Security and Compliance Review

CentralNic

Version 0.4

Compliance and Scope Assessment
Author: Carl Shallow
Account Manager: Anthony Brown
Date: 10/12/2009

MIS Corporate Defence Solutions Ltd
MIS House
Hermitage Court
Hermitage Lane
Maidstone
Kent
ME16 9NT
Tel: +44 (0) 1622 723 400
Fax: +44 (0) 1622 728 580
Email: uk.sales@mis-cds.com
Web: www.mis-cds.com

Document Record

Version History

Version	Date	Author	Details of Update
0.1	10th December 2009	Carl Shallow	First Draft
0.2	12th December 2009	Carl Shallow	Changes to policy list
0.3	16th December 2009	Carl Shallow	Added focus
0.4	18th Dec 2009	Carl Shallow	Added details from additional documentation

Index

1 INTRODUCTION

MIS Corporate Defence Solutions Ltd (MIS CDS) conducted a security review for CentralNic on the 25th November 2009, a site visit on the 27th November, and an extensive follow-up review of systems, procedures and documents. The purpose of this exercise is to perform an independent security review as part of the requirements for a tendering process.

The report focuses on the security of the equipment within data centres but also includes some of the security practices within the CentralNic office that could affect the operation of the servers in the data centre.

CentralNic was established in 1995 as an independent global domain name registry committed to making it easier for Internet users to establish new and distinctive domain names with regional and country-specific identities.

Headquartered in London, CentralNic currently has a portfolio of more than 20 domain names available to users worldwide, including **EU.COM** (Europe), **UK.COM** (United Kingdom), **US.COM**, (United States), **CN.COM** (China) and **RU.COM** (Russia).

2 ABOUT MIS CDS

MIS CDS was founded in 1992 as an independent security consultancy. The company has remained a security-specific organisation, holding over a decade's worth of experience in providing companies with bespoke IT security solutions, including Payment Card Industry (PCI) and ISO270001 auditing. After 17 years of supplying security advice, services and technology, MIS CDS is the UK's longest standing IT security-specific organisation.

With its headquarters in the UK, MIS CDS primarily deals with UK based businesses. However, MIS CDS has fulfilled many secure solution deployments across Europe and the US. The company has provided secure inter-office and trading partnership relationships for UK, European and US companies.

MIS CDS is privately owned, allowing for the flexibility of decision and direction that the evolving security market requires, keeping MIS CDS at the forefront of the security industry.

MIS CDS has one of the most highly skilled and professional security teams in the country. This is not merely an opinion but a statement supported by the organisation's market position and validated by customer listings and vendor accreditations. MIS CDS' methodologies are proven, its customer relationships are established, and its technical staff are accredited to the highest standards available within the security market.

MIS CDS is part of the Securedata Holdings. SecureData Holdings is a leading provider of information security and risk management products and services to the channel and end-users in South Africa and selected countries in sub Saharan Africa.

MIS CDS' Customers include: The Financial Times, Virgin Games and Centrica plc, Associated Press, London Borough of Hackney and many more.

3 EXECUTIVE SUMMARY

METHODOLOGY

The review was conducted initially by phone on the 25th November 2009, followed by an on site visit to the CentralNic London office on the 27th November 2009. Since these initial meetings, information has been provided via phone calls and secure downloads.

Both interviews were conducted with Gavin Brown who is the Chief Technology Officer. The first part of the exercise is to get an understanding of the security posture within CentralNic this is achieved by answering series of questions based on best practice security procedures, with the answers then validated. This is the first step in a process of ensuring that CentralNic will be fully compliant with all required security standards required in the tender. The follow-up to this work will be a re-audit of the gaps outlined in this document.

The security framework questions have been designed to cover all aspects of security for all different types and sizes of organisations. It is quite common for organisations to get a negative answer to many of the questions, this is intentional, our value is identifying and prioritising the critical gaps that become known through this review whilst considering the assets and their protection requirements.

FINDINGS

MIS CDS considered that the CentalNic Data Centre network is currently well managed and security arrangements are well thought-out and implemented. There are areas that require additional work or changes to ensure that the operational duties are consistent and secure, however these are minor policy and procedural requirements that do not effect the existing, solid, operational architecture.

The remainder of this document covers the areas of operation that are specific to the tender and how CentralNic adequately perform them for both the data centre and head office operation in London (35-39 Moorgate, EC2R 6AR).

4 FORMAT OF REVIEW

MIS' General Security Review is based on the BS7799 / ISO 17799 and the security industry's best practise. The Review is broken down into six main titles, which are-

1. Security Policy
2. Procedures and Documentations
3. Internal Security issues
4. Business Continuity/Recovery Plan
5. Compliance
6. Perimeter Security and Physical & Environmental Protection.

It is essential that during the review that the assessor is conscious of the level of protection required and the sensitivity of the data or systems requiring protection.

In the case of CentralNic it is critical for the business to maintain continuity of the business and the systems that support it. The following sections cover the areas of how CentralNic achieve this.

4.1 DATA CENTRE SECURITY (PHYSICAL SECURITY)

CentralNic's staff operate from a serviced office in Moorgate street, London. The servers, firewalls, load balancers etc that provide the operational architecture for the business run in a data service provided by Level 3 at Goswell road, London.

