Kurzgutachten

zur Erteilung eines Datenschutz-Gütesiegels für „ennit Cloud“

Im Auftrag der ennit server GmbH

SKYCOMP IT-Solutions - Fachbereich DS-Easy

Stand: 21. Mai 2018

Inhaltsverzeichnis

1. Über die Prüfung von ennit Cloud

Dieses Gutachten fasst die Ergebnisse der datenschutzrechtlichen und IT-sicherheitstechnischen Prüfung des IT-Produktes „ennit Cloud“ für den Antrag auf die Erteilung eines Datenschutz-Gütesiegels durch das Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) zusammen.

Die Prüfungen erfolgten nach dem Prüfschema der Landesverordnung über ein Datenschutzgütesiegel (Datenschutzgütesiegelverordnung - DSGSVO) in der Version 2.0 vom 17.06.2015.

Die Vorlage eines rechtlichen und technischen Gutachtens eines beim ULD akkreditierten Gutachters ist Voraussetzung für die Zertifizierung eines Produktes.

Die Betreiberin ennit server GmbH (im folgenden auch Auftragnehmer genannt) ist nach DIN ISO 9001:2008 und nach DIN ISO 27001:2015 (jeweils Geltungsbereich Betrieb von Standortvernetzung, Rechenzentrums- und Cloudlösungen, Outsourcing und Userhelpdeck) zertifiziert und betreibt ihre Rechenzentren in Schleswig-Holstein.

2. Zeitraum der Prüfung

Die Begutachtung des Produkts „ennit Cloud“ erfolgte in dem Zeitraum vom 01.06.2017 bis 23.05.2018 und beinhaltete neben der Analyse der zur Verfügung gestellten Dokumentationen von der ennit server GmbH auch die Vor-Ort-Begutachtungen der Geschäftsräume und der Rechenzentren der ennit server GmbH.

Das Rechenzentrum 1 (Projensdorfer Straße 324, 24106 Kiel) wurde am 08.06.2017 geprüft. Die Prüfung des Rechenzentrums 2 (Kiel Kanal 2, 24106 Kiel) fand am 01.08.2017 statt.

3. Adresse der Antragstellerin

ennit server GmbH
Ansprechpartner: Herr Uwe Kastens
Projensdorfer Straße 324
24106 Kiel
Telefon: 0431-7097428

4. Adressen des Sachverständigen

Andreas Ebbersmeyer
Blessenberg 18
23701 Eutin
Telefon: 04521-8301410
E-Mail: andreas.ebbersmeyer@ds-easy.de

Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannter Sachverständiger für IT-Produkte (rechtlich / technisch)

5. Kurzbezeichnung des IT-Produkts

ennit Cloud

6. Detaillierte Bezeichnung des IT-Produktes

Die Betreiberin ennit server GmbH stellt in ihren Rechenzentren Infrastructure as a Service (IaaS) auf performanter Hard- und Software mit einer garantierten Verfügbarkeit von 99,5% im Jahresmittel zur Verfügung. Auf dieser Plattform können virtuelle Maschinen (VM) betrieben werden. Weiterhin erlaubt ennit Cloud das eigenständige Management der Systeme.

Pro VM können maximal 8 virtualisierte CPUs (vCPUs), eine garantierte RAM-Kapazität von 64 GB und eine oder mehrere virtuelle Festplatten zugewiesen werden. Der Speicherplatz wird dabei aus einer Share Storage Infrastructure in den Rechenzentren in Kiel zur Verfügung gestellt.

Pro Benutzeraccount können mehrere virtuelle Netzwerke für alle VMs des Accounts genutzt werden. Die Netzwerke werden auf VLAN-Basis isoliert. Pro Netzwerk wird ein virtueller Router oder eine Firewall eingesetzt, die folgende Dienste bereitstellen:

- DHCP: Zuweisen von IP-Adressen, DNS und Default-Gateway an die VMS
- DNS (Domain Name Service): Namensauflösung von internen und externen Adressen
- NAT (Network Address Translation): Internetzugriff der VMs

- Port-Forwarding: Einzelne Ports bzw. Portranges können aus dem Internet erreichbar gemacht werden
- Firewall: Kontrolle einzelner Ports bzw. Portranges, die aus dem Internet erreicht werden sollen
- Loadbalancer: Verteilen von Anfragen aus dem Internet auf eine Gruppe von VMs.

Pro virtuellem Netzwerk und Benutzeraccount wird automatisch oder manuell eine oder mehrere IPv4-Adresse/n aus dem Netzbereich der ennit server GmbH zugewiesen. Diese Zuweisung erfolgt statisch pro Netzwerk. Eine gemeinsame Nutzung von Netzwerken über verschiedene Benutzeraccounts ist nicht möglich. Weitere Netzwerke oder IPv4-Adressen können hinzu gebucht werden.

