INFIGO SOFTWARE SECURITY POLICIES AND PROCEDURES

OVERVIEW

Infigo Software is operating an internal network at the offices, uses external cloud based services and hosts it's own solution via external cloud services (AWS).

This document outlines the different areas and indicates security risks, policies and procedures in place to mitigate them.

Efforts are done based on security best practices and loosely based on the CLASP (Comprehensive, Lightweight Application Security Process) system - where we implement various of the proposed activities.

SECURITY LEVELS:

Critical

Vulnerabilities that score in the critical range have most of the following characteristics

- Exploitation of the vulnerability likely results in root-level compromise of servers or infrastructure devices
- Exploitation is usually straightforward, in the sense that the attacker does not need any special authentication credentials or knowledge about individual victims and does not need to persuade a target user via social engineering to perform any special functions

High

Vulnerabilities that score in the high range usually have some of the following characteristics

- Difficult to exploit
- Exploitation could result in elevated privileges
- Exploitation could result in a significant data loss or downtime

Medium

Vulnerabilities that score in the medium range have some of the following

- Attacker is required to manipulate individual victims via social engineering tactics
- DNS
- Exploits that require an attacker to reside on the same local network as the victim
- Exploitation provides only limited access
- Vulnerabilities that require user privileges for successful exploitation

Low

The low range typically has very little impact on a business. Exploitation of such usually requires local / physical access

OFFICES AND ON-PREMISE ARCHITECTURE

BUILDING SECURITY

Access to the offices are protected via key card and an alarm system, protecting physical access to computer hardware for authorized employers only.

Employees are not allowed to share or exchange the key cards and are responsible for the cards they have been assigned. If the card has been lost or stolen, then the employee must contact management immediately.

Employees are not allowed to bring unattended guests into the building.

Intranet and physical computer hardware

The machines are managed and maintained by our 3rd party supplier Matmos who is responsible for

- Patching and repairing the machines
- Keeping a centralized anti-virus software installed and monitored
- Have the internal intranet firewall and router running and patched
- Maintain ActiveDirectory access
    - User Accounts are created with a need to know base
    - Enforcing Infigo's Password policy
- Maintain and secure the VPN connection
- Maintain the Company Wifi Network
    - Protected with WPA2
- Security scan and audits on the network
- Automatically lock the screen after a short period of time of inactivity
- Email
- Backups

User Policies

- Clean desk policy not leaking confidential information and passwords physically
- Lock computer when leaving the desk
- Handle password and sensitive information confidentiality

Cloud based services

- Jira
- Confluence
- Bitbucket
- Hubspot
- Dropbox
- Zoom
- Slack
- Xero
- Smartsheets
- CharlieHR
- Zendesk
- StatusCake

Where user accounts are created with a need to know base and access level permissions are utilized to protect sensitive and critical data from being exposed.

COOKIES

- We store functional cookies only
- Out the box we do not offer any optional cookies
- Our cookes are non-tracking, required essential session cookies according to GDPR standards. Therefore the cookie banner that we provide as an optional feature covers the legal needs to notify the customer but doesn't offer them the ability to opt-in to any additional cookies/tracking services.

PROCESSES

SECURITY AWARENESS IN DEVELOPMENT TASKS

Each task is carefully created and reviewed by the security implications and we use best practices and measurements to avoid any exposure during the specification step

Activity 1: Institute security awareness program

Ensure project members consider security to be an important project goal through training and accountability

Activity 5: Identify resources and trust boundaries

Providing a structured foundation for understanding the security requirements of a system

Activity 7: Document security-relevant requirements

Activity 10: Apply security principles to design

Harden application design, design secure protocols and APIs

Activity 14: Perform security analysis of system requirements and design

Assess likely system risks, identify high-level system threads

Activity 16: Implement interface contracts

Provide unit level semantic input validation and identify reliability errors

TESTING AND CODE REVIEW

Additional steps after implementation will also look out for security related areas and try to mitigate any vulnerabilities

Activity 1: Institute security awareness program

Activity 17: Implement and elaborate resource policies and security technologies

Following specification

Activity 21: Verify security attributes of resources

SECURITY TESTS

Internal and on-request external Penetration tests

Activity 9: Identify attack surface

Activity 18: Address reported security issues

Activity 20: Identify, implement and perform security tests

Activity 2: Capture security metrics

CUSTOMER COMMUNICATION

If there risks of a medium/high/critical level have been identified, we will have to communicate those to our customers in a sensible manner using a disaster task force

Activity 24: Manage security issue disclosure process

DISASTER RECOVERY

Regular checks to perform disaster recovery on several levels

- Outage and recovery of data / databases
- Outage of a single server
- Outage of a whole environment

Hosting Environment

ENVIRONMENTS

AWS Account setup to establish hard boundaries between environments. All Environments are fully separated and there is no direct access to any of them

We do have the following environments configured:

- Ops: used to run operational servers (CI, etc)
- QA: used to run current test builds
- PP: Preproduction environment to run test sites as a replica of live
- Live: two live environments (UK/US)

INDIVIDUAL USER ACCOUNTS

- Are created on a master account
- No leaked orphans
- Single point for policies and permissions
- Assuming roles for the individual environments
- Using groups and policies on a need to know base (Activity 6)
- Strict password policy
- MFA required to use accounts

ACCESS

- Management and building servers are IP restricted
- Zoned (public/private) subnets and restricted port access on all environments
- Hardened server, no exposed RDP connection, local management only via Systems Manager
- Any access and any commands executed are logged to an S3 audit

SERVERS AND INFRASTRUCTURE SETUP

- Encryption on the file level for any user data
- Servers are being refreshed weekly with latest OS patches
- Infrastructure changes are applied automatically going through a validation and approval process
    - Operating environment is defined (Activity 3)
- Automatic Backups
- Automatic recovery procedures