IT-Sicherheit und DS-GVO

Geoinformatikbüro Dassau GmbH

GBD WebSuite – IT Absicherung

Agenda

- Überblick zum Thema DS-GVO und IT-Absicherung
- Optimierungen GBD WebSuite ab Release 8.1
  - HTTP Security Header
  - SSL/TLS Konfiguration
  - Image Scan Common Vulnerabilities and Exposures (CVE)
  - Software Bill of Materials (SBOM) beim Erstellen eines Images
  - Umsetzung BSI Anforderungen (Webanwendungen und -services)
- Fazit

GBD WebSuite – DS-GVO

Überblick zum Thema DS-GVO

Die **Datenschutz-Grundverordnung (DSGVO)** spielt eine zentrale Rolle im Rahmen der IT-Sicherheit, da sie klare Anforderungen an den Umgang mit personenbezogenen Daten und damit auch an die IT-Sicherheitsmaßnahmen stellt. Dazu gehört u.a.:

- **Sicherheitsanforderungen**
  - **Technische und organisatorische Maßnahmen ergreifen: Maßnahmen wie Verschlüsselung, Pseudonymisierung, Zugangskontrollen und regelmäßige Sicherheitsüberprüfungen implementieren, um den Schutz der Daten sicherzustellen.**
- Verantwortung und Haftung
- Datenschutz-Folgenabschätzung (DSFA)
- Meldung von Datenschutzverletzungen
- Schulung und Sensibilisierung
- Verträge mit Dienstleistern

GBD WebSuite – IT Absicherung

Überblick zum Thema IT-Absicherung

Maßnahmen, um ständigen Zugriff (**Verfügbarkeit**), Schutz vor unbefugter Veränderung (**Integrität**) und Zugriff nur für berechtigte Nutzer (**Vertraulichkeit**) zu gewährleisten.

- **Netzwerksicherheit** (z.B. Firewalls) und **Web-Anwendungssicherheit**
- **Endpoint-Security** (z.B. Antivirus-Software, Sicherheitsupdates)
- **Zugriffskontrollen/Identitätsmanagement** (z.B. Benutzerrechte-Verwaltung, 2FA)
- **Datenverschlüsselung** (z.B. TLS/SSL)
- **Sicherheitsrichtlinien und -schulungen**
- **Backup- und Wiederherstellungspläne** (z.B. Datensicherung und Recovery)
- **Schwachstellen- und Bedrohungsmanagement** (z.B. Penetrationstests)
- **Notfallmanagement und Incident Response** (z.B. Reaktion bei Vorfällen)

GBD WebSuite – IT Absicherung

Web-Anwendungssicherheit – HTTP Security Header

- **Content-Security-Policy (CSP)** kontrolliert, welche Ressourcen (Skripte, Bilder, Stylesheets, ...) von welchen Quellen geladen werden dürfen.
- **X-Content-Type-Options** erzwingt, dass der Browser den vom Server angegebenen MIME-Typ verwendet, um Content Sniffing-Angriffe zu verhindern, MIME-Types können sein text/html, image/png, ...
- **Referrer Policy** kontrolliert, wie viel Referrer-Informationen (von zuvor besuchten Webseiten) an verlinkte Seiten weitergegeben werden, um sensible Informationen zu schützen.
- **Strict-Transport-Security (HSTS)** erzwingt HTTPS-Verbindungen, um Man-in-the-Middle-Angriffe zu vermeiden. (Bsp: Angreifer schalten sich zwischen eine Kommunikation von zwei Geräten)
- **X-Frame-Options** Verhindert die Einbettung der Seite in Frames und schützt vor Clickjacking (Legen von unsichtbaren Ebenen auf eine Webseite, um zu Klicks auf versteckte Elemente zu erreichen.)
- **Permission Policy** steuert, welche Web-APIs und Browserfunktionen auf einer Website oder in eingebetteten Inhalten wie iFrames verwendet werden dürfen.

