Information Security Brief

Overview

Green Power Hub (GPH) is as Software-as-a-Service SaaS application delivered by GreenPowerHub AS.

The application is developed and maintained by employees of GreenPowerHub AS.

GPH is running on Microsoft Azure, a Cloud platform used by over 200 million organizations and conforming to and holding multiple ISO and CSA certifications.

Compliance and certifications

GPH is built upon a stack of services, compliant and certified to multiple standards:

Certification	Azure
CSA STAR Certification	✓
ISO 27001:2013	✓
ISO 27017:2015	✓
ISO 27018:2014	✓
ISO 20000-1:2011	✓ **(new)**
ISO 22301:2012	✓
ISO 9001:2015	✓

The CSA STAR Certification for Azure can be downloaded from the CSA Registry.
ISO reports and certificates can be downloaded from the Service Trust Portal.

ISO/IEC 27001:2013

Currently yearly audits are performed by a third-party accredited certification body.

See Compliance and Audit reports for details.

Transparency

As GPH is running on Azure, the solution is dependent on the insight into the internal processes of Microsoft's Cloud offering. To comply with these dependencies Microsoft has committed to transparency and openness in all aspects of its cloud services. It shares details about

its efforts in the areas of security and privacy through several portals and reports, including:

- Microsoft Trust Centers, which are used to address key issues and concerns expressed by Microsoft customers about specific Microsoft services.
- Law Enforcement Requests Report. In March of 2013, Microsoft began publishing the number of demands it receives from law enforcement agencies as well as how many entities may be affected by such demands.
- Cloud Security Alliance. Microsoft is committed to transparency through its work with and support for CSA,

who launched the Security, Trust & Assurance Registry (STAR) initiative in 2011 to promote transparency in cloud computing.

Application level security

Authentication & Identity management

Identity management is governed through a dedicated Azure Active Directory.

Single sign-on simplifies access to GPH and allow your users to connect without revealing sensitive security information. Federation with internal or other trusted identity providers for your company available on request. See Green Power Hub Security overview document for more details.

Real-time machine learning guards against use of leaked or stolen credentials and blocks suspicious login attempts.

Authorization

GPH is essentially using an role-based security model but where roles are confined/individual within each company in the solution, in essence making it an ABAC or Attribute-based access control system.

All calls are evaluated according to your userid, the company you are requesting access to and your role in that company. In addition, a complete audit trail of all changes in the system are stored with details of who and when performed the change. To perform a request for data you need to have a valid user within the solution, a role within that company with enough permissions for that request and a proven identity by providing a ClaimsPrincipal from a trusted ClaimsProvider.

Auditing & accountability

GPH is built upon event sourcing which at its heart is built upon storing all changes to the system and leveraging that as system state. The benefit of this architecture is, among others, that auditing is built in. Any change to the system is logged with complete timestamp, a key to the user implementing the change, and the changes applied to the system.

Infrastructure level security

Vulnerability Assesment

Vulnerability Assesment scans are performed at regular intervalls (weekly).

Security center

Security Center continuously monitors the configuration of our services to identify potential security vulnerabilities and recommends actions to mitigate them.

OS and runtime patching

Azure manages OS patching on two levels, the physical servers and the guest virtual machines (VMs) that run the App Service resources. Both are updated monthly, which aligns to the monthly Patch Tuesday schedule. These updates are applied automatically, in a way that guarantees the high-availability SLA of Azure services.

Zero-day vulnerabilities

How does Azure deal with significant vulnerabilities?

When severe vulnerabilities require immediate patching, such as zero-day vulnerabilities, the high-priority updates are handled on a case-by-case basis.

Encryption

All communication between client and GPH are encrypted.

Communication between GPHs internal components are encrypted as well.

For communication encryption GPH is using SSL/TLS version 1.2 and RSA 2048bit certificates.

Passwords are not used or stored in GPH. Instead a single-sign-on solution is employed, see authentication section above.

Transparent Data Encryption is enabled on all SQL databases,

Encrypting databases, logs and backups of all data in SQL databases.

References

Trusted cloud overview and compliance
https://azure.microsoft.com/en-us/overview/trusted-cloud/

OS and runtime patching in Azure App Service
https://docs.microsoft.com/en-us/azure/app-service/overview-patch-os-runtime

Compliance offerings: ISO/IEC 27001:2013 Information Security Management Standards
https://docs.microsoft.com/nb-no/microsoft-365/compliance/offering-iso-27001