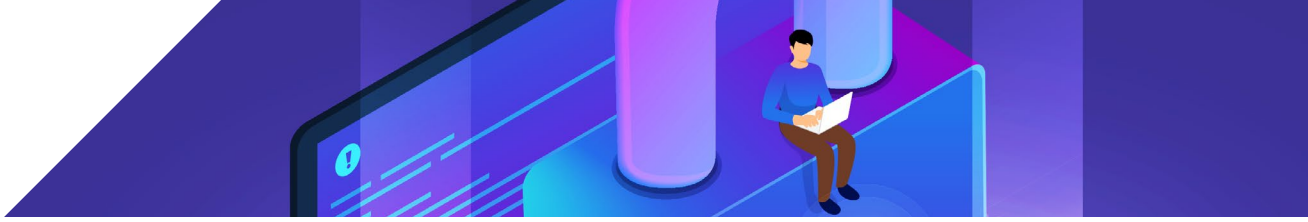
IDI
Billing Solutions

Reduce Your Cyber Risk With A Holistic Patch Management Program

In today's digital age, the telecommunications industry plays a critical role in connecting people and businesses. However, with increased reliance on technology, telecom service providers are also facing a higher risk of cyber-attacks. A robust cybersecurity strategy is essential to protect sensitive data, maintain customer trust, and ensure uninterrupted services. One crucial element of such a strategy is patch management. In this article, we will explore the importance of patch management for telecom service providers and discuss how a holistic patch management program can help reduce cyber risks.



Improve Your Overall Security Posture With Patch Management

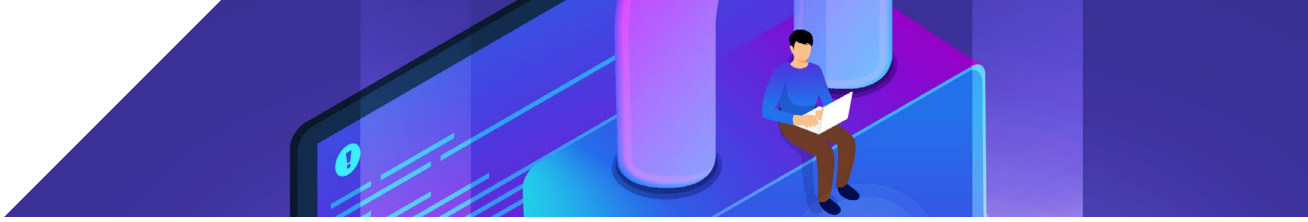
Patch management is the process of identifying, acquiring, testing, and deploying software updates, or patches, to fix vulnerabilities in computer systems, applications, and firmware. These updates are released by software vendors to address security flaws, enhance functionality, and improve overall performance. A thorough patch management program ensures that systems and devices are up to date, reducing the risk of cyber-attacks and improving the overall security posture of an organization.

Keep hackers at bay: Cybercriminals constantly search for vulnerabilities in software to exploit. By implementing a robust patch management program, telecom service providers can stay one step ahead of potential attackers. Regularly updating systems and software with the latest patches reduces the likelihood of successful attacks.

Reduce downtime: Unpatched systems are more susceptible to crashes, performance issues, and service disruptions. Patching vulnerabilities helps minimize the risk of system failures, ensuring smooth operations and reducing downtime. This is particularly crucial for telecom service providers, as any disruption in services can have significant financial and reputational implications.

Create predictability and routines around patching: A consistent patch management program establishes predictable patterns for applying updates. Instead of reacting to vulnerabilities when they arise, organizations can adopt a proactive approach by following a scheduled patching routine. This helps streamline operations and ensures that critical systems and devices are regularly maintained and protected.

Increase compliance: Regulatory frameworks and industry standards often include requirements for patch management. By implementing a comprehensive program, telecom service providers can demonstrate compliance with these regulations, avoiding penalties and maintaining trust with stakeholders.



Key Aspects to a Patch Management Program

Nearly 60% of cyber-attack victims said installing an available patch would have prevented their breach, and 39% said they knew about a vulnerability before an attack occurred—but never fixed it. It's vital for telecom service providers to prioritize a holistic patch management program to stay ahead of cybercriminals.

Asset Management

A comprehensive patch management program starts with effective asset management. Telecom service providers must accurately and consistently inventory and track their resources, including hardware, software, and network infrastructure. This visibility allows organizations to understand the criticality of each system or device and prioritize patch management efforts accordingly.

