NIGC Tech Alert

Vulnerability Management: Securing the Tribal Gaming IT Enterprise

An effective vulnerability management program is a critical element of the strategy to maintain adequate security across the Tribal Gaming IT Enterprise. Vulnerability management is the process of managing the lifecycle of security vulnerabilities which includes discovery, prioritization, and remediation. A vulnerability management program establishes repeatable processes to continuously reduce vulnerabilities and their potential impact through continuous assessments and reporting. Patch management is an essential component of the vulnerability management program. The insights obtained through vulnerability assessments help drive remediation actions and prioritize patch deployment. Many organizations implement some patch management processes but fail to reap the benefits of integrating patch management with a broader vulnerability management program. The table below helps explain the relationship between vulnerability management and patch management.

The likelihood of a vulnerability being exploited in an IT system remains a clear and present danger until remediated. To deal with this constant threat, every tribal organization, large and small, must implement strong IT controls and continuously monitor their effectiveness. Equally important is the establishment of a vulnerability management program supported by strong patch management processes. The execution of these processes requires specialized tools along with significant collaboration between IT Operations and security teams within an organization. The National Indian Gaming Commission (NIGC) has previously published an advisory on the importance of strong patch management.

	VULNERABILITY MANAGEMENT	**PATCH MANAGEMENT**
PURPOSE	• Manage all security vulnerabilities	• Manage software patching
MAIN FUNCTIONS	• Discover, prioritize, assess, remediate & report vulnerabilities	• Test and apply patches or upgrade software to remove security holes, fix bugs or add features
KEY STEPS	• Continuously scan hardware and software assets • Identify vulnerabilities • Evaluate and prioritize vulnerabilities • Drive remediation and mitigation activities • Report on vulnerability posture	• Inventory systems and software • Standardize software versions • Discover and acquire patches • Create and approve patching plan • Install & document changes
RESPONSIBILITY	• Cybersecurity team	• IT Operations team

No vulnerability management program can guarantee a fix for every vulnerability, but being proactive and innovative may significantly reduce the likelihood of a successful exploit. The NIGC offers technical assistance, IT vulnerability assessments, and other resources to assist with vulnerability management to help protect tribal assets.

Please review the following resources:

NIST publication on vulnerability management
https://csrc.nist.rip/library/alt-SP800-40v2.pdf

Information from NIGC’s website concerning IT Vulnerability Assessment regarding Class II Gaming Systems.
https://www.nigc.gov/technology/it-vulnerability-assessment

August 2024

Contact Us: ocio@nigc.gov