Leistungsbeschreibung

Bereitstellung dOnlineZusammenarbeit 2.0 (Messaging/Audio/Video)

Software as a Service (SaaS)

Inhaltsverzeichnis

1 Einleitung

*Das Dokument bestimmt den zu erbringenden Leistungsgegenstand und die Beschreibung der Leistung für den Service **dOnlineZusammenarbeit 2.0**.*

1.1 Ausgangssituation

Die Anforderungen der Zusammenarbeit haben sich im Zuge von Homeoffice und mobiler Arbeit sowie der COVID19-Pandemie verändert. Auf Grund der Corona Krise in Deutschland ist der Bedarf an schnell skalierbaren Videokonferenz- und Onlinekollaborationslösungen für die Aufrechterhaltung der Arbeitsfähigkeit der öffentlichen Verwaltung der Länder sehr wichtig.

Dataport hat Vorkehrungen getroffen, schnell einer großen Anzahl von Nutzern eine Lösung bieten zu können. Dabei geht es um die Herstellung von virtuellen Klassenräumen und digitalem Unterricht für die Schulen und Sicherstellung von virtuellen Konferenzräumen für die Verwaltung.

Mit **dPhoenixSuite 2.0** und seinen Modulen stellt Dataport einen cloudbasierten Web-Arbeitsplatz für den öffentlichen Sektor (Verwaltung, Schulen, Universitäten, Kultur, …) als Service bereit. Zur Wahrung der digitalen Souveränität unserer Auftraggeber werden dabei Alternativen zu den marktbeherrschenden Produkten evaluiert sowie eine On-Premise-Lösung erstellt und optimiert.

2 Leistungsgegenstand

2.1 Beschreibung

dOnlineZusammenarbeit 2.0 (Modul für Messaging/Audio/Video aus **dPhoenixSuite 2.0**) ist eine Lösung zur Kommunikation im Verwaltungs- und Bildungsumfeld. Sie ermöglicht es, vielen Nutzer unkompliziert und ad hoc zu Online-Besprechungen zusammenzukommen. Es beinhaltet die in Matrix/Element integrierte Videolösung Jitsi.

- Dataport bietet eine Audio-/Videokonferenz-Lösung aus der sicheren Umgebung des eigenen Rechenzentrums unter Hinzunahme von Services aus Partner-Rechenzentren in Deutschland.
- Die Lösung lässt sich für die Arbeit aus dem Homeoffice und von verteilten Standorten nutzen, z.B. im Umfeld von Verwaltungen und für den digitalen Unterricht.
- Für die Teilnahme sind keine Installationen auf den Endgeräten notwendig.
- Die Lösung eignet sich auch bei geringen Datenübertragungsraten und ist auf praktisch allen stationären und mobilen Endgeräten (BYOD) Browser-, oder APP-basiert einsetzbar.

2.2 Funktionsumfang

Das Produkt **dOnlineZusammenarbeit 2.0** wird durch Dataport (Auftragnehmer) für den Auftraggeber bereitgestellt. Es erlaubt die digital souveräne Durchführung von Audio- und Videokonferenzen. Zum Einsatz kommt hierbei die Open-Source-Software Jitsi. Jitsi bietet eine sichere und verschlüsselte Audio- und Videokonferenz mittels hop-encryption aus dem sicheren Rechenzentrum von Dataport oder durch Dataport beauftragte Rechenzentren in Deutschland.

dOnlineZusammenarbeit 2.0 unterstützt in allen Protokollen Präsenz- und Sofortnachrichten. Es werden alle gängigen Protokolle bekannter Instant Messenger unterstützt und bei Bedarf im Rahmen der Weiterentwicklung erweitert. In vielen Fällen ist auch Dateiübertragung möglich.

Folgende Funktionen stehen standardmäßig zur Verfügung:

- Desktop-Sharing – Freigabe des eigenen Bildschirmes zur Ansicht und zur Bedienung durch die andere Seite
- Video-/Audiokonferenzen ohne weitere Infrastruktur
- Remote-Konfiguration (Provisioning)
- Direktverbindungen für die Mediendaten P2P über Interactive Connectivity Establishment und Universal Plug and Play (UPnP)

2.3 Merkmale

- Komplett webbasiert, daher Zugriff mit jedem Endgerät,
- Zugriff generell aus allen Netzen möglich,
- Vollständige Nutzung von Open-Source-Software,
- Anwendung ist zu 100 % quelloffen,
- Nutzung der an das Endgerät angebundenen Peripherie für die Kommunikation (z.B. Headsets) möglich

3 Betrieb und Monitoring

Grundsätzlich liegt die Betriebsverantwortung für den Betrieb der Services beim Auftragnehmer. Der Auftraggeber hat keinen administrativen Zugriff auf Server, Datenbanken, Fileservice.

3.1 Sicherheit

- Sicheres Austauschen von Nachrichten sowie das Starten von verschlüsselten Audio- und/oder Videositzungen.
- Benutzerverwaltung mit den Benutzergruppen User oder Administrator
- Anmeldung nur mit Benutzerkennung und Passwort
- Hierarchische Stufen für das Zugriffsrecht
- Protokollierung aller ändernden Zugriffe für den internen Datenschutzbeauftragten möglich
- Der Auftragnehmer stellt sicher, die vom BSI in den IT-Grundschutzkatalogen vorgegebenen A-, B- und C-Maßnahmen, die in den Zuständigkeitsbereich des Auftragnehmers fallen, einzuhalten.
- Die Maßnahmenermittlung und Umsetzung von Sicherheitsmaßnahmen erfolgt auf Basis der Bausteine der IT-Grundschutzkataloge in der beim Auftragnehmer eingesetzten Fassung und unter Einhaltung der für BSI-Zertifizierungen geltenden Übergangsfristen.
- Die für den betrachteten Informationsverbund maßgeblichen Sicherheitsmaßnahmen und der jeweilige Umsetzungsstand werden im Sicherheitskonzept dokumentiert. Sofern

Inhalt

2 Rechenzentren

Die Leistungserbringung erfolgt generell digital souverän in deutschen Rechenzentren.

