FMH

Technische und organisatorische Anforderungen an Cloud-Dienste

Inhaltsverzeichnis

Einleitung **3**

Cloud-Dienst **5**

Anforderungen

Anforderung 1: Applikation und Schnittstellen 8

Anforderung 2: Audit Assurance und Compliance 10

Anforderung 3: Business Continuity Management 12

Anforderung 4: Datensicherheit und Information Lifecycle Management 14

Anforderung 5: Physische Sicherheit 16

Anforderung 6: Verschlüsselung und Schlüsselmanagement 18

Anforderung 7: Governance und Risikomanagement 20

Anforderung 8: Personal 22

Anforderung 9: Identitäts- und Zugriffsmanagement 24

Anforderung 10: Sicherheit der Cloud-Infrastruktur und der Virtualisierungsumgebung 26

Anforderung 11: Interoperabilität und Portabilität der Anwendungskomponenten 28

Anforderung 12: Incident Management, E-Discovery und Cloudforensik 30

Anforderung 13: Bedrohungs- und Schwachstellenmanagement 32

Anhang **34**

Einleitung

In den letzten Jahren hat der Entwicklungsfortschritt im Bereich vernetzter und geteilter Ressourcennutzung zur Verlagerung von Rechenleistung, Speicherplatz oder Anwendungen in eine sogenannte Cloud geführt. Diese Verlagerung führt neben verbesserten Kostenvorteilen auch zu Effizienzgewinnen in Form von verbesserten Skalierungsmöglichkeiten sowie einer einfacheren Systemwartung und meist höherer Ausfallsicherheit. Neben den Vorteilen bestehen jedoch auch Herausforderungen im Bereich der Informationssicherheit. Themen wie Verschlüsselung, Zugriffskontrollen, Governance und Support, Performance, Verfügbarkeit, Backup sowie Disaster Recovery sind zu klären. Insbesondere im Bereich der Rollen und Zuständigkeiten ist zu definieren, welche Aufgaben durch die Cloud-Nutzer (Ärztinnen und Ärzte) und ICT-Dienstleister der Praxen und welche durch den Cloud-Dienst wahrgenommen werden. Die Verantwortung für den Schutz der Daten bleibt stets bei den Ärztinnen und Ärzten.

Zielsetzung

Zur Sicherstellung von Datenschutz und Datensicherheit bei der Bearbeitung von Patientendaten in der Cloud wurden die nachfolgenden technischen und organisatorischen Anforderungen erarbeitet. Ziel dieser Anforderungen ist es, Risiken im Zusammenhang mit der Nutzung von Cloud-Diensten zu reduzieren und die Anwendung der Cloud für Ärztinnen und Ärzte sicher zu gestalten.

Generell sind die vorliegenden Anforderungen für jegliche cloudbasierten Systeme formuliert, in denen besonders schützenswerte Daten bearbeitet werden. Es ist also bei der Verwendung von jedem über die aufgeführten Praxisapplikationen hinausgehenden Cloud-Dienst zu prüfen, ob dieser Dienst Patientendaten bearbeitet. Sofern der Dienst nur Personendaten ohne erhöhten Schutzbedarf enthält, sind die Anforderungen entsprechend geringer.

Zielgruppe

Die technischen Anforderungen richten sich an beauftragte ICT-Dienstleister und Cloud-Anbieter von Ärztinnen und Ärzten. Ebenfalls eingeschlossen sind Hersteller von Medizinprodukten, welche im Rahmen ihrer Serviceleistungen Cloud-Dienste für Ärztinnen und Ärzte anbieten.

Verbindlichkeit

Die technischen und organisatorischen Anforderungen dieses Dokuments haben Empfehlungscharakter. Es liegt im Ermessen der verantwortlichen Ärztinnen und Ärzte oder deren beauftragten ICT-Dienstleister, die Verbindlichkeit der Anforderungen zu definieren. Zur Unterstützung dieses Entscheidungsprozesses sind die Massnahmen in zwei Gruppen unterteilt.

1. Muss-Anforderungen (**M**): Eine Muss-Anforderung bedeutet, dass eine Anforderung im Sinne dieser Empfehlung erfüllt sein muss. Dies gilt sowohl für besonders schützenswerte Personendaten wie auch für Personendaten ohne erhöhten Schutzbedarf. Es wird empfohlen, die Abnahme zu verweigern, falls diese Anforderung nicht erfüllt ist.
2. Soll-Anforderungen (**S**): Eine Soll-Anforderung bedeutet, dass eine Anforderung im Sinne dieser Empfehlung im Regelfall erfüllt sein soll. Für besonders schützenswerte Personendaten soll eine Nichteinhaltung dieser Anforderung vom Cloud-Anbieter oder ICT-Dienstleister begründet werden. Für Personendaten ohne erhöhten Schutzbedarf können diese Anforderungen gestrichen werden.

Abgrenzung

Das vorliegende Dokument unterliegt den folgenden Abgrenzungen:

Umfang

- Der Fokus der Empfehlungen liegt auf der elektronischen Bearbeitung von Personendaten im Gesundheitswesen im Sinne von Abschnitt 3 des Datenschutzgesetzes (DSG) durch private Personen im Zusammenhang mit der Nutzung von Cloud-Diensten. Die Bearbeitung von Personendaten durch öffentliche Organe wie öffentliche Spitäler ist nicht Gegenstand dieser Empfehlungen. Informationen in Papierformat oder andere analogen Informationen werden nicht durch die Anforderungen adressiert.
- Die Anforderungen an Cloud-Anbieter sind unabhängig von den Sicherheitsanforderungen im Zusammenhang mit dem elektronischen Patientendossier (EPD).
- Die Anforderungen an Cloud-Anbieter erheben keinen Anspruch auf inhaltliche Vollständigkeit und abschliessende Behandlung der Themenbereiche. Die Umsetzung sämtlicher Anforderungen garantiert keine vollumfängliche Sicherheit.

Grundlagen

- Die technischen und organisatorischen Anforderungen an Cloud-Anbieter wurden in Anlehnung an die Security Guidance – For Critical Areas of Focus in Cloud Computing V4.0 der Cloud Security Alliance (CSA) definiert.
- Den Anforderungen liegt das Risikoprofil von besonders schützenswerten Daten gemäss Art. 3 Bst. a DSG zugrunde.

Cloud-Dienst

Cloud-Computing ist ein Modell, gemäss welchem gemeinsam konfigurierbare Rechenressourcen, beispielsweise Netzwerk, Server, Speicher, Applikationen oder Services per Netzwerk abgerufen werden können.

In den Arztpraxen werden Cloud-Lösungen für die Ablage von Patientendaten, bestehend aus demographischen und medizinischen Daten, genutzt oder Applikationen als Service, beispielsweise Microsoft-Office 365, bezogen.

Im international anerkannten Standard SP 800-145 des National Institute of Standards and Technology (NIST)[1] sind folgende charakteristische Merkmale eines Cloud-Dienstes festgelegt.

Charakteristikum	Erläuterung
Abrufbarer Self-Service	Der Cloud-Nutzer kann Rechenressourcen, wie zum Beispiel Serverzeit oder Netzwerkspeicher bei Bedarf selbst beschaffen, ohne hierfür mit dem Cloud-Anbieter interagieren zu müssen.
Netzwerkzugriff	Die Rechenressourcen sind über das Netzwerk verfügbar, wobei der Zugriff per Mobiltelefon, Tablet, Laptop oder Arbeitsplatzstationen oder Virtualisierungen von den genannten Geräten möglich ist.
Ressourcenbündelung	Die Rechenressourcen sind gebündelt und können somit durch mehrere Nutzer mit unterschiedlicher Infrastruktur bezogen werden.
Schnelle Elastizität	Die Rechenressourcen können durch Cloud-Nutzer innert kürzester Zeit skaliert werden.
Verwalteter Service	Cloud-Systeme kontrollieren und optimieren automatisch die Rechenressourcen. Die Nutzung der Ressourcen wird überwacht, kontrolliert und kommuniziert, um die Transparenz sowohl aufseiten des Cloud-Anbieters als auch des Cloud-Nutzers zu gewährleisten.

Tabelle 1
Merkmale von Cloud-Diensten

Cloud-Servicemodell

Ein Servicemodell legt fest, welchen Umfang die Dienstleistungen eines Cloud-Anbieters haben. Mit zunehmendem Umfang der bereitgestellten Cloud-Dienste steigen der Verantwortungsbereich und die Einflussmöglichkeiten des Cloud-Nutzers auf die Infrastruktur für die Informations- und Kommunikationstechnologie.

Es wird zwischen Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) und Infrastructure-as-a-Service (IaaS) unterschieden. SaaS-Lösungen beinhalten die Bereitstellung einer vollwertigen Applikation, welche durch den Cloud-Anbieter bewirtschaftet und verwaltet wird. Nutzer einer SaaS-Lösung können mithilfe eines Webbrowsers oder einer Applikation auf dem Endgerät auf Anwendungen von Dritten zugreifen. PaaS-Lösungen umfassen eine komplette Plattform zur Entwicklung, zum Betrieb oder zur Verwaltung von Applikationen, die durch den Cloud-Anbieter verwaltet wird. IaaS-Lösungen umfassen Ressourcen für eine komplette Informatikinfrastruktur, wie zum Beispiel Rechenleistung, Netzwerke oder Speicher.

Die nachfolgende Grafik veranschaulicht die drei Servicemodelle und die dazugehörigen Verantwortungsbereiche.

1 The NIST Definition of Cloud Computing: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Cloud-Akteure

Cloud-Anbieter Der Cloud-Anbieter ist für die Bereitstellung, Wartung und Instandhaltung der Cloud-Dienste verantwortlich, das heisst er ist für die Hard- und Software in Abhängigkeit des Cloud-Servicemodell zuständig.

Cloud-Servicemodell Ein Cloud-Servicemodell repräsentiert ein vordefiniertes Bündel an IT-Ressourcen, welche vom Cloud-Anbieter bereitgestellt werden. Die bekanntesten sind Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Infrastructure-as-a-Platform (IaaS).

