GENERAL security POLICIES

Adminor

- Standard IT agreement compliance (standardavtal avtal 90).
- Internal security practises within the organization.

Personel

- Adminor employes technicians skilled with networking, common routing protocols and brand products such as cisco, mikrotik, juniper and HP.
- Technicians with UNIX and Windows knowledge .
- Adminor has IT-security technicians employed within the organization with a background in managed IT security field.

Optionally we can also offer reviews through thirdparty IT security companies upon customer request .

Network security

- Adminors network is separated into different zones protected by various layers of firewall and credentials depending on which security level is required.

For higher security zones ACL's are defined for which IPs may access the core network.
On medium level security zones services are defined on port level (open/closed).
For lower level zones firewalls only monitor traffic usage for malicious traffic patterns .

- Adminor takes advantage of VPN technology to ensure point to point security as well as SSL transport layer security for various services (control panel accesses, email/pop3/imap, smtp).
- Network intrustion detection (NIDS) for monitoring attack trends.
- Manned abuse contact (abuse@adminor.net) with swift action to reported vulnerabilities and threats (spam, virus outbreaks, hijacked customer systems).

OS level:

- Securitypatches are applied every night . Recommended patches and other updates are applied during normal service windows.
- Firewall services are activated to protect local access.
- Regular intrusion detection scans are run to find signs of intrusions attempts and or malicious access.

Adminor uses host based intrustion detection system such as rkhunter and/or OSSEC .

- Adminor monitors security bulletins and applies urgent security patches for critical vulnerabilities on managed systems.

Physical security

- Server facility has 24/7 CCTV monitoring and security patrols doing rounds at night.
- Server facility is partitioned into different security zones.

Additional security can be offered with private cabinets or fenced areas.

- Access is granted to area and rack cabinets with personal keycard and alarm codes.

Backups and redundancy

- Incremental backups of critical systems daily.
- Backup service offered to customers as an optional service.
- SQL data backed up each night.
- Backups transfered over encrypted connection (SSH) to storage systems.
- Offsite backups available as an optional service.
- Router redundancy with BGP.
- Personel available on-site within agreed stand-by periods.
- First class server facility with UPS and diesel redundancy (n+1 power feeds).