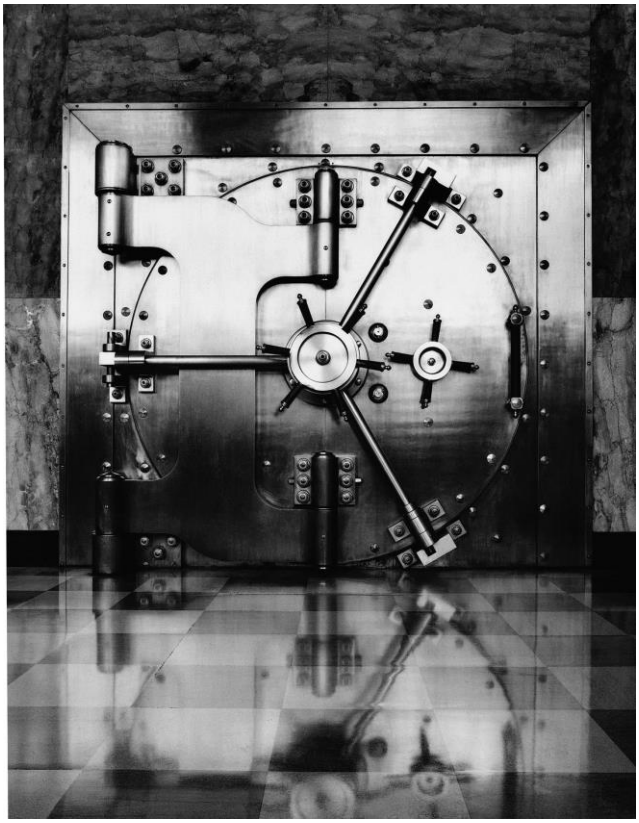
subreport

DEUTSCHLANDS TOR ZUR AUFTRAGSWELT

Angaben zu Datensicherheit und Datenschutz des **El**ektronischen **V**ergabe**i**nformations-**S**ystems subreport ELViS



Stand: Februar 2019

Inhalt

1 Einführung

2 Technische und organisatorische Maßnahmen

2.1 Verschlüsselung
2.2 Fähigkeit der Vertraulichkeit
2.3 Fähigkeit der Integrität
2.4 Fähigkeit der Verfügbarkeit und Belastbarkeit
2.5 Wiederherstellbarkeit der Verfügbarkeit und des Zugangs
2.6 Verfahren zur regelmäßigen Überprüfung
2.7 Verarbeitung personenbezogener Daten nur nach Anweisung

3 Systemverfügbarkeit

4 Mechanismen zum Schutz vor Schadsoftware

5 Absicherung der Netzverbindung

6 Signatur und Verschlüsselung im Vergabeverfahren

6.1 SecPKI Vertrauens-Infrastruktur

7 Daten-Backup

8 Regelungen zum Datenschutz

9 Angaben zum Rechenzentrum

9.1 Standort
9.2 BSI-Zertifizierung nach IT-Grundschutz
9.3 BSI-Zertifikat und Zertifizierungsreport

1 Einführung

Sicherheit seit über 15 Jahren

Am 12.10.2001 führte die Landeshauptstadt Mainz als erste Kommune Europas eine elektronische Vergabe durch. Bis heute arbeitet man dort mit subreport ELViS. Damit ist die Lösung das am längsten am Markt befindliche eVergabe-System. Seit 2001 laufen die Systeme unter hohen Lasten stabil und gleichmäßig, es ist weder zu einem schweren Systemausfall noch zu einem erfolgreichen Hacker-Angriff gekommen. Deshalb vertrauen fast 2.000 Auftraggeber und über 50.000 Unternehmen auf subreport ELViS.

Wir bieten subreport ELViS als Mietmodell an, als Software as a Service (SaaS). subreport und sein technischer Dienstleister übernehmen die komplette IT-Administration und zentrale Dienstleistungen wie Hosting, Betrieb und Updates. Software und Infrastruktur werden vom Kunden einfach als Service genutzt. Die Vorteile: keine komplexe und langwierige Softwareinstallation, transparente und geringe IT-Kosten, schnelle Einsatzfähigkeit, kein Investitionsaufwand, ständige Aktualität im Hinblick auf vergaberechtliche Neuerungen bzw. Updates.

Auf die umfassenden Maßnahmen zum Schutz der Daten von subreport ELViS wird nachfolgend näher eingegangen.

2 Technische und organisatorische Maßnahmen

Die nachfolgenden technischen und organisatorischen Maßnahmen umfassen die vier Schutzziele des Art. 32 Abs.1b) DSGVO, namentlich Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme.

Eine rasche Wiederherstellung nach einem physischen oder technischen Zwischenfall ist gewährleistet. Die technischen und organisatorischen Maßnahmen werden regelmäßig, gem. Art. 32 Abs 1 d) DSGVO, auf Ihre Wirksamkeit hin geprüft.

2.1 Verschlüsselung

Die Maßnahmen zur Verschlüsselung befinden sich auf dem höchsten technischen Stand und finden auf Netzwerk-, Protokoll-, System- und Anwendungsebene in unterschiedlichen Ausprägungen sowohl einzelnd als auch in Kombination Anwendung.

Organisatorische Maßnahmen

- Passwortrichtlinie und geschützte Passwortvergabe

Technische Maßnahmen

- Authentifizierung mit personifizierten SSH-Keys
- Einsatz von VPN bei Remote-Zugriffen
- Verschlüsselung von Notebooks / Laptops / Passwörtern
- Zertifikatsgesicherte, SSL/TLS 1.2 verschlüsselte Internetverbindungen (https)

2.2 Fähigkeit der Vertraulichkeit

Vertraulichkeit heißt, dass personenbezogene Daten vor unbefugter Preisgabe und unrechtmäßigen Zugang geschützt sind. Wir gewährleisten die Vertraulichkeit der Daten wie nachfolgend erläutert.

2.2.1. **Zutritt**

Es wird verhindert, dass Personen, die dazu nicht befugt sind, unkontrolliert in die Nähe der Datenverarbeitungsanlagen kommen.

Kein unerlaubter Zutritt

Organisatorische Maßnahmen

- Anwesenheitszeit von Personen im Sicherheitsbereich wird protokolliert
- Anwesenheitszeit von Personen im Sicherheitsbereich wird kontrolliert
- Einteilung in Sicherheitszonen/Sperrbereiche
- Gruppierung der Zutrittsbefugnisse nach Aufgaben- und Zuständigkeitsgebiet
- Regelmäßige Kontrollrundgänge
- Personenkontrolle durch Empfang / Pförtner bzw. Werkschutz
- Protokollierung von Besuchern / Besucherbauch

2.2.2. **Zugriff**

Es wird gewährleistet, dass nur die zur Benutzung des Systems berechtigten Personen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Personenbezogene Daten können bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

Keine unbefugte Nutzung

Organisatorische Maßnahmen

- Berechtigungskonzept mit Minimalprinzip
- Clean-Desk und Clean-Screen Richtlinie
- Datenvernichtungs-/Datenlösch-Prozess
- Rechteprozess zur dokumentierten Vergabe/Entzug von Zugriffsrechten
- Rückbauprozess bei Produktkündigungen
- Klassifizierung von Informationen nach vorgegebener Richtlinie
- Passwortrichtlinie inkl. Länge, Komplexität und Wechsel
- Regelmäßige Überprüfung der Richtlinien und Prozesse auf Aktualisierung
- Sichere Aufbewahrung von Datenträgern
- Verwaltung der Benutzerrechte durch geschulte Systemadministratoren

Technische Maßnahmen

- Berechtigungsebenen nach Abteilungen und Zugriffserfordernissen
- Automatische und kennwortgeschützte PC-Bildschirmsperre
- Degausser-Entmagnetisierer für magnetische Festplatten
- Datenlösch-Systeme zum Löschen mit DBAN und Secure Erase
- Einsatz von Aktenvernichtern oder Entsorgungstonnen
- Löschung von Datenträgern vor deren Wiederverwendung
- Protokollierung von Zugriffen auf Anwendungen und IT-Systeme
- Verschlossene Entsorgungstonnen von zertifizierten Datenvernichtern
- Verschlüsselung von Notebooks/Laptops

2.3 Fähigkeit der Integrität

Unversehrtheit der Daten

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf „Daten“ angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind.

Organisatorische Maßnahmen

- Berechtigungskonzept mit Minimalprinzip
- Rechteprozess zur dokumentierten Vergabe/Entzug von Zugriffsrechten
- Verwaltung der Benutzerrechte durch geschulte Systemadministratoren

Technische Maßnahmen

- Berechtigungsebenen nach Abteilungen und Zugriffserfordernissen
- Automatische und kennwortgeschützte PC-Bildschirmsperre
- Protokollierung von Zugriffen auf Anwendungen und IT-Systeme

2.4 Fähigkeit der Verfügbarkeit und Belastbarkeit

Ständige Verfügbarkeit

Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von Anwendern stets wie vorgesehen genutzt werden können. Systeme sind belastbar, wenn sie so widerstandsfähig sind, dass ihre Funktionsfähigkeit selbst bei starkem Zugriff bzw. starker Auslastung gegeben ist.

Organisatorische Maßnahmen

- Alarmmeldung bei unberechtigten Zutritten zu Serverräumern
- Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort
- Monitoring aller relevanten Infrastruktur- und IT-Systeme
- Serverräume nicht unter sanitären Anlagen oder mittels Leckage-Wannen gesichert
- Verträge zum Beliefern der Netzersatzanlage mit Kraftstoff 24/7/365

Technische Maßnahmen

(1) Brandbekämpfung

- Brandmeldeanlage mit Aufschaltung zur Feuerwehr
- Feuer- und Rauchmeldeanlagen
- Feuerlöschanlage (Argon/Stickstoff) im Serverraum vorhanden
- Feuerlöscher im Serverraum vorhanden
- Feuerlöscher in Büros und Infrastruktur vorhanden

(2) Klima

- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Klimaanlage für Serverräume

(3) Netzwerk

- Netzwerkanbindung über zwei separate Zuleitungen
- Netzwerkanbindung über mind. zwei unterschiedliche Carrier

(4) Strom

- Autonome Stromversorgung über eigene Trafostation
- Netzersatzanlage vorhanden (Diesel-Aggregat)
- Stromanbindung in Serverracks über zwei separate Zuführungen
- Stromversorgung der Rechenzentrumsräume über zwei Zuleitungen
- Unterbrechungsfreie Stromversorgung

(5) Sonstiges

- Einsatz von Datenspiegelung (RAID)
- Serverräume über der Wassergrenze / ausreichendes Pumpsystem vorhanden
- Wasserschutzeinrichtung (z.B. Leckage-Überwachung) vorhanden

2.5 Wiederherstellbarkeit der Verfügbarkeit und des Zugangs

Notfallsicher

Ergänzend zu den Maßnahmen zur Verfügbarkeit und Belastbarkeit sowie Vertraulichkeit, muss sichergestellt sein, dass IT-Systeme und Daten im Schadensfall oder bei Notfällen schnellstmöglich wiederhergestellt werden können.

Organisatorische Maßnahmen

- Notfallkonzept für relevante Infrastruktur und IT-Systeme
- Testen der Datenwiederherstellung

Technische Maßnahmen

Wir verweisen auf die in Kapitel 2.4, sowie Kapitel 2.2 beschriebenen technischen Maßnahme zur Gewährleistung der Wiederherstellbarkeit.

2.6 Verfahren zur regelmäßigen Überprüfung

Regelmäßige Qualitätskontrollen

Zur Qualitätssicherung und Sicherstellung der Wirksamkeit der getroffenen Maßnahmen werden regelmäßige Überprüfungen der etablierten Prozesse und Methode durchgeführt.

Organisatorische Maßnahmen

- Überprüfung der Maßnahmen im Rahmen der Wirksamkeitskontrolle des Informationssicherheitsmanagementsystems (ISMS- gemäß DIN ISO/IEC 27001)
- Kontinuierlicher Verbesserungsprozess im Rahmen des ISMS

2.7 Verarbeitung personenbezogener Daten nur nach Anweisung

Hoheit des Auftraggebers

Dies bedeutet, dass jeder Auftrag, bei dem dem Auftragnehmer personenbezogene Daten übermittelt werden, gemäß den vereinbarten Regelungen durchzuführen und auch vom Auftraggeber zu kontrollieren ist. Die Verarbeitung der personenbezogenen Daten erfolgt gemäß den Vorschriften des Datenschutzes und den Vorgaben des Kunden.

- Auftragnehmer hat einen Datenschutzbeauftragten bestellt
- Regelmäßige Datenschutz- und IT-Sicherheitsschulung der zugriffsberechtigten Mitarbeiter
- Schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) gegeben
- Verpflichtung der Mitarbeiter des Auftragsnehmers auf das Datengeheimnis
- Weisungen zu Änderungen im Verfahrensablauf erfolgen schriftlich

3 Systemverfügbarkeit

Extrem hohe Verfügbarkeit

Für unsere Plattformen sichern wir in § 3 (2) unserer AGB eine Verfügbarkeit von mindestens 98,5 % im Jahresdurchschnitt zu. Die faktische jährliche Verfügbarkeit unseres Rechenzentrums lag

- 2014 bei 99,99 % (IP) und 100 % (Strom)
- 2015 bei 99,99 % (IP) und 100 % (Strom)
- 2016 bei 99,99 % (IP) und 100 % (Strom)
- 2017 bei 99,99 % (IP) und 100 % (Strom)

Sichergestellt wird diese hohe Verfügbarkeit durch den redundanten Betrieb der Systeme mit freier Skalierbarkeit zur Lastverteilung.

4 Mechanismen zum Schutz vor Schadsoftware

Entmilitarisierte Zone

Die Angriffserkennung erfolgt durch permanentes Monitoring in Verbindung mit hybrider Intrusion-Detection (Netzwerk- und Hostbasiert). Die Serversysteme werden in einer DMZ betrieben, die die dahinter liegenden IT-Systeme vor Angriffen aus dem Internet abschirmt. Zu den weiteren Mechanismen gehören serverbasiertes Logging aller Systemaktivitäten auf Betriebssystem- und Anwendungsbasis und die Durchführung regelmäßiger Datensicherungen nach Datensicherungskonzept.

DDoS Angriffe werden durch die Bereitschaft 24/7 innerhalb einer Reaktionszeit von 60 Minuten bearbeitet, z.B. durch Blockieren in den Firewalls.

Unberechtigte Zugriffe durch SQL-Injection werden durch technische Maßnahmen in der Software und die vorgeschaltete Application-Firewall verhindert. Die Webanwendung prüft die Eingabedaten, so dass vor allem die Metazeichen des betreffenden Datenbanksystems entsprechend maskiert werden, die für Ausnutzung von SQL-Injection verantwortlich sind. Weitergehend werden auch die Eingabedaten auf die Eigenschaften erwarteter Werte geprüft.

5 Absicherung der Netzverbindung

Zertifikats-gesichert

Die Vergabestellen greifen ausschließlich über eine gesicherte Internetverbindung (HTTPS) auf die Vergabeplattform zu. Die Datenübertragung basiert auf zertifikatsgesicherter SSL/TLS v1.2-Verschlüsselung mit Identitätsnachweis. Die Übertragung erfolgt mit einem 2048-Bit RSA/SHA 256-Schlüssel und einer Verschlüsselungstiefe von 128 Bit (bereits seit 2013) und entspricht dem vom BSI empfohlenen Standard laut IT-Grundschutz (TR 02102-2) bis in das Jahr 2022 und darüber hinaus.

Durch eine zwischengeschaltete Firewall können die IT-Systeme der Vergabestellen auf die Plattform zugreifen, der Rückweg (d.h. der Zugriff durch die Plattform auf die IT-Systeme der Vergabestellen) ist auf Protokollebene grundlegend gesperrt.

6 Signatur und Verschlüsselung im Vergabeverfahren

subreport ermöglicht sowohl die Verwendung qualifizierter als auch fortgeschrittener Signaturen/Siegel. Die Entscheidung darüber, welche Signatur/welches Siegel vor Ort genutzt werden soll, obliegt dem Auftraggeber.

Kontrolliertes Vertrauen

Die Übermittlung der Dokumente erfolgt über den Browser unter Verwendung einer abgesicherten und von subreport zertifizierten Java Web Start Anwendung. Die verwendete

Komponente zur Verschlüsselung und Signatur von Dokumenten ist das BSI-zertifizierte SecSigner-Plugin der Firma SecCommerce (https://seccommerce.com/secsigner/).

Zu diesem Zweck betreibt subreport eine eigene PKI (Public-Key-Infrastruktur), die sicherstellt, dass auf den subreport Plattformen ausschließlich Zertifikate verwendet werden können, die von vertrauenswürdigen Anbietern stammen und von subreport für die Anwendung akkreditiert wurden.

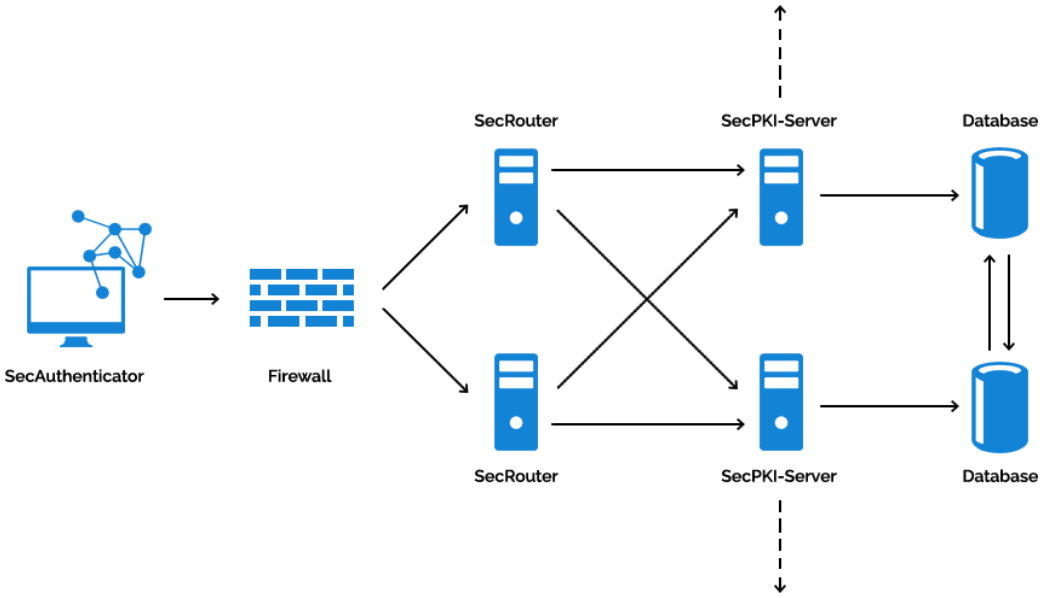
6.1 SecPKI Vertrauens-Infrastruktur

16 Jahre Erfahrung Signatur

Seit 2005 nutzen wir für Verschlüsselung und Signatur im Hinblick auf die elektronischen Angebote mit großem Erfolg die PKI-Infrastruktur der SecCommerce Informationssysteme GmbH. Die PKI-Infrastruktur von SecCommerce wurde BSI-zertifiziert und war eine der ersten Firmen weltweit, die Sicherheit mit Hilfe von elektronischen Signaturkomponenten für Datenarchivierung und Kommunikation großen Versicherungsfirmen, Banken und Behörden zur Verfügung stellte. Damit gehört SecCommerce zu den Pionieren auf dem Gebiet der kryptographischen Lösungen und besitzt mehr als 16 Jahre Erfahrung in der Entwicklung von Public Key Infrastrukturen (PKI), elektronischer Signatur, Authentifizierungslösungen und Smartcard-Technologie. Zu den Kunden gehören u.a. IBM, Airbus, T-Systems, Siemens, Audi, die Techniker Krankenkasse oder die Deutsche Rentenversicherung.

Die SecPKI-Funktionen werden zwischen den Systemen mit TLS 1.2/ SHA256 verschlüsselt übertragen. Diese wird von SecPKI-Server, sowie die Java-SecPKI-API auf der Clientseite unterstützt. Zudem führt der SecPKI-Server die SecPKI-API-Aufrufe nur aus, wenn der Aufrufer dazu berechtigt ist. Der Aufrufer authentifiziert sich daher mit einem X.509-Zertifikat mittels TLS-Client-Authentifizierung oder mit Name und Passwort.

Das SecPKI-System ist in einer Mehrschichtenarchitektur implementiert, deren zentraler Bestandteil der SecPKI-Server ist, der über JDBC an eine Datenbank-Instanz angeschlossen ist. Die folgende Abbildung zeigt als Beispielanwendung für SecPKI zusätzlich die Komponente SecRouter (Option) zur Absicherung des Zugriffs auf Webseiten.



Quelle: SecCommerce

In den über 15 Jahren Echtbetrieb von subreport ELViS ist es bisher zu keinerlei kritischen Situationen im Umfeld der SecCommerce-Lösung gekommen.

