Computer Guidance Corporation Security Protocols

Table of Contents

Overview

In today's world of frequent cyber-attacks, it is important to put hardware, software and security protocols in place to deal with potential threats. CGC has identified four specific categories of threats that warrant enumerated protocols in the event an incident were to occur. This document details the action CGC will undertake to address any threat that may arise from these attacks. While this list doesn't attempt to address all the potential threats, we feel the four categories listed herein can be used as a roadmap when dealing with cyber threats with other various characteristics.

Denial of Service

A denial-of-service attack (DoS attack) is a cyber-attack where the perpetrator seeks to make a network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of Service is typically accomplished by flooding the targeted network with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. CGC will take the following action in the event a DoS attack occurs.

Activities:

1. Identify the target IP(s) of the attack.
2. Review logs and trace back the source IP(s) of the attacker.
3. Contact our data center resources to block the source IP address at the firewall level.
4. Perform a WhoIs lookup on the attackers IP address and if available, notify the registration contact of the DoS activities associated with the IP address.

Communications:

1. Report the event to the CGC management team.
2. If the DoS attack is impacting SaaS access performance, notify the impacted hosted customers of the event and the action being undertaken to address the attack.
3. If appropriate, report the event to law enforcement: https://www.fbi.gov/file-repository/law-enforcement-cyber-incident-reporting.pdf

Vulnerability Identified

Vulnerabilities are areas of potential exploit by a would-be attacker that have been identified before a cyber-attack occurs. Normally identified by technology vendor and security providers, these items are often flaws discovered within software that could be exploited. The provider normally creates updates/actions to take to mitigate or eliminate this type of risk.

Activities:

1. Review the available documentation to determine the scope and potential impact of the vulnerability.
2. Ensure any vendor recommended updates and/or mitigating systems such as antivirus, web/mail filters and firewalls are applied to mitigate the risk.
3. Evaluate the vendor's recommended software updates for performance and stability. Perform system testing of the software updates if warranted.
4. If the vendor's recommended software updates meets performance and stability requirement, implement the updates in the CGC test environment.
5. Once validated in the CGC test environment, the updates can be deployed to the Hosted Implementation Environment.
6. It may be determined to delay the deployment of the software update:
    a. Mitigating systems (antivirus, firewalls, etc.) effectively eliminating the risk.
    b. The vendor's provided update lacks the stability to implement and mitigating systems are effectively eliminating the risk at this time. Continue to monitor the vendor for additional updates to their software.
    c. After evaluation, it has been determined that the risk is low and is mitigated.

Communications:

1. For low impact, common updates such as Windows updates, no notification to the customer or CGC management is required.
2. If it is a medium to high risk vulnerability, report it to the CGC management team.

3. If it is a medium to high risk vulnerability and the customer may also have on premise equipment impacted by the risk, email communication is typically used to provide customers information as warranted.

Virus/Malware Outbreak

Malicious content such as malware, viruses, and ransomware are risks in any computing environment. In the event system(s) are infected, CGC will undertake the following activities and communication.

CGC Internal Systems

Activities:

1. Identify the scope and nature of the malicious content.
2. Identify the contagion rate and isolate the malicious content by terminating programs, services and/or network connectivity.
3. Attempt to determine the source of the malicious content.
4. Evaluate damage:
    a. Data loss/corruption
    b. System corruption
5. Evaluate industry tools available to remove the malicious content and/or repair damaged files.
6. Utilize system backups to recover any unrepairable damaged files.

Communications:

1. Inform CGC management of the malicious event.
2. Communicate any system impact to the affected data owners.
3. If appropriate, report the event to law enforcement: https://www.fbi.gov/file-repository/law-enforcement-cyber-incident-reporting.pdf

Hosted Customer Systems

Activities:

1. Identify the scope and nature of the malicious content.
2. Identify the contagion rate and isolate the malicious content by terminating programs, services and/or network connectivity.
3. Attempt to determine the source of the malicious content.
4. Evaluate damage:

   a. Data loss/corruption
   b. System corruption
5. Evaluate industry tools available to remove the malicious content and/or repair damaged files.
6. Utilize system backup to recover any unrepairable damaged files.

Communications:

1. Inform CGC management of the malicious event.
2. Inform impacted customer(s) of the malicious event.
3. Continuous customer(s) communication during the source identification and repair/recovery activities.
4. If appropriate, report the event to law enforcement: https://www.fbi.gov/file-repository/law-enforcement-cyber-incident-reporting.pdf

Data Breach

In the event of a Data Breach, the following actions will be taken.

Activities:

1. Identify the scope and nature of the data breach.
2. Isolate the source systems by terminating programs, services and/or network connectivity, until the cause of the data breach is identified and addressed.
3. Collect all log information associated with the source system.
4. Establish a security forensics team to determine the detailed cause, impact and remediation associated with the data breach. This may include external security experts depending on the nature and severity of the incident.
5. Implement corrective actions to address the cause of the data breach.
6. Additional activities may be determined by CGC Management based on the results gathered by the security forensics team.

Communications:

1. Inform CGC management of the data breach event.
2. Inform impacted customer(s) of the data breach event.
3. Continuous customer(s) communication during the security forensic activities.