Cloud-Implementierungsmodell Ein Cloud-Implementierungsmodell referenziert sich auf die Art der Implementierung des Cloud-Servicemodells. Dies sind Public Cloud, Private Cloud, Community Cloud und Hybrid Cloud.

Cloud-Dienst Ein Cloud-Dienst umfasst die Gesamtheit aller Ressourcen und Dienstleistungen, die ein Cloud-Anbieter dem Cloud-Nutzer über das Internet zur Verfügung stellt respektive anbietet. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschliesslich durch technische Schnittstellen und Protokolle.

Cloud-Nutzer Cloud-Nutzer sind sämtliche Parteien, welche einen Cloud-Dienst nutzen. In diesem Dokument bezieht sich der Begriff auf Ärztinnen und Ärzte und deren beauftragten ICT-Dienstleister.

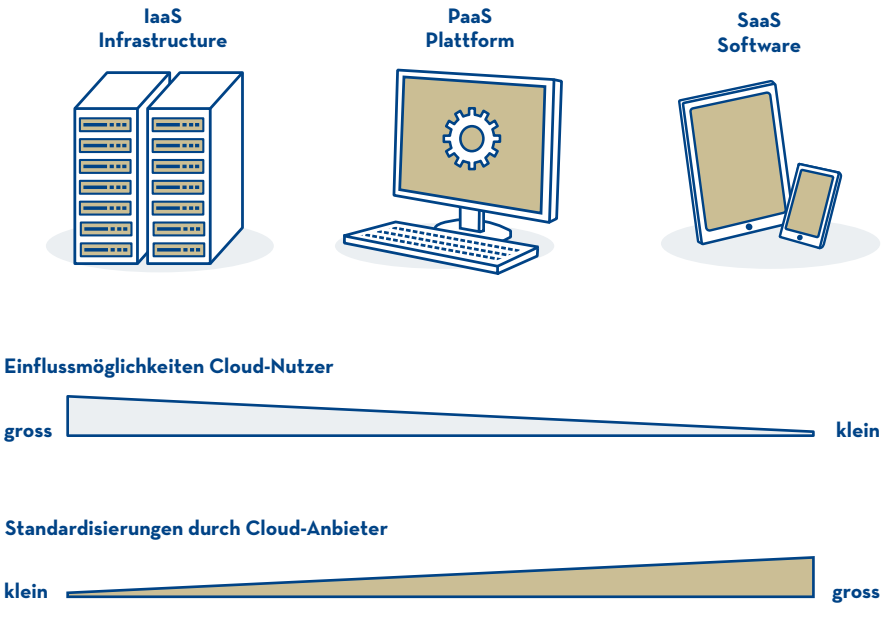


Figure 1
Übersicht Cloud-Service-modelle Anlehnung an Cloud Security Alliance. (CSA)

Verantwortlichkeiten	SaaS	PaaS	IaaS
Daten	○	○	○
Anwendung	●	○	○
Laufzeitumgebung/Container	●	●	○
Betriebssystem	●	●	○
Virtualisierungsschicht	●	●	●
Bereitstellung und Betrieb Hardware	●	●	●
Physische Sicherheit	●	●	●

○ Cloud-Nutzer ● Cloud-Anbieter

Figure 2
Zuständigkeiten Cloud-Nutzer und Cloud-Anbieter in Anlehnung an CSA

Cloud-Implementierungsmodell

Bei der Implementierung von Cloud-Diensten wird zwischen vier Modellen differenziert:

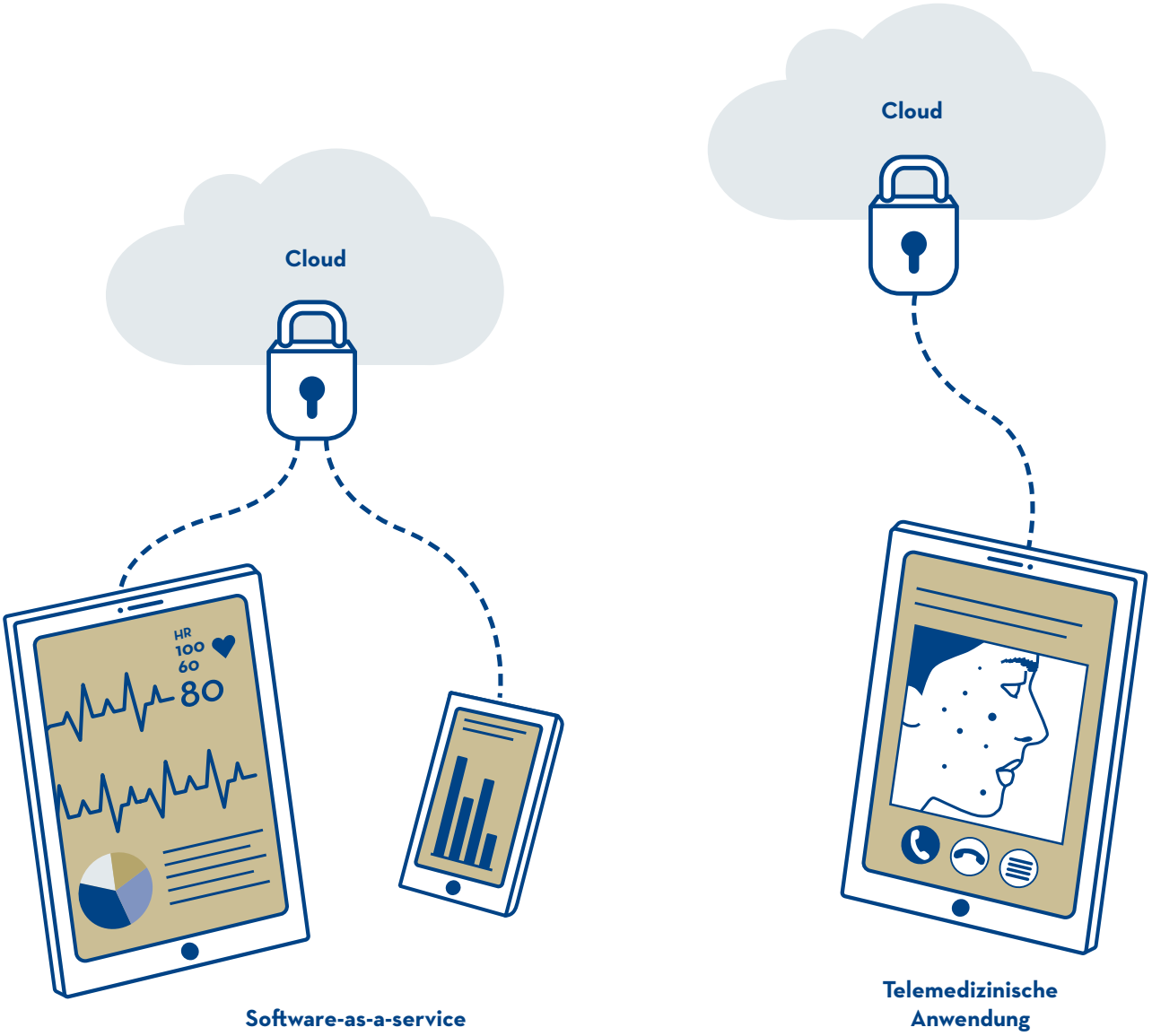
Public Cloud Die Cloud-Infrastruktur ist einer grossen Anzahl Nutzern oder einer grösseren Industriegruppe zugänglich und im Besitz einer Organisation, welche Cloud-Dienste anbietet. Beispiele sind Dropbox, Google Drive oder Microsoft Office 365.

Private Cloud Die Cloud-Infrastruktur wird für ein bestimmtes Unternehmen betrieben. Sie wird entweder vom Unternehmen selbst oder von einem beauftragten Dritten administriert, wobei die Infrastruktur innerhalb oder ausserhalb des Unternehmens lokalisiert sein kann.

Community Cloud Die Cloud-Infrastruktur ist für einen Verbund von Unternehmen, die gemeinsame Interessen (beispielsweise gleiche Branche oder gleiche Sicherheitsanforderungen) haben, betrieben und wird entweder von einem verbundenen Unternehmen oder beauftragten Dritten administriert, wobei die Infrastruktur innerhalb oder ausserhalb der Unternehmen lokalisiert sein kann.

Hybrid Cloud Die Cloud-Infrastruktur ist eine Mischform aus den oben beschrieben Implementierungsmodellen. Der Begriff Hybrid Cloud wird auch verwendet, wenn es um Lösungen geht, welche sowohl On-Premise- wie auch cloudbasierte Komponenten beinhalten.

