Overview of the IT Security Related Aspects in the Got Ethics Whistleblower Solution

Overview

Portals and Reporting Channels

Web based portals

The whistleblower system consists of a web based reporting portal and a case management system. The system is a SaaS (Software as a Service) – only a web browser and an internet connection are required to use the system.

App

It is possible to include an app. The app is native, the design is customized to each individual customer and is available for iPhone and Android.

Phone Hotline

Furthermore, it is possible to include a phone hotline where whistleblowers can leave a voice message that is transferred directly into the case management system.

E-mail

Optionally, the system can be configured to receive e-mails. This is particularly useful if you already have an existing hotline based on e-mail reporting. However, it is difficult to achieve anonymity for e-mails, so this solution is recommended only in a transition period until the informants get used to use the safer channels (web, app or phone).

Technology

Servers

The system is based on the following servers:

- Operating system: Microsoft Windows Server 2016.
- Database server: Microsoft SQL Server 2016.

The servers have been hardened - all services that are not necessary to run the solution has been disabled, no security information is revealed in the HTTP headers etc.

3 Tier Solution

The application is a 3-tier design. Presentation and logic tier is pure C# (ASP.NET) and JavaScript. No 3rd Party plugins are used for the core and critical components (encryption etc.). Data tier is ADO.NET and Microsoft SQL Server.

Privacy Enhancing Technologies

To be able to safeguard the sensitive data, the relevant privacy enhancing technologies (PETs) have been implemented (privacy by design). The different technologies are described in this document.

Organizational Security

Information Security Management System (ISMS)

IT Security Committee
Got Ethics A/S have established an IT Security Committee consisting of the management and a senior developer.

IT Security Policy
A formal IT security policy is in place and has been implemented.

A senior developer is reviewing the implemented safety concepts on a regular basis and discussing proposals for improvements with the rest of the development team on a regular basis.

Risk Assessment
A formal risk assessment has been conducted.

Catalogue of Processes/Instructions
The IT Security Committee has prepared a set of instructions/processes that is a significant part of the ISMS.

Regular Assessments
The IT security policy, the risk assessment and the instruction catalogue are discussed on a regular basis and updated when changes are needed.

Every Friday we have internal meetings where the need of any system development requirements are being discussed.

Employees

Employee Lifecycle

When Employees are Hired
We obtain criminal record prior to hiring new employees.

When Employees Leave the Company
We have procedures in place ensuring that access to physical locations and IT systems are revoked when an employee leaves the company

Code of Good IT Behavior
All employees have signed Got Ethics A/S' code of good information security behavior.

Non-Disclosure Agreements
All employees have signed a Non-Disclosure Agreement.

Certifications

Ethical Hacker

At least one employee is Certified Ethical Hacker (CEH). The purpose of the CEH credential is to:

- Establish and govern minimum standards for credentialing professional information security specialists in ethical hacking measures.
- Inform the public that credentialed individuals meet or exceed the minimum standards.
- Reinforce ethical hacking as a unique and self-regulating profession.

Audit Reports

On an annual basis, BDO prepare an ISAE 3000 audit reports stating that the whistleblower system complies with the European General Data Protection Regulation (implementation of technical and organizational measures). Furthermore, the audit report is based on the framework set out in the ISO 27001 standard.

Change Management

We have implemented change management procedures ensuring:

- all change requests and testing is documented in an issue management system.
- all code is reviewed by a system developer different from the system developer who has written the code.
- all code is tested thoroughly before migrated to the production environment.
- penetration tests are performed each time a new version is migrated to the production environment.

Network and Application Security

OWASP Compliance

The system is OWASP top 10 compliant and is scanned for compliance with every software release.

Man in the Middle Attack Prevention

All traffic between servers and client encrypted with a DigiCert SHA2 SSL certificate. Internal traffic between servers is encrypted with self-signed 2048-bit RSA certificates.

Distributed Denial of Service (DDoS)

Implementation of relevant processes ensure that the server is protected against a critical knockout.

Protection Against Malicious Software

Normal antivirus programs do not protect against zero day viruses. Therefore, we have developed our own system "File Detox" that cleans the files uploaded in the system.

File Detox creates a mirror of the original file where only information that is known to be safe is copied to. For example:

- document files (e.g. word) into a new pdf document.
- sound files (e.g. mp3 files) into a new mp3 file.
- movie files (e.g. mp3 files) into a new mp4 file.
- Image files (e.g. jpg and png files) into a new jpg file.

