ManageEngine
ADSolutions

Final Preparations for the GDPR

Lucky

Lucky@manageengine.com

Know your presenter

Name: Lucky

Role: Manager Presales & Support

Email: Lucky@manageengine.com

Agenda

- GDPR details
- How to best design and manage users, groups, and organizational units in Active Directory
- Data Discovery and Suggestions on file, database, and folder design strategies
- How to track all object changes and resources access
- Solutions for breach detection and reporting

GDPR Details

GDPR Articles

- Article 5-1(d)
  - *“accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay”*
- Article 5-1(f)
  - *"protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (‘integrity and confidentiality’)"*
- Article 32 – Security of processing
- Article 33-3(a)
  - *“describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned”*

How to best design and manage users, groups, and organizational units in Active Directory

Design AD for the GDPR

- Basics to consider
  - Name groups that access personal data for easy recognition
  - Create OU(s) to locate groups that access personal data
  - Optional: create OU(s) to locate user accounts that access personal data
  - Do not use existing groups to also configure access to personal data
    - Will be difficult to separate access to personal data and other resources
    - Volume of tracking information will be much larger
    - Harder to create report in case of breach

Design AD for the GDPR

- Technologies to consider
  - Group Policy
    - Group membership
    - Mapped drives to personal data
    - User rights for computers storing GDPR data
    - Etc.
  - Delegation
    - Management of user accounts
    - Management of groups and group membership
  - Monitoring, reporting, and alerting of changes
    - Group Policy changes to users and groups accessing personal data
    - Group membership changes for groups accessing personal data

Data Discovery &Suggestions on file, database, and folder design strategies

Design storage for personal data

- Basics to consider
  - The GDPR is only for personal data
  - Personal data could be located nearly anywhere
    - Must locate and document all personal data
    - Personal data could be in databases, spreadsheets, documents, desktops, etc.
  - Storing personal data with other company data will complicate compliance
  - Separating personal data will create obvious separation for security configurations
  - Separating personal data will allow for easier monitoring of access

Design storage for personal data

- Configurations to consider
  - Access control lists
    - Direct permissions
    - Inherited permissions
  - Encryption
    - Microsoft
    - 3rd party
  - Monitoring, reporting, alerting of access
    - Anomalous access
    - Changes to access control lists

How to track all object changes and resource access

Tracking changes and access

- What needs to be tracked
  - Group membership changes
  - Group policy changes
  - Delegation changes in AD
  - ACL changes to personal data files/folders
  - Access to personal data

Tracking changes and access

- How to track changes
  - Microsoft auditing via Group Policy
  - Agents installed on servers storing personal data

Tracking changes and access

- Microsoft auditing via Group Policy
  - Step 1: Configure Audit Policy in Group Policy
  - Step 2: Configure SACL on files and folders storing personal data
- Agent
  - Typically client/server solution
  - Agent is installed on target computer where personal data is stored
  - Server side is app or HTML based with configurations on which files and folders need to be tracked

Tracking changes and access

- Key aspects of tracked changes
  - Monitoring for routine and anomalous changes
  - Reporting
  - Alerting

Solutions for breach detection and reporting

Solutions to breach detection

- Basics to consider
  - Many ways to breach the network
  - Focus on common breaches
  - Focus on security controls and access
  - Need solutions that don't just monitor, but also alert and take action
  - Forensics and detailed reporting are essential

Solutions to breach detection

- Solutions to consider
  - Monitor for known breach behavior
    - SQL injection
    - Firewall rule changes
    - Service installation across multiple computers
    - Privilege escalation
  - Solution needs to include
    - Thresholds for reduced false positives
    - Detailed alerting
    - Correlation for complex monitoring and attack detection
    - Historical reporting

Summary

- GDPR details
- How to best design and manage users, groups, and organizational units in Active Directory
- Suggestions on file, database, and folder design strategies
- Deep dive into access control list design and strategies
- How to track all object changes and resource access
- Solutions for breach detection and reporting

ManageEngine

Thank you!

Lucky@manageengine.com