A1 Applikation und Schnittstellen

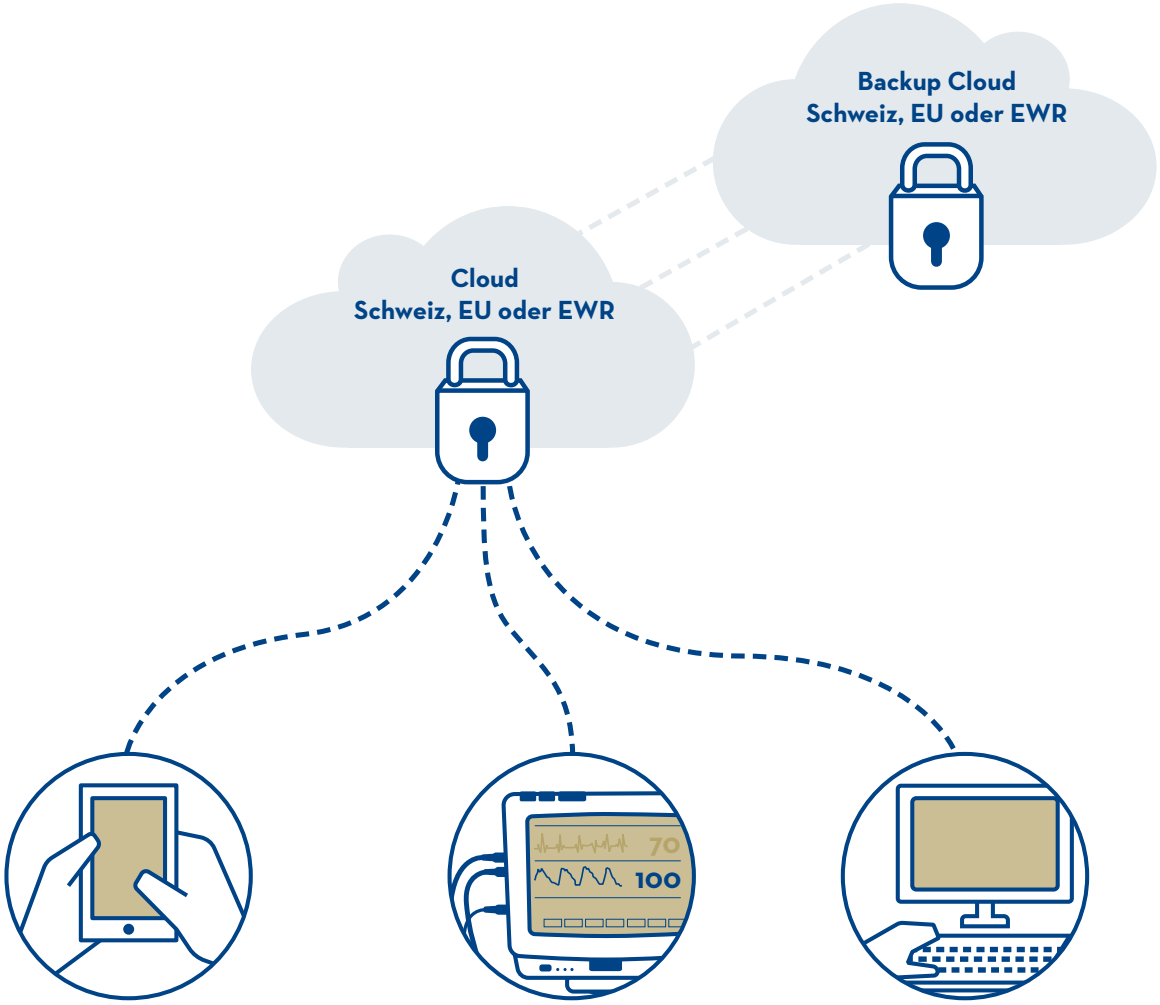


Secure Development Life Cycle (SDLC) hat bei der Migration und Bereitstellung von Anwendungen in der Cloud zunehmend an Bedeutung gewonnen. Cloud-Anbieter sollten sicherstellen, dass Best Practices im Bereich der Informationssicherheit sowohl für die Applikation selbst als auch für die Schnittstellen während des gesamten Lebenszyklus der Anwendungen integriert sind.

Anforderungen

A-1.01	M	**Anforderung an Schnittstellen** Anwendungen und Application Programming Interfaces (API) müssen gemäss Sicherheitsstandards (z. B. OWASP für Webanwendungen) entworfen, entwickelt, bereitgestellt und getestet werden.
A-1.02	S	**Aufruf Webservice** Der Aufruf eines Webservice von einem Client soll über ein Gateway mit Application Firewall und API Management erfolgen.

A2 Audit Assurance und Compliance



Der Bereich Audit Assurance und Compliance thematisiert die Einhaltung der geltenden Gesetzgebung, die Einhaltung von geltenden internen Vorgaben, anerkannten Standards, beispielsweise ISO 27001 sowie die Sicherstellung von Compliance während eines Audits.

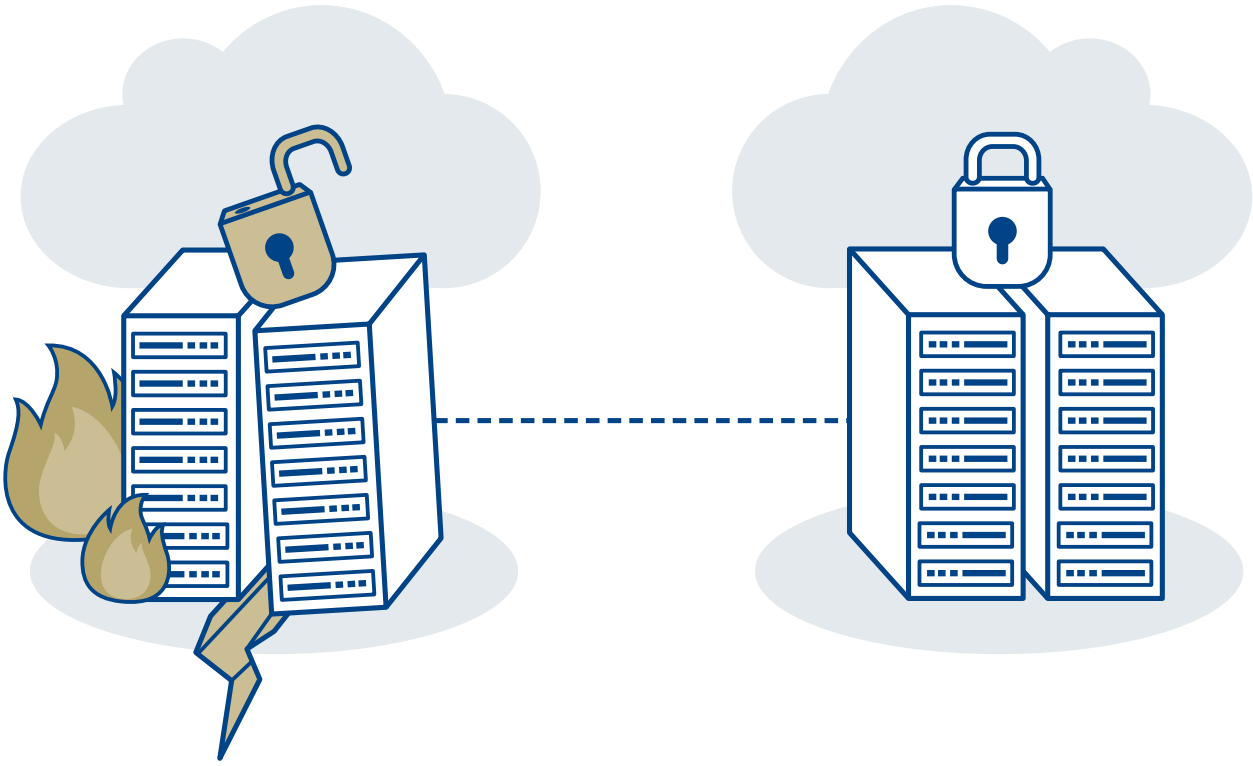
Gesetzliche Vorgaben, welche im Zusammenhang mit der Nutzung von Cloud-Diensten berücksichtigt werden müssen, sind das Bundesgesetz über den Datenschutz (DSG), insbesondere Art. 10a DSG, Datenbearbeitung durch Dritte. Gemäss diesem Artikel darf die Bearbeitung von Personendaten an Dritte übertragen werden, sofern die nachfolgenden Kriterien erfüllt sind:

- Es besteht keine gesetzliche oder vertragliche Geheimhaltungsverpflichtung, welche die Auslagerung verbietet.
- Der Cloud-Anbieter bearbeitet die Daten nur so, wie es der Cloud-Nutzer (Ärztin oder Arzt) selbst tun dürfte.
- Der Cloud-Nutzer muss sicherstellen, dass die Datensicherheit beim Cloud-Anbieter gewährleistet wird.
- Die Einhaltung der vertraglichen Vereinbarung muss regelmässig geprüft werden.

Anforderungen

A-2.01	M	**Ort der Datenhaltung inklusive Backups** Die Datenhaltung des Systems muss den gesetzlichen Anforderungen gemäss Art. 6 DSG (grenzüberschreitende Bekanntgabe) entsprechen. Die Datenhaltung und -verarbeitung muss innerhalb der Schweiz, der Europäischen Union oder im Europäischen Wirtschaftsraum erfolgen.
A-2.02	S	**Rechtsicht und Gerichtsbarkeit Cloud-Anbieter** Der Cloud-Anbieter soll den Gerichtsstand geografisch in der Schweiz oder in der Europäischen Union haben.
A-2.03	M	**Offenbarungs- und Ermittlungsbefugnisse (Dateneinsicht durch staatliche Akteure)** Der Cloud-Anbieter muss transparente Angaben über die Offenbarungs- und Ermittlungsbefugnisse, welche den staatlichen Akteuren eingeräumt werden, bekannt geben.

A3 Business Continuity Management



Im Bereich Business Continuity Management liegt der Fokus auf der Aufrechterhaltung und Wiederherstellung von kritischen Geschäftsprozessen bei Ausfall von IT-Systemen oder im Katastrophenfall, um die Geschäftstätigkeit möglichst zeitnah wieder aufnehmen zu können. Das Business Continuity Management (BCM) liegt im Zuständigkeitsbereich des Cloud-Anbieters und muss in seiner Wirkungsweise und Vollständigkeit nachgewiesen werden. Ein starker Indikator hierfür ist die nachgewiesene Zertifizierung nach ISO 22301.