GBD WebSuite – IT Absicherung

Web-Anwendungssicherheit – HTTP Security Header

Security Report Summary

A+

Site:	https://staging-v.gbd-websuite.de/
IP Address:	116.203.102.2
Report Time:	04 Nov 2024 07:49:46 UTC
Headers:	✔ Strict-Transport-Security ✔ Content-Security-Policy ✔ Permissions-Policy ✔ Referrer-Policy ✔ X-Content-Type-Options ✔ X-Frame-Options
Advanced:	Wow, amazing grade! Perform a deeper security analysis of your website and APIs: Try Now

Raw Headers

HTTP/2	200
date	Mon, 04 Nov 2024 07:49:46 GMT
content-type	text/html; charset=utf-8
strict-transport-security	**max-age**=31536000; includeSubdomains
content-security-policy	**default-src** 'self'; **img-src** * data: blob:
permissions-policy	**geolocation**=(self), **camera**=(), **microphone**=()
referrer-policy	**strict-origin-when-cross-origin**
x-content-type-options	**nosniff**
x-frame-options	**SAMEORIGIN**
content-encoding	gzip

Quelle: https://securityheaders.com/

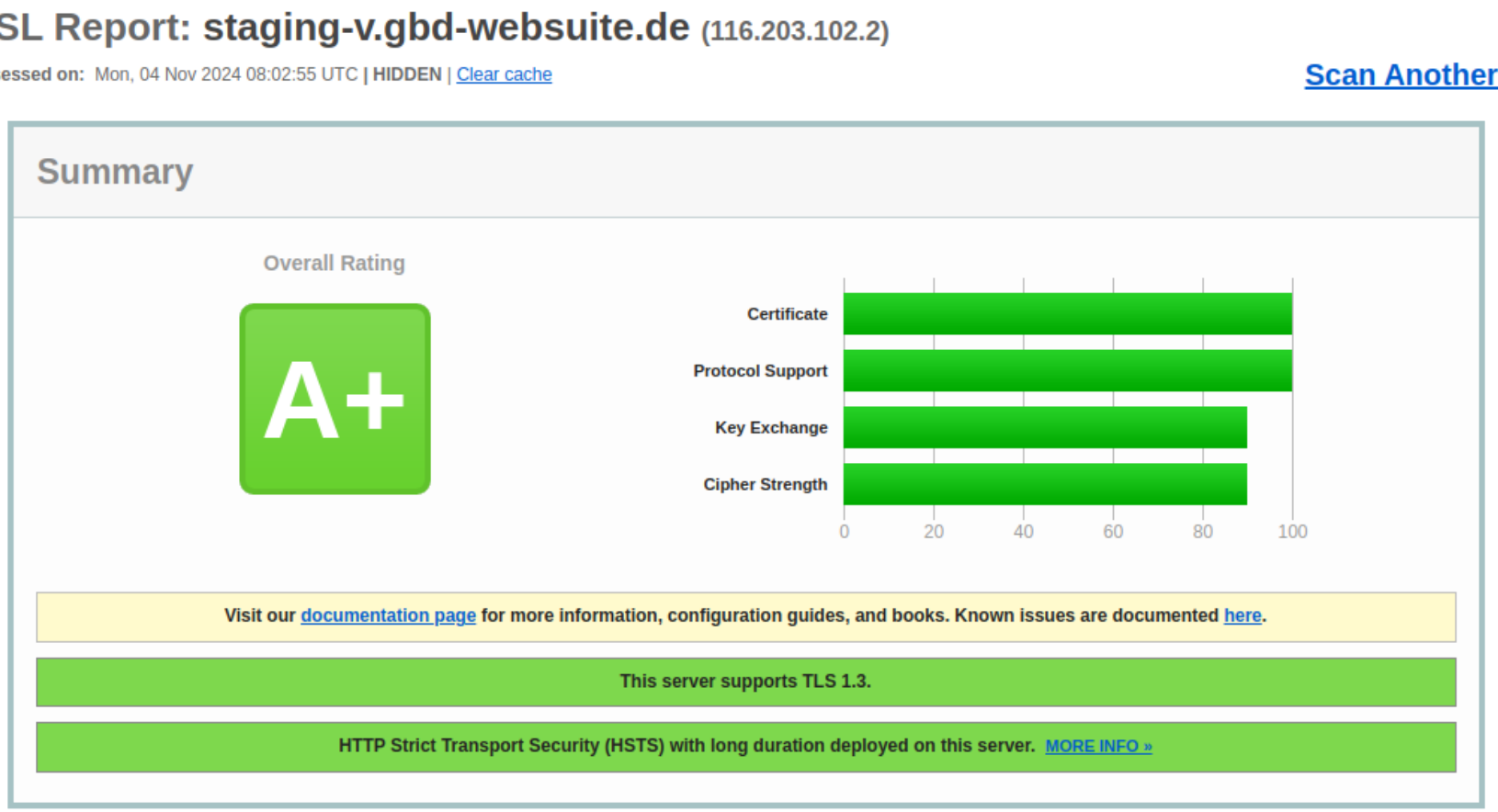
GBD WebSuite – IT Absicherung

Web-Anwendungssicherheit - SSL/TLS Konfiguration

- Einrichtung und Verwaltung von Sicherheitsprotokollen (SSL = Secure Sockets Layer und TLS = Transport Layer Security) für eine sichere Übertragung von Daten im Internet.
- Im Bereich Web-Anwendungssicherheit spielt die SSL/TLS-Konfiguration eine entscheidende Rolle, da sie die erste Verteidigungslinie gegen Angriffe auf die Datenübertragung darstellt. Wichtig bei Passwörtern, Zahlungsinformationen oder personenbezogenen Daten.
- Grundvoraussetzung für die Aktivierung von HTTP Security Headern wie HSTS (HTTP Strict Transport Security).

GBD WebSuite – IT Absicherung

Web-Anwendungssicherheit - SSL/TLS Konfiguration



Quelle: https://www.ssllabs.com/ssltest/analyze.html

GBD WebSuite – IT Absicherung

Web-Anwendungssicherheit - Common Vulnerabilities and Exposures (CVE)

- System zur standardisierten Identifikation und Benennung von öffentlich bekannten Sicherheitslücken und anderen Schwachstellen in Computersystemen.