This process removes viruses (even zero-day viruses), macros and piggybacked code from the files. Furthermore, revealing meta data is removed in the file detoxing process.

File Detox supports the most used file formats.

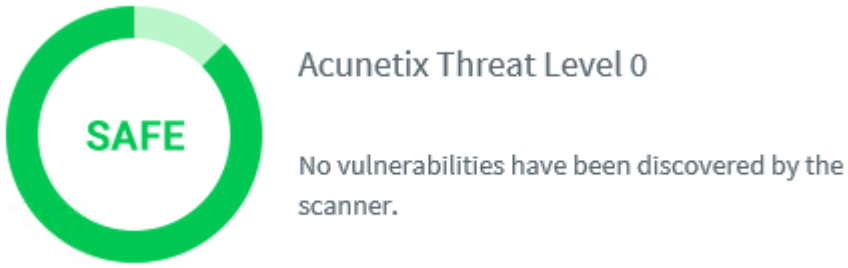
Penetration Tests

Internal Penetration Tests

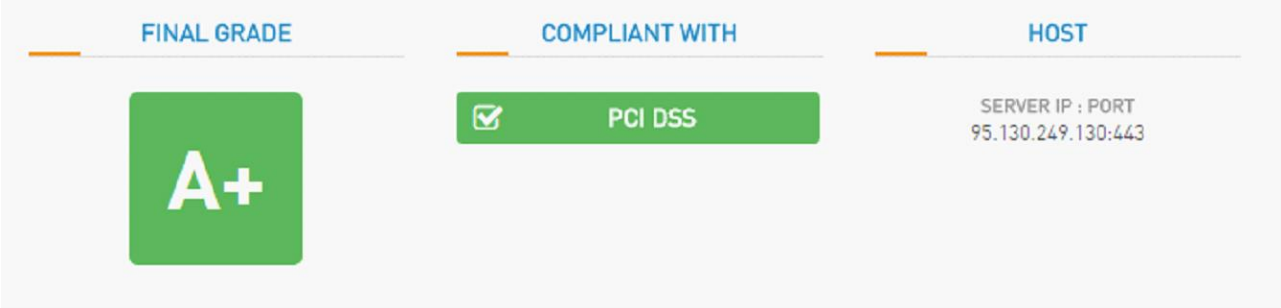
Every time a new version of the system has been released, we run a penetration test on the system to verify that there are no vulnerabilities.

The results of the latest penetration test are shown below.

Acunetix Web Vulnerability Scanner:



HTBridge test of SSL:



Independent Penetration Test
HiSolutions AG Germany in (https://www.hisolutions.com) has performed an independent penetration test. HiSolutions has been carrying out penetration tests for well over 20 years and employs a team of highly trained professionals. Their high expertise is also reflected by a certification as a penetration testing provider issued by the German Federal Office of Information Security (http://bsi.bund.de).

Patch Management

The OS (Windows Server) and the database server (MS SQL Server) are patched automatically when a new patch is available. All servers are monitored for available updates every hour.

Access Restriction to the Production Server

Physical Access
The relevant access restrictions have been implemented (ISO 27001 certification), e.g.:

- Facility surrounded with a detection-equipped fence.
- 24/7 manned control center (including security staff) on site.
- Personal key card required and all use logged.
- Strict access authorization program in place.
- Security camera monitoring.

The hosting provider does not have access to log in to the production server. More details can be found in the chapter "Physical security".

Remote Access
Only 3 employees within Got Ethics A/S have remote access to the production server.

Remote access must use a VPN tunnel authenticated by individual certificates and user credentials. The persons with remote access to the production server cannot read the sensitive data/files submitted to the system as the encryption keys that must be used to decrypt the data is not available to these employees (it is kept by the customers at their location).

Firewall
All firewall ports are closed except from the ports used explicitly by the system.

Data Security

Separation of Data

Separation of Customer Data on the Production Server
Each customer's data are stored in separate databases in the database server.

On the web server, each customer's portal is created in separate sub domains (web sites) in IIS.

Separation Development and Test
Development and test is performed on a separate server placed in a server room in Nupark in Holstebro, Denmark.

Data from the production environment is never used in the test and development environment.

Encryption

Each of our customers' systems are encrypted with individual encryption keys.

Neither Got Ethics A/S nor the hosting provider has access to the encryption keys that is required to decrypt the data and thus cannot read the sensitive information in the reported incidents.

Data Stored in the Database
All sensitive personal data are encrypted in the database:

- Asymmetric encryption: 2048 bit RSA algorithm.
- Symmetric encryption: 256 bit AES algorithm.