7 Daten-Backup

Mit einem Backup wird die Sicherheit der Daten durch das Anlegen einer separaten, unabhängigen Kopie erhöht. Bei einem Verlust der Originaldaten kann man auf die Kopie zugreifen und die Daten somit wiederherstellen. Um die Datensicherheit zu gewährleisten existiert ein Backup-Konzept, das regelmäßige Sicherungen der Daten vorsieht. Die wichtigsten Merkmale lauten u.A.:

- ✓ Die Backups sind verschlüsselt.
- ✓ Die Backups werden räumlich getrennt von den Produktivdaten gelagert.
- ✓ Es werden regelmäßige Restore-Tests durchgeführt.

8 Regelungen zum Datenschutz

DSGVO konform

subreport legt größten Wert auf den Schutz personenbezogener und sonstiger vertraulicher Daten der Nutzer ihrer Website und Dienste. subreport verpflichtet sich, sämtliche datenschutzrechtlichen Bestimmungen, insbesondere die Bestimmungen der Datenschutzgrundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG), streng zu beachten. Dazu zählt, dass die Mitarbeiter

- die ihnen anvertrauten Daten und Datenträger, wenn sie nicht unmittelbar daran arbeiten, unter Verschluss halten;
- ihre Rechner, ihre Software und ihre Passworte keinem Unbefugten zugänglich machen;
- nicht mehr benötigte Datenträger mit personenbezogenen Daten datenschutzgerecht vernichten, damit eine missbräuchliche Weiterverwendung nicht möglich ist.

Darüber hinaus verweisen wir auf die AGB sowie die subreport-Datenschutzrichtlinie auf unserer Homepage.

Datenschutz-Schulungen der zugriffsberechtigten Mitarbeiter beim Hosting Dienstleister erfolgen nachweislich regelmäßig. Es finden regelmäßige Sicherheitstests und Revisionen statt.

9 Angaben zum Rechenzentrum

Marktführer Managed Hosting

Gehostet wird subreport ELViS bei der PlusServer GmbH im Connecta Parc in Düsseldorf. Die PlusServer ist Marktführer im Bereich Managed Hosting in Deutschland, Österreich und der Schweiz. Basierend auf einem umfangreichen Produktportfolio, das für die Bedürfnisse des Mittelstands sowie großer Unternehmen optimiert ist, entwickelt PlusServer individuelle Hosting- und Cloud-Lösungen. In zehn Rechenzentren mit höchstem Sicherheitsstandard, davon sieben in Deutschland, hostet PlusServer aktuell mehr als 5.000 Firmenkunden aus 52 Ländern. Kunden wie Zalando, Bayer, Lufthansa City Center, REWE oder DB zeugen dabei von der hohen Qualität und der Vielfalt der technischen Lösung.

9.1 Standort

Der Standort des Rechenzentrums, in dem subreport ELViS gehostet wird, lautet:

In der Steele 33a
40599 Düsseldorf
DEUTSCHLAND

9.2 BSI-Zertifizierung nach IT-Grundschutz

Das Rechenzentrum in Düsseldorf zeichnet sich insbesondere durch eine Zertifizierung nach IT-Grundschutz durch das Bundesamt für Sicherheit in der Informationstechnologie aus. Diese bestätigt ein vorbildliches Informationssicherheits-Managementsystem (ISMS). Zu den wichtigsten Merkmalen zählen u.A.:

- ✓ ISO-27001-Zertifizierung
- ✓ BSI-Zertifizierung nach IT-Grundschutz-Standard
- ✓ Mehrfach redundante Glasfaseranbindungen
- ✓ USV- und generatorgestützte Stromversorgung
- ✓ Hochsicherheitsrechenzentrum mit Zugangskontrolle, Sicherheitsbereiche mit unterschiedlichen Zugangszonen, Alarmanlage und Videoüberwachung
- ✓ Brandfrüherkennungssystem und Löschanlage
- ✓ Indirekte freie Kühlung durch energieeffizienter Klimaanlage mit n+1-Redundanz
- ✓ Kalte/warme Gänge mit Rack-Temperaturüberwachung
- ✓ A/B-Stromzuführung zu jedem Rack.

