IT Security Brief

Maropost is an enterprise-level SaaS based web-application that combines digital messaging campaign list management and deployment.

The application is offered as a "hosted rich internet application". Users require a modern browser, for example IE 7+, Firefox, Chrome, or Safari, to access it. The browser sessions use a 128-bit encrypted SSL connection. The servers are hosted in a secure facility with 24/7 monitoring, redundant power, nightly and real-time backups complying with international standards for data security and management.

Application Security

Maropost has powerful client security controls, including those that allow clients to do the following:

- Specify the IP addresses individual users are allowed to send campaigns from
- IP address validation
- User-level IP address restriction
- Organizational-level IP address restriction
- Control user actions post-login with multiple permission levels, including:
- User interface access rights
- API access rights
- Individual access rights (add/update/delete contacts, export lists, etc.)
- Functional access rights (send mailings, view reports, administrative, etc.)
- File/Folder access rights
- Database access rights

Application Security is also addressed by keeping client data separate from the application, providing an audit trail of user actions performed on the system and encrypting passwords.

Additional Security Measures

Additionally, Maropost has implemented security measures outside of the application specifically designed to prevent unauthorized access to the application and to client data. Additional security controls are implemented under the following categories:

Secure Architecture: The Maropost enterprise network uses primarily Cisco networking equipment. Networking equipment is configured consistent with the manufacturers' best practices for operational stability and security. All servers and the networking equipment is owned by Maropost and operated by Rackspace Private Limited.

Secure Transmissions and Sessions: Connection to the Maropost environment is via SSL 2.0/TLS 1.2 ensuring that our users have a secure connection from their browsers to our service. Individual user sessions are identified and re-verified with each transaction, using a unique token created at login required for all communications with Maropost

data centres. We have SFTP server and 128-bit encryption for FTP file transfers with additional VPN and PGP encryption protection available.

Network Protection: Perimeter CISCO firewalls block unused protocols. Intrusion prevention and detection sensors report events to a security event management system for logging, alerts, and reports and internal access control lists segregate traffic between the application and database tiers.

Internal and Third-Party Testing Assessments: Maropost tests all code for security vulnerabilities before release, and regularly scans our network and systems for vulnerabilities. Third-party assessments are also conducted regularly.

Monitoring: Our Information Security department monitors notification from various sources and alerts from internal systems to identify and manage threats.

Data Centres: Our service is collocated in dedicated spaces at top-tier data centres maintained dedicatedly by Rackspace Private Limited.

Disaster Recovery: Maropost performs cross data centre replication for disaster recovery. Data is transmitted across encrypted links and disaster recovery tests verify our projected recovery times and the integrity of client data.

Backups: All data is backed up to disk at each data centre on a rotating schedule of incremental and full backups. Data is replicated to other data centres via an encrypted tunnel.

Regulatory Compliance: Maropost uses data centres which are based on Safe Harbor certification and have annual ISO/IEC 27001 audits.

Incident Response

Incident response is negotiated with each client and is part of their SLA (Service Level Agreement). A standardized version and Inbox SLA is part of the Maropost's policy documentation.

Spam Compliance

Maropost complies with all aspects of the following legislations:

- US anti-spam legislation
- Can Spam
- Canadian Privacy Legislation
- PIPEDA
- Canadian Anti-Spam Law CASL (http://fightspam.gc.ca)

Data Backup

The data is backed up from the application and database servers twice per week which includes one incremental backup and one full backup. The data is backed up in a different datacenter to comply with Disaster control measures. Our data centres meet all the PCI DSS specifications.

Policies and Change Management

Change Management is in place to control changes to all critical company and client information resources (such as client data and information, hardware, software, system documentation and operating procedures). The documented process covers management responsibilities and procedures in addition to employee agreed to policy and is subject to audit.

Maropost's comprehensive change control process includes the following phases:

- Logged Change Requests;
- Identification, prioritisation and initiation of change;
- Proper authorisation of change;
- Data/database access login/out access with full user action audit trail;
- Requirements analysis;
- Inter-dependency and compliance analysis;
- Impact Assessment;
- Change approach;
- Change testing;
- User acceptance testing and approval;
- Implementation and release planning;
- Documentation;
- Change monitoring;
- Defined responsibilities and authorities of all users and IT personnel;
- Emergency change classification parameters.

In addition to the above, all Maropost employees are required to sign Non-Disclosure Agreements and Acceptable User Policies. These policies are strictly enforced and frequently audited by our internal operations team. All policies are reviewed with the executive stakeholder responsible for overseeing the work in addition to responsibilities requiring the approval of Maropost's Privacy Officer.

All changes to policy and the subsequent communications to employees and clients are handled by the appropriate executive stakeholder and/or the Privacy Officer.

Business Continuity & Disaster Recovery

The managed environment is hosted in a High Availability (HA) setup. Each network device, which includes the switches, firewall, and the network interfaces on all of our dedicated servers, for both the internal network(which operates at the speed of 10G) and the external network(which operates at a speed of 1G) have been paired and

configured to run in a bonded setup. In case of a failure of a network interface, the other participant of the bonded interface switches over and resumes the network traffic. The firewall and the network switches are configured identically.
Due to this automatic fail over, re-installation of instances on failed hardware can be done without interruption. In the event of a catastrophic failure and ability to only access cross data centre backup may require up to 24 hours.