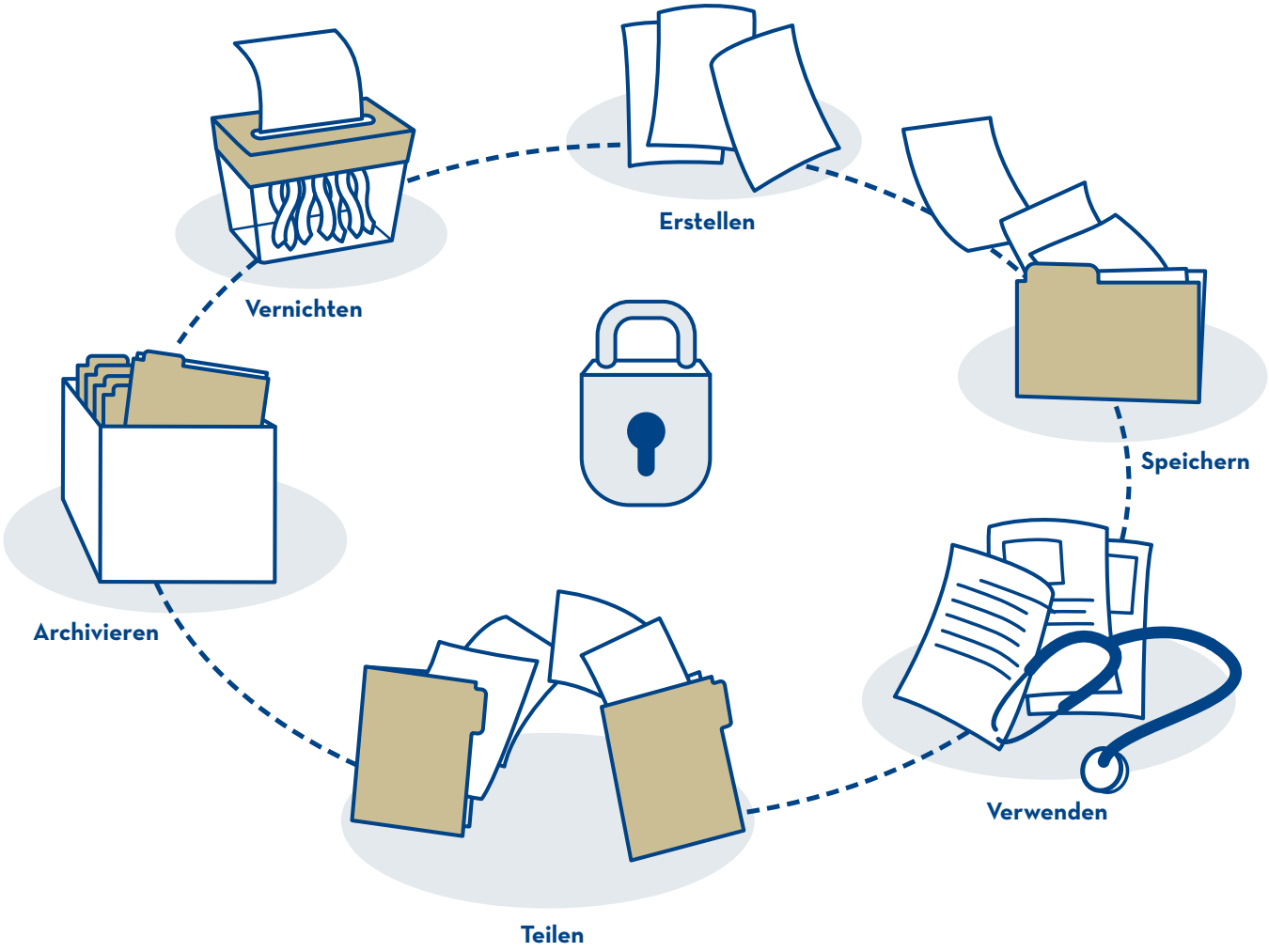
Die Wiederherstellung von Daten und Anwendungen (Disaster Recovery Planning) ist im Fall eines Verlusts von Daten oder Ausfalls von IT-Systemen ebenso von zentraler Bedeutung. Dazu benötigt der Cloud-Anbieter eine Datensicherungsstrategie (Backup-Strategie), da er für das Backup und die Wiederherstellung zuständig ist. Die Einzelheiten zum Thema Backup sind im Rahmen des SLA[2] zwischen Cloud-Anbieter und der Ärztin oder dem Arzt zu regeln.

2 Vgl. dazu auch «Rahmenvertrag für Cloud-Services» der FMH: www.fmh.ch/themen/ehealth/praxisinformatik.cfm#i137104

Anforderungen

A-3.01	M	**Datensicherung und Datenwiederherstellungs-Prozesse** Die Verfahren zur Datensicherung (Backup) und Datenwiederherstellung (Restore) müssen definiert und dokumentiert sowie an die Anforderungen des Endkunden angepasst sein. Die Restore-Prozesse müssen regelmässig überprüft werden, ein Testprotokoll muss dem Endbenutzer auf Anfrage zur Verfügung gestellt werden. Die Datensicherung muss in verschlüsselter Form erfolgen und dem aktuellen Stand der Technik entsprechen.
A-3.02	M/S	**Business Continuity Management** Der Cloud-Anbieter muss gegenüber dem Cloud-Nutzer nachweisen, dass der Cloud-Dienst über ein effektives Business Continuity Management verfügt. Beispielsweise soll er dies über eine Zertifizierung gemäss ISO 22301 nachweisen.

A4 Datensicherheit und Information Lifecycle Management

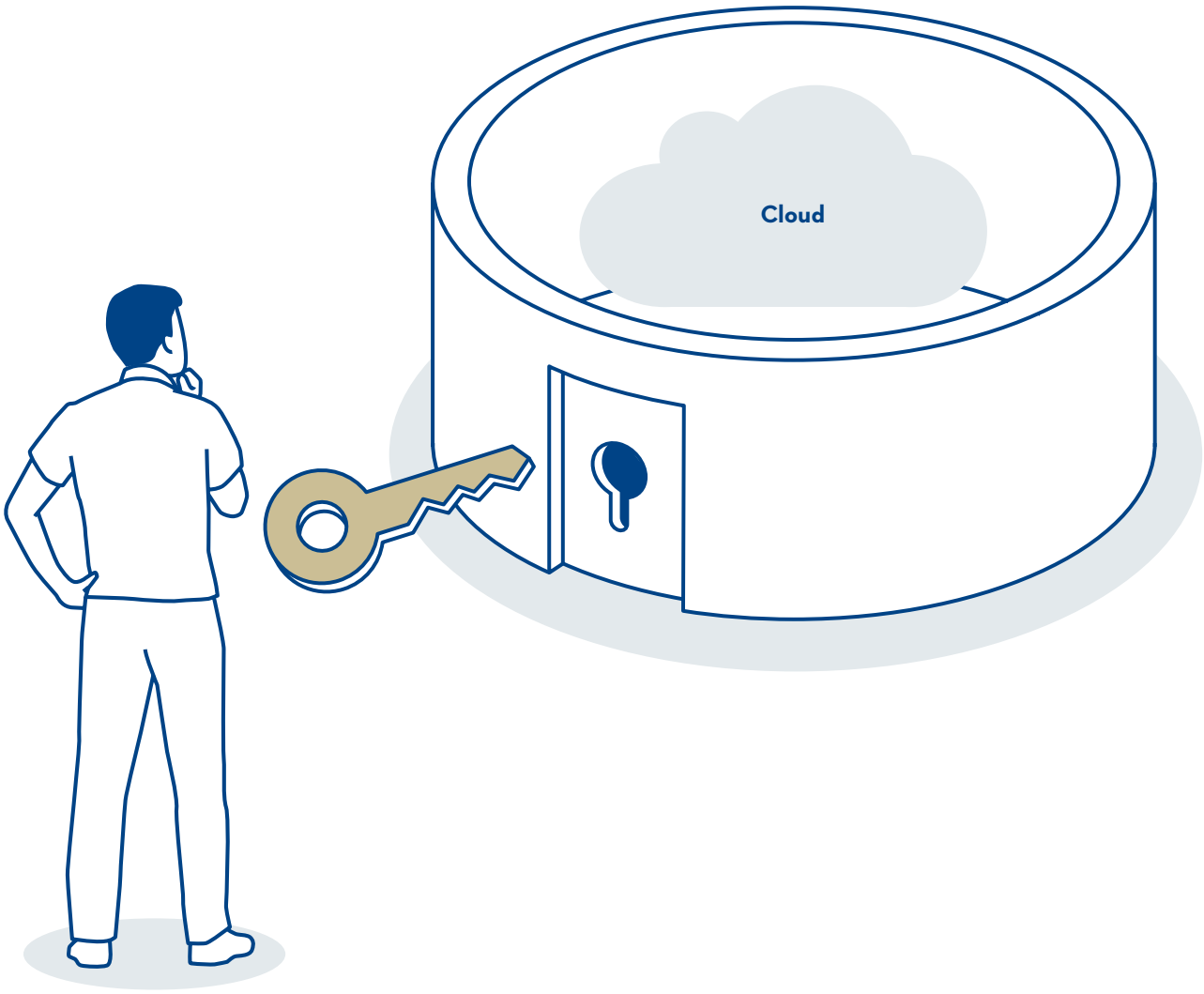


Information Lifecycle Management ist ein umfassender Ansatz zur Verwaltung der Daten einschliesslich der zugehörigen Metadaten. Es ist sicherzustellen, dass die gesetzlichen Vorgaben der Daten über den gesamten Lebenszyklus, das heisst von der Erfassung bis hin zur Löschung oder Archivierung, eingehalten werden. Diese Vorgaben betreffen beispielsweise die gesetzlichen (kantonalen) Aufbewahrungs- und Verjährungsfristen für Krankengeschichten oder das in der europäischen Datenschutzgrundverordnung verankerte Recht auf Portabilität der Daten oder das Recht auf Vergessen.

Anforderungen

A-4.01	M	**Portabilität und Export von Daten** Es muss in regelmässigen Abständen oder bei Vertragsende möglich sein, die Daten in weiterverarbeitbare elektronische Standardformate zu exportieren. Im Optimalfall verfügt der Cloud-Dienst über eine Funktionalität, wodurch der Datenexport ohne Beteiligung des Cloud-Anbieters erfolgen kann.
A-4.02	M	**Datenlöschung** In den folgenden Fällen muss der Cloud-Anbieter unter der Berücksichtigung der Aufbewahrungspflicht eine vollständige Löschung der Inhalts- und Randdaten inklusive der Datensicherungskopien (Backups) des Cloud-Nutzers vornehmen: – beim Wechsel der Speichermedien zu Wartungszwecken – auf Verlangen des Cloud-Nutzers – bei Beendigung des Vertragsverhältnisses Die dafür eingesetzte(n) Methode(n), beispielsweise durch mehrfaches Überschreiben der Daten oder Löschen des Schlüssels, verhindert(n) eine Wiederherstellung der Daten mit forensischen Mitteln.
A-4.03	M	**Auskunftsbegehren** Der Cloud-Nutzer muss sicherstellen, dass der Cloud-Anbieter die Begehren auf Auskunft gemäss Art. 8 DSG und Widerruf der Einwilligung für die Datenbearbeitung sicherstellen kann, sodass der Cloud-Anbieter über sämtliche bei ihm vorhandenen Personendaten Auskunft geben kann oder im Fall eines Widerrufs die Personendaten vollständig gelöscht werden.

