MIS|TI™ PRESENTS

InfoSecWorld

Conference & Expo 2018

# BUILDING AN INSIDER THREAT PROTECTION PROGRAM

*Ana Roldan*

*AVP/CISO*

*Miami Dade*

# *Why do we have insider threats?*
# *Insider Threats Statistics*

- Insider Threats are responsible for 43% of data breaches (source code42)
- Top insider threats are identified as ‘privileged users’ – managers are 59% more likely to pose the greatest threat, followed by contractors and consultants 57% and regular employees 51%  (source - CIO Insight and Crowd Research Partners)
- Almost 95% of cybercrime is caused by negligent users (source – Intel)

# *INSIDER THREATS*

*VS*

# *OUTSIDER THREATS*

# *Types of Insider Threats*

- **Careless Insider** – someone who accidentally sends the wrong information to someone who shouldn't have received it

- **Negligent Insider** – knowing that there is a data security policy but takes steps to avoid it

- **Malicious Insider** – Someone with access to systems and takes advantage of their access for personal gain, insider threats can do more serious harm than external hackers

# *INDICATORS OF SUSPICIOUS BEHAVIOR*

# *Indicators of Suspicious Behavior*

- Working unusual hours
- Unusual computer use
- Inappropriate use of social media
- Vague answers to pointed questions
- Accessing restricted areas
- Unexplained disposal spending
- Making personal issues public
- Discontent with supervisors
- Disloyalty to the organization

# *What do employees take with them?*

- Customer information
- Sales lists
- Credit card information
- Health information
- Financial records
- Customer databases
- Strategic plans
- Employee personal information
- Proprietary formulas

# *Do your employees know what to do?*

- Implement a formal Security Awareness program
- Identify inappropriate behaviors – create policies and enforcement controls around how to report concerning or disruptive behaviors by co-workers
  - What to report?
  - When to report it?
  - Whom to contact?

# *HOW ARE YOU VULNERABLE*

# *How are you vulnerable?*

- Insufficient strategies and solutions such as visibility and alerting
- Lack of user behavior analytics - VISIBILITY
- Exfiltration of sensitive data moving outside of the firewall and mobile devices or through remote access
- Lack of security awareness training

# *How are you vulnerable?*

- Privilege account abuse  - who has access and WHY?
  - Admins
  - Consultants and vendors
  - DBA's and Developers
- Vendor Accounts
  - How are you keeping track?
  - How do you know if they have left employment?
  - Is remote access restricted and monitored?

# *How are you vulnerable?*

- System Accounts
  - Who has knowledge of these accounts?
  - Accounts that run as a process
  - Accounts that are embedded in scripts
  - Are you resetting the passwords periodically?
  - Check-out – check-in that monitors usage

# STEPS TO IDENTIFY RISKY USERS

# Steps to Identify Risky Users

- Anomalous behavior
- Employees who resign (Red flags) – monitor mode until their last day
  - Monitor their internet activity
  - Excessive file upload to cloud file sharing services (Dropbox, OneDrive, etc.)
  - Remote access (VPN) after hours
  - Email activity

# Steps to Identify Risky Users

- Rule based alerts examples using security intelligence and user behavior analytics :
  - User IT admins granting access to other users
  - Individuals that are elevating privileges
  - Unauthorized activity on servers
  - Suspicious internet activity
  - Activity on cloud file sharing services
    - Excessive uploads
  - Downloading of software

# HOW TO MITIGATE YOUR EXPOSURE TO INSIDER ATTACKS?

# How to mitigate your exposure to insider attacks

- Build a team and get executive buy-in
  - HR
  - Legal
  - Executive staff
  - IT
  - Security
- Implement a solution that provides security intelligence and user behavior analytics
  - Log correlation SIEM solution and assign risk level aligned with specific level of monitoring and alerts

# How to mitigate your exposure to insider attacks

- Identify which employees represent the greatest risk and assign a level of monitoring based on risk level
  - Employees
  - Privilege account users (DBA's, developers, admins)
  - Consultants

# How to mitigate your exposure to insider attacks

- Identify old legacy applications that are vulnerable and limited to upgrades by implementing compensating controls to secure them

# How to mitigate your exposure to insider attacks

- Understand what is normal and what is not normal on your network.  By doing that and getting that kind of visibility, it helps you understand how robust your IT security is and it helps you understand if you have good security practices
  - Which accounts are not being used
  - Which accounts are stale
  - Which end points are stale

# How to mitigate your exposure to insider attacks

- Which users have weak passwords (password policy)
- Which users are doing things that may not be right from a security standpoint
- Privilege account users
- Consultants
- Vendors

# How to mitigate your exposure to insider attacks

- Reduce vulnerabilities
  - Prevention
  - Detection
  - Response
  - Incident Response Plan and team – TEST IT!

# HOW TO FEEL MORE SECURE

# How to feel more secure

- Take a holistic view of your infrastructure of where your vulnerabilities are:
  - End points
    - Desktops – Thumb drives, standard secure images, endpoint security
      - Consider Virtual Desktop Infrastructure (VDI)
    - Laptops
    - Encryption
    - Servers
    - Remote access – printing and saving locally from home personal devices

# How to feel more secure

- Visibility - Log Correlation SIEM Solution
- Tools that provide "User Behavior Analytics" – *Anomaly* detection software helps organizations identify abnormal *user behaviors* and avoid potentially serious problems
- The biggest challenge is making sense and interpreting the data that you are collecting
- Data Loss Prevention (DLP) solutions

# How to feel more secure

- Security awareness training
  - Phishing attacks
  - Emails with attachments and links
  - Send out periodic security awareness newsletters
  - Screen savers with security messages
  - Communicate, communicate, communicate

# Q&A

MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

# THANK YOU

## PLEASE FILL OUT YOUR EVALUATIONS!

*Ana Roldan*

*AVP/CISO*

*Miami Dade*