2006 Alaska Information Assurance Workshop

2006 Alaska Information Assurance Workshop

Hosted By

The University of Alaska Fairbanks
Advanced Systems Security Education, Research, and Training (ASSERT) Center

September 5th and 6th, 2006

Detection: Managing the Challenges

Julie J. C. H. Ryan, D.Sc.
School of Engineering and Applied Science
George Washington University

Daniel J. Ryan JD
Information Resources Management College
National Defense University

Detection as a Process

- **Which phase of security is the most important?**
  - **Protection**
  - **Detection**
  - **Reaction/Correction**
- **A trick question**
- **Each is equally important**
  - **Allocation of scarce resources**
  - **Doing something once things go wrong**

Why Equal?

- When you decide to take steps to protect some asset, you are making a value judgment
  - When you decide not to spend the resources to protect against potential problems, it may be a value judgment or it may reflect the reality that it may be impossible
- Once you've spent resources on protection, makes no sense not to put processes in place to detect problems
  - Otherwise, why bother?
- Continuity of operations, crisis reaction, and business continuity efforts contingent on detection capabilities

Types of Detection Efforts

- Four classes of problems that need detection
  - Problems that were protected against
    - Failure of the protection mechanism
    - Occurrence of the problem despite protection mechanism
  - Problems that were not protected against
    - Occurrence of the problem
  - Problems that no one had a clue could occur
    - Existence of problem
    - Occurrence of the problem
  - Insider problems
    - Abuse of trusted access

Timing of Detection

- How fast does detection have to occur? It depends….
  - How fast can bad things happen as a result of the problem?
    - Nanoseconds? Then detection has to happen in nanoseconds
    - A day? Then detection needs to happen within 24 hours
- Speed of detection contributes to overall security status
  - Security needs can be evaluated in time
    - Burglar takes 15 minutes to break window, grab goodies, and egress through window
      - That means detection and reaction needs to occur within 15 minutes
    - Add 30 minutes of protections (bars, fences, etc)
      - Detection and reaction time increases to 45 minutes

The Detection Timeline Problem

- Sometimes, detection occurs well after problems have occurred
  - Robert Hanssen detected spying many years after first begun
  - Aldrich Ames same thing
  - Same thing happens with computer system compromises
- If detection efforts are not robust or are not followed, actual detection will not occur effectively or efficiently
  - Testing the detection mechanisms is as important as testing the protection mechanisms
  - Testing the triggering of follow-on activities is important as well

Detection Resources

- **Detection activities require special attention**
  - **Personnel**
    - **Special skills, special trust levels**
  - **Facilities**
    - **Segregated analysis centers, protected capabilities**
  - **Equipment**
    - **Specialized equipment, specialized handling capabilities**
  - **Interface with law enforcement**
    - **Potential for criminal or military responses**
  - **Policy framework**
    - **Make sure no laws are violated conducting detection efforts**

What Happens After Detection

- **Just as it is not enough to simply protect assets, it is not enough to simply detect problems**
  - **There must be a business process in place to transition from detection to reaction/correction processes**
- **In many instances, these processes may need to occur simultaneously, which may cause problems**
  - **Crisis reaction**
  - **Business recovery**
  - **Continuity of operations**

Contact Information

Julie J.C.H. Ryan, D.Sc.
1776 G. Street NW #101
Washington DC, 20052
jjchryan@gwu.edu
http://www.seas.gwu.edu/~infosec/

The George Washington University is an NSA Certified Center of Academic Excellence in Information Assurance Education and meets the Federal Training Standards for Information Systems Security education. We offer Graduate Certificate, Master's, and Doctoral level education in Information Security Management for professionals from all educational backgrounds. GWU is located in the heart of Washington DC very near the White House and other government offices.