TÜVRheinland®
Genau. Richtig.

Bericht

- Vertraulich -

Prüfung der technischen und organisatorischen Maßnahmen der Rechenzentren

bei der

HETZNER

Hetzner Online GmbH

Version 1.0

Bericht Nr. 63013815-01

Köln, den 27. Januar 2022

TÜV Rheinland i-sec GmbH

Allgemeine Informationen zur durchgeführten Untersuchung

Auftraggeber:	Hetzner Online GmbH Industriestraße 25 91710 Gunzenhausen
Beauftragtes Institut:	**TÜV Rheinland i-sec GmbH** Am Grauen Stein | 51105 Köln Freigerichter Straße 1-3 | 63571 Gelnhausen Dudweilerstraße 17 | 66111 Saarbrücken Zeppelinstr. 1 | 85399 Hallbergmoos Köln HRB 30644 | USt.-ID-Nr: DE812864532 Tel.: +49 221-806 0 / Fax 0221-806 2295 E-Mail: service@i-sec.tuv.com
Untersuchungsumfang:	Prüfung der technischen und organisatorischen Maßnahmen der Rechenzentren an den Standorten: • Nürnberg (Letzte Ortsbegehung am 25.01.2019) • Falkenstein (Vogtl.) (Letzte Ortsbegehung am 27.01.2022) • Helsinki (Letzte Ortsbegehung am 20.02.2020)
Mitgeltende Unterlagen:	Auftragsdatenverarbeitungsvertrag inkl. Anlage 2: Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO der Hetzner Online GmbH
Projektleiter:	Bernd Zimmer
Projektmitarbeiter:	-

Projektleiter

Köln, den 27. Januar 2022

Inhaltsverzeichnis

1 Zusammenfassung

Die TÜV Rheinland i-sec GmbH bestätigt der Hetzner Online GmbH die Einhaltung der, den Kunden bereitgestellten, Informationen zu den getroffenen technischen und organisatorischen Maßnahmen gemäß Art. 28 DS-GVO. Die Prüfung basierte auf den allgemein zugänglichen technischen und organisatorischen Maßnahmen, abrufbar unter https://www.hetzner.com/AV/TOM.pdf. Die vorgenannten technischen und organisatorischen Maßnahmen sind Bestandteil des Auftragsverarbeitungsvertrages zwischen der Hetzner Online GmbH (Auftragnehmer) und dem Kunden (Auftraggeber).

Bei der Prüfung wurden keine Abweichungen festgestellt.

2 Grundlagen und Methodik

Dieser Abschnitt beschreibt Ausgangssituation, Geltungsbereich, Zielsetzung und Prüf- und Bewertungsgrundlagen der durchgeführten Untersuchung.

2.1 Ausgangssituation und Zielsetzung

Die Firma Hetzner Online GmbH ist am Markt im Bereich des Hostings bzw. des Housings als Auftragsverarbeiter im Sinne des Art. 28 DS-GVO tätig. Im Rahmen dieser Tätigkeit werden DS-GVO konforme Auftragsverarbeitungsverträge mit den Kunden abgeschlossen. Die Verträge beinhalten (gemäß Art. 28 Abs. 3 lit. e DS-GVO) technische und organisatorische Maßnahmen, die Gegenstand dieser Prüfung sind.

Seit Oktober 2016 ist die Hetzner Online GmbH nach dem internationalen Standard ISO/IEC 27001:2013 zertifiziert. Die Zertifizierung ist bis September 2022 gültig und umfasst alle Standorte in Deutschland und Finnland. Als Geltungsbereich des Zertifikats ist genannt:

Der Anwendungsbereich des Informationssicherheits-Managementsystems umfasst die Infrastruktur, den Betrieb und den Kundensupport der Rechenzentren.

