Tribal Cybersecurity Readiness

Opening IT Operations — Hackers Are Ready...Are You?

Introduction

Malicious cyber activity costs the U.S economy billions of dollars each year. The NIGC Information Technology Audit team has prepared this handout to help raise cybersecurity awareness within the Indian gaming industry. These tips are intended to encourage review of IT controls, processes and procedures so that tribal operations can avoid and minimize damage from cyberattacks.

Cybersecurity Preparedness

What are the common methods of cyberattacks?

a. Malware – Malware is malicious software that can infect IT systems and provide access to hackers, alter or transmit critical company information, or ransom data (ransomware).

b. Denial of Service (DoS) – A DoS attack is when attackers send mass amounts of requests to company web servers in an attempt to consume all computing resources to the point where the company servers can no longer accept any additional requests. Business operations may be impacted when the DoS attack prevents company servers from accepting legitimate requests.

c. Remote Access Attacks - Unauthorized access to agency resources may be obtained via a vendor's remote access connection or an internal agent's VPN connection. With the increase in remote access due to telework and other considerations related to the COVID-19 pandemic, hackers will likely attempt to exploit misconfigured webservers, unpatched and discontinued legacy platforms, weak passwords and open remote desktop protocol (RDP) ports.

d. Phishing & Spear Phishing – These types of attacks harvest sensitive information such as user credentials by exploiting unsuspecting users through spoofed emails containing malicious links and attachments. Attackers use spoofed email addresses that are designed to appear to come from recognized sources such as government, banking and shipping company email addresses (IRS.gov, USPS.com, Amazon.com, etc.). Spear phishing is when attackers customize the spoofed emails for particular users that may be more likely to click on links or download attachments.

What are ways to avoid or minimize a cyberattack?

a. Access Controls - Ensure that all vendors are vetted, licensed, and approved to access IT systems. Vendor agents should be tracked via robust access and logging/tracking systems in order to track the who, what, when, where and why a vendor agent accessed the system. See 25 *CFR 543.20(h) Remote Access.* IT departments should ensure that accounts and RDP sessions are closed and disabled when no longer in use to prevent subsequent attacks. See 25 *CFR 543.20(e) Logical Security*.

b. Patch Management and Vulnerability Assessments – Software security updates should be constant and regular, especially on critical systems. Keeping software and hardware up to date will reduce the chances of malware attacks succeeding. See *25 CFR 543.20(k) Software downloads*. A network vulnerability assessment can identify unpatched and vulnerable systems.

c. Incident Management and Recovery Plan – IT system users should be aware of the appropriate actions to take in case of a cyberattack. Documented and tested disaster recovery and business continuity plans are essential. Consider the use of a 24/7 security operation center (SOC) to monitor critical systems. A recovery plan should be in place that describes how to resume operations after an outage. See 25 *CFR 543.20(i) Incident Monitoring and Reporting*.

d. Data Backup/Testing – Backing up data is critical for operational consistency and recovery after catastrophic events. A plan should be in place to backup data and to test recovery from the backups because data loss can occur at any time. There are different types of backups that include a) full b) incremental and c) differential backups. See 25 *CFR 543.20(j) Data Backups*.

e. Insurance – Ransomware and other cyberattacks can impact operations for hours, days or weeks and result in the loss of revenue, increased personnel and vendor costs for recovery efforts, and additional expenses for hardware and software replacement. Many private insurance carriers provide insurance to help mitigate the full impact of a cyberattack.

f. Training – Cybersecurity is the responsibility of all users of IT systems. Users should be trained to recognize phishing and malware attacks and to be familiar with Incident Management and Recovery Plans.

Resources

1. Ransomware groups continue to target healthcare, critical services; here's how to reduce risk - https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/

2. COVID-19 Remote Work Causes Spike in Brute-Force RDP Cyberattacks - https://healthitsecurity.com/news/covid-19-remote-work-causes-spike-in-brute-force-rdp-cyberattacks

3. 5 Biggest Cyberattacks of 2019 (So Far) and Lessons Learned - https://www.gflesch.com/blog/biggest-cyberattacks-2019

4. Be Prepared for a Cyberattack (FEMA) - https://www.fema.gov/media-library-data/1558564285012-6f81784140c5b5116240a804610eaf12/Cyberattack_InfoSheet_061418.pdf

5. Guide to Cyber Threat Information Sharing (NIST) - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

6. Automated Indicator Sharing (CISA) – https://us-cert.cisa.gov/ais

7. The Cost of Malicious Cyber Activity to the U.S Economy - https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf