TEKsystems
Own change

TEKsystems Global Services

Data and Application Security

Presented by: Ananda Vardhan Chagamreddy

Date of Presentation: 13-Aug-2020

TEKsystems
Own change

DATA SECURITY

Impact & Importance of Information Security

Few Recent Examples:

- 2013 – University of Texas Anderson Cancer Center paid $4.3 Million for HIPAA violations
- 2016 – Uber paid $148 Million for data breach related to Driver and user accounts
- 2018 - British Airways is facing $650 Million for data breach related to payment card details
- 2018 - Facebook facing $1.6 Billion for 2018 data breach related to user account
- 2019 – “Worst year on record for breaches” - *Risk Based Security, a research firm*

Types of Data

- *PUBLIC Data – open to all users and no security measures are necessary*
- *LIMITED ACCESS Data – only authorized users have access to this type of data*
- *PRIVATE Data – data open to a single user i.e. the owner of that particular data*

Security

Security is the protection of information, systems and services against disasters, mistakes and exploitation, so that the probability of incidents is minimized.

Securing Data

Access Controls

- *Access Controls regulate the reading, copying, changing and deletion of data and programs.*

Flow Controls

- *Flow Controls can prevent a service program from leaking the customer's confidential data.*

Inference Controls

- *Method of preventing data about specific individuals from being inferred from statistical information in a database about groups of people.*

Technology available to secure Data

- *Cryptography*
- *Biometric Systems*
- *Malicious Code and Antivirus Solutions*
- *Firewall*
- *Intrusion Detection System (IDS) – Host based and Network based*
- *Virtual Private Network (VPN)*
- *PKI and Digital Certificates – Public Key Infrastructure*
- *SSH Encryption*
- *SSL Encryption*

Impact of Information Breach

Organization

- Loss of Reputation
- Loss of Business
- Liabilities & Lawsuits

Employee

- Suspension
- Termination

Leaders

- Suspension
- Termination

Customers & Cloud Providers

- Lawsuits from their customers
- Liabilities
- Loss of Business
- Loss of Reputation

Aspects of Data Security

Prevention	Measures taken to protect organizational data from being damaged
Detection	Measures taken to detect any damage done to the organizational data and to find out the source, means and extent of damage
Reaction	Measures taken to recover from the damage and to prevent from recurrence

Major Areas covered under Data Security

- Password & Encryption
- Social Engineering
- Phishing
- Physical Access
- Portable Device and Remote Access
- Taking Devices for a drive
- Data Disposal
- Data Breach

Special Attention – Customer Domain

Few Domains that require special attention

- Healthcare
- Banking
- Financial
- Security
- Insurance
- Logistics

Special regulatory acts you need to be aware of

- GDPR (mainly EU region)
- Data Protection Act (UK)
- HIPAA (USA)

PII Data – Be Aware & Sensitive

Personally Identifiable Information (**PII**):

- Data that identifies a specific individual
- Information that can be used to distinguish one person from another
- Highly sensitive; must be protected at all costs

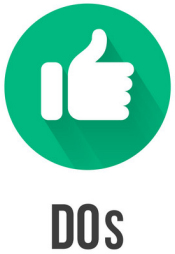
- Name
- Address
- Date of Birth
- Contact Details
- Social Security Number
- Membership to Organization
- Employment Details
- Religion / Race / Ethnicity

- Bank Details
- Financial Account details
- Investment Records
- Insurance Details
- Credit Card Details

- Health Care records
- Disability
- Mental / Physical Health Condition

*** These are just examples*

Action Items – Do's



- Complete / Revisit any compliance certification – Internal and Customer specific
- Ask for only required data
- Access the customer instance only if you are authorized
- Disable user accounts immediately after rolling off the user
- If PII data is not obfuscated/encrypted – notify customer
- When in doubt, contact your Project Manager
- Where appropriate, use only customer provided email facility for project-specific communication
- Report suspicious activity and cyber incidents to your Manager and InfoSec team

Action Items – Don’ts

DON’Ts

Credentials:

- Do not share your personal (both Organization and Customer specific) credentials
- Do not share DB, Application credentials meant for use only by you
- Do not keep same passwords for different accounts
- Do not hard-code passwords in Code
- Do not share username/password to shadow resources (get pre-approved access credentials created by the customer

Access:

- Do not ask for data that is not required
- Do not access the data / environment from public places and/or using unsecured WiFi
- Do not access any unauthorized content using customer network (e.g. Social Media)

Data & Code:

- Do not move data / code outside customer infrastructure
- Do not use the data for unauthorized purpose
- Do not print customer specific data / code / content
- Do not download customer specific data to your mobile

Action Items – Don’ts

Miscellaneous:

- Do not use customer provided email accounts for Organization internal communication
- Do not forward customer sensitive data to Organization email id
- Do not leave your device unprotected
- Do not act against compliance even if your supervisor (offshore or onsite) asks you
- Do not take short-cuts to complete work sooner
- Do not copy customer / Organization content / data to personal GitHub / BitBucket / public repositories (e.g. Google Drive, Drop box etc.)

TEKsystems
Own change

APPLICATION SECURITY

Application Security

Examples of Applications

- Patient Records Systems
- Financial Systems
- Insurance Systems
- Military Applications

Facts

- 30% of security risks happen at Application Layer
- Web Application attacks represent the ***greatest threat*** to an organization's security. These attacks represented ***40%*** breaches in 2015.

  -Verizon's 2016 Data Breach Investigations Report

Affects of security failure at Application level

- *Sensitive Data Store breach*
- *Theft of critical business data*
- *Theft of personally identifiable information (PII)*
- *Website defacement*
- *Denial of service*
- *Financial loss to Organization*
- *Bad reputation to Organization and in some cases end of business*

Real-time examples

- *JP Morgan: leak of largest no. of records to date. Affected 76 million households and 7 million small businesses. PII is compromised.*

- *Bell Canada: biggest security breach of a Canadian company. 22,421 user names and passwords, 5 credit cards numbers. 40,000 customer records were affected.*

Ways to ensure Application Security

- *Authentication*
- *Session Management*
- *Role based access controls to users*
- *Data Security configuration*
- *Protection of sensitive data. Eg: Credit Card, Tax Payer ID, authentication credentials etc.*
- *Function level access control*
- *Preventing cross site request forgeries*
- *Avoid using components with known vulnerabilities*

Conclusion and Q & A

- *Data Security*
- *Application Security*

TEKsystems
Own change

THANK YOU