Das Zertifikat und das „Statement of Applicability“ sind auf der Website der Hetzner Online GmbH abrufbar unter: https://www.hetzner.com/unternehmen/zertifizierung/

2.2 Geltungsbereich

Datacenter-Parks an den Standorten:

- Falkenstein/Vogtland
- Nürnberg
- Helsinki (Finnland)

2.3 Prüf-/Audit-Grundlage

Als Prüfgrundlagen wurden verwendet:

- Technische und organisatorischen Maßnahmen der Firma Hetzner Online GmbH, die unter dem Link https://www.hetzner.com/AV/TOM.pdf abrufbar sind.
- EU-Datenschutz-Grundverordnung (EU DS-GVO)

2.4 Vorgehensweise

Im Rahmen einer Ortsbegehung (in 2020 sowie 2022) wurden die technischen und organisatorischen Maßnahmen an den Standorten zum jeweiligen Prüfdatum nachvollzogen und die Konformität mit den Angaben der Hetzner Online GmbH überprüft.

Neben der Ortsbegehung wurden Interviews mit den beteiligten Mitarbeitern durchgeführt und die getroffenen Maßnahmen mit den beschriebenen, respektive mit Kunden vertraglich vereinbarten Maßnahmen, verglichen und bewertet.

Folgende Personen wurden beim Audit befragt:

Margit Müller	Datenschutzbeauftragte
Simon Beißer	IT Sicherheitsbeauftragter
Sebastian Lippold	Informationssicherheitsbeauftragter

3 Ergebnis der Prüfung:

Die von der Hetzner Online GmbH gemachten Angaben in der „*Anlage 2 zum Auftrag gemäß Art. 28 DS-GVO: Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO und Anlage*“ sind implementiert und entsprechen den vertraglich zugesicherten Maßnahmen.

4 Ergebnisse im Detail

I. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Zutrittskontrolle**
    - **Datacenter-Parks in Nürnberg, Falkenstein und Helsinki**
        - elektronisches Zutrittskontrollsystem mit Protokollierung
        - Hochsicherheitszaun um den gesamten Datacenter-Park
        - dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation-
        - Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocation Rack)
        - Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
        - 24/7 personelle Besetzung der Rechenzentren
        - Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines Hetzner Online GmbH Mitarbeiters
    - **Verwaltung**
        - elektronisches Zutrittskontrollsystem mit Protokollierung
        - Videoüberwachung an den Ein- und Ausgängen
- **Zugangskontrolle**
    - für Dedicated Server, Colocation Server, Cloud Server und Storage Box
        - Server-Passwörter, welche nur vom Auftraggeber nach erstmaliger Inbetriebnahme von ihm selbst geändert wurden und dem Auftragnehmer nicht bekannt sind.
        - Das Passwort zur Administrationsoberfläche wird vom Auftraggeber selbst vergeben - die Passwörter müssen vordefinierte Richtlinien erfüllen. Zusätzlich steht dem Auftraggeber dort eine Zwei-Faktor-Authentifizierung zur weiteren Absicherung seines Accounts zur Verfügung.
    - für Managed Server, Webhosting und Storage Share

- Zugang ist passwortgeschützt, Zugriff besteht nur für berechtigte Mitarbeiter vom Auftragnehmer; verwendete Passwörter müssen Mindestlänge haben und werden in regelmäßigen Abständen erneuert

- **Zugriffskontrolle**
  - bei internen Verwaltungssystemen des Auftragnehmers
    - Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
    - Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers
  - für Dedicated Server, Colocation Server, Cloud Server und Storage Box
    - Die Verantwortung der Zugriffskontrolle obliegt dem Auftraggeber.
  - für Managed Server, Webhosting und Storage Share
    - Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
    - Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers
    - Für übertragene Daten/Software ist einzig der Auftraggeber in Bezug auf Sicherheit und Updates zuständig.

- **Datenträgerkontrolle**
  - **Datacenter-Parks in Nürnberg und Falkenstein und Helsinki**
    - Festplatten werden nach Kündigung mit einem definierten Verfahren mehrfach überschrieben (gelöscht). Nach Überprüfung werden die Festplatten wieder eingesetzt.
    - Defekte Festplatten, die nicht sicher gelöscht werden können, werden direkt im Rechenzentrum (Falkenstein) zerstört (geschreddert).

