JDP SECURITY OVERVIEW

Introduction

JDP has recertified as EI3PA, PCI DSS complaint. This means that JDP has implemented industry best practices for handling and storage of sensitive personal and credit card data. EI3PA certification is among the strictest certifications in the industry, and JDP is proud of its certifications. Our Data center has a number of other relevant certification including AICP Standards SOC 1 & SOC 2 (fka SSAE16).

Application Infrastructure

The Instascreen™ application is a cloud services application that provides instant background screening data to the company requesting background-checking services. The background screening data comprises criminal, credit, drivers license, and other background records information from trans-jurisdictional sources, both public and private.

The InstaScreen™ application itself runs in a secure, state-of-the-art, PCI and SSAE16 compliant colocation facility located in Salt Lake City, Utah, and is replicated onto a PCI and SSAE16 compliant fail-over facility in Denver, Colorado. The application runs on multiple load-balanced application servers that access database servers segregated inside of secured, firewalled, data zones.

Infrastructure Stability

JDP's colocation facility was built with stability and security in mind. The colocation facility has redundant OC3 lines providing Internet access, and has a stable power supply from an area of the United States where the power grid has a history of stability. Additionally, the colocation facility has real-time power redundancy, with on-site power generation and fuel storage to deal with any possible power interruption.

Physical Security

The colocation facility has access controls that put it in a league with secure government facilities. The perimeter is secured with a six-foot high chain link fence with a barbed wire top guard. The bottom of the fence is secured with bottom bars over concrete or asphalt floor. Access gates have barbed wire top guards and require authentication through card keys for entry.

The physical building is secured with auto locking steel doors, governed by multi-factor user authentication. To gain entry, a user must provide a validated card key, which in turn must be matched to that user's biometric palm scan. Users can only enter through double-locked "mantrap"-style atriums. All ingress and egress traffic is recorded by CCTV camera systems, and the facility is staffed 24/7/365 by highly trained technicians.

JDP SECURITY OVERVIEW

Digital Perimeter Security

The InstaScreen™ application follows industry best practices, beginning at the network perimeter. All communications with clients are authenticated and encrypted through Secure Socket Layer (SSL) or Transport Layer Security (TLS) protocols. External access into the application servers is governed by an enterprise firewall system that limits incoming connections to only minimum ports needed for application access.

Any incoming requests to the application are handling by application servers residing in the firewall DMZ (intermediate access zone or "demilitarized zone"). Application servers talk to database servers only over specific, secure ports. These database servers reside in secured internal network zones and have no direct connection to the outside world.

Perimeter firewalls run intrusion prevention and detection services, and false logon attempts are recorded, logged and emailed to system administrators for investigation.

Network Security

In addition to securing traffic through use of secure zones, only authorized users can even gain access to production equipment. Users are limited on a "need to use" basis, and granted permissions on the lowest access level possible for completion of specific tasks.

Users logging onto equipment require validation through multi-factor authentication. When a user attempts to log onto the system, not only must the user know his/her username and password, but the user must also receive a confirmation key that is transmitted to a device that only that user has access to. All user passwords conform to complex password standards, and user passwords can have lengths in excess of 16 characters, to improve resiliency against password cracking.

All equipment is patched to the most recent iterations of their operating systems, and only the minimal set of application software that allows the server to perform its mission is installed.

User Security

System administrators are all career JDP employees, and undergo periodic background screening to ensure that their profiles are current. Users all undergo training in secure network usage, and use complex password convention, with industry best practices for password storage and changes.

JDP SECURITY OVERVIEW

Maintenance & Support

As JDP grows, management continually appraises the need to keep hardware and software infrastructure ahead of what is required. JDP is constantly evaluating server performance, and in the last quarter, has rotated servers to state-of-the-art models, implemented security improvements across the board, and is implementing improved enterprise firewalls in anticipation of increased traffic demands.

In addition, JDP provides in-depth continuing education and training of its support staff to ensure that support personnel are the most competent, helpful, and secure support staff in the industry.

Software Application

Security is a high priority and an integral part in the design and development of JDP's InstaScreen™ applicant screening system. Attention is given to high publicity threats such as viruses, denial of service attacks, and other malicious activities over the Internet, as well as maintaining the integrity and confidentiality of sensitive application data such as credit reports, social security numbers, and other personal identifying information. JDP's development staff uses industry-leading technology to secure InstaScreen™ and its operating environment, including client authentication (password-controlled access), data encryption, public-private key pair, firewalls, intrusion detection, filtering routers, and data backups. Each of these components act as a layer of protection to safeguard information from unauthorized users, deliberate malfeasance, and inadvertent loss.