Vulnerability Management

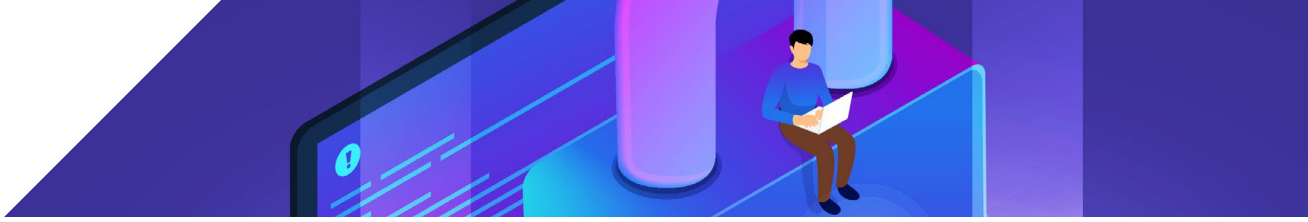
Once assets are identified, a thorough vulnerability assessment should be conducted to identify potential weaknesses. This assessment helps prioritize patching efforts by identifying the most critical vulnerabilities that need immediate attention. Automated discovery tools can scan the network to detect vulnerabilities and categorize them based on their severity.

Patch Management

After identifying vulnerabilities, the next step is remediation and updating. This involves testing patches in controlled environments to ensure compatibility and functionality. Once patches are proven to be effective, they can be deployed across the organization's systems and devices. Continuous improvement is crucial in patch management, as new vulnerabilities are constantly discovered, and updates need to be applied promptly.

Reporting and Reassessing

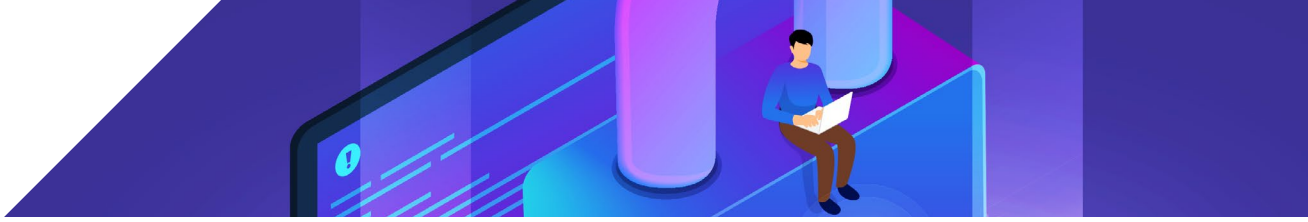
A holistic patch management program should incorporate a robust monitoring and reporting mechanism. This allows organizations to track the success of patch deployments, identify any failed installations or system vulnerabilities, and take immediate action to rectify them. Regular reporting also provides valuable insights into the overall patching progress, enabling organizations to make data-driven decisions and continually improve their cybersecurity measures.



Coordinating the different aspects of a patch management program can be challenging for telecom service providers, so it's important to be aware of potential issues that could arise. Telecom service providers typically have a diverse range of assets, and addressing vulnerabilities on all fronts may not be feasible at once. Resource allocation and prioritization conflicts may become apparent, requiring careful assessment and decision-making to ensure critical systems are patched promptly. Effective patch management also involves the collaboration of multiple teams or departments, so ensuring effective coordination and communication among these teams is crucial to streamline patch deployment and minimize disruptions.

Minimizing Your Cybersecurity Risk From Vendors

With the increased focus on supply chain risk management, it's more important than ever to be aware of how your vendors maintain their security posture. At IDI Billing Solutions, we understand how vital it is for vendors of telecom service providers to prioritize cybersecurity measures and continuously update their patch management programs to stay ahead of cybercriminals. IDI uses a sophisticated asset management software to maintain its asset inventory and has a robust vulnerability management program that focuses on identification, prioritization, remediation, and reporting for all endpoint and network devices. All systems are patched monthly by IDI, or more frequently based on criticality.



To produce secure, high-quality software, IDI Billing Solutions requires all software code changes to follow a secure code review process prior to general availability. IDI software developers must follow secure coding best practices and guidelines as recommended by the Open Web Application Security Project (OWASP). All software changes are thoroughly tested first on several layers of the infrastructure that don't contain customer data before being verified as stable and released to production systems.

By conducting vulnerability assessments, application and network penetration testing, and implementing a centralized patch management system, IDI instills confidence in our customers that their data is protected. As business needs, regulations and risk management landscape change, IDI continues to enhance our security posture with an ever evolving and robust patch management program.

Build A Better Security Experience With IDI.

Through innovative technology, people, partners, and systems, IDI is committed to providing a highly secure, world-class, cloud-based B/OSS platform, along with the insightful counsel and specialized expertise required to help you navigate the modern digital landscape.

As the telecom industry continues its rapid evolution, IDI's commitment to customer security remains at the forefront of everything we do — and that includes upholding current and future global industry standards. Talk to us today to learn more about IDI's compliances and how we protect our customers.

Call **888.924.4110**, or contact us **here.**