Security Incident Management Essentials

Compiled as a service to the community by
Internet2, EDUCAUSE, and REN-ISAC

Background and Overview

The Computer Security Incidents – Internet2 (CSI2) working group organizes activities to better identify security incidents and improve the sharing of information about the incidents. The goal is to improve the overall security of the network and the parties connected to the network.

One of the goals of the working group is to publish information identifying tools, tool output and information-sharing frameworks.

Being connected to the network means being exposed to a variety of threats, which seem to increase exponentially every year. Organizations have evolved a variety of formal and informal methods for identifying, investigating and sharing information about these threats. Still, many colleges and universities face a daunting security task, with limited resources and staff, to identify and act on compromised devices and mitigating the ongoing threat.

To help with this situation, CSI2 has developed a list of Security Incident Management Essentials. This document provides a starting point for IT security, offering:

- a summary and outline of the essential security tools and processes
- summaries and links to additional resources
- insight on establishing priorities, including specifying which tools are quickest to implement and will provide instant protection.

Who is CSI2?

The Computer Security Incidents - Internet2 (CSI2) Working Group organizes activities to better identify security incidents, and facilitate the sharing of information about such incidents. The goal is to improve the overall security of the network and the parties connected to the network. Additional information is available at http://security.internet2.edu/csi2. The working group operates under the umbrella of the EDUCAUSE/Internet2 Higher Education Information Security Council.

What is Incident Management?

The SANS (SysAdmin, Audit, Network, Security) Institute provides information security training and certification. According to SANS,

> "Information Security Incident Management is not composed of a single process, but rather includes a number of operational and technical components which provide the necessary functions in order to support the traditional 'Preparation, Identification, Contain, Eradication, Recovery, Lessons Learned' incident process model, including longer term monitoring, strategic planning, and trend analysis."

Following this traditional incident process model, CSI2 Security Incident Management Essentials will:

1. Provide you with the key questions to ask and answer concerning your security preparation
2. Identify specific processes and tools to use to contain and eradicate threats
3. Outline methods for recovering compromised devices on your network and mitigate the potential damage from system breaches,
4. Provide you with other security measures you can use to prevent threats from harming your network in the future.

Security Preparation – Where do I Start?

Common Contact Addresses for Security and Site Maintenance

A good (and simple) place to start is to establish (or update) your common contact addresses for security and site maintenance. The chart below recommends the format and specific addresses to use, consistent with ARIN and EDUCAUSE requirements, which are also discussed below.

Using these contact addresses, as opposed to an individual's address, provides continuity for your organization and minimizes the administrative work required when people leave your organization or when their roles change.

Recommended:

MAILBOX	AREA	USAGE	ARIN POC Title
ABUSE@domain.edu	Customer Relations	Inappropriate public behavior	Abuse POC
POSTMASTER@domain.edu	SMTP	RFC821, RFC822	
NOC@domain.edu	Network Operations	Network infrastructure	NOC POC
SECURITY@domain.edu	Network Security	Security bulletins or queries	

Optional:

MAILBOX	AREA	USAGE
HOSTMASTER@domain.edu	DNS	RFC1033-RFC1035
WEBMASTER@domain.edu	HTTP	RFC 2068
WWW@domain.edu	HTTP	Synonym for WEBMASTER

Reference:
Internet Mail Consortium Request for Comment: RFC2142 - Mailbox Names for Common Services, Roles and Functions. http://www.faqs.org/rfcs/rfc2142.html

Spam Considerations for these Addresses

- Consider leaving the security and abuse addresses unfiltered when it comes to spam. Often, mail sent to these addresses will be flagged as spam, as the message may be reporting spam. However, if your filtering system reports more than 99 percent spam, you may want to filter.
- Consider white-listing known, trusted reporting organizations such as the REN-ISAC (see "resources" at the end of this document for information about REN-ISAC).
- If you are going to filter for spam, bounce the filtered emails so the senders of legitimate notifications are aware that their message was flagged as spam.

Notifying/Updating ARIN and EDUCAUSE

ARIN – the American Registry of Internet Numbers – provides services related to the technical coordination and management of Internet number resources in the U.S. and elsewhere. ARIN requires an Admin point of contact (POC) and at least one Tech POC associated with each site. Abuse and NOC POCs are optional, although highly useful for those seeking to resolve security and other issues associated with a site.

To learn more about ARIN POCs, and the ARIN database in general, visit
https://www.arin.net/knowledge/database.html

For information on the process of submitting POCs to ARIN, see
https://www.arin.net/resources/request/poc.html

For a template to use in submitting POCs, see
https://www.arin.net/resources/templates/poc.txt

EDUCAUSE

EDUCAUSE is the sole registrar for names in the .edu domains. In addition to maintaining information with ARIN, colleges and universities also must manage their domain information with EDUCAUSE.

