Datenschutz-Vorabkontrolle

für die Lösung

„Safety Web“

bei

DEKRA Media GmbH
Dahlener Str. 570
41239 Mönchengladbach

Stand: 09.09.2015
Verfasser: Dr. Ralf Schadowski

ADDAG GmbH&Co.KG
Krefelder Strasse 121
52070 Aachen
Telefon 0241-44688-20
EMail Datenschutz@Schadowski.com

Inhalt

Der Verfasser

Der Verfasser des Dokumentes ist der ordentlich bestellte externe Datenschutzbeauftragte der Dekra Media GmbH.

Sachkunde/Aktivitäten:

- TÜV cert sachkundiger Datenschutzbeauftragter
- nach europäischer Norm DIN EN ISO/IEC17024 zertifizierter und überwachter Datenschutzbeauftragter
- Sachverständiger und Fachgruppenleiter für Datenschutz und IT Sicherheit im Bundesverband BISG e.V
- Aktives Mitglied in der Gesellschaft für Datenschutz und Datensicherheit GDD e.V.

Information zu Dekra Media

Seit mehr als zwei Jahrzehnten entwickelt DEKRA Media für seine Kunden mediengestützte Lösungen. Die Entwicklung von Web Based Trainings, angebunden an ein umfassendes Unterweisungsportal für den Arbeitsschutz, ist ein Bereich der vielfältigen Entwicklungsprojekte von DEKRA Media.

Information zu DEKRA Safety Web

DEKRA Safety Web ist ein Arbeitsschutzportal auf dem die verpflichtenden jährlichen Unterweisungen im Arbeitsschutz online absolviert werden können. Ein umfangreiches Dokumentationssystem ermöglicht Unternehmen, Vorgesetzten und Arbeitsschutzfachkräften einen lückenlosen Nachweis über absolvierte Unterweisungen zu erbringen.

Aufgabe der Bewertung:

Es ist zu bewerten, ob die Lösung DEKRA Safety Web den aktuellen Anforderungen im Sinne des BDSG entspricht und ob eine Nutzung aus Sicht Datenschutz zulässig ist.

Bewertung:

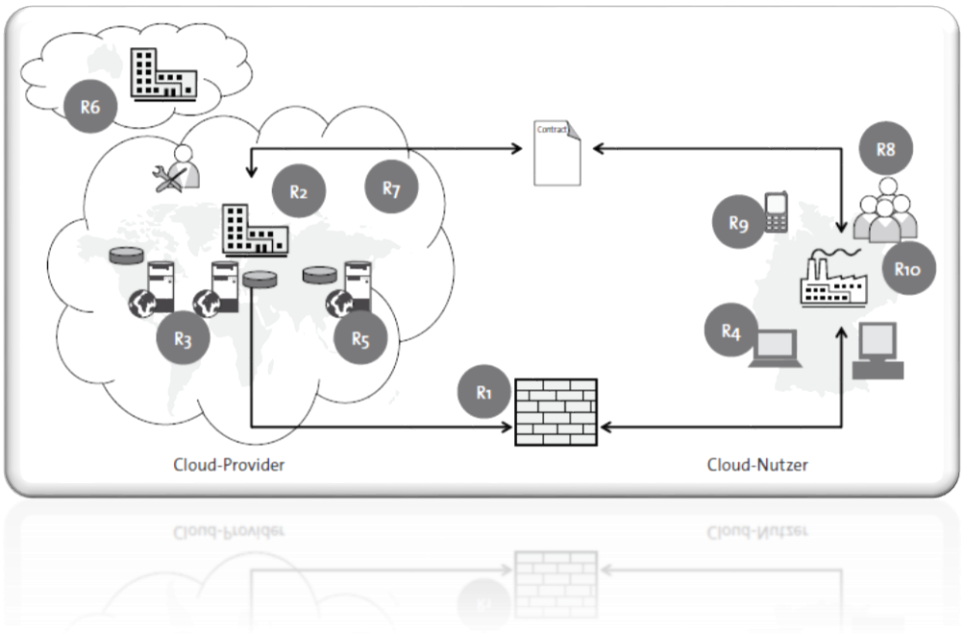
Die Verarbeitung personenbezogener Daten auf DEKRA Saftey Web ist zulässig.

