RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: HUM-W03

Proactive Measures to Mitigate Insider Threat

Andrew Case
Director of Research
Volexity
@attrc

#RSAC

Insider Threats – Statistics

- PWC 2015:
  - Roughly 70% of incidents at financial institutions involved current and former employees
  - 60% at industrial manufacturing organizations
- Verizon DBIR 2015: 20.6% of breaches are characterized as “insider misuse”

Insider Threat Defenses – Passive/Default

- Examples
  - Production systems without extra logging or security measures
  - No automated alerts or remote logs generated
- Pros
  - Simplest to implement
  - Provides the evidence needed for post-mortem forensics
- Cons
  - Only useful after damage is caused
  - Can be fully disrupted by anti-forensics
  - Often very expensive and non-repeatable

Insider Threat Defenses - Detection

- Examples
  - Log file accesses, software installation, and USB device usage
  - Generate alerts on access to file storage services (e.g., Dropbox)
- Pros
  - If implemented correctly, finds activity before it causes harm
  - Less inhibiting than full prevention
- Cons
  - If implemented incorrectly, finds activity after irreparable harm
  - Requires active effort by the security team

Insider Threat Defenses - Prevention

- Examples
  - Prevent all removable media from being used
  - Block access to personal email and file storage services
  - Block end-users from installing software
- Pros
  - Stops a technique before it can be used
  - Cheapest once implemented
- Cons
  - Often clashes with a company's office culture
  - Can inhibit department-specific productivity

Application to Real World Cases

- We will now look at several real-world insider-threat cases that I investigated
- Combined, the insiders took over 100 million dollars of IP/customers from their previous employers (my clients)
- As I describe these cases, think about how your company would currently fare against such malicious activity and what, if any, mechanism(s) you have in place to detect the activity before irreparable harm is done

The Bank Heist - Background

- Employee of a financial institution sees greener pastures at a competitor
- Contacts competitor about bringing him and his team to the competitor
  - Along with their very wealthy clients
- Proceeds to take nearly every document related to the clients, his team's records, and client management forms

The Bank Heist – Forensic Analysis

- File servers and internal web apps were scraped for sensitive information
- Moved data out of organization control through USB, personal email, and printing
- Files were locally deleted after being exfiltrated
- The forensic timeline showed over 100 files taken and the precise times that the actions occurred

Proactive Measures – File Search

- Secure Network Architecture
- Monitoring File Share Accesses

Proactive Measures – File Exfiltration

- USB
- Printing/Scanning
- Personal Email
- Cloud Storage*

* This case is several years old and cloud services were not very popular then but are used extensively in modern, similar scenarios

Abuse of Power - Background

- Plant manager at a manufacturing company was using “down time” of the company’s machines to run a side business
- He purchased some materials on his own, some were ordered through the company’s accounts
- Was only caught through a machine malfunction

Abuse of Power – Forensic Analysis

- The rogue manager had logged into control systems during non-client billable hours
- The manager scheduled manufacturing jobs outside of any legitimate work order
- The manager deleted associated files in a failed attempt to cover his tracks

Proactive Measures – Accounts & Systems

- Technical measures
  - Monitor user logins
  - Monitor system usage
- Business measures
  - No critical business processes should be controlled by one person

Offline Exfiltration - Background

- Victim organization had very tight data exfiltration controls
- Laptops utilized full disk encryption (FDE)
  - ... but desktops did not!
- Path to exfiltration:
  1. Copy sensitive files to desktop during business hours
  2. Remove hard drive before leaving and take home
  3. Offline mount hard drive and copy files

Offline Exfiltration – Forensic Analysis

- If done properly, this leaves no traces for (reasonable) forensics to find
- The employee in this instance could create, modify, and delete files from the disk at will
- Was only caught after making other “mistakes” and confessing to the disk removal

Proactive Measures - Full Disk Encryption

- Utilize FDE for everything!
- Be wary of offline decrypt capabilities
  - The user knows his/her own password…

Anti-Forensics - Background

- Two key employees leave the victim company simultaneously
- Soon after, important clients end contracts
- Previous employees' equipment investigated for signs of improper client interactions

Anti-Forensics – Forensics Analysis

- Employees utilized heavy anti-forensics
- Both factory reset their company provided Android phones
- Employee 1 ran CCleaner before returning his computer
- Employee 2 replaced the hard drive with one bought from Amazon

Anti-Forensics – Proactive Measures

- Tracking application downloads and installs
- Application whitelisting

Proactive Measures – Employee Termination

- Companies work against themselves by not properly assessing and preserving employee equipment (laptops, desktops, phones, tablets) post termination
- These policies, or lack thereof, can inhibit forensic investigation, legal proceeding, and recovery and understanding of stolen data

Bad Policy Examples

- Re-install/re-purpose systems immediately upon employee termination
- No check of all system components against IT inventory
- No check of historical removable media usage

Get Proactive Against Insider Threat

- Within a month you should be able to identify:
  - Deficiencies that could allow for exfiltration
  - Deficiencies in key employee oversight
  - Policy deficiencies related to employee termination
- Within three months be able to:
  - Remediate critical deficiencies
  - Have a working plan to remediate all deficiencies

Wrapping Up & Q/A

- If you aren't being proactive then you are just waiting to become a victim
- While insider threats are the most prevalent, they are also the most preventable through proactive policy and technical controls
- Contact info:
  - acase@volexity.com (3DE6E0C8)
  - @attrc