iQ.Suite aaS Informations-sicherheitsrichtlinie

Datum: 13.04.2022

1 Überblick

"iQ.Suite aaS" ist ein Security Cloud Service, der sich in die Office 365 / Exchange Online-Umgebung des Kunden integriert, um verschiedene Sicherheitsfunktionen wie Malware-Schutz, SPAM-Schutz, Nachrichtenverschlüsselung, Verhinderung von Datenlecks, Schlüssel- / Zertifikatsverwaltung, Signaturmanagement, Abwesenheitsmanagement und andere bereitzustellen.

2 Zweck

Zweck dieses Dokuments ist es, grundlegende Anforderungen und Standards für "iQ.Suite aaS" festzulegen. Es informiert den Cloud Service Customer (CSC) über die Sicherheitslandschaft der Services sowie über die geteilten Verantwortlichkeiten zwischen dem Kunden und dem Cloud Service Provider (CSP).

3 Umfang

Diese Richtlinie gilt für "iQ.Suite aaS" und alle damit verbundenen Assets – Mitarbeiter, Kunden, Prozesse, Richtlinien, Infrastruktur und Daten.

4 Politik

4.1 Baseline Informationssicherheit und Datenschutz

Bei der Konzeption und Implementierung der "iQ.Suite aaS" hält sich das Team dahinter an unterschiedliche Industriestandards, Richtlinien und Best Practices. ISO/IEC 27001:2013 Sicherheitskontrollen werden unter Berücksichtigung der zusätzlichen Richtlinien in ISO/IEC 27017:2015 "Code of Practice for Information Security Controls based on ISO/IEC 27002 for Cloud Services" implementiert. Der Dienst läuft auf westeuropäischen Instanzen von Microsoft Azure, einem der führenden Cloud-Anbieter mit nachweislich hohem Sicherheitsniveau und Einhaltung internationaler Standards und Vorschriften. "Secure Development and Deployment Guidance" des National Cyber Security Centre wird für die Softwareentwicklung und -bereitstellung befolgt. Es werden kontinuierliche Sicherheitstests durchgeführt, einschließlich der Überprüfung auf OWASP-Schwachstellen und der Durchführung regelmäßiger Penetrationstests. Die Konfiguration und Bereitstellung der zugrunde liegenden Cloudinfrastruktur folgt den Azure-Sicherheitsbasislinien. "iQ.Suite aaS" ist gemäß den Anforderungen der EU-Datenschutz-Grundverordnung (DSGVO) konzipiert und funktioniert. Im Sinne des Art. 28 DSGVO werden geeignete technische und organisatorische Maßnahmen getroffen, um die Einhaltung der Verordnung sicherzustellen.

4.2 Geteilte Rollen und Verantwortlichkeiten

Je nach Bereitstellungsmodell ist die Aufteilung der Verantwortlichkeiten zwischen CSP und CSC unterschiedlich. Diese Verantwortlichkeiten variieren für die drei primären Cloud-Bereitstellungsmodelle: IaaS (Infrastructure as a Service), PaaS (Platform as a Service) und

SaaS (Software as a Services), wobei für IaaS der CSC die Mehrheit der Verantwortlichkeiten und für SaaS die Mehrheit der Verantwortlichkeiten beim CSP liegt. Nach dieser Definition für SaaS berücksichtigt "iQ.Suite aaS" die Sicherheit auf physischer, Infrastruktur-, Netzwerk- und Anwendungsebene. In Bezug auf die Identitäts-, Zugriffs- und Rechteverwaltung wird die Verantwortung zwischen dem CSP und dem Kunden geteilt, wobei der CSP die Mittel für eine sichere Verwaltung der Benutzer bereitstellt und der Kunde für deren ordnungsgemäße Verwendung verantwortlich ist. Sicherzustellen, dass die Daten korrekt klassifiziert sind und die Verwendung der "iQ.Suite aaS" den für den Kunden geltenden regulatorischen Verpflichtungen entspricht, liegt in der Verantwortung des Kunden.

4.3 Risiken durch autorisierte Insider

Azure Security Center wird verwendet, um Insider-Bedrohungen und Versuche, Ressourcen von autorisiertem Personal zu kompromittieren, zu erkennen. Es verwendet neue, kontinuierlich verbesserte Verhaltensanalysealgorithmen, um bösartige Aktivitäten zu erkennen. Alle Mitarbeiter, die an der Entwicklung, Implementierung und dem Betrieb der "iQ.Suite aaS" beteiligt sind, durchlaufen regelmäßig Schulungen zu ihren Informationssicherheits- und Datenschutzpflichten.

