DUCK TECHNOLOGIES

IT Solutions

Security Incident Response Protocol

Version 1.3 Prepared by: Matt Super

5/18/2009

The purpose of the Security Incident Response Protocol is to provide an efficient, organized plan of action for handling any potential security or intrusion threat to the internal network of small to mid-sized businesses.

Contents

Purpose

The Security Incident Response Protocol document provides an efficient, organized plan of action for handling any potential security or intrusion threat to the internal systems of small to mid-sized organizations. Outlined in this document are appropriate steps for identifying a breach of security, isolating and eliminating the intrusion point following an incident and gathering information to maximize the chances of identifying the source of the attack. Also defined are the identities, roles and responsibilities of the Security Incident Response Team which is responsible for putting this protocol into action.

The Security Incident Response Team

The Security Incident Response Team is responsible for upholding and protecting the integrity of the internal information systems. Their mission is to provide an efficient, effective response to security related incidents with the goal of returning systems to a secure and normalized operating state as quickly as possible while minimizing any possible negative impacts to the company. By performing their duties they strive to prevent incidents which may result in a drastic loss of profits, public confidence in the company and the theft of valuable information assets.

The Security Incident Response Team is authorized to take appropriate action to contain, resolve and investigate any security breach or incident. This action is to be performed in an effective, timely and cost-effective manner. Actions taken will then be reported to management in an after-action report and if necessary reported to any appropriate authorities as well. The Lead Security Incident Response Officer will coordinate these efforts.

The Security Incident Response Team is also responsible for staying abreast of relevant and current security information and will subscribe to various industry resources to accomplish this.

Activation of the SIR Team

Events which warrant the activation of the Security Incident Response Team are any event in which the integrity of the internal network has been breached or is suspected to have been compromised. The following incidents are examples of such circumstances:

<u>Characteristics of incidents in which a security breach may have occurred:</u>

- Evidence (unexplained e-mail, system log entries, programs, new files or folders)
- Virus outbreaks or infections
- Anomalous traffic to or from a suspected target
- Unexpected changes in resource usage
- System slowdown or failure
- Changes in default or user-defined settings
- Changes to system files
- User account lock out
- Appliance or equipment failure
- Unexpected enabling or activation of services or ports
- Protective mechanisms disabled (firewall, anti-virus)

Characteristics of incidents in which preventative measures should be taken:

- Theft of computer equipment where sensitive data is stored
- Loss of storage media (removable drive, CD-Rom, DVD, flash drive, magnetic tape)
- Printed materials containing sensitive data mishandled or left unsecured
- Illegal entry (burglary)
- Suspicious or foreign hardware connected to the network
- Normally-secured datacenter area found unsecured
- Presence of unauthorized personnel in secured areas

Security Incident Response Team Members

Each of the following action team roles must be assigned a primary contact:

- Lead Security Incident Response Officer
- Secondary Security Incident Response Officer
- Tertiary Security Incident Response Officer

Security Incident Management Team Members

Each of the following management team roles must be assigned a primary contact:

- Organizational Chief Executive Officer
- Chief Incident Containment Consultant
- Secondary Incident Containment Consultant
- Tertiary Incident Containment Consultant

Security Incident Response Team Responsibilities

Lead Security Incident Response Officer

- Central point of contact for all security incidents
- Determines the severity and scope of the incident
- Responsible for contacting appropriate executive management personnel
- Determines what actions should be taken to immediately contain and isolate the breach
- Plays the lead role in identifying and correcting the incident
- Coordinates efforts of the members of the Security Incident Response Team
- Determines which Team members will play an active role in the response
- Provides training on breach containment methodology and techniques
- Escalates to the Security Incident Management Team members as appropriate
- Prepares a written summary of the incident and corrective action taken after the fact

Secondary Security Incident Response Officer

- Secondary point of contact for all security incidents
- Assists the Lead SIRO in all steps of the incident containment process and investigation
- Acts as the Lead SIRO if the Lead is unavailable for any reason

Tertiary Security Incident Response Officer

- The third point of contact for all security incidents
- Must be familiar with emergency breach isolation protocols
- Acts as a contingency against both the Lead and Secondary SIROs being unavailable or unable to respond in a timely manner

Security Incident Management Team Roles

Organizational Chief Executive Officer

- Primary stakeholder of the organization
- Will be contacted immediately in the event of a breach
- Will be kept apprised of the situation and given regular updates as events unfold

Chief Incident Containment Consultant

- Oversees the management of the breach response from the end user and client sides
- Responsible for documenting any confidential personal information which may have been breached
- Provides assistance and expertise throughout the investigation regarding issues related to the privacy of customer and employee personal information
- Responsible for dispensing appropriate communication to affected parties
- Assesses the need to change privacy policies, procedures and/or practices as a result of the breach

Secondary Incident Containment Contact

- Secondary managerial point of contact for all security incidents
- Assists the Chief ICC in all steps of the incident containment process
- Acts as the Chief ICC if the Chief is unavailable for any reason

Tertiary Incident Containment Consultant

- The third managerial point of contact for all security incidents
- Acts as a contingency against both the Chief and Secondary ICCs being unavailable or unable to respond in a timely manner

Security Incident Response Team Assignments and Contact List

Team Member	Contact	Phone	email
Lead Security Incident Response Officer			
Secondary Security Incident Response Officer			
Tertiary Security Incident Response Officer			

Security Incident Management Team Assignments and Contact List

Team Member	Contact	Phone	email
Organizational Chief Executive Officer			
Chief Incident Containment Consultant			
Secondary Incident Containment Consultant			
Tertiary Incident Containment Consultant			

Preventative and Proactive Measures

Preventative and proactive measures are actions taken in the interest of minimizing the chances of a breach and identifying the occurrence of a breach as early as possible to contain the damage. These measures should be taken by the network administration team and audited periodically to ensure that they are being performed.

