Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

GDK Schweizerische Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren
CDS Conférence suisse des directrices et directeurs cantonaux de la santé
CDS Conferenza svizzera delle direttrici e dei direttori cantonali della sanità

eHealth Suisse

Umsetzungshilfe Datenschutz und Datensicherheit im EPD

Umsetzungshilfe für Datenschutz- und Datensicherheitsverantwortliche von Gemeinschaften und Stammgemeinschaften

Bern, 27. Juni 2017

ehealthsuisse
Kompetenz- und Koordinationsstelle von Bund und Kantonen
Centre de compétences et de coordination de la Confédération et des cantons
Centro di competenza e di coordinamento di Confederazione e Cantoni

Impressum

Autoren: Redguard AG, Eigerstrasse 60, 3007 Bern
Die bei der Erstellung oder Prüfung involvierten Personen sind im Anhang ersichtlich.

Identifikation dieses Dokuments
OID: 2.16.756.5.30.1.127.1.3.1.3.1

Weitere Informationen und Bezugsquelle:
www.e-health-suisse.ch

Zweck und Positionierung dieses Dokuments

Die Umsetzungshilfe Datensicherheit wurde erarbeitet von der Redguard AG, fachlich begleitet durch die Begleitgruppe. Der Bericht ist zugänglich unter www.e-health-suisse.ch. Umsetzungshilfen von „eHealth Suisse“ geben den betroffenen Akteuren Hinweise, wie sie eine Aufgabe im Umfeld der digitalen Vernetzung angehen können. Die angesprochenen Akteure können selber entscheiden, ob sie sich an die Vorschläge halten wollen.

Im Interesse einer besseren Lesbarkeit wird auf die konsequente gemeinsame Nennung der männlichen und weiblichen Form verzichtet. Wo nicht anders angegeben, sind immer beide Geschlechter gemeint.

Inhaltsverzeichnis

1 Einleitung

Elektronisches Patientendossier

Mit dem elektronischen Patientendossier (EPD) sollen die Qualität der medizinischen Behandlung gestärkt, die Behandlungsprozesse verbessert, die Patientensicherheit erhöht und die Effizienz des Gesundheitssystems gesteigert sowie die Gesundheitskompetenz der Patientinnen und Patienten gefördert werden.

Das Bundesgesetz über das elektronische Patientendossier (EPDG) und die Verordnungen des Ausführungsrechts (EPDV, EPDFV und EPDV-EDI inkl. Anhänge) traten am 22. März 2017 in Kraft. Ab dem Zeitpunkt der Inkraftsetzung des Gesetzes haben Spitäler drei Jahre Zeit, das elektronische Patientendossier einzuführen. Pflegeheime und Geburtshäuser haben fünf Jahre Zeit.

In der Verordnung wurden die technischen und organisatorischen Rahmenbedingungen für das EPD geregelt. Dazu gehören auch die technischen und organisatorischen Zertifizierungsvoraussetzungen (TOZ – Anhang 2 der EPDV-EDI) für die Stammgemeinschaften und Gemeinschaften.

Insbesondere im ambulanten Bereich der Gesundheitsversorgung ist bei der ICT-Durchdringung ein Handlungsbedarf feststellbar: Bei der Ärzteschaft dokumentiert beispielsweise rund ein Drittel der Praxen ihre Patienteninformationen digital (SISA II – Institut für Hausarztmedizin der Universität Zürich). Die Branche hat fast 20 Jahre gebraucht, um diese Durchdringung zu erzielen. Im Zusammenhang mit dem EPD wird sich dies in absehbarer Zeit ändern. Die Zahl der digital dokumentierenden Leistungserbringer könnte rasch zunehmen. Da das EPD für die Gemeinschaften und Stammgemeinschaften – ein Zusammenschluss von Gesundheitsfachpersonen und deren Einrichtungen – eine grössere Umstellung darstellt, soll das vorliegende Dokument, welches basierend auf den technischen und organisatorischen Zertifizierungsvorschriften und unter Berücksichtigung von internationalen Best Practices erstellt wurde, den Datenschutz- und Datensicherheitsverantwortlichen der Gemeinschaften und Stammgemeinschaften als Hilfsmittel im Bereich Datenschutz und Datensicherheit dienen.