4.4 Multi-Tenancy und Cloud Service Kundenbetreuung

"iQ.Suite aaS" ist ein mandantenfähiger Dienst, der die Datenspeicherung und -verarbeitung jedes Kunden trennt, um sicherzustellen, dass seine Daten nicht auf andere Kunden oder interne Daten für die Servicedaten zugegriffen oder kombiniert werden. Die logische Mandantenisolation wird auf Datenbankebene mit einer dedizierten Azure SQL-Datenbank für jeden Client implementiert. Die virtuelle Infrastruktur des Dienstes befindet sich in einem separaten und isolierten Netzwerk.

4.5 Zugang zu Cloud-Service-Kundenressourcen durch Mitarbeiter des Cloud-Service-Providers

"iQ.Suite aaS"-Supportadministratoren haben standardmäßig keinen Zugriff auf Cloud-Kundendaten. Bei Bedarf kann der Kunde dem Supportadministrator Berechtigungen erteilen, um die Identität einer Rolle im Kundenmandanten anzunehmen, um bei der Fehlerbehebung zu helfen.

4.6 Kommunikation mit Cloud-Service-Kunden während des Änderungsmanagements

Die Architektur der "iQ.Suite aaS" ermöglicht eine nahtlose Wartung und Implementierung von Änderungen ohne Ausfallzeiten und Unterbrechungen für den Cloud-Service-Kunden und unterstützt die Fähigkeit des Cloud-Service-Providers, seine Verfügbarkeits-SLAs zu erfüllen. Informationen über wichtige Änderungen sowie Features und Fixes in neuen Releases werden den Kunden im Vorfeld des Releases mitgeteilt.

4.7 Dienstprotokollierung

Datensätze im Zusammenhang mit der Verwendung von "iQ.Suite aaS" werden gesammelt und in den Cloud-Service-Protokollen mit (UTC) Zeitstempeln protokolliert. Cloud-Service-Kunden erhalten Lesezugriff auf diese Protokolle über die Web-Benutzeroberfläche des Dienstes, die die Zeitstempel automatisch in die Uhr des Computers des Kunden umwandelt. CSP-Administratoren haben keinen Zugriff auf die vom CSC generierten Protokolle, da diese Informationen in der Kundendatenbank gespeichert sind. Aufzeichnungen sind vor Manipulationen geschützt und können als Beweismittel bei forensischen und Vorfalluntersuchungen dienen.

4.8 Zugriff auf und Schutz von Cloud-Service-Kundendaten

Der Zugriff auf "iQ.Suite aaS" durch CSC-Benutzer und CSP-Support-Administratoren und -Benutzer ist nur für autorisierte Microsoft 365-Konten verfügbar. Darüber hinaus wird die Zwei-Faktor-Authentifizierung unterstützt, um eine sicherere Anmeldung zu gewährleisten. Der Zugriff auf den Dienst erfolgt über eine verschlüsselte Web-over-TLS-Verbindung, die alle Daten während der Übertragung schützt. Die Vertraulichkeit von Kundendaten wird durch die Verwendung von Azure Defender for Azure SQL, Transparent Data Encryption in Azure SQL und die Speicherung aller Daten auf einem 256-Bit-AES-verschlüsselten Speicher sichergestellt. Die von Azure gehostete Firewall schützt die virtuelle Infrastruktur und schränkt den nicht autorisierten Netzwerkdatenverkehr ein.

4.9 Lifecycle-Verwaltung von Cloud-Service-Kundenkonten

Während der anfänglichen Bereitstellung von iQ.Suite aaS stellt der Kunde ein eigenes Azure AD-Konto bereit, das als globaler Mandantenadministrator in iQ.Suite aaS konfiguriert werden kann. Nach dem Konfigurieren dieses Zugriffs verfügt der Kunde über alle Funktionen, um dem Dienst Benutzer hinzuzufügen/zu entfernen, Rollen und Rechte zu ändern, benutzerdefinierte Rollen zu erstellen und sie Benutzern zuzuweisen. Kundenadministratoren des Cloud-Dienstes sind für die End-to-End-Verwaltung aller Cloud-Service-Kundenkonten verantwortlich.

