Managing privileged accounts

Overview

- What is a privileged account and why do we care?
- Where are privileged accounts?
- What strategies can we use?
- What does it cost me?
- How can we verify/audit privileged accounts?

Managing privileged accounts

What is a privileged account and why do we care?

What is a privileged account and why do we care?

- Privileged accounts have access to configuration, data and settings these that a normal account can not reach. And can change these.
- System and network administration accounts
- Database and application administrators
- Local accounts who can execute privileged commands
- 3rd party support personnel (e.g. manufacturers, contractors, outsourced service)
- Temporary access (e.g. temp workers, auditors)
- Accounts that can access privileged data
  - Write permissions
  - Read permissions

Managing privileged accounts

Where are privileged accounts?

Where are privileged accounts?

- Servers
- Databases
- Appliances
- Mobile devices
- Applications
- Others
- 3rd parties
- Managers, special roles
- Delegated access

Managing privileged accounts

What strategies can we use?

What strategies can we use?

- Rigorous policies and procedures
  - Review existing policies and procedures
  - Modify existing or add new policies and procedures
  - Inform and enforce policies and procedures

- Remove/reduce privileged access
  - Entitlement reviews
  - Dedicated groups for privileged access
  - Separate privileged from non-privileged access
  - Use multi-factor authentication for privileged access

Managing privileged accounts

What strategies can we use (cont'd)?

- Logging

➢ What – use NIST, PCI, CSC, Cobit frameworks

➢ Where – wherever privileged accounts exist

➢ How do we “separate the wheat from the chaff” in the logs – careful configuration, use off-the-shelf appliances

➢ How do we react to alerts – categorize in priority levels, define recipients, have CIRT plans and teams

Managing privileged accounts

What strategies can we use (cont'd)?

- Actively manage privileged accounts and access

- Enforce/automate separation of privileged access – use different accounts or IDs for administrative functions
- Enforce/automate password rotation – use one-time passwords for privileged accounts or IDs
- Implement multi-factor authentication for privileged accounts
- Implement strict firewalling for administrative access to devices

Managing privileged accounts

What does it cost me?

What does it cost me?

- What does it cost NOT to do anything?
  - Anywhere from $20 to $155 per record in the case of a breach

- Analysis
  - It depends on complexity and maturity of the organization
    - Asset Management
    - Risk Analysis
    - Centralized account management

Managing privileged accounts

What does it cost me (cont'd)?

- Implementation
  - It depends on the size of the organization and the willingness of supporting security in the budget
    - Policies and procedures should be “normal way of doing business” anyway
    - Separation of duties and entitlement review might run into “culture shock”
    - Logging depends on a good asset management
    - Active management can be very costly

- Maintenance
  - Corresponds to the implementation

Managing privileged accounts

How can we verify/audit privileged accounts?

How can we verify/audit privileged accounts?

- Are clear definitions in place (e.g. in policies)?
- Are entitlement reviews done – are they included in hiring and firing procedures?
- Are privileged and non-privileged access separated?
- How is separation, logging and/or active management being implemented and enforced?

Managing privileged accounts

Questions?

Thomas Bullinger
consult@btoy1.net