Two levels of encryption keys are used: The "master key" and the "data encryption keys". The master key is VERY large but slow to encrypt/decrypt. This key is used to protect the data keys. The data keys are shorter (and faster) but changed regularly. In principle, each row in the database can be encrypted with different data keys (this is not the case).

The Master key and the data keys are encrypted in a way that only an administrator user/case investigator is able to decrypt and read the submitted reports. Not even Got Ethic A/S' IT developers are able to decrypt and read the submitted reports.

The administrator users' passwords are not stored in the System in clear text. Only a salted pbkdf2 hash of the passwords are stored.

Data Transmission
All data transmission is encrypted with a DigiCert SHA2 SSL certificate.

Encryption Key Management
The customer specific encryption key can either be created by Got Ethics A/S or by the customer depending on the customer's choice.

Got Ethics A/S Generates the Master Encryption Key
Got Ethics A/S generates the encryption key and sends it as a certificate to the customer by registered mail. Got Ethics A/S has no copies of the encryption certificate.

The Customer Generates the Master Encryption Key
Got Ethics A/S sends a code (one time use) to the customer by e-mail along with a hyperlink to a web page that handles the migration of the system from the demo environment to the production environment.

When the customer enters the code, the migration process starts and the encryption certificate is created and automatically downloaded to the customer's computer.

As the encryption certificate is the only "back door" to the system if all administrator users should forget their password, is very important that the customer keeps the encryption key in a safe place where it will not be destroyed or lost.

Master Key Management
The master encryption keys can be changed by demand. The customer contacts Got Ethics A/S and we set the system in "key generation mode". Only one administrator can log on to the system at this time, but Issues can still be reported. The designated employee logs on and press a button on the dashboard. New encryption keys are generated and a new encryption certificate is sent to the customer by registered mail.

Data Key Management
Changing the data encryption keys is done transparently and does not require any interaction with the customer or the users of the system.

Physical Security

We use the following sub-contractors:
- Hosting Center – Germany.
- Hosting Center – Canada.
- Telephone Company (if phone hotline is included) – Denmark.
- Independent translation company (if translation services are included) - Denmark

The customer choses between either the German hosting center or the Canadian hosting center. The German and the Canadian hosting centers are independent, and no data will ever be transferred between them.

If we decide to change a sub-contractor it must comply with the following criteria:
- only to sub-contractors with at least the same level of IT security as the existing one.
- the customer can terminate the contract if the customer does not agree with our choice.
- the German hosting center will never be replaced by another hosting center outside the EU.
- the Canadian hosting center will never be replaced by another hosting center outside Canada.

The hosting providers cannot login to the (unmanaged) servers. All data on the servers are encrypted – neither Got Ethics A/S nor the sub-contractor have access to the private key that is needed to decrypt the data.

Hosting – Germany

The System is hosted by Microsoft Azure Germany. This is an isolated branch of Microsoft Azure Cloud, where it is guarantied that data never leaves Germany and all personal is German or approved by German authorities.

The data center is ISO 27001 certified which implies implemented security (see below), uninterruptible power supply (UPS), fire detection and suppression, environment and air conditioning etc.

Compliance reports (including ISO 27001 certification) can be downloaded from the Azure trust Center at https://www.microsoft.com/en-us/trustcenter/compliance/iso-iec-27001

A data processor agreement between Microsoft Azure and Got Ethics A/S apply.

Hosting - Canada

The System is hosted by the company Cogeco Peer 1 on a dedicated virtual server in Montreal.

The backup is located on a dedicated virtual server in Toronto.

A data processor agreement between Gogeco Peer 1 and Got Ethics A/S apply.

Availability

Backup and Archiving

Backup

Hosting center - Germany
The backup is handled by Azure Recovery Services. Backups are stores on geographically distinct locations.

Hosting center - Canada
The backup server is hosted on a dedicated virtual server in a hosting center in a different city than the production server.

Frequency (Germany and Canada)
A backup of the database is made each day. The daily backup is kept for 30 days whereupon it is deleted. At the end of each month, a monthly backup is made. The monthly backup is kept for 5 years where after it is deleted.

Archiving

- A case can be marked as „Completed" whereupon it will be moved to a separate folder where it will remain until it is deleted.
- Completed cases will remain in the system encrypted with the customer's dedicated encryption key until deleted.

Recovery Tests
Recovery tests are done on a quarterly basis and reviewed by the annually external audit.

