maytech
ONLINE BUSINESS SOLUTIONS

FTP-Stream : Resilience & Uptime Statement

Maytech provide FTP hosting services to business and public service worldwide. The service is used by our customers for business critical operations and as such is designed for high volume and high availability. This document outlines the infrastructure and policies adopted to provide high availability and disaster recovery.

Server Centers

Maytech operate the service from servers located in private suites at Redbus Interhouse, London E14, and NAC, Cedar Knolls, New Jersey. The buildings benefit from strong physical and electronic security, uninterruptible power and fire suppressant systems.

Connectivity

At both data centres we take feeds from multiple transit providers. In the event that one provider's service is down or degraded our gateway routers automatically reroute traffic through an alternative link.

Hardware

The FTP service is based on Sun SPARC hardware and Sun storage arrays. All servers have mirrored hot-swap disks (RAID 0), twin power supplies, twin Ethernet, and hot-swap fans.

Storage arrays are setup in RAID 6 configuration. Both servers and storage are are backed up by failover devices that can take over in case of a major failure. Failover is automatic and takes approximately 3 minutes.

Operating Systems

Servers run Solaris 10 UNIX, which is widely regarded to provide unrivalled stability and security.

All Sun updates and patches are systematically applied

Monitoring

All our systems are monitored 24/7. In the event that any connection, device or service is unavailable or degraded the duty engineer gets an e-mail and a text message.

Customer Data – Resilience

Customer data is stored over multiple drives and devices. The storage arrays are configured as RAID 6 which means that several drives would have to simultaneously fail to compromise data integrity. Furthermore each RAID array is synced to a secondary array. The probability of data loss through hardware failure is infinitesimally small.

Customer Data – Backup

Maytech retain onsite snapshots of customer data for seven days. Any files accidentally deleted over this period can be restored. We do not keep enduring incremental backups or offsite backups of customer data.

External Threats

Maytech take all precautions against external threats. Our network is fully protcted by stateful packet inspection firewalls, we operate a number of techniques to protect against malicious attacks such as Denial of Service Attacks.

Uptime

It is occasionally necessary to bring the service down for upgrade or maintenance. This normally takes place at the weekend with 5 days warning. We have had two maintenance slots in 2008 of approximately 45 minutes and 75 minutes. We have had no unplanned downtime in 2008.

Disaster Recovery

In the event of a disaster which prevents us from offering service from one of our data centers we would be in a position to quickly resume service from the alternative facility.

Revised March 2008