Risikobewertung gemäß BITKOM

Über Bitkom

Bitkom ist der Digitalverband Deutschlands. 1999 als Zusammenschluss einzelner Branchenverbände in Berlin gegründet, vertreten wir mehr als 2.300 Unternehmen der digitalen Wirtschaft, unter ihnen 1.000 Mittelständler, 300 Start-ups und nahezu alle Global Player. (Quelle: www.bitkom.de)

Die Bitkom hat in einem Orientierungsleitfaden zum Thema Cloud diese Risikopunkte erarbeitet und empfiehlt jedem Cloud Entscheider vor dem Beginn der Nutzung einer Cloud Nutzung diese Punkte professionell bewerten zu lassen. (Quelle: BITKOM_Leitfaden_Cloud_Computing-Was_Entscheider_wissen_muessen)



R1 Internetanbindung
R2 Serviceende
R3 Updateservice bei Multi-Mandanten
R4 Angriffe auf den Browser
R5 Logging / Vertraulichkeit
R6 Sub-Serviceprovider
R7 Verkauf Cloud Partner Ausland
R8 exportkontrollrechtliche Vorschriften
R9 Mobiles / WLAN / Dritte
R10 Migration der Buchhaltung

Risikobewertung

R		Risikosituationen	Bewertung
R1	Internet-anbindung	Die Verfügbarkeit der **Internetanbindung**, sowohl der eigenen, als auch der des Provider, sind ein Risiko für die Verfügbarkeit der Anwendung und somit der Geschäftsprozesse. Der Internetzugang ist daher mehr als nur ein Instrument zu Informationsgewinnung der Mitarbeiter.	**(1)PlusServer hat eine hervorragende Internetanbindung und Verfügbarkeit. DEKRA Media verfügt über eine Backup Internetleitung eines zweiten Providers, um ggf steuernd einzugreifen. Die Internetanbindung des Nutzers sollte dem Stand der Technik entsprechen.**
R2	Serviceende	**Stellt der Anbieter seinen Service ein, z. B. durch Insolvenz oder im Rahmen einer Fusion**, besteht das Risiko, dass der Service dem Nutzer nicht mehr zur Verfügung steht. Dann muss ein kurzfristiger Ersatz gefunden und die Daten müssen schnell auf die neue Plattform migriert werden.	**(1) PlusServer Fusioniert mit HostEurope und ist somit der größte Hoster Europas. Somit ist das Risiko eher als gering einzustufen.**
R3	Updateservice bei Multi-Mandanten	Das Update eines Service auf einen nächsten Release-Stand kann in einer Multi-Mandanten-Umgebung zu unerwünschten Seiteneffekten in der eigenen Anwendung führen. Der Nutzer sollte hierbei eigentlich in die Test- und Freigabeprozesse aktiv eingebunden sein. Der Anbieter muss allerdings, um kosteneffizient zu arbeiten, möglichst einheitliche Services anbieten, so dass es normalerweise kein Mitspracherecht der Kunden hinsichtlich des Upgrade-Zeitpunkts gibt.	**(0) Es werden keine Release Updates ohne unser Einverständnis durchgeführt.**
R4	Angriffe auf den Browser	**Angriffe auf und über den Web Browser** des Mitarbeiters, der den Service nutzt (z. B. Cross-Site-Scripting), stellen ein zusätzliches Risiko für die Integrität und Vertraulichkeit der Daten dar.	**(2) Die meisten Nutzer bei Dekra Media haben keine Eingabemöglichkeit. Eine entsprechende Nutzungsrichtlinie bei den Anwendern auf Kundenseite sollte vorhanden sein.**
R5	Logging / Vertraulichkeit	Werden seitens des Anbieters, z.B. für eine Fehlersuche, Protokolldaten herausgegeben, besteht das Risiko, dass in dem Protokoll auch Informationen von anderen Kunden (z. B. personenbezogene Daten) enthalten sind. Je nach Protokollierungseinstellung (Debug-Log) können hier kritische Daten irrtümlicherweise herausgegeben werden.	**(1) Protokolldaten liegen der DEKRA Media IT-Abteilung vor.**