User authentication: Password-controlled access requires users to authenticate with a private login ID and password before accessing the system. After authenticating to the system, sessions remaining inactive for a period of time will expire and require the user to re-authenticate before continuing. In addition, user accounts that remain unused for an extended period of time are automatically disabled. User passwords are protected in the system using sophisticated hashing schemes and should never be shared. Passwords must be reset at least every 90 days, differ from the previous four passwords, be at least 8 characters in length, and contain at least one letter and one digit. The password recovery feature allows a user to retrieve his or her login ID and/or reset a forgotten password after correctly answering several pre-configured security questions and a CAPTCHA.

IP Restrictions: System access can be further restricted at the client or user level by IP address(es). Any attempt to access InstaScreen™ from an IP address outside the authorized range is rejected.

JDP SECURITY OVERVIEW

Encryption: All transactions are performed in a secured environment. Access to InstaScreen™ requires the use of HTTPS. Supported web browsers automatically secure the session communications using the Transport Layer Security (TLS) 1.x protocol using a minimum of 128-bit encryption. All data is encrypted as it travels between the client web browser and the InstaScreen™ servers and can only be decrypted with a public and private key pair to protect against eavesdropping, server impersonation, and stream tampering.

Firewalls, Intrusions Detection and Filtering Routers: The InstaScreen™ servers are protected by firewalls, intrusion detection, and filtering routers that verify the source and destination of communications. The routers and firewalls are configured to reject any unauthorized, suspicious, or disallowed traffic. Routers keep out traffic that does not emanate from either end of the secured session between the client and the server.

Physical Security: The physical server machines are hosted at a state-of-the-art collocation facility that is staffed on-site 24/7 to provide an immediate response to any incident. Access to the facility is restricted to authorized personnel and is secured by both password-protected keypads and biometric scans. Door, glass, and motion events at the facility are digitally recorded and archived as well as observed live by facility staff for any suspicious activity. UPS systems and a 500-kilowatt diesel generator ensure electrical service to the facility. Multiple fiber providers provide Internet connectivity with diversified entry points into the facility. The cooling system incorporates redundant components, excess capacity, and high-efficiency technologies to maintain an optimal operating environment for the servers.

Data Integrity - Server Hardware: All servers are configured with RAID disc subsystems with hot spares, or in some cases RAID6 (no hot spares are needed for RAID6 configuration). All servers have new replacement disks for standby hardware replacement. Application servers are configured with RAID1 mirrored disks with in-server hot spares and standby new disk replacement. Database servers are configured with RAID6 or RAID5 with hot spares as well as standby disk replacement.

Data Integrity - Database Failover: The primary database server is synchronized to two other high availability backup database servers. Furthermore, the main database server synchronizes with an off-site high-availability backup database server located in a secure collocation facility in Denver, Colorado.

System Integrity: To ensure maximum uptime and to provide for fail-over of critical system components, JDP implemented a parallel fail-over firewall. Casualties to the primary firewall have a minimal impact on production, and the fail-over firewall automatically kicks in. Our load-balancing equipment is also provisioned for fail-over configuration.

All servers have dual power supplies. Power supplies are plugged into different power circuits to ensure that if one power circuit fails, the servers will continue to receive power from the alternate power circuit. The power is administered by the collocation facility, which in turn has its own provisions for backup generator power in the event of a state-wide power outage.

JDP SECURITY OVERVIEW

Data Integrity - Backups: Periodic database snapshots are dumped off onto backup repositories and after a holding period, saved onto hard disks for archive. Database log files are archived to allow the restoration of databases to give points in time in the event of a need for data retrieval. Administrative files are automatically saved onto NAS on a rolling Monday through Friday basis.

Data Integrity - Application: The application is load balanced and cloned across four application servers. All application servers have RAID1 disk subsystems with installed hot spare and new hardware standby. The application is saved on a staging server, and application snapshots are taken and stored on a repository. After a holding period, the application is offloaded onto removable storage for archive.

Client Responsibility: Clients are expected to guard their password carefully and not share it with or disclose it to anyone for any reason. JDP staff will never ask a client for their password. Clients must also ensure the security of their InstaScreen™ sessions by completely logging out of the system when finished and not leaving active sessions unattended. Paper and electronic copies of reports must be carefully controlled to prevent the unauthorized distribution or disclosure of personally identifying applicant information.

A robust and secure system requires a multi-faceted solution with hardware, software, and education. Critical to the success of any secure system is the education of its user community and employees on the importance and sensitivity of information. Knowledge of why and how data is secured, and the permissible uses of all information, is essential in maintaining the integrity of the system and its contents.