Cloud Computing Security

Rajendra Kachhwaha
rajendra1983@gmail.com

March 06, 2017

Outline

Personally identifiable information

- Personally Identifiable Information (PII)
  - Defined as “information that can be used to uniquely identify, contact or locate an individual, or can be used with other sources to uniquely identify a person”
  - PII is subject to regulations HIPAA, EU, PCI DSS
- Planning for Secure PII
  - Identify, categorize and prioritize PII hosted within your systems – all three data states must be secured
  - Identify potential security vulnerabilities with reference to data state
  - Develop data use policy
  - User education

Personally identifiable information

- PII Security Controls
  - Encryption

    High security controls include encryption of data at rest, data in use, or data in transit.
  - Threat prevention techniques

    Preventing the disclosure of personal information through various mechanisms such as inadvertently storing files on removable flash drives that are encrypted.
  - Data access control and rights management

    Applied to data that is flagged as being PII sensitive.
  - Data masking

    We can control the display of data or which data is actually made available to calling applications.
  - Data tokenization

    We're never really exposing sensitive information directly to users or applications that requested. Instead we have a token that represents the original data. This way, we're ensuring the integrity of the original sensitive data.

Personally identifiable information

- PII Security Controls
  - Data Loss Prevention (DLP)
    - Prevent accidental loss using automatic and defined file and content rules
  - Policy development and application of controls
    - Storage media
      - Removable storage devices – portable drives, USB
      - CD-ROM
    - Network Transfer
      - Manage proliferation of PII
      - Networks, modems, wireless
      - Bluetooth

Emerging Data Protection Technologies

- Application of appropriate protection technologies
  - Dependent on data asset classification – PII, importance, sensitivity
  - Dependent on data asset state – at rest / in use / in motion etc.
  - Dependent on cost, time, manpower resources
- Cloud Service Providers support many protection mechanisms as part of the cloud service
  - Microsoft Azure: hardware and data encryption, SQL table data masking, key management
  - Amazon Web Services EBS volume encryption

Emerging Data Protection Technologies

- Mapping protection technologies
  - Masking and tokenization at the Application level where user role hierarchies exists
    - Avoids the design of multiple front-end user-facing interfaces
    - Avoids data breaches within ad hoc querying tools
  - Utilize encryption for sensitive and classified data
  - Utilize transport level encryption where sensitive data is supplied or viewed over the internet
  - Map the requirement to encrypt with data classification – does everything need to be encrypted?

Emerging Data Protection Technologies

- Bit Splitting (Cryptographic Splitting)
  - AES-256 encrypted data is split at the binary level (bit level) into a number of shares
  - The individual shares are protected by the application of a HASH (SHA-256)
  - The splitting is done randomly and is controlled by a key
  - The number of splits (shares) can be user defined
  - The protected shares are saved to different locations (separate disks) located within the storage pool
  - The storage pool incorporates redundancy to protect the individual data shares

Emerging Data Protection Technologies

- Homomorphic Encryption
  - New technology pioneered by IBM
  - Allows computations to be performed on encrypted data (ciphertext)
  - Useful in cloud computing environments to ensure the confidentiality of data that is supplied from disparate confidential sources
    - E.g. - an encrypted salary from one data source being multiplied by an encrypted bonus rate from another data source – at no point is the data required to be decrypted