Network Analysis

- Run tracing tools such as sniffers, Transmission Control Protocol (TCP) port monitors, and event loggers to detect signs of external attacks
- Evaluate the access logs of firewall(s) in place for signs of a breach

Server Operating Systems Analysis

- Ensure all service packs and security patches are current on critical servers
- Ensure that backups are in place and current for all critical data
- Examine the system logs regularly of critical systems for unusual activity

User Systems Analysis

- Monitor user data, business applications and services for signs of an attack
- Ensure that antivirus software is active and current on user systems
- Monitor user systems and activities for erroneous or purposeful loosening of security measures currently in place and/or unauthorized software installations

Security Incident Response Protocol

A security breach is any act which bypasses or contravenes our established security protocols, practices or procedures or any unauthorized access which compromises the security, confidentiality, or integrity of information maintained by the organization. When a security breach or incident has occurred, the Security Incident Response Team will be activated and immediately begin execution of the following actions:

Secure the Perimeter and Isolate the Affected Systems to Prevent Further Damage:

1. The Lead SIRO shall perform a brief preliminary analysis of the situation to determine the scope and nature of the incident.

2. If email compromise is a threat: halt the Mail Server Message Store to prevent unauthorized email access and communications.

3. If account security is a threat: lock out any suspected compromised user accounts from the system.

4. If internal network integrity has been compromised: halt all critical server communications via physical removal from the network (where appropriate) to effectively halt incoming and outgoing communications.

5. If overall security has been compromised or the threat is deemed severe, disable network communications at the primary incoming Firewall or contact point to cut off the internal network entirely.

Contact appropriate Incident Response Team members and Management Team members

1. Notify applicable Team members that a breach has taken place. This notification should occur via a direct communication by telephone or face-to-face contact. Voice-mail and e-mail are not considered direct notification.

2. Respective lead and alternate Team members shall exchange information to ensure their knowledge of the incident is current.

3. Communicate to applicable Management Team members the severity of the breach, the steps that are being taken, the extent of the damage and an estimate on the time until systems are able to operate normally once again.

Identify and Contain the Breach

1. Determine the potential extent of the breach. Identify data stored and compromised on all test, development and production systems and the number of systems at risk.

2. Determine the source of the breach:

    - Identify the initial compromised system and the timeframe involved.
    - Review the network to identify all compromised or affected systems. Launch diagnostic tools to scan the internal network for security holes, discrepancies or compromised systems. Diagnostic tools include antivirus, antispyware, port scanners and security evaluation tools. Consider hosted websites, test and production environments and virtual private network connections.
    - Save all appropriate system, firewall and audit logs for each device affected. Logs should be saved to a secure location and reviewed as soon as possible.

3. Once the suspected source of the breach has been identified, apply relevant security patches or fixes to resolve it. Consider altering other aspects of the network suspected of aiding in the breach as well as deemed appropriate by the Lead SIRO as well such as passwords, firewall configurations and remote access rights.

Reestablish Network Communications and Assess After Action Needs

1. Reconnect any communication lines which were broken in the effort to isolate the breach.

2. Actively monitor network traffic and systems for signs of continued intruder access.

3. Save all system and audit logs and evidence for potential law enforcement investigations. Document the actions taken by the Security Incident Team members involved along with dates and times. Record all data gathering tools used in the breach investigation.

4. Determine if any company confidential, client or privileged information was at risk or if any inappropriate client communications may have occurred.

5. If client information or communication was involved, notify the Chief Incident Containment Consultant. The Chief ICC will then coordinate any needed legal and public relation steps necessary in notifying the affected parties and damage control.

Prepare an After Action Report for the Organizational CEO

I. Executive Summary
   a. Overview of the incident
   b. Extent and type(s) of damage perpetrated
   c. Confidence level that the compromise has been contained

II. Investigative Methodologies Used
   a. Forensic data gathering tools used in the course of the investigation

III. Findings
   a. Number and identity of systems compromised
   b. Type(s) of data and information at risk
   c. Identity of all systems analyzed and compromised systems, including:
      i. NetBIOS name
      ii. Internet Protocol addresses
      iii. Operating System
      iv. Function of system and type(s) of data stored on it
   d. Timeframe of the breach
   e. Any data accessed and exported by the intruder
   f. Establish the suspected technique used and source of the breach

IV. Action Taken by the Security Incident Teams
   a. Description of the steps taken to ensure the threat was eliminated
   b. Description of actions taken to ensure a similar threat will not occur again

V. Recommendations