4.10 Service-Überwachung

Die kontinuierliche 24/7-Überwachung und -Alarmierung versorgt das Support-Team der "iQ.Suite aaS" mit Informationen über den Zustand und die Leistung des Dienstes sowie über Sicherheitsereignisse oder Vorfälle. Sowohl Azure- als auch Drittanbieter-Überwachungslösungen werden verwendet, um die Überwachungsanforderungen besser abzudecken. Der CSC kann bestimmte Aspekte des Betriebs des Cloud-Dienstes in den Protokollen überwachen, die in der Web-Benutzeroberfläche zur Verfügung gestellt werden.

4.11 Umgang mit Sicherheitsvorfällen und Datenschutzverletzungen

In Cloud-Diensten teilen sich sowohl der CSC als auch der CSP das Risiko von Sicherheitsvorfällen und Datenschutzverletzungen, weshalb ihre ordnungsgemäße und rechtzeitige Handhabung von großer Bedeutung ist. Jede Partei ist verpflichtet, der anderen Partei jeden festgestellten oder vermuteten Sicherheitsvorfall oder Datenverstoß, der sich nachteilig auf eine von ihnen auswirken kann, innerhalb von 24 Stunden zu melden (z. B. Verlust vertraulicher Daten, Offenlegung personenbezogener Daten, schwerwiegender Dienstausfall usw.). Benachrichtigungen von CSP an CSC werden an die im Dienstleistungsvertrag angegebenen offiziellen Kontakte gesendet. Benachrichtigungen von CSC an den CSP werden an security@digitall.com gesendet. Der Cloud Service Provider hat einen 5-stufigen Prozess für die Verwaltung von Sicherheitsvorfällen und Datenschutzverletzungen implementiert – Erkennung, Bewertung, Eindämmung, Lösung und Schließung. Beide Parteien arbeiten aktiv zusammen, um die negativen Auswirkungen zu mildern und den Sicherheitsvorfall zu lösen, indem sie digitale Beweise oder andere Informationen untereinander auf der für eine wirksame Lösung erforderlichen Detailebene austauschen. Der CSP und der CSC müssen ihren Verpflichtungen zur Mitteilung von Datenschutzverletzungen an die zuständigen Behörden nachkommen.

4.12 Datensicherung

Zur Sicherung von Kundendaten werden unterschiedliche Strategien implementiert. Point-in-Time-Restore (PITR) ist seit 7 Tagen verfügbar. Darüber hinaus werden alle 12 Stunden differenzielle Backups erstellt. Die langfristige Aufbewahrung ist so konfiguriert, dass vollständige Backups für 4 Wochen aufbewahrt werden. Georedundante Sicherungen werden in Rechenzentren in Westeuropa und Nordeuropa durchgeführt und sicher auf verschlüsseltem Azure-Speicher gespeichert. Backup-Jobs werden von CSP-Mitarbeitern überwacht und im Fehlerfall Maßnahmen ergriffen. CSC kann die Wiederherstellung von CSP anfordern, indem es sich an das iQ.Suite aaS Support-Team wendet.

4.13 Technisches Schwachstellenmanagement

Die kontinuierliche Schwachstellenverwaltung wird von Azure Defender für Azure SQL und Azure Defender für Server durchgeführt, die über eine integrierte Lösung zur Schwachstellenbewertung von Qualys verfügen. Identifizierte Schwachstellen werden entsprechend ihrer Kritikalität zeitnah behoben.

4.14 Service und Business Continuity

"iQ.Suite aaS" ist auf Ausfallsicherheit ausgelegt. Um den kontinuierlichen Betrieb zu gewährleisten, wird bei der Gestaltung des Dienstes ein Redundanzansatz verfolgt. Verfügbarkeit und Integrität des Diensts werden durch die Implementierung von Datensicherungen, Lastenausgleich und Azure-

Verfügbarkeitsgruppen sichergestellt. Verschiedene Business-Continuity-Szenarien, einschließlich Pandemie, werden definiert und jährlich getestet.

5 Zugehörige Dokumente

- Informationssicherheitsrichtlinie – BP-IS-PLCY-00
- ISO/IEC 27001:2013 Norm, Abschnitte Annex A.
- Norm ISO/IEC 27017:2015

6 Definitionen und Begriffe

- CSP – Cloud-Service-Provider
- CSC – Cloud Service Kunde