For information on EDUCAUSE policies and procedures, to go
http://net.educause.edu/edudomain/policy.asp

To make changes to your current .edu domain information go to
https://net.educause.edu/edudomain/domain_login.asp

Processing Threats –
How do I begin to process internal and external notifications?

Use group aliases – Once you have your contact mailboxes established (e.g. abuse@ and postmaster@), you must determine how to distribute this mail. At a minimum, we recommend creating a group alias, rather than forwarding this mail to an individual. Also, we recommend you include someone in a management position in your organization (for example, the person responsible for the oversight of IT and/or security). Creating a group alias provides a seamless way to delegate work when the primary contact person is on vacation or away from email for an extended period of time.

Leverage work-flow technology – If your organization has some type of work-flow technology, like a centralized ticketing system, we recommend leveraging that technology to process, alert, prioritize and archive the messages coming to your contact addresses.

Many organizations use RT (Request Tracker), an open-source issue tracking system (http://www.bestpractical.com/rt). Such a system provides a method to prioritize, search, escalate, and report on issues; as well as providing a history to help the organization analyze trends. Even if your organization does not use all of these features initially, establishing a system with this capability, and the ability to generate reports, could be of benefit in the future.

Identifying Compromised Machines and Hosts

How do I identify hosts reported by internal and external sources?

MAC address database – Create a database of MAC addresses associated with a computer name, physical location and person (email address).

Static IP database – Create a database of IP addresses/CIDR ranges associated with a computer name, physical location and person (email address).

DHCP logging – Use a MAC address from DHCP logs to find computers.

NAT/PAT/Proxy logs – Enable a level of logging that allows you to identify the internal hosts when given a TimeStamp and SourcePort.

Leverage authentication logs to identify computers and people – central authentication logs, Active Directory logs, Webmail logs, SMTP auth logs.

Network Access Control (NAC) authentication logs provide instant pairing between usernames, MACs, and (internal) IPs. Typical products leveraged in higher education include NetReg (and derivatives), Cisco NAC, Impulse SafeConnect, and Bradford Campus Manager.

How do I verify or look for compromised machines (either proactively or retroactively)?

Network Intrusion Detection Systems

- **Snort** – Snort is a free, open-source network intrusion detection and prevention system capable of performing real-time traffic analysis and packet logging on IP networks. www.snort.org
- **Bro** – Bro is an open-source, Unix-based network intrusion detection system that passively monitors network traffic and looks for suspicious activity. www.bro-ids.org

Network Flow (NetFlow)
NetFlow is a set of services for IP applications, including network planning, security, denial of service monitoring capabilities, and network monitoring. NetFlow provides information about network users and applications, peak usage times, and traffic routing. A good description is at http://en.wikipedia.org/wiki/Netflow.

- **Free Flow Tools** – The website "Network Uptime" lists several free netflow tools that provide ways to collect and display netflow information. (www.networkuptime.com/tools/netflow/). Other useful tools include:
    - **Argus** – The network Audit Record Generation and Utilization System (Argus) Project is an open-source IP audit tool used by many universities, corporations and government entities to record internal traffic flows and flows entering and leaving their networks. http://qosient.com/argus.
    - **NfSen** (Netflow Sensor) is a graphical web-based front-end that allows you to display and easily navigate through your netflow data. It provides for processing data within a specified time span, create a history, and create alerts based on various conditions. http://nfsen.sourceforge.net

DNS logging

- **BIND logging** – BIND (Berkeley Internet Naming Daemon) is the most frequently used DNS server, with software maintained by the Internet Systems Consortium (www.isc.org). When enabling logging in BIND, you can specify which information the server logs and where the log messages are sent. For complete information on BIND, see www.isc.org/software/bind

- **Windows DNS logging** – In Windows, when the DNS client service receives a request to resolve a DNS name that is not contain in its cache, it queries an assigned DNS server for an IP address for the name. By enabling DNS debug logging, you can log all DNS-related actions such as zone transfers, DNS queries and resource record updates. See a description of enabling logging here: http://thelazyadmin.com/blogs/thelazyadmin/archive/2006/02/16/DNS-Tips-_2300_14-_2D00_-DNS-Logging.aspx

While considering logging, also consider the techniques you will use to identify bad activity within those logs. Generally, you want to gather information about malware behavior and then look for signs of that behavior in your logs and scans.

There is good advice from a SANS (SysAdmin, Audit, Network, Security) diary called Malware Intelligence: Making it Actionable" (http://isc.sans.org/diary.html?storyid=4756). Things to look for, in terms of detecting a compromised machine, include:

- Does it connect out to a known Command and Control system?
- Does it make known HTTP requests?
- Does it advertise itself in the user-agent?
- Does it scan for a particular port?
- Does it generate P2P traffic?
- Does it set up a backdoor listener?