Die ennit server GmbH erlaubt den Auftraggebern (im Folgenden auch als Kunde bezeichnet) den Zugriff auf ein webbasiertes Management-Interface. Mit diesem Interface können die Auftraggeber im Rahmen der freigeschalteten Limits folgende Tätigkeiten ausführen:

- Installation von neuen VMs
- Löschen nicht mehr genutzter VMs
- Starten/Stoppen von VMs
- Einloggen auf die Konsole
- Einbinden von CDROM- und DVD-Images
- Hochladen von CDROM- und DVD-Images
- Hochladen von Templates
- Umwandeln von Snapshots in Templates
- Einrichten von Portweiterleitungen
- Pflege von Firewallregeln (nur bei Einsatz eines virtuellen Routers).

Ein Fernzugriff auf eine VM muss vom Auftraggeber vorab in der Firewall freigeschaltet werden.

Die Auftraggeber können ihre VMs per Snapshot sichern und auch wiederherstellen. Die Snapshots werden hierbei direkt von den virtuellen Festplatten ausschaltkonsistent erzeugt, da die Informationen im RAM bei einem Snapshot nicht erfasst werden hat der Snapshot bei einer nicht gestoppten VM den Zustand, als wenn sie ausgeschaltet worden

wäre. Hierbei werden nur die auf Platte gespeicherten Daten gesichert. Eine Sicherung von Daten im RAM findet nicht statt. Die Anzahl der verfügbaren Snapshots richtet sich hierbei nach dem gebuchten Paket. Ein agentenbasiertes Backup kann gegen Aufpreis gemäß Leistungsbeschreibung Managed Backup gebucht werden, dieses gehört jedoch nicht zum Zertifizierungsgegenstand.

Die ennit server GmbH führt an den virtuellen Maschinen kein Management durch. Die Systempflege obliegt den Auftraggebern. Weiterhin findet auch keine Überwachung der VMs des Auftraggebers statt. Diese Optionen können gegen Aufpreis gebucht werden. Dieses Management gehört jedoch nicht zum Zertifizierungsgegenstand.

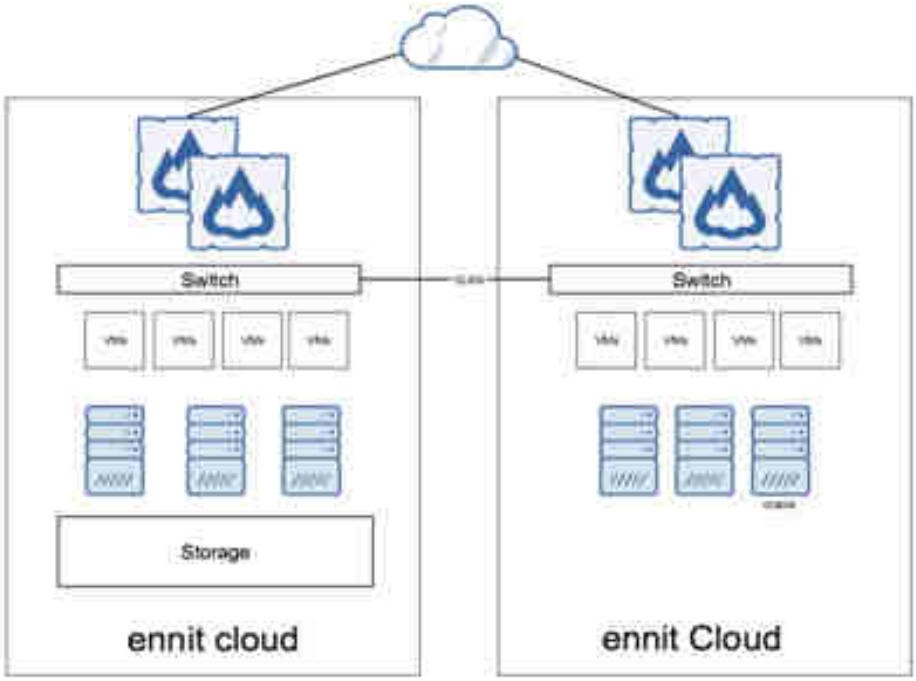
Die Protokollierung der Logdaten erfolgt über syslog auf einem zentralen Loghost. Dieser ist für den Auftraggeber nicht unmittelbar zugreifbar. Es besteht die Möglichkeit die logevents einzelner Komponenten weiterzuleiten. Dies ist jedoch als getrennte Dienstleistung zu betrachten und wird in diesem Gutachten nicht betrachtet.

7. Zweck und Einsatzbereich

Bereitstellen von virtuellen Systemen unter Windows oder Linux im B2B-Bereich.