A5 Physische Sicherheit

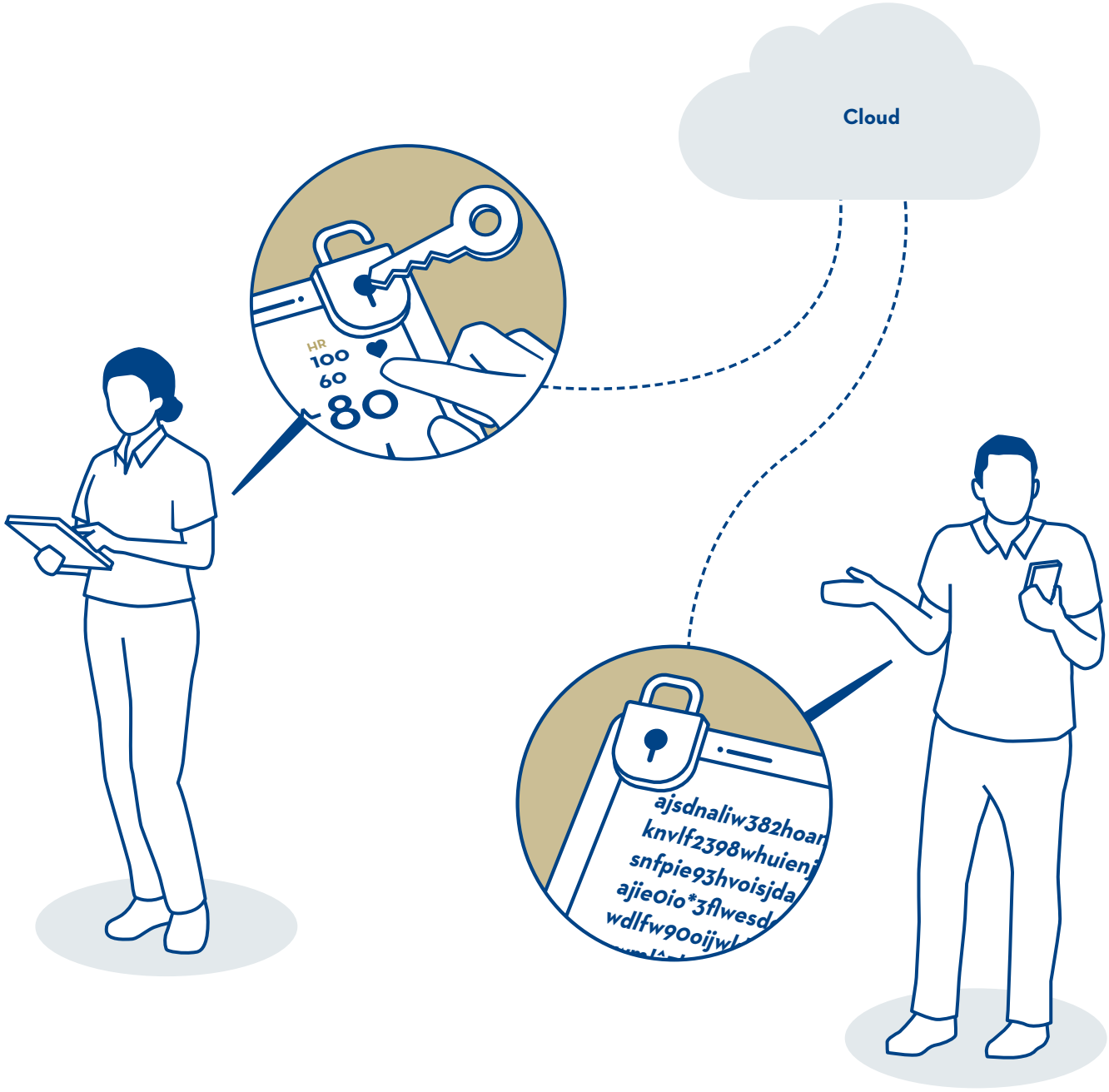


Um eine angemessene physische Sicherheit zu gewährleisten, ist es wichtig, dass die Verantwortlichkeiten der Mitarbeitenden des Cloud-Anbieters klar definiert sind und entsprechende Massnahmen zum physischen Schutz des Rechenzentrums implementiert sind.

Anforderungen

A-5.01	**M**	**Physischer Zugriff auf Datenzentrum** Der physische Zugriff von Benutzern und Support-Mitarbeitern des Cloud-Anbieters auf Informationsressourcen muss eingeschränkt sein. Es müssen physische Sicherheitsmassnahmen implementiert sein. Beispiele hierfür sind physische Authentifizierungsmechanismen und elektronische Überwachungs- und Alarmierungssysteme.

A6 Verschlüsselung und Schlüsselmanagement



Unverschlüsselte Daten in der Cloud oder zu weit gefasste Zugriffsrechte können die Vertraulichkeit, Integrität und Verfügbarkeit der Daten gefährden. Um das Risiko einer Verletzung der Vertraulichkeit und Integrität der Daten zu mindern, müssen die gespeicherten Daten (Data at Rest) sowie die übertragenen Daten (Data in Transit) mit kryptografischen Verfahren entsprechend geschützt werden.

Anforderungen

A-6.01	M	**Speicherverschlüsselung der Inhaltsdaten (Data at Rest)** Die Daten beim Cloud-Anbieter müssen in jeder Phase des Lebenszyklus der Daten verschlüsselt gespeichert werden. Die für die Verschlüsselung verwendeten privaten Schlüssel dürfen ausschliesslich dem Cloud-Nutzer bekannt gemacht werden. Der Cloud-Anbieter darf keine Möglichkeiten haben, die Daten einzusehen.
A-6.02	M	**Schlüsselmanagement** Es muss ein effektives Recovery-Verfahren existieren, um im Notfall die verschlüsselten Daten wiederherzustellen. Falls es notwendig ist, den Schlüssel wiederzubeschaffen, existiert ein effektives Recovery-Verfahren. Eine Möglichkeit ist es, dafür Teilschlüssel an verschiedene Akteure zu verteilen, welche im Tresor verwahrt werden und im Notfall nach einem Konsensverfahren verwendet werden.
A-6.03	M	**Transportverschlüsselung (Data in Transit)** Die Kommunikation muss über ein aktuelles Internet-Standardprotokoll erfolgen. Die Kommunikation über alle ein- und ausgehenden Verbindungen zur und von der Cloud-Infrastruktur einschliesslich der Schnittstellen innerhalb der Cloud-Infrastruktur muss authentisiert und verschlüsselt erfolgen. Die Kommunikation muss mindestens mit TLS 1.2 verschlüsselt werden.
A-6.04	M	**Verschlüsselungsverfahren** Es müssen Verschlüsselungsverfahren gemäss den aktuellen Best-Practice-Ansätzen eingesetzt werden. Die nachfolgenden Verfahren oder gleichwertige Verfahren sind zugelassen. – Hashing-Verfahren: SHA2-256, SHA2-384, SHA2-512 oder SHA3-256, SHA3-384, SHA3-512 – Symmetrische Verfahren: AES-256 – Asymmetrische Verfahren: RSA-2048, ECDSA-224 oder Ed25519 Adaptierte Verfahren oder Eigenentwicklungen sind nicht zugelassen. Es sind aktuelle Protokolle zu verwenden. Protokolle mit bekannten kritischen Sicherheitslücken dürfen nicht eingesetzt werden.

A7 Governance und Risikomanagement

Governance (Steuerung) der Datensicherheit und des Datenschutzes umfasst die Bereiche Vorgaben, Prozesse und interne Kontrolle zur Validierung, ob die Vorgaben betreffend Datenschutz und Datensicherheit durch den Cloud-Anbieter eingehalten werden. Der Cloud-Anbieter legt offen, ob er über ein funktionierendes Informationssicherheitsmanagementsystem (ISMS) verfügt. Die Trennung der Verantwortlichkeiten sowohl für den Datenschutz und die Datensicherheit als auch das Risikomanagement zwischen dem Cloud-Nutzer und dem Cloud-Anbieter hängen vom gewählten Servicemodell ab.

Anforderungen

A-7.01	S	**Transparenz Zertifizierungen** Der Cloud-Anbieter soll vorhandene Zertifikate und vorhandene Auditberichte zur Verfügung stellen: – Zertifizierung nach ISO/IEC 27001 – Prüfberichte nach ISAE340, SSAE16 oder SOC2-Berichte – von den zuständigen Datenschutzbehörden akzeptierter Nachweis über die Einhaltung des Datenschutzes
A-7.02	M	**Auditrecht** Sofern keine Auditberichte von Drittparteien vorgelegt werden können, muss dem Cloud-Nutzer durch den Cloud-Anbieter vertraglich zugesichert werden, dass der Cloud-Nutzer selbst oder durch einen beauftragten Dritten die Durchführung von Audits oder von technischen Überprüfungen (z. B. Penetrationtests) vornehmen kann.
A-7.03	M	**Service Level Agreement (SLA)** Das SLA zwischen Cloud-Anbieter und Cloud-Nutzer muss das Service Level für den Endkunden (die Arztpraxis) abdecken.
A-7.04	S	**SLA-Reporting** Der Cloud-Anbieter soll auf Anfrage einen Bericht zur Verfügung stellen, in welchem mindestens folgende Angaben enthalten sind: – Kennzahlen über die definierte Verfügbarkeit, Performance oder Datenkapazität des Dienstes – Ansprechzeiten und Reaktionszeiten der Serviceorganisation des Anbieters – Definition von Wartungsfenstern und weiteren geplanten Ausfallzeiten – Definition von Frequenz und Qualität der Wartungsprozesse – Definition der gelieferten Artefakte wie Testberichte oder Backupmedien – Massnahmen und Konsequenzen bei Nichteinhaltung der Vereinbarungen – Ereignisse und Vorfälle in der Berichtsperiode
A-7.05	M	**Subdienstleister** Der Cloud-Anbieter muss alle Subdienstleister gegenüber dem Cloud-Nutzer sowie ein Nachweis der Geheimhaltungsverpflichtung offenlegen.[3]
A-7.06	M	**Notifikation bei geplanten Ausfällen** Der Cloud-Anbieter muss den Cloud-Nutzer über geplante Ausfälle mindestens zehn Arbeitstage im Voraus per E-Mail informieren.