R6	Sub-Serviceprovider	Während des laufenden Vertrages kauft sich der Service-Provider IT-Kapazitäten (z. B. einen Datenbank-Service) von anderen Cloud-Anbietern ein, mit dem Ziel, die eigenen Kapazitäten zu erweitern. Hier besteht das Risiko, dass Daten zum Teil oder vollständig, zeitweise oder auf Dauer ins Ausland verlagert werden. Im konkreten Beispiel handelt es sich um einen beim zuständigen Finanzamt genehmigungspflichtigen Vorgang. Etwaige Verstöße können finanziell geahndet werden. Das Risiko für den Nutzer bleibt selbst dann bestehen, wenn er von seinem Dienstleister über den Vorgang informiert wird, selbst aber keine Eingriffsmöglichkeit hat, um den Transfer nachweislich zu unterbinden.	**(0) nicht vorhanden, entfällt.**
R7	Verkauf Cloud Partner Ausland	Wird der Anbieter des Service von einer anderen (z. B. ausländischen) Unternehmung aufgekauft, kann es je nach Geschäftsgebaren dazu führen, dass die Daten in ein ausländisches Rechenzentrum verlagert werden. Dies ist auch der Fall, sofern der Cloud-Anbieter keine Garantie geben kann, dass sich die Daten exklusiv im Zugriff der deutschen Steuerbehörden Staatsgebiet der Bundesrepublik) befinden.	**(0) nicht vorhanden, entfällt.**
R8	exportkontroll-rechtliche Vorschriften	Dem Cloud Computing immanent ist der unbekannte bzw. nicht hinreichend zu identifizierende Standort der am Datentransfer beteiligten Server. Daher bestehen Unwägbarkeiten hinsichtlich der einzelnen involvierten Länder. Zur Vermeidung unberechtigter Zugriffe, die einen Verstoß gegen exportkontrollrechtliche Vorschriften bedeuten können, ist eine Identifizierung und Aussonderung von Daten (bzw. der diese speichernden Server), deren Transfer wegen exportkontrollrechtlicher Relevanz nicht zulässig ist, erforderlich.	**(0) nicht vorhanden, entfällt.**
R9	Mobiles / WLAN / Dritte	Dadurch, dass der Service über das Internet erreichbar ist, besteht das Risiko, dass Mitarbeiter von nicht vertrauenswürdigen Endgeräten (z. B. Internet Café, Mobile Device) auf den Service zugreifen. Alle Informationen, die über solche Endgeräte laufen, können potentiell von Dritten mitgelesen werden. Im Fall von mobilen Endgeräten können diese Daten verloren gehen oder gestohlen werden.	**(1) Mitarbeiter mit Zugang zu Administrativen Bereichen sind hinreichend geschult. Das wird auch den Kunden empfohlen.**

R10	Migration der Buchhaltung	Bei der Migration der Buchhaltung auf ein neues System sind eine Schlussbilanz und eine Eröffnungsbilanz zu erstellen, die auch der Prüfung durch den Abschlussprüfer und ggf. der Finanzverwaltung unterliegt. Kann die Vollständigkeit und Korrektheit der übertragenen Daten nicht oder nur manuell verifiziert werden, entsteht ein Risiko hinsichtlich Vollständigkeit und Richtigkeit sowohl für den Jahresabschluss des Nutzers, als auch hinsichtlich der Besteuerungsgrundlagen.	**(0) nicht vorhanden, entfällt.**

Legende in der Spalte Bewertung:

1 = unbedeutendes Risiko
2 = mittleres Risiko
3 = bedeutendes Risiko
0 = Trifft nicht zu

Software auf den Servern

- Linux Ubuntu /14.04.3 LTS
- Apache/2.4.7 (Ubuntu)
- Postfix /2.11.0
- PHP /5.5.9-1ubuntu4.11
- Mysql /5.5.44-MariaDB
- ProFTP /1.3.5rc3

Die in der Distribution Ubuntu 14.04 enthaltenen Version von MariaDB ist ausdrücklich nicht die aktuellste, sondern entspricht dem stabilen Stand der Distribution. Sicherheitslücken werden durch die Patches behoben, die derzeit monatlich vom DEKRA Media Support eingespielt werden.