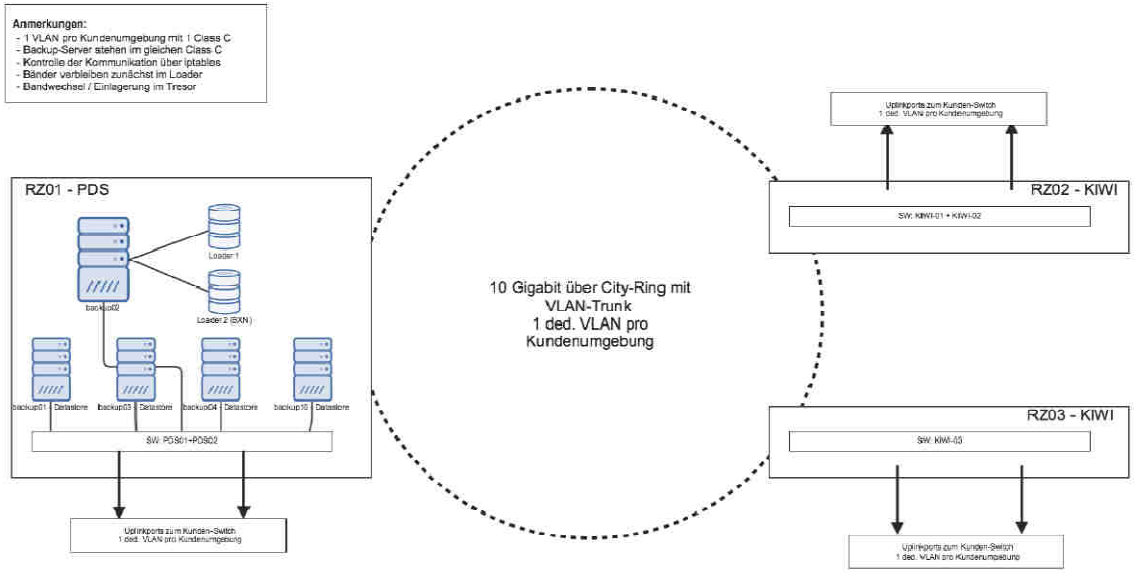
Hierfür wird mit dem Kunden neben dem Leistungsvertrag auch ein Auftragsdatenverarbeitungsvertrag gemäß § 11 BDSG geschlossen.

8. Modellierung des Datenflusses



physische Sicht

Übersichtsskizze - Managed Backup



9. Version des Anforderungskataloges

Es wurde nach dem Prüfschema des Gutachtens für die Produktzertifizierung in der Version 2.0 vom 17.06.2015 vorgegangen.

10. Angewandte Evaluationsmethoden

Inhaltsanalyse und Sichtung vorhandener Dokumentationen

Offene Befragungen von Mitarbeitern der ennit server GmbH

Sichtung vorhandener Unterlagen der DIN ISO 9001:2008 (Geltungsbereich: Betrieb von Standortvernetzung, Rechenzentrums- und Cloudlösungen, Outsourcing und Userhelpdeck)

Sichtung vorhandener Unterlagen der DIN ISO 27001:2015 (Geltungsbereich: Betrieb von Standortvernetzung, Rechenzentrums- und Cloudlösungen, Outsourcing und Userhelpdeck)

Vor-Ort-Besichtigungen der Geschäftsräume und der beiden Rechenzentren in Kiel

11. Prüfungsergebnisse

Der Kunde erhält neben den im ADV-Vertrag enthaltenen Übersichten über die getroffenen technischen und organisatorischen Maßnahmen eine umfassende Produktdokumentation mit den bereitgestellten Spezifikationen und Leistungsbeschreibungen. Auch erhalten die Kunden ein Datenschutz-Hinweisblatt, in dem sie auf weitere datenschutzrelevante Informationen wie die Grundlagen für Datenspeicherungen nebst ihrer regelmäßigen Löschfristen hingewiesen werden. Die Anforderung an die Transparenz wird damit vorbildlich erfüllt.

Das Produkt „ennit Cloud“ erfüllt die Anforderungen an den Grundsatz der Datenvermeidung und Datensparsamkeit, da nur die notwendigsten Daten zur Auftragserfüllung gespeichert werden. So protokolliert die Firewall lediglich aufgetretene Unregelmäßigkeiten im Rahmen der Angriffsbekämpfung. Hierbei protokolliert die ennit server GmbH nur DENY-Regeln und weitere Systeminformationen ohne

personenbezogene Daten. Diese werden 7 Tage aufbewahrt und im Rahmen des Logcyclings überschrieben. Folgende Sekundärdaten werden protokolliert:

Sowohl das Rechenzentrum 1, als auch das Rechenzentrum 2 liegen in Schleswig-Holstein und sind sowohl nach DIN ISO 9001:2008, als auch nach DIN ISO 27001:2015 für den Geltungsbereich Betrieb von Standortvernetzung, Rechenzentrums- und Cloudlösungen, Outsourcing und Userhelpdeck zertifiziert. Alle Mitarbeiter der ennit server GmbH werden regelmäßig in den Bereichen Datenschutz und Datensicherheit geschult.

