echo.it SECURITY

Last revision:

May 1st 2016

Contact person:

Bo Hansen Hansen

bo@newplatforms.dk

+45 60684727

Scope and Audience

This document is for people who need insight into technical aspects of echo.it's platform, as well as measures and procedures in operation for ensuring the stability, availability and security.

echo.it Platform

echo.it is available as Software as a Service. All customers share the same code base and are part of the same infrastructure. Features and patches are maintained centrally and released for all customers simultanously.

The echo.it platform consists of several layers: applications, API, server and network.

Software as a Service

SaaS is a when software is delivered over the Internet as a service. Instead of installing software on a local server or employee computer, the software runs on the provider's servers. This means that the software is available 24/7 from any location and that software updates are automatically applied for all customers on a central location. The provider manages and maintains the software, including servers, security, availability and performance.

Applications

echo.it currently provides three applications: web, iOS and Android.

Web

The web application is available through all browsers, including desktop, tablet and smartphone browsers.

Stack

echo.it's web application builds upon known and widely used technologies. The main components of the stack are: PHP, MySQL, jQuery, Backbone.js.

Compatibility

We strive to keep our web application compatible with most browsers. We ensure that the web application works completely in the most widely used browsers: Chrome, Firefox, Safari and Internet Explorer 9 or newer. This compatibility list is reviewed in a yearly cycle.

iOS and Android

echo.it also provides smartphone applications for iOS and Android. These are available in the App Store and Google Play.

The iOS app is compatible with iOS 8 or newer.

The Android app is compatible with version 4.0 or newer.

API and Data Export

echo.it plans to provide a public API for interacting with the platform and exporting data for analysis. The API will follow the REST pattern with OAuth for authentication and authorization.

Operational Security

echo.it employs a range of controls to secure that it's platform and applications are available and accessible.

Unit tests are implemented to ensure the integrity of the code base. These must run successfully before a deploy to production servers are allowed. End-to-end tests likewise are in place to secure that the main functionality of the platform is always working before any deployment.

New features and changes are created in a private development environment by the developer. When a feature or change is done, they will be pushed to a staging environment where unit tests run and a manual test of the recent changes are done. If every test is successful, the changes are pushed to the production environment.

Best practice documents are employed to ensure code compliance and take precautionary measures to avoid misunderstandings.

Data Security

It is echo.it’s highest priority to keep our customers' data secure and prevent unauthorized access. When we select suppliers it is with emphasis on data security.

Customer Data Segregation

echo.it's platform follows the *Shared Database, Shared Schema* architecture to offer a multi-tenant software solution. Data are segregated using unique tenant IDs in the database and secured using logic in the private API.

Confidentiality

Every employee in echo.it are legally obliged to keep confidentiality. Employees from echo.it may need access to customer data, but are obliged to handle these with the utmost discretion.

Remote Access

Remote access to echo.it's databases are restricted to whitelisted IP addresses or through VPN. Whitelisted IP addresses are restricted to echo.it offices and employees' home addresses. Employees must be able to provide a personal IP address and any WiFi connected must be secured by highest setting available.

Encryption of Data

Private data stored in echo.it's databased are encrypted. So are authentication tokens.

Servers and Network

echo.it's servers are located in the EU. Some data, such as images, may be distributed to a CDN to offer faster data transfer for users outside EU.

To ensure stability and availability, we have a server setup that are easily scalable. Below diagram illustrates our server configuration.

Software

Our servers are configured with a LEMP stack.

Stack

Much of our software stack is open source and the setup is based on a LEMP configuration. LEMP is an term for the Linux, nginx, MySQL and PHP stack. echo.it uses Ubuntu Linux.

Patching

Patching our software stack is taken care of by our hosting partner. This ensures that any patch that are released for our stack, will be applied within few hours.

Data Transfer

Data transfers in and out of our data center are always done through a secure connection. Users access our server through a secure HTTP connection with 128-bit encryption. Access by developers for maintenance and administration are only made through SSH.

Network Architecture

We trust our provider to deliver 100% uptime on the network connection to our servers. Many controls are in place to ensure this uptime.

DDoS attacks are mitigated using network-level traffic monitoring and analysis, server-level anomaly detection, traffic filtering and re-routing.

Backup

All data are backed up every 24 hours. Backups are written to three storage disk, all on separate nodes or locations that have dual power supplies.

Data Center

echo.it currently outsources hosting to Hetzner Online GmbH which operates with the following means of security and redundancy:

Total Bandwidth	1,15 Tbit
Network Availabilty	min. 99%
Redundant Network	✔
100% Switched Network	✔
High-speed access to all Internet Uplinks	✔
24/7 Monitoring	✔
Air-Conditioned Data Center	✔
Redundant UPS - battery	15 min
Diesel Generator	✔
A video-monitored, high-security perimeter surrounds the entire data center park. Entry is only possible via electronic access control terminals with a transponder key or admission card. All movements are recorded and documented. Ultra-modern surveillance cameras provide 24/7 monitoring of all access routes, entrances, security door interlocking systems and server rooms. A generated password enables on-site personnel to authenticate and issue a transponder key for the interlocking doors to the rack. The visit is logged, and the footage recorded is archived in the administration interface for monitoring purposes. The uninterrupted power supply (USV) is ensured with a 15-minute backup battery capacity and emergency diesel-generated power. All UPS systems have redundant design. Direct free cooling allows for the environmentally friendly cooling of hardware. Climate	

control is effected via a raised floor system. A modern fire detection system is directly connected to the fire alarm center of the local fire department.
We monitor the server 24 hours a day for failures. System failure is handled both during business hours and outside. Emergency failure correction is conducted on a best-effort basis, with normal start-up in less than an hour. We reserve the right to deal with requests which are not emergencies during normal business hours only. An emergency is defined as server failure or the failure of a server service.

Location

The echo.it platform is currently deployed in Germany only, but is prepared to be spread to more regions as the need arises.

Procedures and Policies

Several procedures and policies are employed for core operational tasks.

Bugs

A bug reporting procedure is in place to ensure that bugs are properly reported. The procedure specified how to report and who is responsible for verifying that a bug is properly reported. Bugs are resolved automatically in the reporting tool when the fix is released to production.

Data Access

The policy for employee data acess is that only developers from echo.it have access to the databases. Account Managers may have access to individual platforms to support and facilitate customers in setting up and maintaining their installation. All customer data is handled with discretion and employees are signed to keep confidentiality.

Monitoring

echo.it servers are monitored 24/7 through several agents. If an agent triggers an alert, echo.it CTO receives an instant notification.

Uptime Agent

Monitors uptime and accessibility to our servers through Ping and HTTP checks.

Performance Agents

Three agents monitor our servers' CPU, memory usage and Linux load average to alert if the servers are handling higher than usual traffic.