Diese Vorgehensweise ist im Enterprise-Bereich Standard um eine stabile Plattform für die Anwendungen bereitzustellen. Wenn zum Beispiel der Apache manuell aktualisiert würde, wird das Paket damit aus der Distribution heraus genommen und erhält keine Sicherheitspatches mehr. Die Softwarestände obliegen der Pflege durch die DEKRA Media GmbH.

PlusServer

„Darüber hinaus erstreckt sich unser Rechenzentrumsnetz über das gesamte Bundesgebiet und wird durch Standorte in der EU sowie den USA ergänzt. So haben etwa international operierende Unternehmen die Möglichkeit, einen Teil ihrer Server im Herzen der Vereinigten Staaten unterzubringen. Dabei gilt auch an diesem PlusServer-Standort das deutsche Datenschutzgesetz, da hier das Sitzlandprinzip Anwendung findet und der Auftragsverarbeiter, also PlusServer, seinen Sitz in Deutschland hat. Selbstverständlich erhalten Sie unabhängig vom gewählten Standort eine gleichbleibende und qualitativ hochwertige Leistung. Wir hosten ausschließlich in Tier-3-Rechenzentren, um Ihnen eine hohe Verfügbarkeit aller Services zu gewährleisten. Alle Informations-Sicherheits-Management-Systeme und Business-Continuity-Systeme in unseren Rechenzentren sind nach ISO27001 und BS25999 zertifiziert. Zudem bieten wir SLAs von bis zu 99,99 Prozent.“

Quelle: https://www.plusserver.com/standorte

Anschrift:

PlusServer AG
Daimlerstraße 9-11
50354 Hürth

Die PlusServer AG ist der Hoster für DEKRA Safety Web.

Der Serverstandort für DEKRA Safety Web ist ausschließlich in Straßburg / innerhalb der EU. Eine Geo-Redundanz ist nicht gebucht und ausgeschlossen.

Die Auftragsdatenverarbeitung nach §11 BDSG ist gezeichnet und liegt vor.

Es liegen gültige Zertifizierungen auf IT-Sicherheit vor.

Die technisch organisatorischen Maßnahmen liegen schriftlich vor und sind von DEKRA Media akzeptiert / entsprechen den Anforderungen.

Zertifikat Hochverfügbarkeit

Das Rechenzentrum ist auf Hochverfügbarkeit geprüft durch den TÜV Saarland:

Zertifikat

TÜV SAARLAND
Geprüftes Rechenzentrum

Geprüftes Rechenzentrum hochverfügbar Stufe 3

Die Zertifizierende Stelle der tekit Consult Bonn GmbH, TÜV Saarland Gruppe, bestätigt hiermit, dass die Firma

PlusServer AG

Daimlerstraße 9-11, D- 50354 Hürth

berechtigt ist, das Prüfzeichen „Geprüftes Rechenzentrum" für ihr

Datadock, 1er étage, 1 Rue du Havre, F-67100 Strasbourg

als Ergebnis einer erfolgreichen Sicherheitsüberprüfung in Anlehnung an BSI-Grundschutz und ISO 27001 zu führen. Der Nachweis wurde durch eine Auditierung vor Ort erbracht und beinhaltete folgende Punkte:

- Hochverfügbares Rechenzentrum
- Hochverfügbarer, nachhaltiger Betrieb
- Dokumentation und Betriebsführung
- Bauliche und technische Anforderungen
- Organisatorische Anforderungen

Grundlagen dieser Zertifizierung sind

- der Anforderungskatalog "hochverfügbares Rechenzentrum Stufe 3 V2.0"
- der Prüfbericht TR01693

Das Zertifikat gilt ausschließlich für das auditierte Rechenzentrum zum Zeitpunkt der Prüfung und berechtigt den Inhaber unübertragbar, das abgebildete Prüfzeichen werblich im Gültigkeitszeitraum zu nutzen, sofern keine wesentlichen Änderungen des Rechenzentrums innerhalb der Laufzeit des Zertifikats vorgenommen werden.

