How to Tell When an Insider is About to Go Bad

MiniMetriCon Conference – Feb 14, 2011
Lightning Talk!!!

Dr. Fred Cohen
President - California Sciences Institute
CEO – Fred Cohen & Associates

Insiders Go Bad

- Insiders
  - Systems administrators / privileged users / high level executives / employees who work there
- Go
  - Transition of some sort
- Bad
  - Do things they shouldn't – for example...
    - Take control and don't release it
    - Leak classified data to Wikileaks
    - Cause systems to fail (and save the day?!?)
    - Corrupt content intentionally
    - Take money from the organization

What is most common?

- They have a common pattern of behavior
  - 80+% of caught display this sequence
    - Do something bad
    - Don't get punished
    - Escalate (likely loop once or more)
    - Do something really bad
    - Get fired / prosecuted / etc.
  - As they escalate, they tend to “cover up” more and better than before

An insider about to go bad?

- If you see rat droppings, likely rats
  - Look for disciplinary problems
  - Look for “it's OK” management attitude
  - Look for cover-up attempts
- Metrics:
  - How do you measure “disciplinary problems”?
    - Especially when management lets it slip...
  - How do you detect cover-ups?
    - Seek inconsistencies

Cover-up detection

- Alterations produce trace inconsistencies
  - If they are not don the “normal way”
- Look for inconsistencies – but...
  - Must be associated with cover-ups
  - Must have low or 0 base-rates
  - Better if they are more generic classes
  - Better if particularization is feasible
- Or – generate your own...
  - Create added traces to produce more readily detectable inconsistencies
  - Low base rates, etc. also needed ...

References

- M Keeney, E. Kowalski, D. Cappelli, A. Moore, T, Shimeall, S. Rodgers, “Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors”, Jan 2005.
- E. Shaw, K. Ruby, and J. Post, “Insider Threats to Critical Information Systems: Typology of Perpetrators, Security Vulnerabilities, Recommendations”, Aug 31, 1999. ASD-C3I – OIO - Contract # 98-G-7900, Task Letter Number 001:Insider Threat Profile.
- E. Shaw, K. Ruby, and J. Post, “Insider Threats to Critical Information Systems: Characteristics of the Vulnerable Critical Information Technology Insider (CITI) Contract Nr. N39988-97C-7850, Sep 25, 1998.
- E. Shaw, K. Ruby, and J. Post, “The Insider Threat to Information Systems - The Psychology of the Dangerous Insider ”, Security Awareness Bulletin, No. 2-98, 1998.
- F. Cohen, "Analysis of redundant traces for consistency", IEEE International Workshop on Computer Forensics in Software Engineering (CFSE 09), Seattle, Washington, USA, July 20-24, 2009.

Thank You

http://calsci.org/ - calsci at calsci.org
http://all.net/ - fc at all.net