PROTECTING YOUR DATA

Etactics

www.etacticsinc.com

Web Security & Encryption

- All data in motion is fully encrypted using SSL
- Any highly sensitive data can also be encrypted in the database, or at rest (passwords, files, unstructured data)
- A server side business layer is written in the latest version of Java
- AES-128 for legacy database fields
- AES-256 for new database fields and new applications, Cookie Values, Cookie Names, Key Values in motion
- TripleDES for encrypting URL parameters
- RSA 2048 or better for asymmetric encryptions (key exchange)
- SHA-256 for storing password hashes
- MAC-128 for data integrity hashes

Encryption Key Management

- Keys or passwords cannot be stored in the source code, source code documentation, or in plain view in configuration files. The only exception is context.xml file on the server where Tomcat stores connection parameters to the database.

- Each employee receives a personal certificate stored in the personal keystore protected by the user password. The password must be strong and cannot be stored anywhere on the system. A certificate ensures every person has an assigned public and private key (RSA using at least 2048 bits).

Coding Practices

- URL request utilizing GET and QueryString must be immune to enumeration
- POST should be used everywhere where is it possible. GET can be utilized in some cases. Programmers must use provided "core" functionality and libraries to render any links, AJAX calls , or redirects.
- All the authorization and cryptographic functions must fail "safely."
  - When error occurs, the program must fail and report an error. For example, if authorization server or database is "down," then the program cannot fail in a manner to grant the access. If decryption fails program cannot return empty value as decoded plain text but it must raise the exception and stop processing.
- HTTPS, SFTP, VPN and SSH are allowed communication protocols to the systems. With the exception of SSH that can be used only from whitelisted Ips.
- The permission for opening any port other than 443 for https must be requested in writing and addressed to Security Officer. No one can make request to the Data Center provider managing the firewalls to open a port or make any changes to firewall settings.
- Audit Log entries are stored on the trusted system with implemented data integrity signature. Developers are required to use provided "core" functionality to submit auditable events to Log Server.

Access Control

- We employ a highly sophisticated context firewall across our entire network that helps detect and drop malicious items that could be related to hacking, and also allows us to Geoblock traffic coming from anywhere suspicious

- In the application itself we employ a web firewall to protect against SQL Injections and other web based threats
  - A permission based authentication system
  - Supports Single Sign-On
  - Active Directory
  - Two-Factor Authentication

In the world we live in today, data protection has become an integral part of company operations and across all industries. At Etactics, we recognize that our customers entrust us with their data and expect us to make every effort to protect it.

☎ (330)342-0568 ✉ sales@etacticsinc.com 🌐 www.etacticsinc.com