3 Siehe auch: Rahmenvertrag Cloud Services www.fmh.ch/themen/ehealth/praxisinformatik.cfm#i137104 und darin enthaltene Anhänge

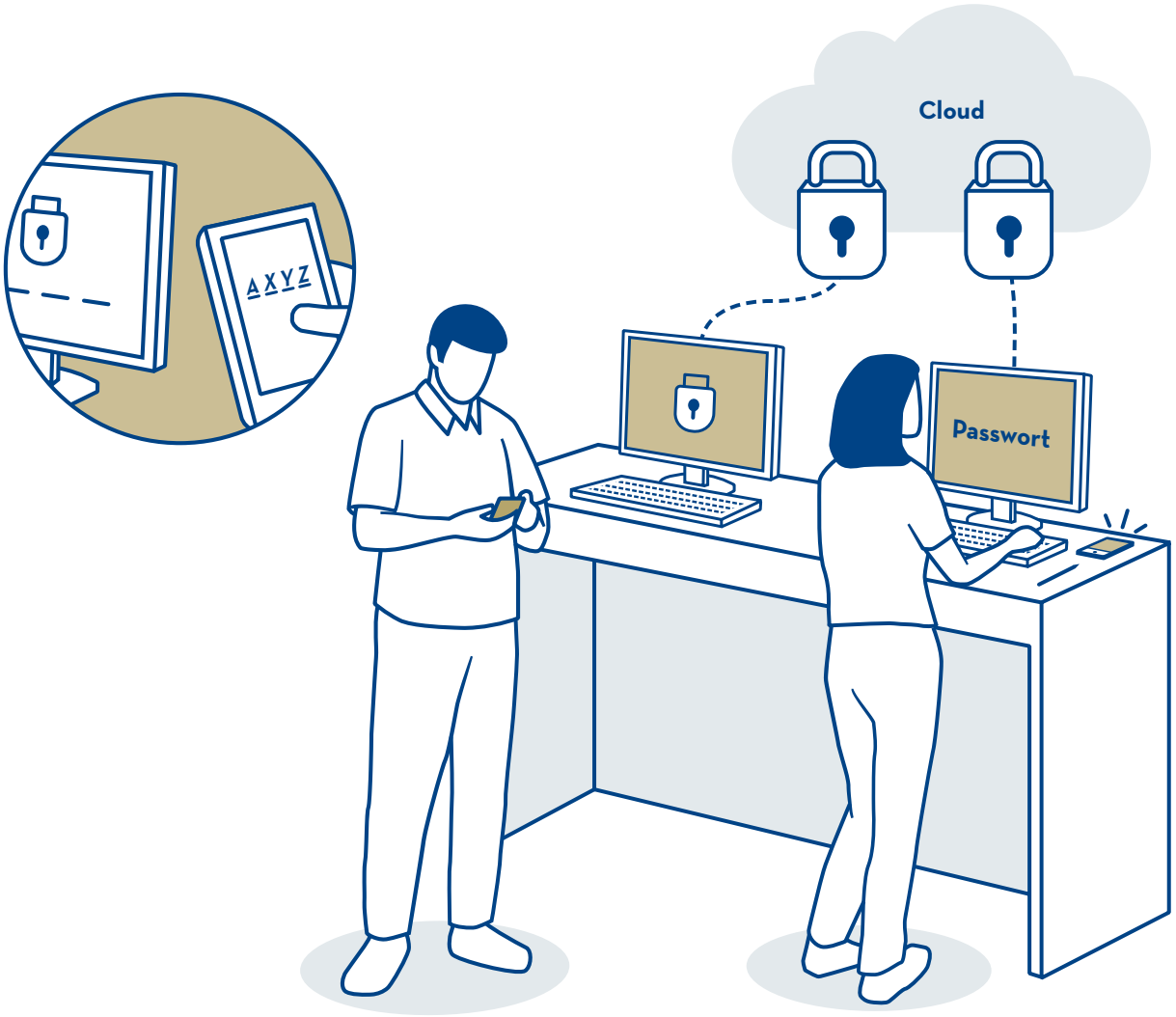
A8 Personal

Das Personal spielt im Bereich der Informationssicherheit eine wichtige Rolle. Der Zweck dieser Anforderungen ist es, das Risiko zu minimieren, dass das Personal des Cloud-Anbieters die Vertraulichkeit, Verfügbarkeit oder Integrität der Daten gefährdet.

Anforderungen

A-8.01	M	**Arbeitsverträge** Arbeitsverträge des Cloud-Anbieters müssen Bestimmungen für die Einhaltung von Richtlinien für Datenschutz und Informationssicherheit enthalten.
A-8.02	M	**Schulung und Sensibilisierung** Die Mitarbeitenden des Cloud-Anbieters müssen eine regelmässige Schulung und Sensibilisierung in Bezug auf Datenschutz und Informationssicherheit erhalten.

A9 Identitäts- und Zugriffsmanagement

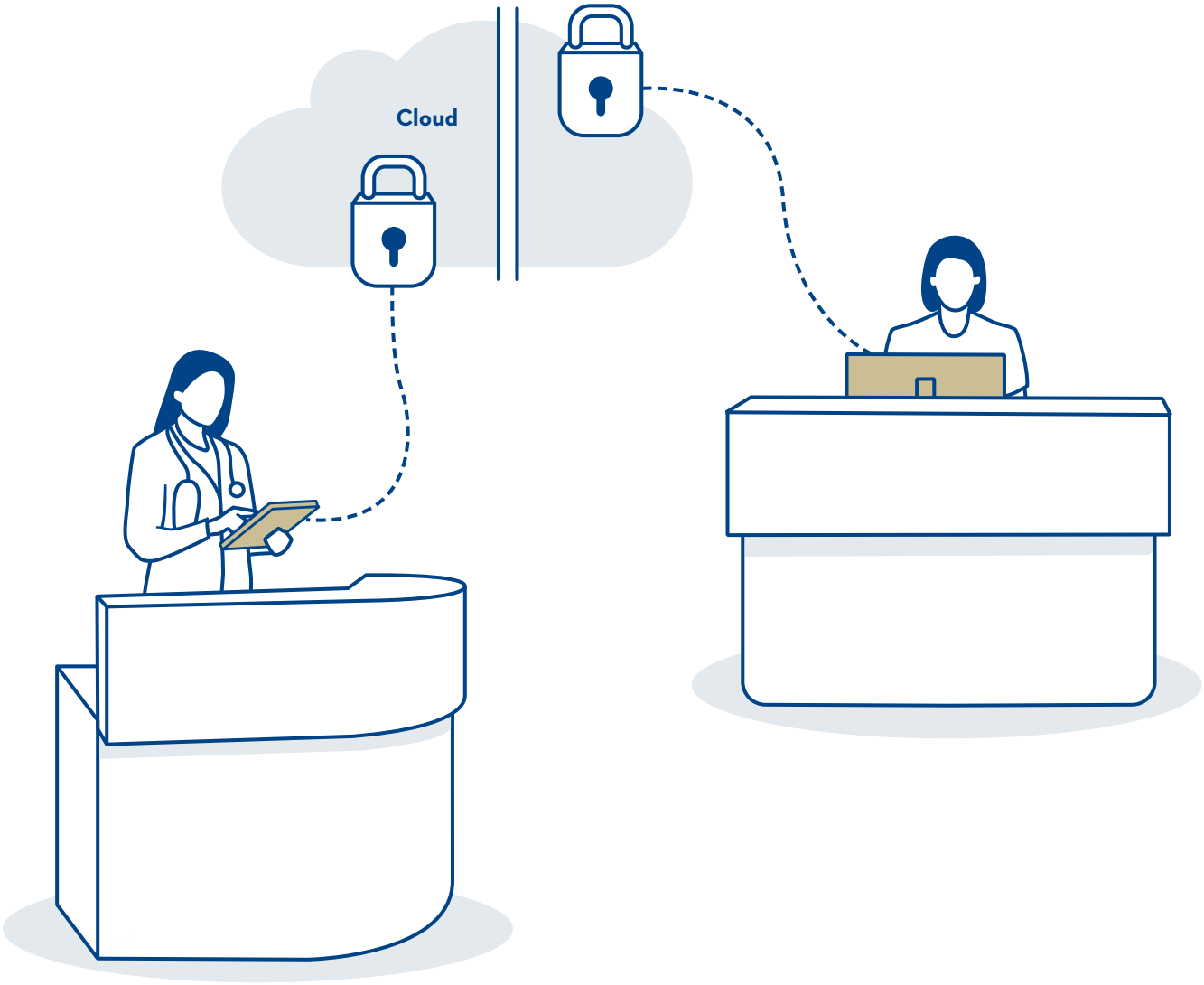


Die Kontrolle über den Zugriff auf die Daten ist eine effektive Massnahme zum Schutz vor unerlaubter Ansicht von sensitiven Informationen und zum Schutz der Datenintegrität. Dabei sind Grundsätze, wie das «Need to know»- oder das «Least Privilege»-Prinzip zu berücksichtigen. Die Umsetzung der Authentifizierung kann über Ein- oder Mehrfaktorverfahren erfolgen.

