Insider Threat Assessments

A methodology for improving insider threat deterrence and detection

9/12/2019

Ben Stewart, Security Innovation

About Me

- Ben Stewart
- Security Engineer & Researcher
- Background in Financial Services
- Blockchain Center of Excellence Lead
- Automation Aficionado

Insider Threat 101

Insider threats are common

Out of the whopping 41,686 security incidents and 2,013 data breaches profiled in the 2019 Verizon Data Breach Investigations Report, **34%** involved internal actors (Verizon LLC, 2019). The individuals tasked with protecting your enterprise are a great asset but also pose a tremendous threat.

Common motivations:

- Personal financial gain
- Revenge
- Dissatisfaction
- Respect
- Accidental

Increasing risk

The likelihood of an insider threat **increases** for organizations that store sensitive **customer data**, have valuable **intellectual property,** or support **critical infrastructure**.

Although multiple industries meet these criteria, history has proven that Financial Services or other infrastructure is often a target with devastating results. We have seen prized assets catalogued, exfiltrated, and sold to the highest bidder.

What is an Insider Threat?

Simply put, a security risk to the organization that comes from within the business itself.

Common threat actors:

- Current and former employees
- Contractors
- Contributors in the supply chain
- Anyone that has/had access to the business in some way

It’s a hard problem to solve

The insider threat is one of the most complicated and costliest to detect of all types of attack.

Why?

Answer: The attack originates from within and doesn’t have to be intentional

Types of Insider Threats

- **The Careless Worker**: Misuser of assets
  - Installs unauthorized applications
  - Has unapproved workarounds
- **The Inside Agent:** Stealing information for outsiders
  - Recent behavioral changes
  - Does not follow company policies
- **The Disgruntled Employee:** Destroying property
  - Was glanced over for a promotion
  - Demonstrates change in approachability
- **The Malicious Insider:** Stealing information for personal gain
  - Unusual working hours
  - Increased access requests
- **The Feckless Third Party:** Compromising security
  - Negligent use of company assets

Kill Chain and IOCs

Step 1: Reconnaissance

A malicious insider will generally start by seeking out files and data to steal. The key to catching an attacker in this stage is to keep an eye on users who access unusual locations or run unusual applications.

High risk user activities:

- Unusually rapid rate of opening files in a short period of time
- Accessing new or unusual locations in a document repository
- Network scanning and use of network tools
- An unusual increase in error or access denied messages
- Failed attempts to mount USB devices and access external websites
- Running applications that they've never run before (known hacking applications)

Step 2: Circumvention

Attackers research options for getting data out of an organization. This can run the spectrum from simple, straightforward means like file-sharing websites to more complex methods like proxy servers or VPN connections.

High risk user activities:

- Use of tools like VPNs, proxy servers, or TOR to mask internet activity
- File transfers through alternative protocols (IM, Email, Social Media, etc.)
- Use of blacklisted tools
- Sharing of information via sites like PasteBin or communities like Reddit or social media networks
- Disabling or bypassing security software

Step 3: Aggregation

Attackers will aggregate the data they're preparing to exfiltrate.
Detection should be centered on monitoring unusual file activity.

High risk user activities:

- Unusual amounts of file copies, movements, and deletions
- Unusual amounts of file activity in high-risk locations and sensitive file types
- Unusual creation of files that are all exactly the same size
- Saving files to an usual location

Step 4: Obfuscation

Attackers *almost* always attempt to cover their tracks before stealing data. Methods range from renaming files to disabling security tools to encryption.

High risk user activities:

- Use of encryption or encoding tools
- Unusual rates of file compression
- Hiding sensitive information in image, video, or other misleading file types
- Unusual rates of file renaming

Step 5: Exfiltration

During this step, an attacker will perform the actual theft by exfiltrating the sensitive data and information. Hopefully, you caught the rogue insider long before they get to this point.

High risk user activities:

- Unusual destinations of file transfers
- Unusually large rate of file transfers
- Use of external drives or other media not under control of the organization

An Attackers Toolbox

- Publicly available tools are adding sophistication to every step of the insider threat kill chain
- Whether using the sound produced from a CDROM drive, the Spotify API, or cloaking one form of data in another, sensitive data is leaving organizations under the radar of common detection tools. These novel techniques are ever changing and widely available.
- Awareness about these attacks is important
  - Awesome Data Exfil Repository: https://github.com/benstew/awesome-data-exfiltration
  - Mitre ATT&CK Matrix: https://attack.mitre.org/matrices/enterprise/

Defensive Tools Landscape

Don’t spin your wheels

Organizations have been focusing more on ways to mitigate insider threats, but this is impossible to do without a clear understanding of:

- What data is valuable?
- Where it is stored?
- Who is accessing it?

It’s vital to understand the relationship between users, systems, and data. Threat modelling, intelligence gathering, attack surface analyses and IAM can do wonders.

Bare minimum tool belt

“An effective insider threat program incorporates a number of technical controls to assist with preventing, detecting, and responding to concerning behaviors and activity" (Spooner et al, 2018)

- User Activity Monitoring (UAM)
- Data Loss Prevention (DLP)
- Security Information and Event Management (SIEM)
- Analytics
- Digital Forensics

User Activity Monitoring (UAM)

Monitor and track user behavior on devices, networks, and other company-owned IT resources. Organizations will adopt a range of activity monitoring tools to help detect and stop insider threats. The range of monitoring and methods utilized depends on the objectives of the company.