Security (Building and Facilities)

Level 3 is equipped to maintain security on a 24 x 7 basis.

All Level 3 Network Gateways feature positive physical controls that continually monitor and archive access to the facility areas. Photo identification (ID) access cards are used as the first layer of security. These devices are located at authorized entry points for securing critical areas within a gateway. All perimeter doors are centrally monitored from the Level 3 NOCs. Authorized customers and vendors are required to have validated palm scans to enter sensitive area. The access control system supports, monitors, and logs access at entryways of the facility.

Redundancy:

The Level 3 co-location facilities are IP-enabled and docked to their Tier 1 backbone and in addition, all Level 3 data centres feature true route diversity. Each Level 3 Gateway is connected to the intercity network and its resident metropolitan network by at least two physically separate building entrances. Whenever possible, the Gateways are connected to the fiber by three entrance facilities. This provides for the greatest protection from network outages caused by events such as fibre cuts that could disable one of the fibre links into the gateway.

In addition to route diversity, Level 3 ensures network access with redundant and duplicate equipment including routers and switches with various port speeds. The following types of port interfaces are available options at co-location facilities:

- 10/100 Ethernet/Fast Ethernet (10 Mbps/100 Mbps)
- 1000SX/Gigabit Ethernet (1000 Mbps)
- 10 Gigabit Ethernet

Redundancy is engineered in the network architecture to ensure continued service in the event of a network failure.

- Dual access routers/switches are located in each collocation facility and offer port speeds of 10/100 Mbps Ethernet, 1 Gbps Ethernet and 10 Gbps Ethernet (as well as other port options previously listed). Level 3 also ensures sufficient capacity for normal and fail-over operations by limiting every internal network link to less than 50 percent utilization. Any time an internal Level 3 Network link approaches 50 percent utilization, capacity on the link is immediately increased. Limiting link utilization to less than 50 percent guarantees redundant capacity in the event of failure of other network links.
- All co-location routers/switches are dual-homed to the IP network.

Additional resilience is obtained by synchronising the operation process and systems in other data centres around the UK and the US (see examples in the Network diagram below)

4.2 SOFTWARE UPDATE PROCEDURE

CentralNic have a sensible software update procedure that meets the requirements appropriate to the architecture and systems involved. The steps involved in this process are as follows:-

1. Always update software packages when a security vulnerability is announced and an errata published.

2. Disruptive updates should be scheduled for maintenance windows.

3. Always perform targeted updates.

4. Policy especially applies to systems running operating systems that do not offer long-term support (ie Fedora, Ubuntu)

5. Prepare a rollback plan in the case of an issue.

6. Check package/release Change Logs before updating.

4.3 REMOTE ACCESS

Remote access is provided to maintain operational support even when staff are not in the office. This is achieved through secure connections that require both password and certificate before access is granted.

Public Key only Authentication is utilised for administrator accounts on all machines. To ensure that logins can be assigned to Staff Members, all operators have separate keys.

Keys are added to and/or removed from all servers by an automatic script which knows the public key of the employee.

sshd provides a configuration variable “LogLevel VERBOSE” which includes the fingerprint of the accepted public key in the logfile.

4.4 FIREWALL AND IDS

CentralNic protect their operations with a combined Firewall and Intrusion Detection appliance. Access to the firewalls is both physically and logically restricted to authorised personnel.

The firewalls are configured to default to reject everything, only accepting those protocols that are explicitly required, to those IP addresses, which specifically require them. The rules are regularly checked as part of the change control process.

4.5 CENTRALISED LOG MANAGEMENT

The logs from the Firewall/IDS are redirected to an external syslog server which is backed up and kept for 6 months. Alerts created by the IDS are immediately sent by e-mail to operators and acted upon.

In addition to this operating system logs are collected by a daily job, compressed, encrypted and signed by PGP to prevent tampering.

Application Logs created through CentralNic products by their users are stored in SQL format on the main database system. This database is replicated through multiple servers (hot backup), and an hourly snapshot is created.

4.6 SECURE DELIVERY AND SENSITIVE DATA PROTECTION

CentralNic utilise PGP and Vault to protect data in transit and at rest. This is available to all staff.

4.7 NETWORK MONITORING

All networks and servers are monitored for both security and operational purposes. A variety of tools are used to achieve this such as Munin etc.

4.8 TEST AND PRODUCTION ENVIRONMENT

The test and production environments are air gapped for security purposes. Code updates require sign off from the Chief Technology Officer (CTO) and are uploaded over a secure tunnel.

Significant code changes are subject to peer review as well as sign off from the CTO.

4.9 BACKUP AND RECOVERY

Although CentralNic do not have a formal, Business Continuity and Disaster Recovery procedure, many aspects of the process are being performed to ensure key data and operations are recoverable.

CentralNic adopt these key considerations for backing up data

1. Completeness. Backups must be complete or they are useless.

2. Redundancy. Taking a backup of critical data is pointless if the location to which it is backed up is subject to the same risk of damage as the source. Therefore, it is important to back up to multiple locations.