Bedeutung der Datensicherheit

Mit Hilfe des elektronischen Patientendossiers können Gesundheitsfachpersonen auf behandlungsrelevante Daten ihrer zu behandelnden Personen (Patienten), die von anderen am Behandlungsprozess beteiligten Gesundheitsfachpersonen erstellt und dezentral erfasst wurden, zugreifen und diese allenfalls in ihren Praxis- und Klinikinformationssystemen ausserhalb des elektronischen Patientendossiers speichern. Sie müssen sich hierzu einer zertifizierten Gemeinschaft oder Stammgemeinschaft anschliessen, und ihre Patienten müssen ihnen die notwendigen Zugriffsrechte erteilen. Zudem eröffnet das elektronische Patientendossier auch den zu behandelnden Personen die Möglichkeit, ihre Daten einzusehen, selber eigene

Daten zugänglich zu machen wie auch die Vergabe der Zugriffsrechte zu verwalten.

Das Führen eines elektronischen Patientendossiers ist für die zu behandelnden Personen freiwillig. Im Sinne der informationellen Selbstbestimmung entscheidet jede Person selber, ob sie ein elektronisches Patientendossier führen will und in welchem Umfang sie ihren Gesundheitsfachpersonen Zugriffsrechte erteilt.

Der Schutz der im elektronischen Patientendossier verarbeiteten Daten hinsichtlich unerlaubter Einsichtnahme oder Datenabfluss (Vertraulichkeit), unerlaubter Änderungen (Integrität) sowie zeitgerechter Bereitstellung (Verfügbarkeit) hat einen sehr hohen Stellenwert. Dabei wird über die involvierten Organisationen hinweg ein einheitliches Sicherheitsniveau angestrebt. Dieses ist von zentraler Bedeutung, zumal das Vertrauen der Patienten einen zentralen Erfolgsfaktor darstellt. Die letztendliche Verantwortung für die Sicherstellung des Datenschutzes sowie die angemessene Datensicherheit liegt bei der jeweiligen Gemeinschaft.

1.1 Angesprochene Leserschaft

Zielgruppen

Das vorliegende Dokument richtet sich primär an die Datenschutz- und Datensicherheitsverantwortlichen der Gemeinschaften und Stammgemeinschaften.

Zweitrangig richtet sich das Dokument auch an Hersteller und Lieferanten von EPD-spezifischen Produkten oder Dienstleistungen sowie an Zertifizierungsstellen.

