Privileged Access Management: Unsticking Your PAM Program

Lance Peterman
Identity & Access Management Architect
Merck
@lpeterman
A little about me...

- Obligatory horse photo...
- Opinions are my own
Agenda

- What is PAM?
- Why PAM is necessary?
- In the News
  Recent Data Loss / Breaches
- PAM as a Program/Service
  - The Practice
  - Collaboration is Key
  - Reference Architecture
  - Use Cases
- Adoption Approach/Keys to Success
- Challenges & Final Thoughts
What is Privileged Access Management?
What is PAM?
Privileged access: is defined as any feature or facility of a multi-user information system that enables the user to override system or application controls (e.g. Administrator, Root, or similar high-level privileges)
**Privileged accounts or identities**

- Hold special or extra permissions within a system, application or database
- These accounts can grant broad access to underlying business information in systems
- Ideally, only used by authorized individuals when elevated privileges are required to fix urgent problems, or...
- Misuse can significantly affect the organizations business (risk)*
The use of privileged accounts should be managed and the password monitored when stored digitally. Privileged account activity should be logged and traceable to a unique user.
Identity is the New Perimeter

Old Model

New Reality

Identity is a top security control today that can determine what you are authorized to do, regardless of your location.
Breaches, Old and New
Service Accounts

- Compromise of privileged accounts resulted in 3.4m individual taxpayers and businesses losing sensitive data [1]
- Root account compromised? Nope...
- Good taxpayers of South Carolina were compensated for this with...1 year of credit monitoring
Local Admin Privileges

- 30,000 PCs had hard drives erased through compromise of a privileged account.
- Insider attack suspected, abusing privileged accounts.
- Most common privileged account?
  - Local admin on the user’s workstation.
  - Does your organization vary that password?
  - Does your primary user have Local admin privileges?

Spear Phishing & MFA

- Spear Phishing targeted key IT resources
- Does your primary network account have privileged access?
- Two factor authentication...Finally
Default Passwords?

Two 14 year olds used an online user manual to find out how much money was in the machine, adjust surcharges and see transaction details.

Two teenagers managed to hack into a Winnipeg ATM using an old operators manual. Photograph: Sarah Lee

Two Canadian 14 year olds successfully managed to take control of an ATM in their lunch hour using an old manual, and forcing the Bank of Montreal (BMO) to upgrade its security systems.

Matthew Hewlett and Caleb Turon found an old ATM service manual online and used it to access the operator mode of a cash machine in Winnipeg when they discovered that the bank had not changed the default password.

What does that tell us?

- The threat landscape is changing...DAILY
- “The compromise of privileged access is a key stage in 100% of all advanced attacks.” – CyberSheath Report 4/13
- This is the critical attack vector for internal and external threats
- 45% of hackers directly target privileged credentials - Thycotic
- Verizon DBIR – “97% of all breaches are preventable through basic and intermediate controls.”
- 43% of respondents in a 2012 survey did not have a PAM practice or wasn’t sure if they did
The Practice of Privileged Access Management (PAM)

- Designed to answer:
  - Who/what has Privileged access
  - When it was used
  - Where it was used from
  - What was done

- Technology is only One part of the equation – People & Process are essential

- Has to be part of your governance process, not just a one off enrollment*
PAM is a Collaborative Effort

- Make PAM part of your security DNA
- Ask questions about privileged access when reviewing applications & risk
- Educate & Engage business owners when possible

Cleanup of current privileged access in all environments

Define & run a new/modified process to manage access (Grant, revoke, manage exceptions. All aligned with policy)

Integrate the new model with Enterprise IT Processes (ITIL, SDLC, DevOps, ITSM)
For security to truly work it has to be a part of everyone's job similar to quality & safety - One group cannot make an organization secure

9:14am · 19 May 2016 · Hootsuite
Privileged Access Management

- Password Vault
- Session Management & Recording
- PAM Policy Management
- Discovery & Policy Enforcement
- Session Review

Information Technology Resources

- Policy Store
- SRM/Ticketing
- Workflow
- CMDB / Change Management
- Logging & Audit
- SIEM / Analytics

Identity & Access Management

- Identity Management
- Non-person Credential Management
- Access Certification
Some PAM Use Cases – Vaulting Pattern

PAM Password Access

1. Request Password
2. Check Out Password
3. User Accesses System
4. Check In Password
Some PAM Use Cases – Session Pattern

PAM Session Access

1. Request Session
2. PAM Opens Proxy Session
3. User Interacts with Session
Other PAM Use Cases

- Script/batch management
- Local workstation admin management
- Cloud infrastructure, SaaS accounts
- Virtualization platforms
- Look at ALL hardware platforms, including industrial systems
Adoption Approach

- Orient/Advertise the Program Early and Often

- Pre-Engagement - *business area*
  - Inventory of privileged accounts & their use
  - Documentation of access processes (if available)
  - List of candidate systems
  - Prioritization of critical systems based on key criteria
    - Regulatory constraints
    - Data Type (PII / IPSI)
  - Create/Revise access processes
Adoption Approach

Engagement/Onboarding - *PAM team and business area*

- Review inventory & target systems
- Setup schedule for deployment
- Test – Verify results
- Update business processes
- Deploy into production
- Verify Use! *
REMEMBER, IT'S BETTER TO SAY YOU MEET COMPLIANCE REQUIREMENTS THAN TO ACTUALLY IMPROVE SECURITY
Keys to Success

- Fault tolerance (MUST be redundant)
- Architect for performance & geography
- Adoption MUST have senior leadership support & driven by policy
- Process First Approach, then focus on tooling
- Consider integration with your CMDB*
Keys to Success

- Be creative, one size does not fit all
- When selecting a vendor, consider cloud implications
- Eat your own dog food first
- Don’t think you’re too small for this...
- Oh, and don’t virtualize your vault*
Kevin Mitnick
@kevinmitnick

@janwinter15 @ClausHoumann I was able to compromise CyberArk twice because the client made configuration mistakes, like using ESXi.

9 RETWEETS 18 LIKES

2:27 PM - 27 Dec 2014
Challenges & Final Thoughts

- Clash with teams on tools & process (classic security vs. convenience) is common, use it as an opportunity.
- Out of band accounts (auto-discovery key here).
- Priorities (this is where Sr. leadership is key).
- Make it a KPI (if not measured against it, not going to focus on it).
- Cloud messes all of this up...except where it doesn't.
- API’s? When is it privileged access?
- Role of analytics...
Questions?

Twitter: @lpeterman