Anforderungen

A-9.01	M	**Authentifizierung Benutzer (Cloud-Nutzer)** Die Authentifizierung der Cloud-Nutzer muss über eine Multi-Faktor-Authentifizierung erfolgen.
A-9.02	M	**Authentifizierung Administratoren (Cloud-Nutzer)** Die Authentifizierung der Cloud-Administratoren muss über eine Multi-Faktor-Authentifizierung erfolgen.
A-9.03	M	**Wiederherstellung von Zugriffsdaten** Ein effektiver Prozess für die Wiederherstellung der Zugriffsdaten muss als Fallback zur Verfügung stehen.
A-9.04	S	**Identity Provider** Es soll sichergestellt sein, dass die Einbindung eines externen Identity Provider in die Cloud-Lösung möglich ist.
A-9.05	S	**Single Sign-on** Für zusätzliche Sicherheit und erhöhte Benutzbarkeit soll ein Single Sign-on-Protokoll wie OAuth 2.0 unterstützt werden.
A-9.06	M	**Anbindung Identity-Store an das Active Directory (AD) der Arztpraxis** Eine Anbindung an den Identity Store der Arztpraxis muss möglich sein, sofern ein solcher vorhanden ist. Die Anbindung ist dabei so auszugestalten, dass dem Cloud-Anbieter nur die notwendigen Daten («Need to know»-Prinzip) zur Verfügung gestellt werden. AD-Passwörter sollen dabei nicht beim Cloud-Anbieter gespeichert werden.
A-9.07	S	**Authentifizierung Maschine zu Maschine** Zur Authentifizierung von Maschine zu Maschine soll ein zertifikatbasiertes Verfahren eingesetzt werden.
A-9.08	M	**Zugriff durch Administratoren des Cloud-Anbieters** Es muss sichergestellt sein, dass die Administratoren des Cloud Anbieters keinen Zugriff auf die unverschlüsselten Daten des Cloud-Nutzers haben.
A-9.09	M/S	**Zugriff zu Administration** Die administrativen Zugriffe durch den Cloud-Anbieter sollen aus einem dedizierten Netz erfolgen oder müssen mittels Multi-Faktor-Authentifizierung gesichert sein. Sämtliche administrative Zugriffe müssen protokolliert und bei Bedarf durch den Cloud-Nutzer eingesehen werden können.

A10 Sicherheit der Cloud-Infrastruktur und der Virtualisierungsumgebung



Die Sicherheit der Cloud-Infrastruktur und Virtualisierungsumgebung umfasst die Themen Netzwerksicherheit, Schutz der Auslastung sowie die Sicherheit von Hypervisor, Container und softwarebasierten Netzwerken.

Anforderungen

A-10.01	M	**Getrennte Datenhaltung** Der Cloud-Anbieter muss aufgrund der gewählten Architektur und den zur Verfügung gestellten Dokumenten glaubhaft darlegen, dass der angebotene Cloud-Dienst eine angemessene logische Trennung der Daten von den Daten anderer Cloud-Nutzern sicherstellt (Mandantentrennung). Der Cloud-Anbieter muss im Vorfeld für technische Fragestellungen einen geeigneten Ansprechpartner zur Verfügung stellen. Folgende Dokumentationen sollen durch den Cloud-Anbieter zur Verfügung gestellt werden: – Systemarchitektur – Systemdokumentation – Betriebshandbuch – Sicherheitskonzept – Notfall-/BCM-Konzept
A-10.02	M	**Netzwerksicherheit** Zum Schutz des Netzwerkes muss der Cloud-Anbieter – eine Firewall, – Intrusion-Detection- und Intrusion-Prevention-Systeme, – eine Application Firewall (XML/WAF) sowie – einen «Distributed Denial of Service»-Schutz vorsehen.
A-10.03	M	**Schutz vor Schadsoftware** Der Cloud-Anbieter muss zum Schutz vor Schadsoftware Antiviren-Software und/oder Intrusion-Detection-Systeme auf der Ebene des Servicemodells sowie des Netzwerkperimeters vorsehen.

A11 Interoperabilität und Portabilität der Anwendungskomponenten

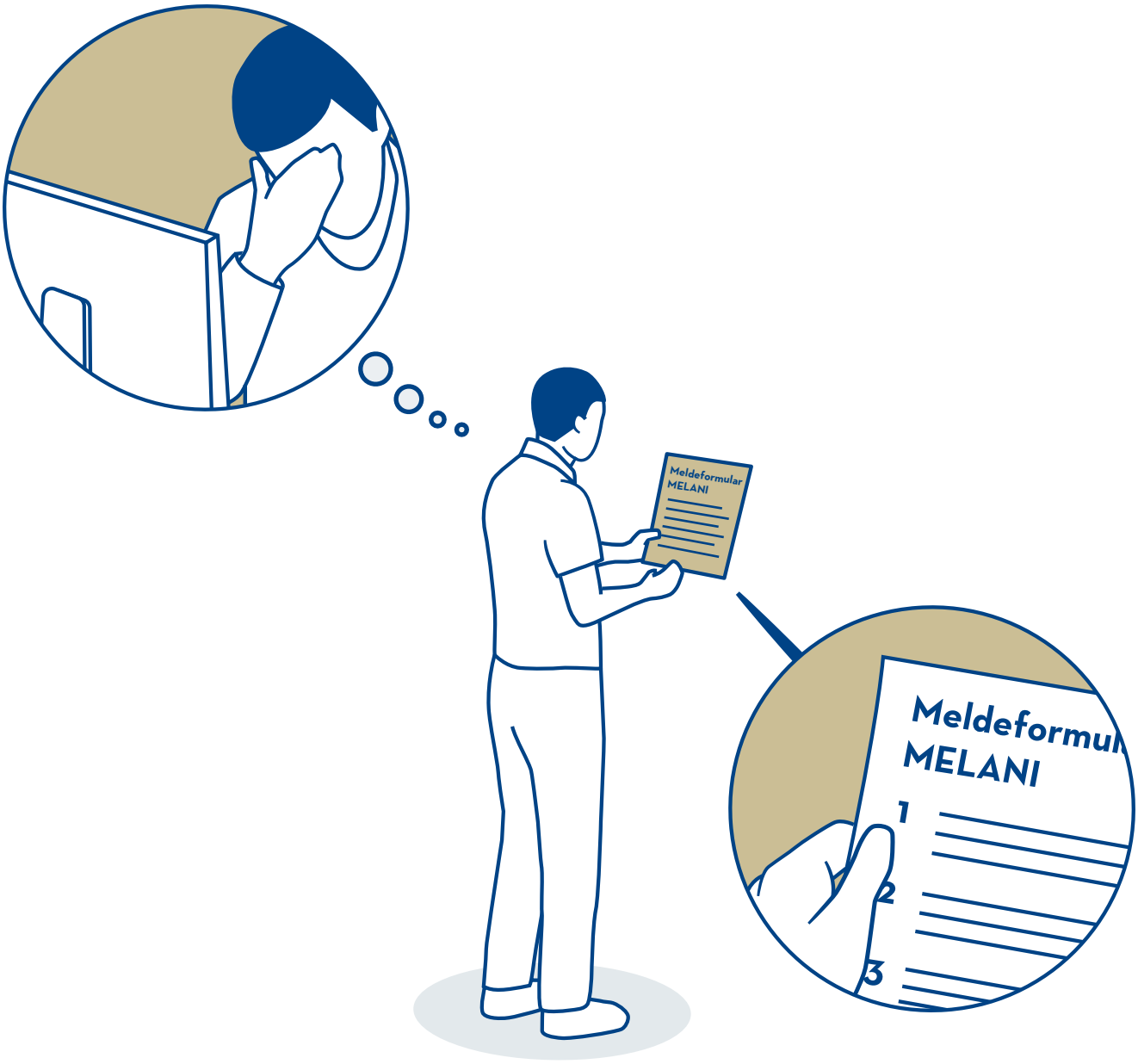
Interoperabilität ist die Voraussetzung dafür, dass die Komponenten eines Cloud-Ökosystems zusammenarbeiten können. In einem solchen Ökosystem können die Komponenten aus verschiedenen Quellen stammen, sowohl aus der Cloud als auch aus herkömmlichen On-Premise-Komponenten. Interoperabilität verlangt, dass diese Komponenten durch neue oder andere Komponenten von verschiedenen Anbietern ersetzt werden können und weiterhin funktionieren.

Die Portabilität definiert die einfache Möglichkeit, Anwendungskomponenten an einen anderen Ort zu verschieben und wiederzuverwenden, unabhängig von Anbieter, Plattform, Betriebssystem, Infrastruktur, Standort, Speicher, Datenformat oder APIs.

Anforderungen

A-11.01	M	**Virtualisierung** Der Cloud-Anbieter muss eine etablierte Virtualisierungsplattform und Standard-virtualisierungsformate (z. B. OVF) verwenden, um die Interoperabilität sicherzustellen.
A-11.02	S	**APIs** Der Cloud-Anbieter soll offene und veröffentlichte APIs verwenden, um die Interoperabilität zwischen Komponenten zu unterstützen und die Migration von Anwendungen zu erleichtern.
A-11.03	M	**Standardisierte Netzwerkprotokolle** Der Cloud-Anbieter muss sichere, standardisierte Netzwerkprotokolle für den Import und Export von Daten und zur Verwaltung des Dienstes verwenden. Der Cloud-Anbieter muss eine Übersicht der verwendeten Interoperabilitäts- und Portabilitätsstandards zur Verfügung stellen.

