Global Information Assurance Certification Paper

Circle of Security

Stephen P. Norton - November 13, 2000

The goal of an information security program is to protect the integrity, confidentiality, and availability of information[1]. An effective information security program consists of a cohesive system of resource protection, system monitoring, data collection, and coordinated responses to detected incidents.

Although not a new or unique concept, the "Circle of Security"[2,3] generally consists of three contiguous and continuous phases: **Protection**, **Detection**, and **Response**. These three phases provide for a never-ending cycle of refinement and evolution of the security envelope. The cycle provides for reasonable and prudent protective measures, constant and consistent monitoring for detection of anomalies (events), and the appropriate responses to such anomalies

Protection Phase

The **Protection** phase consists of those steps necessary to safeguard information resources. Comprehensive policies and procedures in conjunction with a risk management program will provide the framework for identifying the types of protection needed, and where the protective tools should be placed.

Protection Phase Components:

- Information Security Policies
- Risk Management
- Authentication
- Access Controls
- Content Filtering
- Encryption
- Security Awareness

Information Security Policies

Written information security policies and the determination of acceptable behavior is paramount to an effective security program and establishes an enforceable set of rules. Security policies should be reviewed and updated as necessary.

Risk Management[4]

All risk cannot be avoided. Risk should be managed and mitigated where possible. An effective risk management program will incorporate risk analysis and assessment. Risk analysis is a process that identifies and assesses threats and vulnerabilities to an information system, and determines acceptable levels of risk, and provides for appropriate countermeasures.

Primary sources of threats: [5]

- Natural disasters
- Intentional, malicious attacks

- Unintentional threats through errors or omissions

Common vulnerabilities: [5]

- Restrictive user account policies
- Weaknesses in operating systems, and applications, and protocols
- Improperly configured security devices
- Lack of adequate protective measures or unprotected access points

Authentication

Extensive measures must be taken for authentication to ensure access to the network and its systems by properly authorized users. Various levels of authentication include something you know (passwords), something you have (tokens), and something you are (biometrics). These levels provide increasingly stronger assurances as to the identity of the user.

Access Controls

Access Controls are those policies, procedures, and tools that control access to resources. Logical access controls typically come into play in the form of system user profiles for access to network resources. Firewalls are access control tools designed to provide access control protection between trusted networks (corporate) and untrusted networks (Internet, B2B partners). Ideally, a layered firewall approach is most effective in placing a network's core resources, behind multiple of firewalls with correspondingly more restrictive access controls.

Content Filtering

A multi-tiered, or "Defense in Depth"[6] approach is also recommended as the best way to deal with attacks from malicious code such as worms, viruses, Trojan horses, or hostile Java and ActiveX applets. Protective measures should be placed at Internet or untrusted network gateways, mail and file servers, and workstations.

Different vendors may have different attack signature databases. Utilizing different vendor solutions may provide a higher level of protection rather than the use of a single vendor at all levels. Vendor products that utilize a method of checking the actions of code, rather than simply checking for known signatures should be implemented at one or more stages.

Encryption

The integrity of data in storage and in transit can be assured through encryption and the use of digital certificates. Encryption scrambles the data so as to make it unreadable to unauthorized viewers of the data. Digital certificates can be used to verify the sender of the data in transit and to provide assurance that the data was not tampered with during transit.

Security Awareness

End-users must be aware of the threats to the network and its resources, and assist in taking protective measures.

Detection Phase

Detection should be considered more important than protection. Even the most comprehensive security systems cannot protect against all attempts to compromise security measures. The Detection phase provides for constant and consistent monitoring for inappropriate system activity and adherence to policies. The multi-phase approach provides for detection of intrusions at network access points, intrusions or misuse of critical systems, and analysis of system policies and procedures. Audit trails provide additional sources for identifying events and provide historical records of such activity.

Detection Phase Components:

- Network and Host Based Intrusion Detection
- Network and Host Monitoring
- Auditing

Network and Host Based Intrusion Detection

An intrusion detection and response system can either be network-based, host-based, or a hybrid of both. Neither system is able to detect all known threats and attacks. The most effective method is to combine the two into a real-time system that can detect known attack signatures and patterns, as well as suspicious activity, including probes of the network or critical systems and unauthorized attempts to modify access control mechanisms. The system should be configurable to provide for immediate and automated alerts to such activity, and provide for configurable actions such as logging and automatically terminating the session.

