TOM civento 1

Technische & Organisatorische Maßnahmen

Dokumenteninformation

Bezeichnung	Version
TOM civento	Version 1
Status	**Zuletzt geändert am**
Geprüft	11.09.2025 09:06 UTC

Inhaltsübersicht

1. Datenminimierung

1.1. Reduzierung der Verarbeitungsoptionen

Die verarbeiteten Daten werden auf das erforderliche Minimum reduziert und nach Zweckerreichung der Gefahrenabwehr gelöscht.

Folgende Daten werden gelöscht: Diagnosedaten, technische Daten

Die Löschung erfolgt automatisiert.

2. Verfügbarkeit

2.1. Schutz vor Schadsoftware

Für das System werden folgende zusätzliche Maßnahmen zum Schutz vor Schadsoftware ergriffen: Endpoint Protection Service, Firewall, Regelmäßige Sicherheitsupdates, Regelmäßige Updates, Virenscan bei Empfang von Dokumenten

2.2. Backup der Daten

Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien u. ä. werden gemäß einem getesteten Konzept angefertigt.

Folgende Backup-Regelungen werden angewendet: inkrementelle Backups, vollständiges Backup

2.3. Redundanz und Ausweichräume und –netze

Die Infrastruktur für den Betrieb der Anwendung wird bei der ekom21 betrieben.

Eine Virtualisierte Infrastruktur ist Standard bei Rechenzentrumsbetrieb durch die ekom21. Die Anwendung wird gemäß diesem Standard betrieben.

Folgende Komponenten sind redundant ausgelegt: Anwendungsserver, Web-Server

Im Not- oder Katastrophenfall werden Ausweichräume oder -netze genutzt.

Bei einem Ausfall/einer Störung der Anwendung erfolgt eine automatische Benachrichtigung per Siehe HA im Command Center an: Command Center, Systemadministration.

2.4. Reparaturstrategien und Ausweichprozesse

Ein Penetrationstest wurde durchgeführt.

Es gibt einen Lastausgleich für: Server

Der ekom21 interne Wiederanlaufplan findet Anwendung.

3. Integrität

Es erfolgen regelmäßig Tests zur Feststellung und Dokumentation der Funktionalität, von Risiken sowie Sicherheitslücken und Nebenwirkungen von Prozessen.

Die IT-Systeme werden so eingeschränkt, so dass diese keine oder möglichst wenige Nebenfunktionalitäten aufweisen.

3.1. Audit

Es findet eine regelmäßige Integritätsprüfung/Audit statt.

Die Anwendung ist im BSI-Untersuchungsgegenstand.

4. Nichtverkettung

Der Zweck der genutzten Systeme, für den die Anwendung eingesetzt wird, wird eingehalten.

5. Vertraulichkeit

5.1. Anonymisierung & Pseudonymisierung

Die Daten werden auf folgenden Ebenen pseudonymisiert oder anonymisiert: Logs, Parameter.

Die Daten werden für folgende Fälle oder Teilprozesse pseudonymisiert oder anonymisiert: Logs- & Monitoring-Ebene, Parameter.

Zuordnung der verschiedenen Fälle oder Teilprozesse zu der jeweiligen Aktion (Pseudonymisierung/Anonymisierung):

Aktion, z.B. Deaktivierung User	**Art, z.B. Pseudonymisierung**	**Ebene, z.B. Frontend, Produktivumgebung**
Logs	Pseudonymisierung	Front- Backendsysteme
Parameter (Zugangsdaten für Schnittstellen)	Pseudonymisierung von Zugangsdaten	Backendsysteme

5.2. Systemumgebung

Die Mandantentrennung erfolgt folgendermaßen: logisch

Produktiv- und Testsystem werden folgendermaßen voneinander getrennt: physisch

Die Speicherung und die Verarbeitung erfolgen physisch getrennt voneinander.

In der Testumgebung werden anonymisierte Daten bzw. Testdaten ohne Personenbezug verwendet.

5.3. Protokollierung & Verschlüsselung

Auf Serverebene wird Folgendes protokolliert: Anmeldevorgänge, Audit-Log, Datenzugriffe, Eingabe bei der Erhebung und Ergänzung von Daten, Fehler, Für den Betrieb notwendige Aktionen, gescheiterte Zugriffsversuche, Konfigurationsänderungen, lesende Zugriffe, Löschvorgänge, schreibende und/oder ändernde Zugriffe, Übermittlungsvorgänge, Veränderung oder Korrektur von gespeicherten Daten

Auf Anwendungsebene wird Folgendes protokolliert: Anmeldevorgänge, Datenzugriffe, Eingabe bei der Erhebung und Ergänzung von Daten, Für den Betrieb notwendige Aktionen, gescheiterte Zugriffsversuche, Konfigurationsänderungen, lesende Zugriffe, Löschvorgänge, schreibende und/oder ändernde Zugriffe, Veränderung oder Korrektur von gespeicherten Daten

Die Protokolldaten werden gegen Veränderung und Verlust gesichert.

Die Zuordnung der Systemkomponenten zur jeweiligen Verschlüsselungsart: Transportverschlüsselung: gem. ekom21 RL - Transportverschlüsselung

Das ekom21 interne Standard-Kryptokonzept wird angewendet.

Die ekom21 Richtlinie zum Identitätsmanagement (Identity Management) wird angewendet.

Es gibt ein Rechte- und Rollenkonzept.

Die Administratorenrechte werden unter verschiedenen Personen aufgeteilt.

Die Vergabe von Administratorenrechten erfolgt an eine minimale Personenanzahl.

Es gibt Vertretungsregelungen für abwesende Mitarbeiter in Bezug auf die Anwendungsbetreuung und Administration.

5.4. Authentisierung / Passwortvergabe

Ein sicheres Authentisierungsverfahren ist implementiert.

Die Authentifizierung erfolgt mittels eines Passworts über eine(n) Verzeichnisdienst.

Es erfolgt ein automatischer Abmeldevorgang des Benutzers aus der Anwendung aufgrund von Inaktivität.

6. Transparenz

Betroffene können ihre Auskunftsrechte folgendermaßen geltend machen: Kontaktaufnahme zur Kommune

Einwilligungen, deren Widerruf und Widersprüche der Betroffenen werden folgendermaßen dokumentiert: Kann pro Lösung implementiert werden

6.1. Versionierung

Versioniert werden: Dateiaustauschformate, Dokumente, Programmversionen

7. Intervenierbarkeit

7.1. Betroffenenrechte

Die Anwendung weist folgende Datenfelder im Zusammenhang mit den Betroffenenrechten auf: Die Datenfelder ergeben sich aus prozessspezifischen Modellierungen

Es gibt die Möglichkeit, notwendige Datenfelder (z.B. für Sperrkennzeichen, Benachrichtigungen, Einwilligungen, Widersprüche etc.) zu schaffen.

Konsistente Berichtigungen, Sperrungen und Löschungen aller zu einer Person gespeicherten Daten können zusammengestellt werden.

7.2. Einschränkungen Funktionalitäten

Einzelne Funktionalitäten (Module oder Anwendungsteile) können ohne Mitleidenschaft für das Gesamtsystem deaktiviert werden.

Durch folgende Maßnahmen werden differenzierte Einwilligungs-, Rücknahme-, Widerspruchs sowie Lösch- und Berichtigungsmöglichkeiten geboten: Die Datenberichtigung wird kundenseitig organisatorisch gelöst, organisatorische Maßnahmen

Es können Optionen bereitgestellt werden, mit denen Betroffene die Anwendung datenschutzgerecht einstellen können.