9.3 BSI-Zertifikat und Zertifizierungsreport

siehe Folgeseiten

Bundesamt
für Sicherheit in der
Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63, 53133 Bonn

Einschreiben mit Rückschein
PlusServer GmbH
Welserstrasse 14
51149 Köln
Deutschland

Yona Raekow

HAUSANSCHRIFT
Bundesamt für Sicherheit in
der Informationstechnik
Godesberger Allee 185-189
53175 Bonn

POSTANSCHRIFT
Postfach 20 03 63
53133 Bonn

TEL +49 (0) 228 99 9582-6051
FAX +49 (0) 228 99 10 9582-6051

gs-zert@bsi.bund.de
https://www.bsi.bund.de

Betreff: Bescheid über den positiven Abschluss des 1. Überwachungsaudits gem. Prüfschema für ISO 27001-Audits auf der Basis von IT-Grundschutz

Bezug: Zertifizierung BSI-IGZ-0267-2017 von "Infrastruktur im Rechenzentrum PlusServer GmbH"
Aktenzeichen: D24-720-09-02
Datum: 16. Januar 2018
Seite 1 von 1

Sehr geehrte Damen und Herren,

das 1. Überwachungsaudit des Verfahrens BSI-IGZ-0267-2017 ist mit Datum vom 04. Januar 2018 positiv abgeschlossen worden. Das Überwachungsaudit wurde durchgeführt von Jörg Deusinger, zertifizierter Auditor für ISO 27001-Audits auf der Basis von IT-Grundschutz (Zertifizierungsnummer: BSI-ZIG-0146-2015). Das Zertifikat sowie der Zertifizierungsreport vom 13. Dezember 2016 sind weiterhin gültig.

Hinweis:
Die Gültigkeit von ISO 27001-Zertifikaten auf der Basis von IT-Grundschutz ist begrenzt. Treten während der Gültigkeitsdauer wesentliche Änderungen (wie z.B. größere Änderungen im Managementsystem, Änderungen in der Organisation, Änderungen im Outsourcing, Standortwechsel, Änderungen von Tätigkeitsfeldern) am zertifizierten Untersuchungsgegenstand auf, muss der IT-Sicherheitsbeauftragte diese dem BSI schriftlich mitteilen. Das BSI entscheidet dann, ob eine vorzeitige Re-Zertifizierung erforderlich ist.

Mit freundlichen Grüßen
Im Auftrag

Raekow

Bundesamt
für Sicherheit in der
Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63, 53133 Bonn

Yona Raekow

HAUSANSCHRIFT
Bundesamt für Sicherheit in
der Informationstechnik
Godesberger Allee 185-189
53175 Bonn

POSTANSCHRIFT
Postfach 20 03 63
53133 Bonn

TEL +49 (0) 228 99 9582-6051
FAX +49 (0) 228 99 10 9582-6051

gs-zert@bsi.bund.de
https://www.bsi.bund.de

Einschreiben mit Rückschein
PlusServer GmbH
Hohenzollernring 72
50672 Köln
Deutschland

Betreff: Bescheid über den positiven Abschluss des 2. Überwachungsaudits gem. Prüfschema für ISO 27001-Audits auf der Basis von IT-Grundschutz

Bezug: Zertifizierung BSI-IGZ-0267-2017 von" Infrastruktur im Rechenzentrum PlusServer GmbH (vorher OpenIT GmbH)"
Aktenzeichen: D24-720-09-02
Datum: 24. Januar 2019
Seite 1 von 1

Sehr geehrte Damen und Herren,

das 2. Überwachungsaudit des Verfahrens BSI-IGZ-0267-2017 ist mit Datum vom 02. Januar 2019 positiv abgeschlossen worden. Das Überwachungsaudit wurde durchgeführt von Jörg Deusinger, zertifizierter Auditor für ISO 27001-Audits auf der Basis von IT-Grundschutz (Zertifizierungsnummer: BSI-ZIG-0146-2018). Das Zertifikat sowie der Zertifizierungsreport vom 13. Januar 2017 sind weiterhin gültig.

Hinweis:
Die Gültigkeit von ISO 27001-Zertifikaten auf der Basis von IT-Grundschutz ist begrenzt. Treten während der Gültigkeitsdauer wesentliche Änderungen (wie z.B. größere Änderungen im Managementsystem, Änderungen in der Organisation, Änderungen im Outsourcing, Standortwechsel, Änderungen von Tätigkeitsfeldern) am zertifizierten Untersuchungsgegenstand auf, muss der IT-Sicherheitsbeauftragte diese dem BSI schriftlich mitteilen. Das BSI entscheidet dann, ob eine vorzeitige Rezertifizierung erforderlich ist.

Mit freundlichen Grüßen
Im Auftrag
Raek
Raekow