Die Dienste werden in Rechenzentren der Nachunternehmen TelemaxX und Equinix erbracht, für die eine Zertifizierung nach ISO 27001:2013 vorliegt.

3 Technische und Organisatorische Maßnahmen

Dataport verpflichtet sich gegenüber dem Auftraggeber zur Umsetzung der folgenden Technischen und Organisatorischen Maßnahmen (TOM).

3.1 Vertraulichkeit gem. Art. 32 Abs. 1 lit. b DSGVO

3.1.1 Zutrittskontrolle

Dies umfasst Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z. B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Technische Maßnahmen:

- Alarmanlage
- Automatisches Zugangskontrollsystem für Systemräume
- Zwei-Faktor-Systeme, wie z. B. Chipkarten oder Transpondersysteme
- Zusätzlich manuelle Schließsysteme für Systemschränke
- Sicherheitsschlösser
- Vergitterung von Zugangsschächten
- Türen mit Blindknauf
- Klingelanlage mit Videoüberwachung und Gegensprechanlage
- Videoüberwachung der Gebäude
- Betriebsgeländeabsicherung, wie z. B. Zäune, Stacheldraht etc.

Organisatorische Maßnahmen:

- Regelungen für Schlüsselausgabe
- Rezeptions- bzw. Pförtnerdienste
- Besucherprotokolle, dabei: generell nur begleitende Besuche im Objekt

- Mitarbeiterausweis mit Ablauf und Erneuerungsmodus, angekoppelt an Prozess „Einstellung/Ausstellung/Hausverbot“
- Schriftliche Regelung bzgl. der Begleitung von Besuchern in bestimmten Sicherheitszonen
- Sicherheitsüberprüfung auch für Wach-, Reinigungs- und Empfangspersonal und eigene wie fremde Mitarbeiter im IT-Bereich
- Bildung von Sicherheitszone(n) für verschiedene Gebäudebereiche

3.1.2 Zugangskontrolle

Dies umfasst Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z. B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ und „sicheren“ Passworts).

Technische Maßnahmen:

- Zugangskontrolle zu Systemen mindestens mit Benutzernamen und Passwort
- Zugangskontrolle zu Systemen mit Zwei-Faktor-Authentifizierung für Administratoren
- Teilweise automatische Überprüfung der Passwortqualität
- Einsatz von Anti-Malware-Systemen, Endpointprotection oder Integritätssicherung von Softwarekomponenten
- Firewall zur Separierung von Sicherheitszonen
- Einsatz von verschlüsselter Kommunikation bei administrativen Zugängen
- Verschlüsselung von Datenträgern
- Hardware-Absicherung durch passwortgeschützte Firmware-Konfiguration
- Sperre von externen Schnittstellen auf Servern (z. B. USB)
- Automatische Bildschirmsperre
- Teilweise Administration über Jump-Hosts / Administrationsplattform

Organisatorische Maßnahmen:

- Verwaltung und Dokumentation von Benutzerberechtigungen
- Regelmäßige Überprüfung der Benutzerberechtigungen
- Zuweisen von Berechtigungen mit klar definierten Rollenprofilen
- Zentrale Passwortvergabe
- Vorgaben zur Passwortqualität

- Vorgaben für sicheres Löschen und Vernichten
- Richtlinie „Clean Desk“
- Richtlinie für Datenschutz und Informationssicherheit
- Verschlüsselte Kommunikation mit dem Kunden zur Auftragsabwicklung
- Vermeidung der Nutzung von SuperAdmin-Kennungen in der Regeladministration
- Hinterlegung von Notfallkennungen und Zugangsdaten, sichere Verwaltung dieser Daten und technisch abgesicherten Prozess zur Änderung nach Entnahme einer Kennung im Notfall
- Regelungen wurden etabliert, so dass die Nutzung von Administrationskennungen nur für die notwendigen Aufgaben genutzt werden und nicht für andere Arbeiten oder z. B. Internetzugriffe
- Umfängliches Schutzkonzept der Endgeräte von Administratoren durch Anti-Malware-Agenten, Sperren von nicht freigegebenen Programmen, Internetzugriff nur per Proxy, Einschränkung der Betriebssystemrechte, Deaktivieren nicht benötigter Betriebssystemfunktionen etc.
- Prozesse für die Durchführung eines Lifecycle-Managements für Endgeräte mit Ausgabe, Betrieb, überwachter Löschung und überwachter fachgerechter Entsorgung

3.1.3 Zugriffskontrolle

Dies umfasst Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z. B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Technische Maßnahmen:

- Aktenentsorgung nach DIN 66399
- Physische Löschung oder Vernichtung von Datenträgern
- Protokollierung von Administrationstätigkeiten
- Protokollierung von Anwendertätigkeiten
- Eventbasierte automatische Kontrolle der Protokolldaten
- Auswahl und Festlegung der verwendeten Kryptographie-Algorithmen
- Nur verschlüsselte Zugriffe für die Anwender