Dieses Zertifikat ist bis zum 31. Oktober 2016 gültig.

Zertifikat-Nr. Z2014/1284

Bonn, den 30. Oktober 2014

GEPRÜFT tekit Member of TÜV Saarland Group TÜV SAARLAND APPROVED

tekit

TÜV SAARLAND GRUPPE

Zertifikat ISO 27001

Das Rechenzentrum ist auf ISO 27001 geprüft durch den TÜV Saarland:

Zertifikat

TÜV SAARLAND

Geprüftes Rechenzentrumsmanagement nach ISO 27001

Die Zertifizierende Stelle der tekit Consult Bonn GmbH, TÜV Saarland Gruppe, bestätigt hiermit, dass die Firma

PlusServer AG

Daimlerstraße 9-11, D- 50354 Hürth

für ihr

Datadock, 1er étage, 1 Rue du Havre, F-67100 Strasbourg

eine erfolgreiche Überprüfung ihres Rechenzentrumsmanagements in Anlehnung an BSI-Grundschutz und ISO 27001 bestanden hat. Der Nachweis wurde durch eine Auditierung vor Ort und Prüfung der Betriebsunterlagen erbracht und beinhaltete folgende Punkte:

- Hochverfügbarer, nachhaltiger Betrieb des Rechenzentrums
- Dokumentation und Betriebsführung
- Organisatorische Anforderungen

Grundlagen dieser Zertifizierung sind:

- Anforderungskatalog "hochverfügbares Rechenzentrum Stufe 3 V2.0"
- Prüfbericht TR01693
- Teile der ISO 27001 und 27002

Das Zertifikat gilt ausschließlich für das auditierte Rechenzentrum zum Zeitpunkt der Prüfung.

GEPRÜFT tekit Member of TÜV Saarland Group TÜV SAARLAND APPROVED

Dieses Zertifikat ist bis zum 30. November 2016 gültig.