Die für das Produkt „ennit Cloud“ genutzte Hardware befindet sich primär im Rechenzentrum 2. Im Rechenzentrum 1 wird für das beschriebene Produkt die Datensicherung als auch das Monitoring betrieben. Die Komponenten sind in beiden Rechenzenten jeweils in 19 Zoll Racks mit über Dieselgeneratoren gestützten, unterbrechungsfreien Stromversorgungen verbaut. Im Rechenzentrum 2 sind die Racks in zwei Brandabschnitten untergebracht, Die Serverräume im Rechenzentrum 1 und im Rechenzentrum 2 sind mit Klimageneratoren ausgestattet und haben eine Raumtemperatur von 20 bis 24 Grad Celsius bei einer Luftfeuchtigkeit von ca. 40%. Die vorhandenen Brandschutzeinrichtungen sind für den Brandschutz von Datenverarbeitungsanlagen geeignet. Die Branderkennung erfolgt über Raucherkennungsfrühwarnsysteme.

Beide Rechenzentren sind mit elektronischen Einbruchschutz- und Videoüberwachungssystemen ausgestattet. Die Kameras in den Rechenzentren sowie die Server, die die Daten speichern, werden in einem eigenen Netzwerk betrieben, deren Zugriff durch eine Firewall geschützt ist. Die Videoaufzeichnungen müssen gemäß PCI/DSS-Vorgaben für Rechenzentren 100 Tagen vorgehalten werden und werden direkt im Anschluss automatisch gelöscht.

Zur Sicherstellung der Funktionsfähigkeit der Server werden diese mittels Monitoring durch die ennit server GmbH überwacht. Dies erfolgt über IP-basierende Netzverbindungen.

Das Backup wird auf Basis von SEP Sesam mit Datenspeicherung mit einer garantierten Haltezeit von 21 Tagen als Backup2Disk2Tape im Rechenzentrum 1 realisiert. Auf Kundenwunsch kann das Backup verschlüsselt werden. Die Sicherungen werden einmal

pro Woche als Fullbackup und an den anderen Tagen als inkrementielle Sicherung durchgeführt.

Die getroffenen technischen und organisatorischen Maßnahmen sind vorbildlich.

12. Beschreibung, wie das Produkt den Datenschutz fördert

Die beiden für das Produkt „ennit Cloud“ eingesetzten Rechenzentren haben eine Verfügbarkeit von 99,5% im Jahresmittel und sind nach DIN ISO 9001:2008 für den Geltungsbereich „Betrieb von Standortvernetzung, Rechenzentrums- und Cloudlösungen, Outsourcing und Userhelpdeck“ unter der Zertifikatsnummer 0192/16 bei der isocert zertifiziert. Das Zertifikat ist gültig bis 15. September 2018. Weiterhin sind die beiden Rechenzentren der ennit server GmbH auch nach DIN ISO 9001:2008 für den Geltungsbereich „Betrieb von Standortvernetzung, Rechenzentrums- und Cloudlösungen, Outsourcing und Userhelpdeck“ unter der Zertifikatsnummer 0329/15 bei der isocert zertifiziert. Das Zertifikat ist gültig bis 31. Dezember 2018. Beide Rechenzentren befinden sich in Schleswig-Holstein.

Die Transparenz des Produktes ist durch eine umfangreiche Dokumentation gewährleistet. Datenflüsse, eingesetzte Hard- und Software, Arbeitsabläufe und Monitoring-Incidents werden hier ausführlich beschrieben. Ebenso sind die Handlungsabläufe hierin definiert. Das Fachpersonal des Anbieters ist rund um die Uhr an 365 Tagen im Jahr erreichbar.

Eine Vermeidung von personenbezogenen Daten wird in jedem Arbeitsbereich angestrebt. So speichert beispielsweise die Firewall lediglich Daten beim Auftreten von Unregelmäßigkeiten zum Zwecke der Gefahrenabwehr.

13. Bestätigung

Hiermit bestätige ich, dass das oben genannte IT-Produkt den Rechtsvorschriften über den Datenschutz und die Datensicherheit entspricht.

Eutin, 23. Mai 2018

Andreas Ebbersmeyer

Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannter Sachverständiger für IT-Produkte (rechtlich / technisch)