Proxy Networks Information Security Policy for Hosted Services

Introduction

This Information Security Policy covers the two separate layers that make up the service. One is internal to Proxy Networks and touches all organizational aspects related to the product. The other deals with all security concerns of the Hosted Services outside of Proxy Networks, on their respective cloud solutions.

Policy Statements

- This policy should be communicated to all new employees and updates should be sent out immediately, following review cycles as mentioned below.
- Every employee should respond, by email, with acknowledgement of their respective security role and responsibilities after receiving and reading a new or updated policy.
- This policy should be kept up to date with best practices. This includes what is learned from outside sources as well as from what we've learned managing our own and customer's data and dealing with incidents.
- All employees are responsible for protecting Proxy Networks confidential information, as well as the confidential information of Proxy Networks customers.

Internal Information Security Policy

Security roles and responsibilities

- Only members of the Support team have access to Hosted Services.
- Members of the Support team should use internal secure storage of identities used to manage Hosted Services.
- The Support team manager is responsible for maintaining a history of identities and disabling unused identities used to access Hosted Services.
- Every employee of Proxy Networks should be responsible to log and communicate any incident which may reduce the quality of the service (see Incident Management Process).
- Only members of the Support team can close "incidents" (see Incident Management Process).

Incident Management Process

An **Incident** is an unplanned event which lowers the quality of the service or threatens to do so.

It is important to maintain a simple process which can be consistently followed in all incidents.

- **Log incident**: reporting party, time and date, description, unique number or name for tracking. Notice: this step can be done by any employee of Proxy Networks whoever "witnesses" and recognizes the incident.
- **Classify incident and give it priority**: Classifying incidents gives you an ability to decide who is best suited to investigate and diagnose it and priority gives you an understanding of how to handle communication, triage and escalation.
- **Notification**: Notify all parties affected by the incident about it.
- **Investigation**: Investigate and diagnose the incident.
- **Resolution**: Provide resolution and recovery to all parties affected by incident. Close the incident after all affected parties have been satisfied. Development process

Secure development process

- Coding should be done in accordance with standards as defined in the documents stored in our repository under "Documentation\CodingStandards".
- We should have a formal weekly build, which should be evaluated by QA.
- All reported bugs should be tracked in our Bugzilla repository.
- All reported bugs should undergo triage process where they are assigned and prioritized.
- All P1 priority bugs should be resolved before release.
- All bugs should only be closed after QA's evaluation ("Resolved - Verified" status).
- All software should undergo performance, resource and stress testing before beta releases.
- All software should undergo security testing before beta and public releases (see "Vulnerability and penetration testing" below).
- Sever software developed by us should support audit logging to track the system's and user's interactions.
- All software should have a debug logging option with clearly defined debug scripts for development, QA and production environments.
- Every change in the software should be evaluated for the scope of debug and audit logging and steps should be taken to keep logging up to date with the changes.

Third party libraries and software

- All third-party software used for development should be from well-known and reputable sources, licensed and signed with licenses recognized by the Windows operating system.
- All third-party libraries should have appropriate licensing, which should be noted in our documentation.
- When downloaded, libraries should be tested against checksums published on their secure sites (this is most important for the OpenSSL library).

Vulnerability and penetration testing

- All software should undergo security testing before beta and public releases.
- Security testing should be done with tools like Acunetix Vulnerability Scanner and those under SSLLabs.com.
- All security issues should be immediately addressed and trigger a new release.

Data security

All customer's data which includes contacts, contracts and license keys should be stored in the NetSuite service.

Firewall rules

Our internal firewall should be configured for access only to these services: VPN, PROXY Pro Gateway and Web Console servers.

AV protection rules

All computers should be protected with Symantec Endpoint Protection.

Data storage and backup

Periodic backups should be done on key servers in the server room.

Management of security assets (certificates, keys and secrets)

- All security certificates should be stored in the Windows Certificate Stores with the physical copies maintained by our CTO.

- All administrative identities for Hosted Services should be managed by the Support team in secure password storage.

Software updates

- All computers should be up to date with all Windows software updates.

Information Security Policy of Hosted Services

Administrative access

- All administrative access is performed by the members of the Support team.
- Customers can request administrative access to their "dedicated" instances.
- All security identities should have a password expiration set to 6 months or less.
- Every member of the Support team who is authorized to access Hosted Services should have his/her own security identity to access cloud management tools (AWS, Azure) and hosted instances.

User's access

- Users of Hosted Services have access to Proxy Networks Web Console and Gateway Server which are configured according to the customer's defined organizational rules.
- All User's communications are protected by TLS v1.2.

System's Logging

- Server-side Proxy Networks software should have audit logging enabled at all times.
- Scope of the logging should be reevaluated after every new release, change in the system's configuration and after any incident report.
- Temporary changes in logging should only be done for the purposes of resolving an incident and should be tracked by members of the Support team.
- Windows' Security Audit Logging should be configured on all systems.

Firewall

Hosting firewall should be configured for access only to these services: Microsoft RDP, Proxy Gateway and Web Console servers. RDP is to be allowed only from our internal corporate network.

Intrusion detection tools

Upon a customer request, dedicated hosting can be configured with one of the Intrusion detection tools provided by the cloud hosting service (AWS, Azure).

Management of security assets (certificates, keys and secrets)

All private keys used on Hosted Services should be stored in their respective secure storages. On Windows it should be one of the "Key storage providers". Physical copies of the keys should be held by respective owners.

Software updates

Both, updates to our software and to Microsoft Windows are done once a month during scheduled down time. In the case of a security issue, our Incident Management Process is invoked.

Inventory

The Support team should maintain an inventory of all cloud resources (computation instances, storage instances etc.) for every shared and dedicated Hosted Service.