Network-based Intrusion Detection is advantageous because it can detect threats and attacks *before* they reach critical systems. Agents or sensors are typically placed along the perimeter of the network behind firewalls and other access points to detect unauthorized activity that may compromise the perimeter defenses. Network agents can also be placed on subnets in order to scan traffic that may cross the backbone. Placing agents or sensors in front of perimeter devices has the added advantage of detecting probes and attacks that may be stopped by the perimeter devices, and provides substantial information as to the value and effectiveness of those devices.

Host-based Intrusion Detection can detect threats and attacks on critical systems that may not be detectable by network-based systems including file access and encrypted transmissions. Host-based agents may be better than network-based agents at capturing user identifiers. Critical systems should be identified and protected.

Network and Host Monitoring

Real-time monitoring of the network can detect unauthorized activity by internal users and provide for immediate alerts to technical staff of such activity. Real-time monitoring of system configurations, access control modifications, and user accounts can also lead

to detection of unauthorized or inappropriate activity. Automated responses can include logging the activity and session termination.

Auditing
A system-wide audit program should be implemented to provide for immediate and full logging of activity to provide for user accountability. A central repository for the audit logs will provide for immediate and historical reference in response to an investigation or management request for information. The program should also include security and statistical analysis tools to evaluate the audit logs. The audit program should include procedures to verify the integrity of individual systems and for compliance with existing system and security policies and procedures.

Response Phase

The **Response** phase is triggered by detection of an anomaly or "*event*". An automatic event alert should occur based on inappropriate activity and identified attack signature or patterns. Incident response procedures dictate the action to be taken during and after an event occurs. Technical staff should be trained on these procedures to provide for an appropriate and measured response. Response procedures may require the collection and preservation of evidence (Forensics) which may be necessary in the advent of an investigation or prosecution. Assessment of events and their responses provide for refinement of all phases of the "Security Circle." Disaster recovery procedures may invoke depending upon the severity of the event.

Response Phase Components:
- Incident Response
- Forensics
- Disaster Recovery
- Security Assessment

Incident Response
Immediate and tactful response is necessary in the event of a threat, attack, system compromise, or misuse of network resources. A Computer Security Incident Response Capability (CSIRC) team should be formed and trained to respond to an identified security event. Automated response capabilities should be incorporated whenever possible.

Forensics
Computer forensics is the collection, preservation, analysis, and presentation of computer evidence. If a security event occurs, computer evidence may need to be gathered as the result of an investigation in order to provide assistance with personnel actions, or in the prosecution of those responsible.

Disaster Recovery
Disaster Recovery procedures may be invoked if the severity of the event is high enough to require it. This could result from the destruction of a critical system through

an intentional or unintentional compromise. It may also happen as the result of a natural disaster.

Security Assessment
Detailed analysis of detected events and their responses lead to continual refinement of the three phases. System weaknesses are identified for re-fortification, false positives are eliminated, and thresholds are revised. Security awareness programs are enhanced. Periodic assessment of systems, policies, and procedures provide for effective augmentation of existing security programs, and the implementation of new security measures and countermeasures.

And the cycle continues……

References:

[1]Benson, Christopher, Inobits Consulting (Pty) Ltd. "Security Strategies." URL: http://www.microsoft.com/technet/security/secstrat.asp.

[2]Axent Technologies, "Lifecycle Security Model." URL: http://www.axent.com/Axent/Public/Main?nav=Security&detail=Lifecyclemodel

[3]Microelectronics Center of North Carolina. "Information and Network Security Issues." October 7, 1998. URL: http://www.anr.mcnc.org/cs591w/m03/m03.ppt

[4]Computer Security Resource Center, National Institute of Standards and Technology (NIST). "Engineering Principles for IT Security (EP-ITS) (A technical baseline for achieving security capabilities)." Draft document. URL: http://csrc.nist.gov/publications/drafts/issep.html

[5]Benson, Christopher, Inobits Consulting (Pty) Ltd. "Security Planning." URL: http://www.microsoft.com/technet/security/secplan.asp.

[6]Galik, Captain Dan, United States Navy. "Defense in Depth, Security for Network-Centric Warfare." URL: http://www.norfolk.navy.mil/chips/archives/98_apr/Galik.htm

Other Resources:

Schneier, Bruce. "Secrets and Lies, Digital Security in a Networked World." 2000. Published by Wiley Computer Publishing.