There are a number of open-source monitors and trackers. The list below is not inclusive, but is intended to provide examples. No attempt has been made to evaluate these sites or services and they are not endorsed by Internet2.

DroneBL (www.dronebl.org), an open-source real-time monitor of abusable IPs, which has the goal of stopping abuse of infected machines.

ZeusTracker (https://zeustracker.abuse.ch) provides the ability to track ZeuS (also known as *Zbot* / *WSNPoem*) command and control services and hosts of ZeuS files. ZeuS is a crimeware kit, which steals credentials for various online services like social networks, online banking accounts, ftp accounts, email accounts and other phishing. The main focus is to provide system administrators the possibility to block well-known ZeuS hosts and avoid ZeuS infections in their networks.

MalwareURL (http://www.malwareurl.com/rss.xml?n=1&limit=100) provides a list of known malware sites.

Router blocks – use Wireshark (network protocol analyzer) or router blocks to find infected machines. www.wireshark.org.

How do I create the ability to block compromised hosts?

DHCP blocks – Dynamic Host Configuration Protocol (DHCP) allows devices to be added to a network with little or no manual intervention. A DHCP server manages a pool of IP addresses and information about client configuration parameters such as default gateway and domain name. However, such servers are potentially vulnerable to hackers hijacking the process and configuring clients to use a malicious DNS server or router. In addition, unauthorized clients can masquerade as a legitimate client and gain access to network configuration and an IP address.

You can block clients from accessing the network by blacklisting their MAC address on the DHCP server. A blacklist can tell the server to reject or quarantine requests from the client.

NAT/PAT/Proxy blocks – Network address translation (NAT) is the process where a network device, usually a firewall, assigns a public address to a computer (or group of computers) inside a private network. During PAT (port address translation), each computer on the LAN is translated to the same IP address, but with a different port number assignment. Once such devices or groups of devices are found to be compromised, access can be blocked.

Wireless blocks – You can use one of several methods for blocking access to your wireless network by machines that are compromised or are suspected to be compromised:

- Via DHCP (see above)
- via 802.1x
- via RADIUS

VPN blocks – You can use your VPN configuration to block traffic or make it more difficult to access resources. If you allow access to a wireless network, you can place resources in a VPN, requiring authentication to proceed.

Inject null routes into the router.

Other methods to consider:

- Firewalls
- Access Control Lists (ACL)
- Network Access Control (NAC) quarantine

Metrics – What Should I Measure and Why?

A security metrics program looks at specific network data on a regular basis, providing early clues to changes in attack patterns or environmental factors that may require changes in security strategy. Metrics should be collected and generated on a regular basis (ideally, automatically), and they should be consistent and objective.

When grouped with measurements from other institutions, this information becomes even more valuable and helps develop a standard measurement of computer security within higher education (see the information for REN-ISAC, an organization the collects security information, in the Resources section of this guide).

The Security Metrics Project Team, a part of the Effective Practices Working Group has developed a set of recommended security metrics – a starter set of items that colleges and universities should measure. The working group focuses on identifying and promoting practices, tools, and procedures that will lead to the development of interchangeable metrics representing a comprehensive picture of the security environment. The group compiles best practices and shares them with higher education.

The group has posted its starter metric recommendations on the Internet2 wiki:
https://wiki.internet2.edu/confluence/x/rwFG.

Center for Internet Security (CIS) metrics are published here:
http://www.cisecurity.com/securitymetrics.html

EDUCAUSE Quarterly (July-September 2008 issue) included an excellent article on metric basics.
Use the tiny URL: http://tinyurl.com/EdQuarterly
Or use the original URL:
http://www.educause.edu/EDUCAUSE+Quarterly/EDUCAUSEQuarterlyMagazineVolum/SecurityMetricsASolutioninSear/163096

Resources

Computer and Network Security in Higher Education, particularly chapter 6.
http://www.educause.edu/Resources/Books/ComputerandNetworkSecurityinHi/5746

The EDUCAUSE and Internet2 IT Security Guide:
https://wiki.internet2.edu/confluence/display/itsg2/Home

See especially, the guide's Security Architecture and Models section:
https://wiki.internet2.edu/confluence/display/secguide/Security+Architecture+and+Models

REN-ISAC (Research and Education Networking Information Sharing and Analysis Center)
REN-ISAC (www.ren-isac.net) is a private trust community for sharing sensitive information regarding cyber security threat, incidents, response, and protection. Membership is open to colleges and universities, teaching hospitals, research and education network providers, and government-funded research organizations.

The REN-ISAC receives, analyzes and acts on operational, threat, warning and actual attack information derived from network instrumentation and information sharing relationships. Instrumentation data include netflow, router ACL counters, darknet monitoring, and Global Network Operations Center operational monitoring systems. Information sharing relationships are established with other ISACs, DHS/US-CERT, private network security collaborations, network and security engineers on national R&E network backbones, and the REN-ISAC members.