  → Weitere Informationen: https://cve.mitre.org/cve/identifiers/syntaxchange.html

- Die GBD WebSuite nutzt die Imformation beim Bauen der Docker Images, um auf CVE zu testen. Bei der GBD WebSuite wird dafür Trivy (https://trivy.dev) verwendet. Als Ergebnis wird ein Report erstellt.

GBD WebSuite – IT Absicherung

Web-Anwendungssicherheit - Software Bill of Materials (SBOM)

- Eine SBOM ist eine umfassende Liste (Inventar) aller Softwarekomponenten, Abhängigkeiten und Metadaten, die mit einer Anwendung verknüpft sind.
- Sie ermöglicht ein schnelleres Erkennen von genutzten Bibliotheken und deren Versionen, schafft damit Transparenz und hilft, Sicherheitsrisiken, wie bekannte Schwachstellen (CVE), schneller zu identifizieren und zu beheben.

GBD WebSuite – IT Absicherung

Web-Anwendungssicherheit - BSI Anforderungen

Umsetzung der Basis- und Standardanforderungen des IT-Grundschutz Bausteins APP.3.1 Webanwendungen, z.B.

- A1 Authentisierung
- A4 Kontrolliertes Einbinden von Dateien und Inhalten
- A7 Schutz vor unerlaubter automatisierter Nutzung
- A14 Schutz vertraulicher Daten
- A11 Sichere Anbindung von Hintergrundsystemen
- A21 Sichere HTTP-Konfiguration bei Webanwendungen
- A22 Penetrationstest und Revision

GBD WebSuite – IT Absicherung

Fazit

- IT-Absicherung ist ein umfassender Ansatz, der technische, organisatorische und prozessuale Maßnahmen miteinander kombiniert, um die Sicherheit und Zuverlässigkeit von IT-Systemen sicherzustellen.
- Die GBD WebSuite hat mit Release 8.1 zahlreiche Maßnahmen ergriffen (und wird weitere ergänzen), um die Anforderungen zu den Themen Web-Anwendungssicherheit und Datenschutz-Grundverordnung (DS-GVO) zu erfüllen.
- Die Maßnahmen der GBD WebSuite müssen für eine effektive IT-Absicherung durch weitere Maßnahmen ergänzt werden.

Vielen Dank für Ihre Aufmerksamkeit!

Geoinformatikbüro Dassau GmbH (GBD)

Telefon: +49 211 69937750

E-Mail: info@gbd-consult.de

Web: https://gbd-consult.de