1.2 Vorgehen

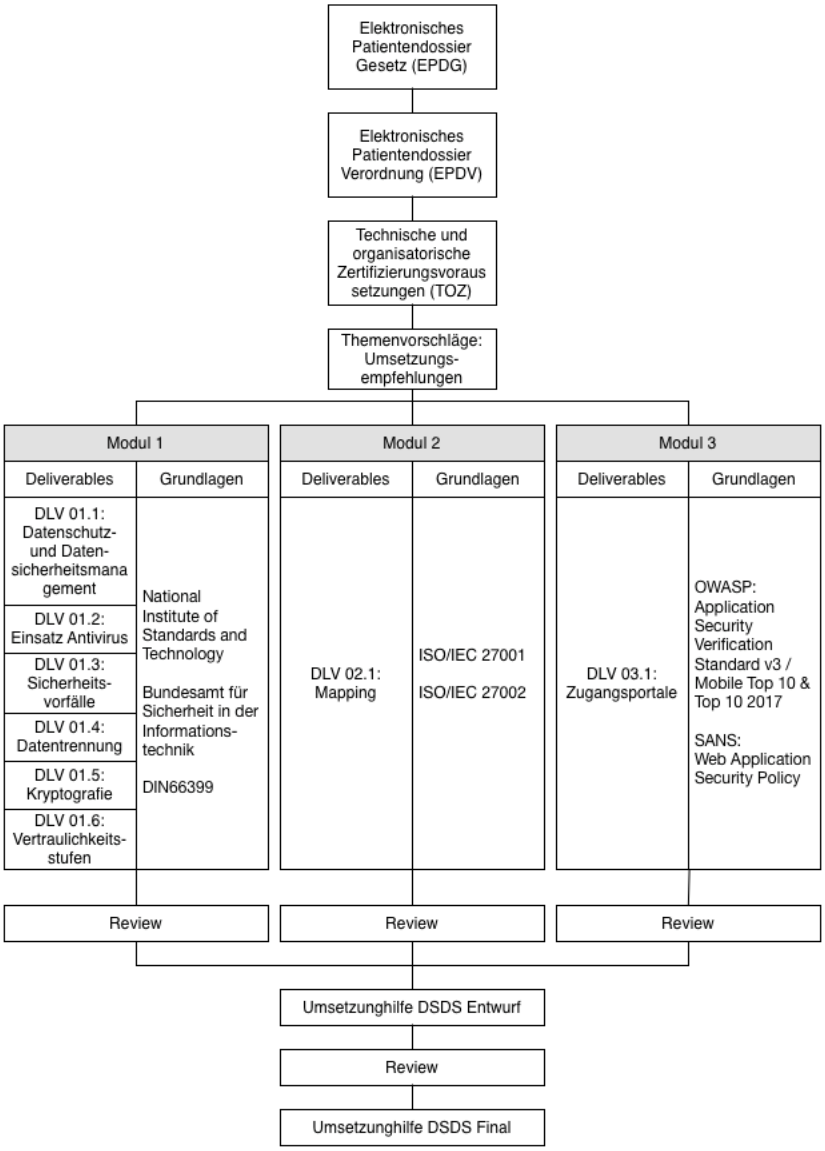

Abbildung 1: Ablauf der Erarbeitung der Umsetzungshilfen EPD

1.3 Aufbau des Dokumentes

Das vorliegende Dokument enthält Umsetzungshilfen zu den nachfolgenden Themen:

- Datenschutz- und Datensicherheitsmanagementsystem (Struktur gemäss TOZ)
- Schutz vor Schadsoftware
- Erkennung und Behandlung von Sicherheitsvorfällen
- Datentrennung
- Einsatz von Kryptografie
- Schutz vor Manipulation der Vertraulichkeitsstufen
- Sicherung der Zugangsportale
- TOZ/ISO Mapping-Tabelle

Die inhaltlichen Schwerpunkte wurden im Rahmen der Erarbeitung gemeinsam mit dem Auftraggeber sowie den Mitgliedern der Begleitgruppe definiert.

1.4 Abgrenzungen

Abgrenzungen

Das vorliegende Dokument unterliegt folgenden Abgrenzungen:

- Die vorliegende Umsetzungshilfe beschränkt sich auf Datenschutz- und Datensicherheitsaspekte.
- Die vorliegende Umsetzungshilfe umfasst ausgewählte Themen aus den TOZ. Die Themen wurden vorgängig mit dem Auftraggeber und der Begleitgruppe abgestimmt.
- Die Umsetzungshilfe strebt weder inhaltliche Vollständigkeit noch eine abschliessende Behandlung der darin enthaltenen Themen an.
- Die Umsetzungshilfe beschreibt lediglich Empfehlungen, wie ein spezifischer Sachverhalt gestaltet oder ausgeführt werden kann.
- Die Umsetzung einzelner Empfehlung bedingt die Zusammenarbeit aller involvierten Organisationen.
- Die Umsetzung der Massnahmen garantiert nicht das Erlangen der Zertifizierung.

1.5 Grundlagen

[EPDG]	Bundesgesetz über das elektronische Patientendossier
[DSG]	Bundesgesetz über den Datenschutz
[EPDV]	Verordnung über das elektronische Patientendossier
[TOZ]	Anhang 2: Technische und organisatorische Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften
[EPD-RA]	Bedrohungs- und Risikoanalyse Elektronisches Patientendossier

