Security +
Data Security

Author: Joseph Lee
Email: joseph@ripplesoftware.ca
Mobile: 778-725-3206

Data Security Hardware Terms

Disk redundancy
- Using fault tolerant disks such as RAID-1, RAID-5, and RAID-10, etc.

FDE Full Disk Encryption
- Encrypts an entire disk

Data Roles and Responsibilities

Owner
- The individual with the overall legal and corporate responsibility
- In a corporation this is usually the CEO and other executive level

Steward / Custodian
- Handle the routine tasks to protect the data
- The custodian will make sure data is backed up or destroyed as per policy made at the executive level

Privacy Officer
- This is an executive position within an organization
- The main person responsible for creating policies that maintain compliance with laws

Backups

Tape
- Benefits of tape are that it lasts a long time, is inexpensive per byte and is fault-tolerant

Full backup
- A complete backup of all data
- Slowest to create

Full / Differential backup
- Backs up all the new data and data that has changed since the last full backup
- Faster to restore than an incremental backup
- Slower to create than incremental

Full / Incremental backup

- Backs up all data since the last full or incremental backup
- Incremental backups also use the last differential backup as a reference point for changes in the data
- Slowest backup type to restore
- Fastest to create

Snapshots

- Captures data at a certain point in time sometimes referred to as an **image backup**
- Snapshots are a full backup can also then be added to incrementally
- A copy of a drive or VM at a moment in time
- Allows to revert to a state of a previous moment in time
- Good use case is for change management to have a copy of the state before applying risk operations such as patches, updates, installing new applications

Testing backups

- Important to verify backups

Storage and Transfer

- Backups should be stored and transferred **clearly** and securely

Destroying backups

- Degaussing, shredding, or burning the media, or data-scrubbed using DOD 7 pass random bits to overwrite the entire drive

Off-site backups

- Off-site backups should be kept in case of fire or flood
- Geographic consideration to keep backups as close as possible without subjecting the backups to the same environmental threats as the main site

Legal implications

- **PII** and **PHI** need to be stored according to laws with respect to **confidentiality**
- Also, data sovereignty refers to the legal implications of the application of the regional laws in the location where your backup data is stored
- Laws differ country to country and you should be aware of any legal implications of storing data in that country

Data Destruction / Data Sanitization

System recycling

- Involves security concerns with the **data sanitization** of any storage media

Cluster wiping

- Removes random data stored at the end of files

- Files are stored in blocks of data of usually about 4KB

Data Retention Policies

- Identifies how long data is retained and sometimes where it is stored
- This may be in response to laws and regulations, or corporate policy
- **Methods of destruction**
  - **Purging**
    - General term meaning that all data has been removed
    - Compare to terms clean, delete or archive, where data may be recoverable
  - **File shredding**
    - Digital shredding of data means to overwrite the media repeatedly with random bits
  - **Wiping**
    - Another term for bit level overwrite process that writes random patterns of data repeatedly to ensure data is unreadable
    - US DoD standard is 7 passes
  - **Burning**
    - Incineration of printed materials
  - **Paper-shredding**
    - Physically shredding paper with a paper-shredder
  - **Pulping**
    - Additional step after shredding documents is to soak the shredded material and turn it into liquid paper mash
  - **Degaussing**
    - Electronic magnet that will render data on tape and magnetic medium unreadable
  - **Destroy / Pulverizing / Industrial shredding**
    - Using sledge-hammer, or industrial shredder to physically destroy the items
    - This is required with optical medium such as DVD or CD since it cannot be overwritten or degaussed
  - **Cryptographic erase**
    - for encrypted data simply relies on deleting the key pair

Basic Forensic Procedures

- **System forensics** is used post incident in order to understand the nature of the breach
- The evidence collected can be used in the prosecution of a crime and to increase security by understanding how the security compromise took place
- An important factor is to avoid any changes to the evidence
- **Order of Volatility**
  - Refers to the order in which you should collect the evidence
  - Volatility refers to the nature of the hardware to alter its state
  - This can cause data loss
  - For example RAM data is lost after the system is powered down, but it may have evidence that is important to understanding the nature of the

breach
    - The order of volatility is below from most volatile to least:
        - Cache memory including CPU caches and hard-drive cache
        - RAM
        - Paging file / swap file
        - Data stored on local hard-disk
        - Logs stored on remote systems
        - Archived media
- **Data Acquisition**
    - **Capture system image** (dd in Linux to create a disk image)
    - Hashing can validate the integrity of the captured data / entire drive to compare it to the original
    - Write protect the collected data / image to avoid modification later
    - Discovering the IP address / MAC address of the attacking computer
    - CCTV can capture surveillance information about person's location and activity
    - Re-calculate the recorded time offset to account for timezone difference
    - Screenshots can capture evidence of what users were doing on a system
    - Witnesses can attest to whereabouts of people
    - **Chain of custody**
        - Provides information about the custody of forensic evidence and can be useful in court of law
    - Legal hold can demand that certain types of data be kept as evidence
    - **Data retention policies**
        - Determine how the data should be treated, not only the legal requirements
        - A company cannot delete past data simply because it was not required by law to keep that data
    - **Data recovery**
        - Possible in some circumstances even when files have been deleted or drives formatted
    - **Logs** can provide evidence as to **system activity** and **application activity**
    - Man-hours and **expenses** are important in lawsuits where **damages may be awarded** to victims to be paid by the perpetrator when successfully prosecuted
- **Role Based Awareness Training**
    - **Data owner (CEO)**
        - Data owners need to make sure their data is classified correctly according to laws and labeled properly
        - They hold the legal responsibility for ensuring the sufficient controls
    - **System administrator**
        - The overall security of a system
    - **System owner**
        - Usually a high-level executive appointed to oversee the system security such as a CSO or CTO
    - **Users**
        - Need to be aware of and follow organizational policies to precent

common types of attacks such as malware, drive-by-downloads, phishing, etc.

- **Privileged user**
  - Require training on the classification, labeling, and handling of the data they are responsible for
  - System Administrators often use two accounts, one for daily tasks, and another for system changes with escalated privileges
- **Executive user**
  - Specific threats and responsibilities they face as high-level executives such as whaling attacks
- **Incident response**
  - Training on how to respond to security incidents
- **Continuing education**
  - Regularly receive additional training and information about emerging trends in the security sector their job functions involve
- **Legal Compliance Awareness**
  - Personnel need to understand the laws that apply to the data they handle
- **Strategic Intelligence / counter-intelligence gathering (Active logging)**
  - What the government can do to react to the attackers such as shut down websites, freeze bank accounts, etc.