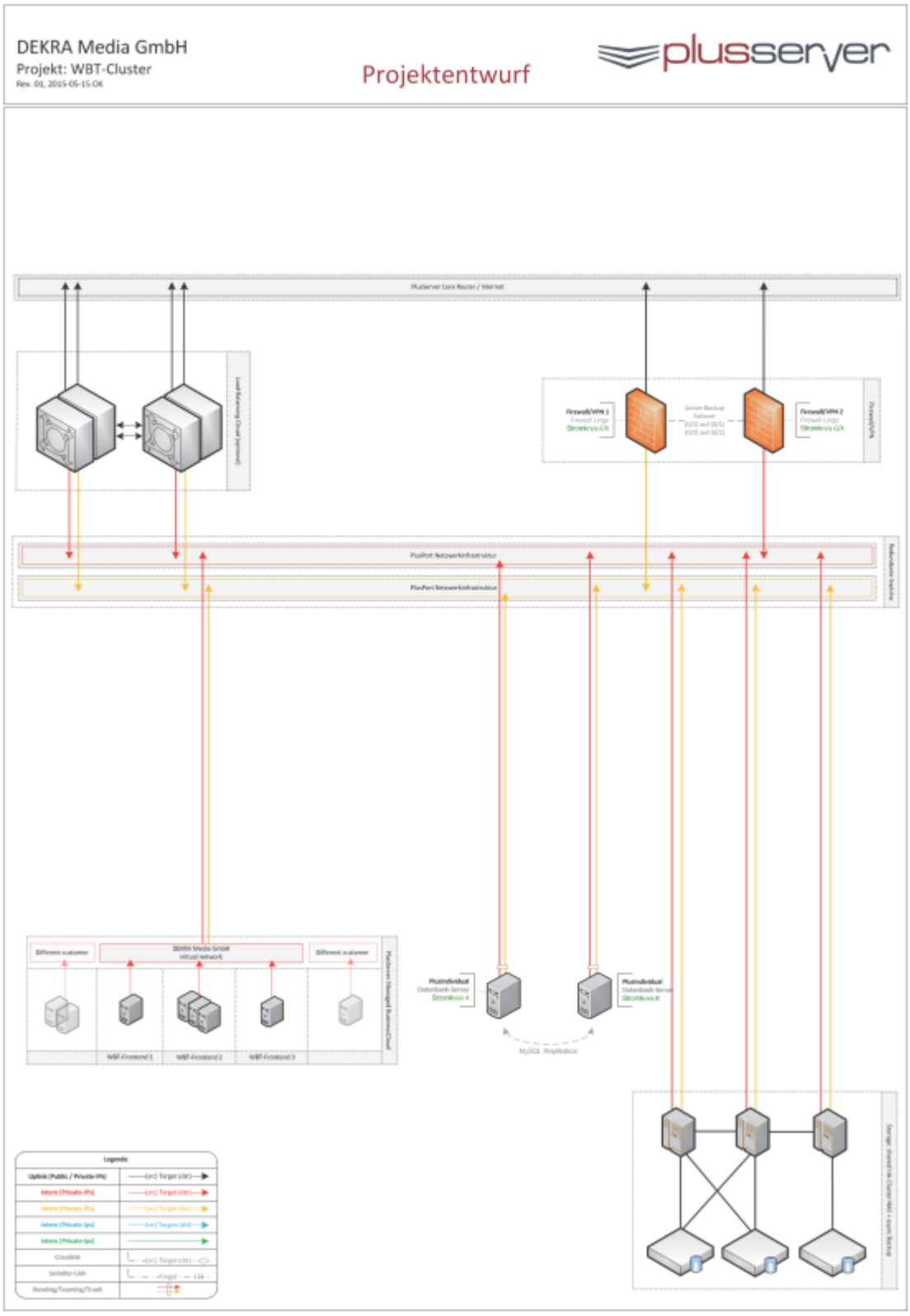
Zertifikat-Nr. Z2014/1285

Bonn, den 30. Oktober 2014

tekit

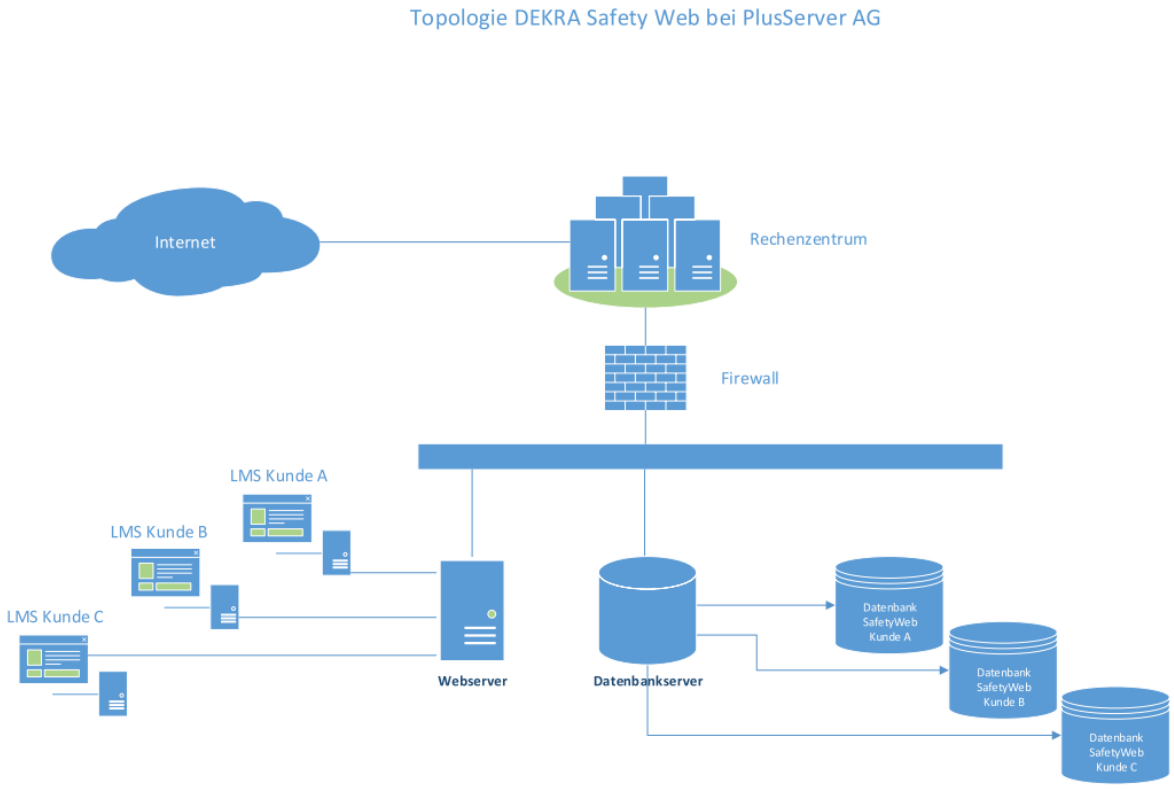
TÜV SAARLAND GRUPPE

Servertopologie bei PlusServer



Die kritischen Maschinen sind redundant ausgelegt und durch Sicherheitsmechanismen gegen Angriffe geschützt.

Datentrennung



Webdienste und Datenbankdienste sind voneinander aus Sicherheitsgründen getrennt.

Die Kundendaten sind untereinander logisch getrennt und können nicht vermischt werden.

Beschreibung des Nutzungsablaufes

Administration der Nutzer

Die Verwaltung der Benutzeraccounts wird wahlweise von DEKRA Media oder vom Kunden selbst über das Frontend der Webanwendung durchgeführt.

Die Benutzerverwaltung ist nur für Benutzer des eigenen Mandanten und ggfs. dessen Submandanten möglich.

Einsicht in bzw. Verwaltung von Benutzeraccounts von anderen Mandanten ist nicht möglich. Im Falle von Kundensystemen ohne eigene Datenbank wird dies durch Prüfung der Zugriffsrechte des eingeloggten Benutzers sichergestellt, bei getrennten Datenbanken ist ein Zugriff auf Datenbanken anderer Kunden generell ausgeschlossen.

Erfassung der Teilnahmen in der Datenbank

Bei Teilnahme an einem WBT wird der Lernfortschritt per http-Request SSL-verschlüsselt an das LMS übermittelt und in die Datenbank geschrieben.

Es ist sichergestellt, dass der aktuell eingeloggte Teilnehmer ausschließlich seinen eigenen Lernfortschritt beeinflussen und einsehen kann.