- **Trennungskontrolle**
    - bei internen Verwaltungssystemen des Auftragnehmers
        - Daten werden physisch oder logisch von anderen Daten getrennt gespeichert.
        - Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.
    - für Dedicated Server, Colocation Server, Cloud Server und Storage Box
        - Die Trennungskontrolle obliegt dem Auftraggeber.
    - für Managed Server, Webhosting und Storage Share
        - Daten werden physisch oder logisch von anderen Daten getrennt gespeichert.
        - Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.
- **Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO)**
    - Für die Pseudonymisierung ist der Auftraggeber verantwortlich

II. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- **Weitergabekontrolle**
    - Alle Mitarbeiter sind i.S.d. Art. 32 Abs.4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.
    - Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.
    - Möglichkeiten zur verschlüsselten Datenübertragung werden im Umfang der der Leistungsbeschreibung des Hauptauftrages zur Verfügung gestellt.
- **Eingabekontrolle**
    - bei internen Verwaltungssystemen des Auftragnehmers
        - Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
        - Änderungen der Daten werden protokolliert.
    - für Dedicated Server, Colocation Server, Cloud Server und Storage Box

- Die Verantwortung der Eingabekontrolle obliegt dem Auftraggeber.

- für Managed Server, Webhosting und Storage Share
  - Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
  - Änderungen der Daten werden protokolliert.

III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Verfügbarkeitskontrolle**

  - bei internen Verwaltungssystemen des Auftragnehmers
    - Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten.
    - Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter).
    - Einsatz von Festplattenspiegelung bei allen relevanten Servern.
    - Monitoring aller relevanten Server.
    - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
    - Dauerhaft aktiver DDoS-Schutz.

  - für Dedicated Server, Colocation Server, Cloud Server und Storage Box“
    - Datensicherung obliegt dem Auftraggeber.
    - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
    - Dauerhaft aktiver DDoS-Schutz.

  - Für Managed Server, Webhosting und Storage Share
    - Backup- und Recovery-Konzept mit täglicher Sicherung der Daten je nach gebuchten Leistungen des Hauptauftrages.
    - Einsatz von Festplattenspiegelung.
    - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
    - Einsatz von Softwarefirewall und Portreglementierungen.
    - Dauerhaft aktiver DDoS-Schutz.

- **Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);**

    - Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Das Datenschutz-Managementsystem und das Informationssicherheitsmanagementsystem wurden zu einem DIMS (Datenschutz-Informationssicherheits-Management-System) vereint.

- Incident-Response-Management ist vorhanden.

- Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklungen berücksichtigt (Art. 25 Abs. 2 DS-GVO).

- **Auftragskontrolle**

    - Unsere Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers. Die AGB enthalten detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers.

    - Die AGB enthalten detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers.

    - Die Hetzner Online GmbH hat einen betrieblichen Datenschutzbeauftragten sowie einen Informationssicherheitsbeauftragten bestellt. Beide sind durch die Datenschutzorganisation und das Informationssicherheitsmanagementsystem in die relevanten betrieblichen Prozesse eingebunden.

5 Allgemeine Hinweise

Im Hinblick auf den Stichprobencharakter der Untersuchung ist darauf hinzuweisen, dass außerhalb der im Zusammenhang mit dieser Untersuchung abgeprüften Aspekte weitere Stärken, aber auch potentielle Risiken vorhanden sein können.

Obwohl die Durchführung der Prüfung größtmöglicher Sorgfalt unterlag, schließt die TÜV Rheinland i-sec GmbH daher Haftung für vorhandene und nicht erkannte potentielle Risiken aus.

Das Prüfergebnis entbindet das Unternehmen in keiner Weise von der Weiterverfolgung seiner Sicherheitsziele.

Das Unternehmen ist in jedem Fall für seine Maßnahmen zur Sicherstellung seiner Sicherheitsziele selbst verantwortlich.

Jede Haftung für eventuelle Schäden, die aus einer falschen Anwendung der hier gegebenen Informationen resultieren, wird ausgeschlossen.