Responsible Administration – The Admin Insider

Dan Conrad, CISSP CEH
Field Strategist– One Identity
Defining the insider threat

**ANY** account with elevated permissions
- Windows
  - Every workstation local admin
  - Service accounts
  - Sets of “admins”
  - Shared accounts

**NonWindows platforms - *. NIX**
Root: Every system has local accounts.

**Network devices**
Firewalls switches, routers, DRACs/ILOs all have local or root accounts with elevated privileges.

**Scripts**
Accounts and passwords used in scripts that run via a process or embedded in an application
Why does this matter (to me)

**Dec 2013:** Major US retailer POS systems attacked. 40 million debit and credit card numbers stolen.

**June 2015:** United States Office of Personnel Management discovered that the background investigation records of current, former, and prospective Federal employees and contractors had been stolen.

**May 2017:** Equifax says a data breach exposed the sensitive personal information of 143 million Americans.

Common Thread: Identity
In my experience....

➢ If you don’t make administration easy for your admins, they will find a way to make it easy and you won’t like how they do it.

➢ If more than one person know the password to an account, auditing the activities of that account is pointless.

➢ Increasing layers of security produces overhead.
Login: admin
Password: admin

Default Admin Creds?
The keys to the kingdom

Admin Now!
Admins are granted access because of time-sensitive tasks.

Superusers
All or nothing permissions

Shared Passwords
Allows for anonymity

Auditing
Who has done what, when, where?
Anatomy of a breach

- Reconnaissance
- Scanning and enumeration
- Gaining access
- Escalation of privilege
- Maintaining access
- Covering tracks
Watch out for admins in hoodies!
The History of Administrative Privileges

- **No** individual accountability – sharing of accounts
- Most powerful/least protected
- **Admins comfortable** with the "keys to the kingdom"
- Missing compliance requirements
- Employee turnover
- Difficult to manage
First Step: Realize the issue

- The first step in remediation is realizing you have a vulnerability
- Issue ignored due to level of effort required to be done correctly
- Manual processes move vulnerability
- STIGs, NIST, regulatory requirements?
- Can this be done manually?
The thought process

✓ Organization and enterprise unique
✓ Define “privileged account” for your organization
✓ Find where accounts live
✓ Determine what to manage
  ✓ All accounts beyond “user”?  
  ✓ Just the top level?  
  ✓ Look the other way?
✓ MFA?
  ✓ The problems solved vs created
  ✓ Just for Admins?
  ✓ Separate admin MFA?
✓ Capabilities and technology
  ✓ What can be done manually
  ✓ Do we need automation?
✓ Determine workable path
Path to Privilege Management

- **Enforce**
  technically what make the most impact

- **Implement**
  controls and policies

- **Decide**
  what to control and how

- **Realize**
  that unmanaged privileged accounts are an issue

- **Comply**

- **Enforce**

- **Implement**

- **Decide**

- **Realize**

Comply
The Day-to-Day Administrator

➢ Administer quickly – Speed Counts!

➢ Auditing changes behavior

➢ Reduce/eliminate/mitigate vulnerabilities
  ➢ PtH
  ➢ Insider Threats

➢ Don’t need more complexity
  ➢ Don’t add complexity to difficult tasks
  ➢ Socialize need for auditing

*If you don’t make administration easy for your admins, they will find a way to make it easy and you won’t like how they do it.*
Why Automate Privilege?

Knowing + Trusted Sharing + Simplify + Efficiency = Stronger Security Posture
Getting to the point – write policy but implement with technology

**Do**

- Control all privileged accounts from a single point
- Use role-based password request with check-out – check-in with approval
- Audit all privileged account use
- Audit and analyze
- MFA enable administration

**Do NOT**

- Bypass top-level buy-in
- Make the administrator’s job more difficult
- Implement without socializing
- Stop short of a complete implementation
- Leave back doors
Use the capabilities of the technology marketplace

Secure & efficient management

Granular delegation & command control to include applications

<table>
<thead>
<tr>
<th>Task 1</th>
<th>Task 2</th>
<th>Task 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>User A</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>User B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User C</td>
<td>✔️</td>
<td></td>
</tr>
</tbody>
</table>

Record, Monitor and Replay

Analyze data to prevent, detect and stop risky users and behavior
The Path to Privileged Access Management

- Privileged Analytics
- Password Vault
- Least Privileged Access
- Session Management
- Privilege Access Governance
Identity Governance and Administration
Unify governance, provisioning, administration, & policies for any system, platform, or applications.

Privileged Access Management
Secure, audit, & analyze privileged access.

Identity Services

AD-centered Identity Management
Manage, administer, & secure hybrid AD. Extend to Unix/Linux and many popular SaaS apps.
Thank you for your time!

For more info visit: OneIdentity.com

Dan Conrad, CISSP CEH
Field Strategist – One Identity
Daniel.Conrad@OneIdentity.com
LinkedIn.com/in/ConradDan