NIGC Tech Alert

SECURING REMOTE ACCESS: A NEW BUSINESS REQUIREMENT

Keeping the IT infrastructure accessible to users from remote locations becomes an integral part of business operations since COVID-19. Securing such access is a challenge to Information Systems Management teams. Researchers agree that by 2025, cybersecurity strategies will prioritize securing remote work environments against external threats. To protect remote employees and company data, those strategies must include endpoint protection, data encryption, identity management, and modernized VPN solutions.

To maintain efficient casino operations, many tribal organizations currently permit remote access into their IT infrastructure for employees and vendors. Unfortunately, malicious actors have exploited vulnerabilities in remote access systems to compromise some Casino networks. In January 2022, the FBI warned that attackers were specifically targeting casino servers and using legitimate system management tools to escalate their permissions on compromised networks. Third-party vendors and services were identified as common attack vectors, with ransomware groups frequently breaching casinos through these trusted insiders.

Tribal operations utilizing remote access software must be vigilant to potential vulnerabilities that attackers can exploit, and can take simple steps now to minimize risks in the following areas:

- **Weak passwords**: Passwords that rely on common dictionary words or do not follow a complex password policy—such as a mix of uppercase and lowercase letters, numbers, and special characters—are susceptible to brute-force attacks. Not changing passwords frequently allows time to compromise them using readily available tools.
- **Outdated software versions**: Using outdated remote access software may involve compromised encryption key and increase the risks of man-in-the-middle attacks.
- **Poor login policies**: Poor login practices include not limiting unsuccessful login attempts, using http basic authentication, and not implementing screen lock or user log off after a period of inactivity.

Additionally, Tribal operations should promote a cybersecurity culture that include techniques, policies and procedures that help detect and respond to attacks in a timely manner. Most of the following techniques can be readily implemented:

- **Audit your network**: Identify systems using remote access and disable the service if it's not needed.
- **Regularly apply system and software updates**: Ensure third parties requiring RDP access adhere to strict remote access policies.
- **Maintain a solid backup strategy**: Safeguard critical system data by implementing a reliable backup routine.
- **Use Multi-Factor Authentication (MFA):** Enforcing an authentication method that require users to provide two or more verification factors to gain access to an online account or a VPN.
- ***Just In Time Privileged Access Management:*** Adopting privileged access management allows for temporary access privileges, when necessary, to reduce the risk of unauthorized access.

However, these practical cybersecurity measures do not protect against social engineering attacks. Attackers could target any casino employee or tribal gaming authority to gain remote access through pop-up messages, phone calls, or other methods. Remember, no legitimate company will randomly call a user to obtain sensitive information or send a pop-up message to your computer requesting access.

The importance of addressing remote access threats to Indian Country cannot be overstated. It emphasizes the need for extra vigilance in maintaining and monitoring network infrastructures.

To preview additional information on securing and protecting remote access software, see Guide to Securing Remote Access Software (cisa.gov) and Protecting Against Malicious Use of Remote Monitoring and Management Software | CISA

November 2024

Contact Us: ocio@nigc.gov