Der Zugriff auf das Reporting der Lernfortschritte aller Teilnehmer eines Mandanten (und ggfs. dessen Submandanten) ist durch Prüfung der entsprechenden Zugriffsrechte im Falle von nicht getrennten Datenbanken bzw. bei getrennten Datenbanken systemimmanent sichergestellt.

Versand von Teilnahmebestätigungen an die Kunden / Personalabteilungen?!

Teilnahmebestätigungen können vom Teilnehmer selbst für seine eigenen Teilnahmen und von Benutzer mit entsprechenden Zugriffsrechten (Administration/Reporting) für alle Teilnehmer des Mandanten und ggfs. Submandanten aus der Anwendung über eine gesicherte HTTPS-Verbindung heruntergeladen werden.

Der Zugriff auf Teilnahmebestätigungen von anderen Benutzern wird wie im vorherigen Punkt beschrieben unterbunden.

Anmeldung der Nutzer

Die Anmeldung der Benutzer und die Übertragung der Zugangsdaten erfolgt über eine gesicherte HTTPS-Verbindung. Zusätzlich wird das Passwort vor der Übertragung clientseitig RSA-verschlüsselt.

Zugriff aus dem Browser beim Kunden über 443

Der Zugriff per HTTPS (Port 443) wird für die Benutzung der Anwendung vorausgesetzt. Bei Zugriffen über http (Port 80) ohne SSL-Verschlüsselung wird automatisch ein Redirect auf HTTPS eingeleitet.

Ende des Gutachtens / der Datenschutz-Vorabkontrolle..

RS090915

Dr. Ralf W. Schadowski
TÜV cert sachkundiger Datenschutzbeauftragter
nach europäischer Norm DIN EN ISO/IEC17024 zertifizierter Datenschutzbeauftragter
anerkannter Auditor IT-Sicherheit
ordentliches Mitglied im GDD e.V.