Redundancy

Microsoft Azure Germany
Azure Site Recovery is used for failover at the German location. All services at the primary location (Germany Central) is hot mirrored to the secondary location (Germany North-East). Furthermore, all data is replicated to 3 different locations within each data center.

SLA

Uptime
We guarantee an uptime percentage of 99.5% measured per calendar quarter.

The system contains a log of historical down time that is accessible by from within the administrator portal.

Any future down time will be notified to the relevant personnel with our customers. The notification setting is defined by each administrator user in the system.

Maintenance Windows
Planned updates are performed Friday evening 8 PM and 12 PM (CET/CEST). Extraordinary critical system updates can be installed daily between 7 am and 8 am. Down time may occur in these maintenance windows. Got Ethics A/S strives to limit down time as much as possible.

Remedy of Errors
Remedy of errors will start within 12 normal working hours (CET/CEST) after the error has come to Got Ethics A/S' attention. Remedy process will continue without undue delay, until the error has been remedied. If the error is insignificant, the error will be implemented in the production environment in the next ordinary maintenance window.

Whistleblower Software

User Access Controls

Access Restriction to the Administrator Portal

Configurable IP Restriction
IP restriction can be activated on the administrator portal. When activated, the administrator portal can only be accessed from the IP addresses/IP ranges registered in the System.

Configurable Password Policy
The System is predefined with a password policy that meets the standards for good password practice.

The password policy can be changed by Licensee. The following parameters can be configured:
- Minimum password length.
- Password must contain at least 1 upper case and 1 lower case letter.
- Password must contain at least 1 number.
- Password must contain at least 1 special character.
- Password expiration period.
- Forced password changed policy.

Configurable Brute Force Protection
Licensee can configure the brute force protection parameters (applies on the reporting portal and the administrator portal):
- Number of minutes the account is suspended.
- Maximum number of failed logins before account suspension.

2-Factor Authentication
The system supports 2-factor authentication with SMS codes. This is an add-on service.

Session Timeout
Automatic session timeout (e.g. password required to log-in again).

Access Restriction to the Communication Module (Anonymous Dialogue)
When a whistleblower submits an issue in the system, he/she is provided with a system generated case ID and is asked to create a case specific password. The case ID and the password are used to log in to the system later to communicate with the case investigator.

The password complexity requirements can be configured in the system (minimum characters allowed, mandatory upper/lower case characters, mandatory numbers, mandatory special characters).

The brute force settings also apply when the whistleblower logs in to the system to communicate with the case investigator.

User Management and Configuration

The customer is in charge of the administrator user management and configuration. Got Ethics do not have access to the portal after it has been migrated to the production environment.

All administrator users have their own unique login that are not to be shared with anyone.

When an administrator user is created, the login (e-mail address) and a time limited temporary password is automatically sent to the administrator user. When the administrator user logs in to the system for the first time, the password must be changed to another password that complies with the password complexity requirements configured in the system.

The administrator users' access rights are highly configurable. In this way each administrator user's access rights can be customized so that he/she only have access to those specific functionalities in the system that are necessary to carry out his/her job.

If an administrator user forgets the password, a new time limited temporary password must be sent manually by another system administrator to avoid the risk of unauthorized system access. The temporary password expires after a predefined period.

Measures to Ensure Whistleblower Anonymity

Logging of IP Addresses etc.

The System and the web server is configured not to log the IP address of the whistleblowers and the System does not use cookies (except from session cookies).

Metadata in Uploaded Files

Metadata that could reveal the identity of the whistleblower in uploaded files are removed in the file detoxing process, please see above regarding "File Detox". However, the metadata will still be available in the originally uploaded file.

Furthermore, the standard text in the system urge the whistleblower to remove any metadata in the file before uploading it.

Logging

All significant actions performed by administrator users are logged.

No information regarding the whistleblower reporting incident in the system are logged.

The Customers' Audit Rights

Our customers are allowed on the spot checks at Got Ethics A/S and with our sub-contractor (hosting provider) provided that the check is announced in due time and the customer pays for the costs related to the on the spot check.

Miscellaneous

DNS Routing

Per default, the link to the portal follows this naming convention: https://[CUSTOMER].whistleblowernetwork.net where [CUSTOMER] is chosen by the individual customers

However, it is possible to use an alternative URL specified by the customer, where:

- the customer is responsible for the alternative URL including the DNS routing
- the customer provides Got Ethics A/S with a copy of the SSL certificate for the alternative URL.