A12 Incident Management, E-Discovery und Cloudforensik

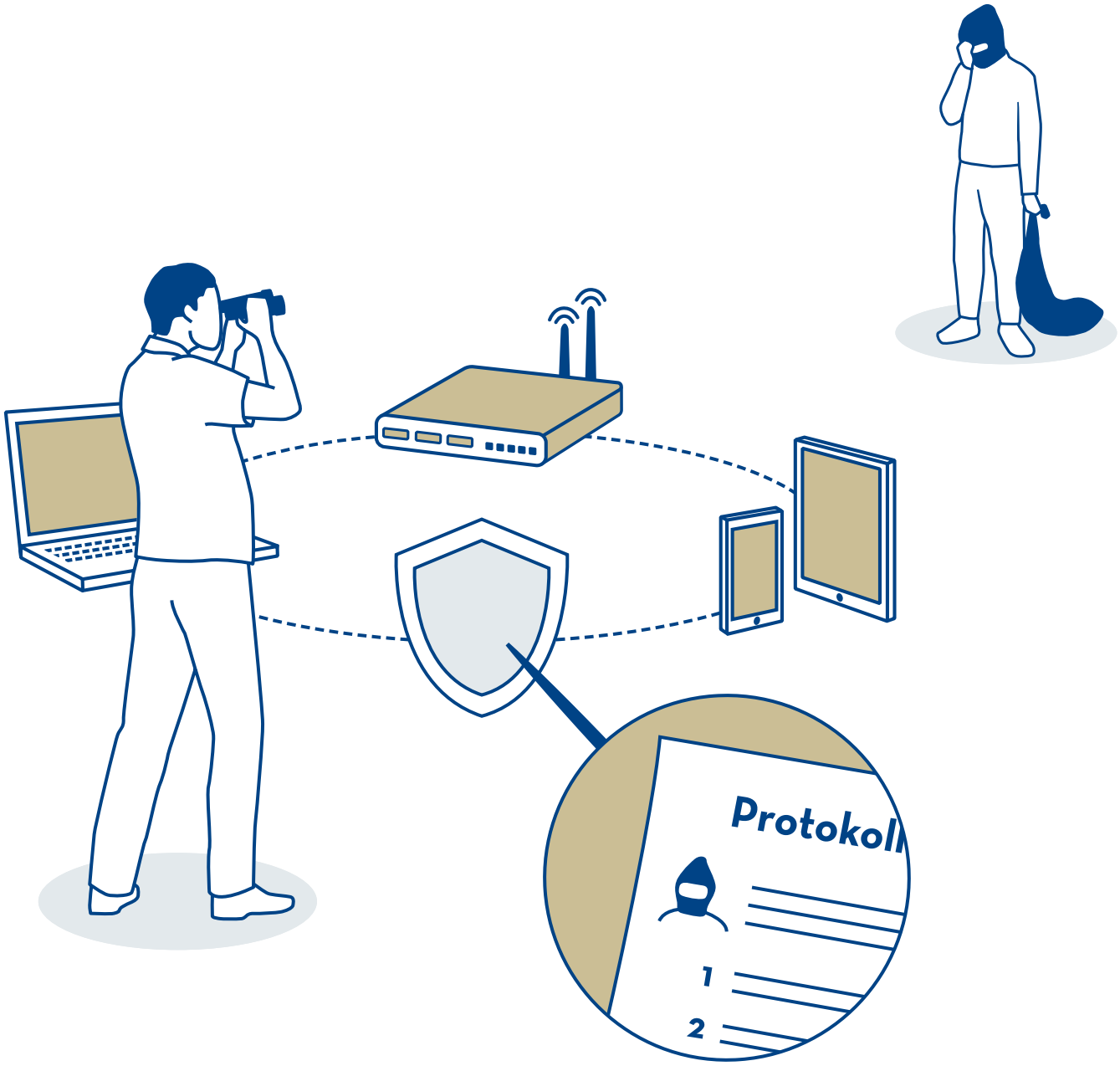


Unter dem Begriff Security Incident Management ist die Erkennung, Behandlung, Notifikation und Behebung von Sicherheitsvorfällen zu verstehen.

Anforderungen

A-12.01	M/S	**Security Incident Management Cloud-Anbieter** Der Cloud-Anbieter muss ein Security Incident Management vorweisen können. Hierzu soll der Cloud-Anbieter beispielsweise eine Zertifizierung nach ISO/IE 27035 vorweisen können.
A-12.02	M	**Meldung von Sicherheitsvorfällen** Der Cloud-Anbieter muss den Cloud-Nutzer über detektierte Sicherheitsvorfälle, welche den Cloud-Nutzer betreffen könnten, innert 72 Stunden informieren.
A-12.03	M/S	**Kontaktstelle für Sicherheitsvorfälle** Der Cloud-Anbieter muss dem Cloud-Nutzer eine bezeichnete Kontaktstelle für Sicherheitsvorfälle bekannt geben.

A13 Bedrohungs- und Schwachstellenmanagement



Um den Befall von Malware der IT-Infrastruktur, der Systemkomponenten und der Endgeräte zu vermeiden, sind Vorgaben zum Schutz sowie Prozesse zur Überwachung notwendig.

Anforderungen

A-13.01	M/S	**Nachweis über technische Überprüfung (z. B. Schwachstellen-Scan oder Penetrationstest)** Der Cloud-Anbieter muss regelmässig eine technische Überprüfung durch eine unabhängige Stelle durchführen. Er soll die Ergebnisse auf Anfrage des Cloud-Nutzers zur Verfügung stellen. Diese technische Überprüfung soll mindestens jährlich stattfinden.
A-13.02	S	**Aufzeichnung von sicherheitsrelevanten Ereignissen** Der Cloud-Dienst soll mindestens die Aufzeichnung der nachfolgenden Informationen für sicherheitsrelevante Ereignisse zulassen: – Zugriffsentscheidungen – Lastverhalten – Veränderungen an Nutzdaten
A-13.03	S	**Aufbewahrung der Protokolldaten** Der Cloud-Anbieter soll sämtliche Protokolle mindestens sechs Monate[4] aufbewahren und dem Cloudanbieter zur Einsicht zur Verfügung stellen können. Die sechs Monate gelten, sofern keine andere gesetzliche Regelung besteht. Weiter ist zu beachten, dass die Regelung gemäss A-4.02 bezüglich Datenlöschung auch für die Protokolldaten einzuhalten ist.

4 Diese sechs Monate haben Empfehlungscharakter. Längere Fristen sind oftmals seitens Cloud-Anbieter problematisch. Bei kürzeren Fristen können wichtige Informationen verloren gehen, welche im Rahmen eines nachträglich festgestellten Vorfalls (Datenverlust, unberechtigter Zugriff) benötigt werden.

Anhang

Glossar

Active Directory Eine Technologie von Microsoft, welche verschiede Services zur Verwaltung von Berechtigungen und des Zugriffs auf Netzwerkressourcen vereint.

Application Firewall Firewall, die die Ein- und Ausgabe sowie den Zugriff einer Anwendung oder eines Dienstes steuert.

Application Programming Interface (API) Technische Schnittstelle eines Programmes, über die es mit anderer Software kommuniziert.

Backup Das Kopieren von Daten auf einen Datenträger, von dem aus sie im Falle eines Geräteausfalls oder anderer Ereignisse wiederhergestellt werden können.

Client Ein Desktop-Computer oder eine Arbeitsstation, welche Informationen und Anwendungen von einem Server empfangen kann.

Container Eine Einheit von Software, die Codes und alle ihre Abhängigkeiten zusammenfasst, damit die Anwendung von einer Computerumgebung zur anderen einfach verschoben und ausgeführt werden kann. Im Gegensatz zu einer virtuellen Maschine (VM) enthält ein Container kein eigenes Betriebssystem oder eigenen Kernel.

Gateway Ein Gateway ist ein Knoten in einem Netzwerk, der als Zugang zu einem anderen Netzwerk dient.

Hypervisor Eine Komponente, welche virtuelle Maschinen erstellt und ausführt. Hypervisors erlauben den Betrieb von mehreren Gastsystemen auf einem Hostsystem.

Multi-Faktor-Authentifizierung (MFA) Authentifizierung, das heisst Verifizierung, ob eine Person diejenige ist, welche sie angibt zu sein. «Multi-Faktor» bedeutet, dass dies mittels mehrerer unabhängiger Merkmale geschieht.

On-Premise Nutzungs- und Lizenzmodell für serverbasierte Computerprogramme (Software). Die Software wird vom Benutzer gekauft und in der Regel auch selbst betrieben. Das Gegenteil ist ein On-Demand-Service, bei dem der Benutzer den Betrieb nicht selber übernimmt, sondern beispielsweise durch den Cloud-Anbieter sicherstellen lässt.

Penetrationstest Ein autorisierter, simulierter Cyberangriff auf ein System, der zur Bewertung der Sicherheit des Systems durchgeführt wird.

RSA Asymmetrisches kryptographisches Verfahren, das sowohl zum Verschlüsseln als auch zum digitalen Signieren verwendet werden kann.

Single Sign-on Single Sign-on bedeutet, dass ein Benutzer nach einer einmaligen Authentifizierung an einem Arbeitsplatz auf alle Rechner und Dienste, für die er lokal berechtigt (autorisiert) ist, vom selben Arbeitsplatz aus zugreifen kann, ohne sich an den einzelnen Diensten jedes Mal zusätzlich anmelden zu müssen.

Transport Layer Security/Secure Sockets Layer Secure Sockets Layer ist ein hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet. TLS ist der Nachfolger des Secure Socket Layer.

Web Service Ermöglicht die Maschine-zu-Maschine-Kommunikation auf Basis von HTTP oder HTTPS über Rechnernetze.

Abkürzungen

AD	Active Directory
API	Application Programming Interface
CSA	Security Guidance – For Critical Areas of Focus in Cloud Computing V4.0 der Cloud Security Alliance.
DSG	Bundesgesetz über den Datenschutz
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
ICT	Informations- und Kommunikationstechnik (engl. Information and Communication Technology)
ISO	International Standards Organisation – die internationale Normungsbehörde.
OVF	Open Virtualization Format
SLA	Service Level Agreement
SSL	Secure Sockets Layer
SSO	Single Sign-on
TLS	Transport Layer Security
WAF	Web Application Firewall

Impressum
Herausgeberin: FMH – Verbindung der Schweizer Ärztinnen und Ärzte, Bern
Text: Redguard AG, Bern; ti&m AG, Zürich
Grafikdesign/Illustration: Hahn+Zimmermann, Bern
Publikation: Mai 2020
www.fmh.ch


ajsdnaliw382hoan
knvlf2398whuienj
snfpie93hvoisjda
ajie0io*3flwesd
wdlfw90oijwl