Examples:

- Video recordings of sessions
- Log collection and analysis
- Network packet inspection
- Keystroke logging
- Kernel monitoring
- File/screenshot capturing

Data Loss Prevention (DLP)

DLP detects potential data breaches/data ex-filtration transmissions and prevents them by monitoring, detecting and blocking sensitive data while *in use* (endpoint actions), *in motion* (network traffic), and *at rest* (data storage).

Further Detail:

- Network
  - Installed at network egress points near the perimeter
  - DLP systems that protect data in-use may monitor and flag unauthorized activities.
  - protect data in-motion monitor sensitive data traveling across a network
- Endpoint
  - Active on internal end-user workstations or servers.
  - Aide with controlling the information flow between groups or types of users
  - Ability to control email and Instant Messaging communications.
- Data Storage
  - In this context, archived information.
  - Longer data is left unused in storage, more likely to be used by unauthorized individuals
  - Protection methods include access control, data encryption and data retention policies

Security Information and Event Management (SIEM)

SIEM combines security information management (SIM) and security event management (SEM to provide real-time analysis of security alerts generated by applications and network hardware.

Necessary Components:

- Data aggregation:
  - Data from many sources, including network, security, servers, databases, applications, providing the ability to consolidate monitored data to help avoid missing crucial events.
- Correlation:
  - Looks for common attributes, and links events together into meaningful, logical groupings among different sources to turn data into useful information. Can be surfaced via some dashboard
- Alerting:
  - The automated analysis of correlated events
- Retention:
  - Long-term storage of historical data to facilitate correlation over time, and to provide the retention necessary for compliance requirements. Generally a requirement for forensics.

Analytics

Security Analytics is an approach to cybersecurity focused on the analysis of data to produce proactive security measures. Ideally you have a unified view of the enterprise, traffic, other business requirements.

Examples:

- Monitored network traffic could be used to identify indicators of compromise before an actual threat occurs.

Digital Forensics

The recovery and investigation of material found in digital devices and systems, often in relation to an incident.

No two insider threat investigations are ever the same

- Standardized process can help the investigation run more smoothly
- Know how to prove what was exfiltrated and whether it was done inadvertently, opportunistically, or maliciously.

Shortcomings

Shortcomings

- Configurations
  - Difficult to test end-to-end
- Error Rate
  - False positives or false negatives
- Lack of Validation
  - Quantify effectiveness
  - Rusty practitioners

Overpromise of AI

- Spend time looking at the ROI for these solutions
- There is no silver bullet for preventing insider threats
- Recognizing anomalous behavior can be challenging since the benchmarks can already be flawed
- Intelligent solutions should not be a crutch or replacement of information security professionals

Insider Threat Assessments

WHY?

Giving organizations a proactive, situational procedure to validate their insider threat program reduces gaps in coverage, limits tool or service misconfigurations, helps prevent system and model oversights, and provides real world practice scenarios.

What this looks like in practice

- Threat Modelling
  - Identifying and prioritizing risks that an organization might face
  - Gap analysis relative to insider threats
- Attack Simulations
  - Passive or active scanning of hosts in network
  - Infrastructure based assessment
- Software specific red teaming – My Favorite!
  - Attacker scoped to specific privileges and duration
  - How much damage can be caused from this position

Insider Threat Assessment Methodology

Insider Threat Assessment Methodology

Goal: Reduce organizational risk by validate configurations and coverage through a situational insider threat assessment.

How: A pragmatic, repeatable methodology to simulate various insider threat actors and to identify/validate potentially vulnerable processes, systems, or access levels.

Planning	Weaponization	Exploitation	Post Exploitation	Reporting
Pre-engagement Interaction	OSINT	Delivery	Privilege Elevation	Affected Areas
Information Gathering	Test Case Creation	Vulnerability Analysis	Command and Control	Steps to Reproduce
Threat Modeling	Configuration Payloads	Initial Access	Collection	Remediation
Critical Asset identification	Identify Exit Points	Defense Evasion	Exfiltration	Observations
Testing Scopes	Aggregate Tools	Lateral Movement	Chaining other Attacks	Conversation
Vendor Connectivity	Attack Tree	Persistence	Actions on Objectives	Comprehension

Deterrence

Deterrence

- Forgotten sibling to detection
- High ROI
- Can take many forms
  - Warning messages
  - Emails
- Building awareness is key
  - Trainings
  - Practice

The Future

AI + UEBA

- Artificial Intelligence continues to make advancements and the intersection with UEBA is promising
- Using patterns of human behavior to detect meaningful anomalies
  - Insider Threats
  - Advanced Persistent Threats
- Instead of looking at a system wide level, tracking the users
- Can help detect malicious behavior that goes unnoticed from other monitoring systems (SIEM or DLP)
- Increase efficiency of Information Security professionals

Insider Threat Resources

- 2019 Verizon Data Breach Investigations Report: https://enterprise.verizon.com/resources/reports/insider-threat-report.pdf
- Insider Threat Kill Chains: https://www.dtexsystems.com/blog/the-insider-threat-kill-chain-5-steps-to-watch-out-for/
- Insider Threat Tool Landscape - (Spooner et al, 2018): https://resources.sei.cmu.edu
- Awesome data exfiltration: https://github.com/benstew/awesome-data-exfiltration
- Red Teaming Toolkit: https://github.com/infosecn1nja/Red-Teaming-Toolkit
- Mitre ATT&CK Matrix: https://attack.mitre.org/matrices/enterprise/
- DLP Wikipedia: https://en.wikipedia.org/wiki/Data_loss_prevention_software
- Forensic Framework: https://link.springer.com/chapter/10.1007/978-3-642-35515-8_22
- National Insider Threat Task Force: https://www.google.com/search?client=firefox-b-1-d&q=national+insider+threat+task+force