Whitepaper

Anforderungen an einen virtuellen Datenraum

Grundlegende Anforderungen an einen virtuellen Datenraum

1. Die **Zugangsberechtigungen** sind **klar abgegrenzt** und vorgegeben
2. Der Datenraum-Besitzer braucht die Gewissheit, dass auch wirklich **nur befugte Personen** auf die Dokumente zugreifen können. (Sicherheitscheck!)
3. Außerdem sollte der volle **Überblick über Zugriffe** und Aufenthaltszeiten gewährleistet sein
4. Ein **Journal** dokumentiert, wer wann welches Dokument herunterlädt, löscht, kopiert oder nur ansieht
5. Die Datenraum-Mitglieder sollten darüber **informiert** werden, wenn neue Dokumente hochgeladen werden
6. Nutzer sollten jederzeit und durchaus auch **von mobilen Geräten** aus, den vollen **Zugriff** auf alle Ihre Daten haben
7. Eine **Kündigung** des Dienstes muss klar geregelt sein (**Datenverbleib**)
8. Einfache, **intuitive Nutzung** (ohne Schulungsaufwand) und flexibel erweiterbar

Compliance-Anforderungen an einen virtuellen Datenraum

Ein Datenraum muss

1. **von** unberechtigten **Zugriffen** vollständig **abgeschirmt** sein – von IT-Mitarbeitern (Admins und Operatoren) genauso wie von Hackern
2. individuelle und **konfigurierbare Nutzungsbedingungen** pro Datenraum zulassen
3. Zeitlich **definierbare Zugriffszeiten** pro Datenraum
4. alle Aktivitäten innerhalb der Arbeitsumgebung verzeichnen (**revisionsicheres Protokoll**)
5. zusätzlich Dokumente mit **Wasserzeichen im View Only Modus** vor unberechtigter Weitergabe oder Vervielfältigung schützen (dynamisch generiert)
6. **massenhafte Downloads verhindern**
7. Dokumente nur zum Lesen freigeben (**Secure Document View**)
8. von einer unabhängigen Stelle zertifiziert sein (z.B. nach dem Trusted Cloud Datenschutzprofil) und das Zertifikat sollte Auskunft geben, welche Daten im Datenraum abgelegt werden dürfen.

Produktivitäts-Anforderungen an einen virtuellen Datenraum

1. **Nach** (Online-) **Buchung & Einrichtung** ist der Datenraum **sofort einsetzbar**.
2. Die **Rechteverwaltung** innerhalb des Datenraums sollte **unabhängig** von der IT **anpassbar** sein.
3. **Nutzer** sollten **ohne Vorlaufzeit** jederzeit vom Projektleiter zum Datenraum **hinzugefügt oder entfernt** werden können.
4. Alle Projektbeteiligten sollten **über** einen normalen **Browser** auf den Datenraum **zugreifen** können.
5. Der Datenraum passt sich der Länge Ihres Projekts an. **Flexible Laufzeitmodelle**
6. Der Dienst ist mit einem **Zertifikat** ausgestattet, welches dem Nutzer seine Kontrollpflicht vor Ort (insb. Rechenzentrumsbesuch) abnimmt (z.B. Trusted Cloud Datenschutzprofil).

Weiterführende Links

Weiterführende Informationen

Datenschutzzertifizierung von Cloud-Diensten – White Paper

Ein Zertifikat nach TCDP erleichtert es Unternehmen, die Kontrollpflichten im Rahmen der Auftragsdatenverarbeitung zu erfüllen. Das Trusted Cloud Datenschutz Profil formuliert objektive Kriterien, mit deren Hilfe man Cloud-Dienste miteinander vergleichen kann.

Tagungsband Sealed Cloud Symposium

Der Tagungsband zum Sealed Cloud Symposium vom 24.09.2014 zum Thema: "Sealed Processing – Schutz der Inhalte und Metadaten" enthält Beiträge von Fraunhofer AISEC, provet / Universität Kassel, SecureNet, Regio-IT, Vodafone, Microsoft Azure, Fujitsu, Deloitte und der Uniscon GmbH.

Sealed Cloud - White Paper

Was ist eine Sealed Cloud und wie funktioniert sie?

Sealed Cloud für Berufsgeheimnisse

Mit Cloud Versiegelung dürfen auch Berufsgeheimnisse in die Cloud. Begründung der §203 StGB-Compliance des Sealed-Cloud-Dienstes iDGARD.

iDGARD White Paper für Unternehmen

Das White Paper diskutiert, warum Privatsphäre im Internet geschäftsrelevant ist und wie Unternehmen ihre Privatsphäre im Web schützen können und dabei noch Geld sparen.

Schutzbedarfsrechner

Mit Hilfe des Schutzbedarfsrechners haben Unternehmen die Möglichkeit, den passenden Schutzbedarf der zu verarbeitenden Daten zu bestimmen und somit den entsprechenden Dienst zu wählen.

Über die Uniscon GmbH

Die Uniscon GmbH wurde 2009 mit dem Ziel gegründet, technische Lösungen zu entwickeln, die es Usern erlaubt, sich im Internet sicher und frei zu bewegen. Mit unseren Produkten legen wir einen technischen Grundstein: Die Erfindung der Sealed Cloud – der Basistechnologie von iDGARD – gestattet Nutzern einen vertrauensvollen Umgang mit dem Internet. Mit unseren Produkten lösen wir das Problem des Datenschutzes – die bis heute größte verbliebene Herausforderung im Bereich der Online-Sicherheit.

Kontakt:

Uniscon GmbH

E-Mail: contact@uniscon.de

Internet: www.uniscon.de

Telefon: +49 (89) 4161 5988 100

Herausgeber:

Uniscon GmbH

Geschäftsführung: Martin Kinne, Dr. Hubert Jäger

Aufsichtsrat (Vorsitz) Lothar Pauly

Agnes-Pockels-Bogen 1 · 80992 München · Telefon 089 / 4161 5988 100 ·

Amtsgericht München HRB 181797