3. Security. Backed up data should not be disclosed to unauthorised parties. Using public servers, or unaudited third-party systems without use of strong cryptography is prohibited.

4. Accessibility. In the event of a disaster, it is critical that data should be restored from backups as quickly as possible. It would be highly undesirable to have to restore data from a remote site over a slow network link. If backup data is encrypted, then preparations must be made to ensure that the passphrases and/or keys required to decrypt the data should be easy to access (subject to their own security requirements), and of course also backed up, via a different mechanism to avoid a single point of failure.

5. Historicity. Back-ups should also be archives: it should be possible to look "back in time" to examine the state of the database or source code at a particular date and time. Some data, such as the CVS repository or wiki database, automatically preserve historical data, and so it is not required to archive this data. Likewise, data such as the Staff Console documents, are "cumulative"

(nothing is ever removed or changed), and so they also don't need to be archived. However, data such as the registry database are subject to updates and deletions, so this data should be backed up on a day-by-day basis.

4.10 DEFAULT ACCOUNT REMOVAL

All manufacturer default user and passwords have been disabled for all the firewalls, servers, routers etc as part of the standard practice for configuration builds.

5 NETWORK DIAGRAMS

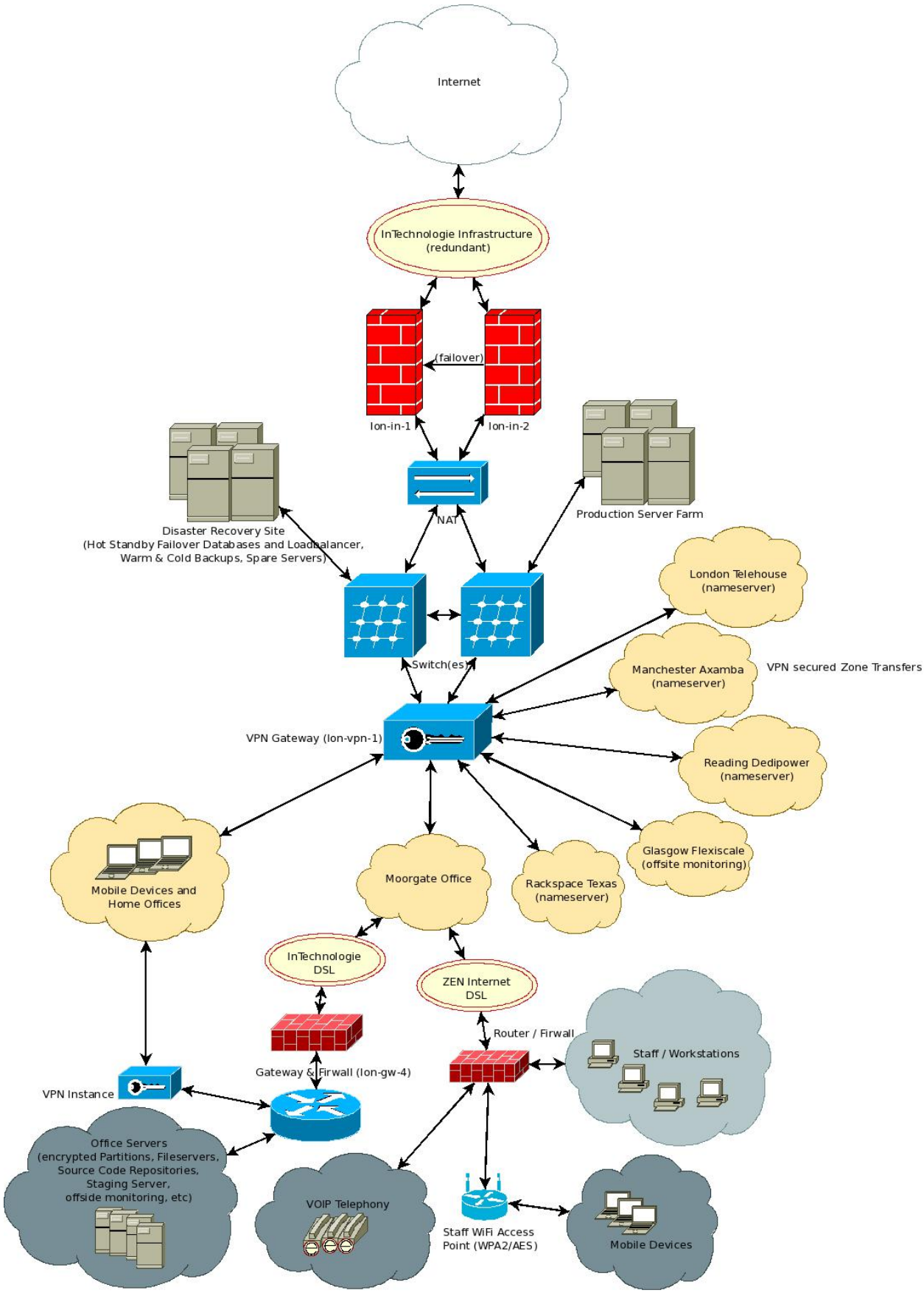

Figure 1 CentralNic Network Diagram