1.6 Verwendete Hilfsmittel und Referenzen

[ISO27001]	ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements – nicht öffentlich verfügbar
[ISO27002]	ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls – nicht öffentlich verfügbar
[OWASP-Top10]	OWASP - Top 10 (2013)
[OWASP-MobileTop10]	OWASP - Mobile Top 10 (2016)
[OWASP-ASVS]	OWASP – Application Security Verification Standard 3.0
[OWASP-TLS-CS]	OWASP – TLS Cheat Sheet
[OWASP-TLS-TG]	OWASP – Testing Guide for SSL/TLS
[SANS-WASP]	SANS – Web Application Security Policy
[DIN66399]	DIN 66399 Büro- und Datentechnik – Vernichten von Datenträgern – nicht öffentlich verfügbar
[BSI-TR02102]	BSI – Kryptographische Verfahren: Empfehlungen und Schlüssellängen
[FIPS140.0]	Security Requirements for Cryptographic Modules
[NIST-SP-800-57]	Recommendation for Key Management
[CERT-Meldungen]	Melde- und Analysestelle Informationssicherung MELANI BSI - CERT US-CERT Ex existieren zudem weitere, teils kostenpflichtige News-Feeds zu Schwachstellen oder sicherheitsrelevanten Ereignissen.
[CA-List]	Folgenden Listen können beispielhaft aufgeführt werden: https://mozillacaprogram.secure.force.com/CA/IncludedCACertificateReport https://gallery.technet.microsoft.com/Trusted-Root-Certificate-123665ca
[Hardening-Guides]	NIST – Guide to General Server Security

	SANS – SCORE Checklists
[Incident-Handling]	ENISA – Good Practice Guide for Incident Management
	SANS – Incident Handlers Handbook

1.7 Begriffsverwendung

Begriff	Definition im vorliegenden Dokument
Organisation	Entspricht einer Gemeinschaft oder Stammgemeinschaft inklusive allfällig beteiligter Dritter
ICT-Infrastruktur	Umfasst die EPD-relevante Systemumgebung. Siehe auch TOZ 4.6.2

2 Datenschutz und Datensicherheitsmanagementsystem

2.1 Einleitung

Einleitung

Die Erfüllung der Anforderungen, welche aus den technischen und organisatorischen Zertifizierungsvoraussetzungen (TOZ) resultieren, erfordert die Umsetzung von verschiedenen Sicherheitsmassnahmen.

Die Umsetzung sowie das Aufrechterhalten des definierten Sicherheitsniveaus bedingen einen systematischen Ansatz. Zur Verwaltung der TOZ-spezifischen Anforderungen und Massnahmen ist demnach ein Managementsystem zu etablieren.

Das Datenschutz- und Datensicherheitsmanagementsystem enthält alle notwendigen Elemente zur Erreichung sowie zur langfristigsten Aufrechterhaltung des geforderten und notwendigen Sicherheitsniveaus. Sofern innerhalb der Organisation bereits ein Informationssicherheitsmanagement (ISMS) oder Datenschutzmanagementsystem (DSMS) besteht, kann dieses unter Berücksichtigung der TOZ-spezifischen Anforderungen erweitert und angepasst werden.

2.2 Verwaltung Gesundheitsfachperson und deren Hilfspersonen

Relevante TOZ-Anforderungen

1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.4.1, 1.6.2, 1.6.3

Prozessziel

Die Prozesse zur Verwaltung der Gesundheitsfachpersonen (inkl. Hilfspersonen) stellen sicher, dass sämtliche Personen korrekt identifiziert, registriert und zur Einhaltung von spezifischen Richtlinien und Handlungsanweisungen verpflichtet wurden. Weiter, dass diese über die korrekten Zugangsmittel sowie Berechtigungen verfügen und diese über das Anstellungsverhältnis hinweg an die aktuellen Begebenheiten angepasst oder beim Austritt widerrufen werden.

Aktivitäten

Verpflichtung zur Einhaltung von Richtlinien: Folgende Aspekte sollten in internen Richtlinien und Handlungsanweisungen organisationsspezifisch festgelegt werden:

- Umgang mit Authentifizierungsmerkmalen
- Umgang mit Informatikmitteln
- Handhabung von sensitiven Informationen und Daten
- Anlaufstelle für sicherheitsrelevante Fragen

Umsetzung: Die Prozesse zur Verwaltung von Gesundheitsfachpersonen haben hohe Anforderungen an die Nachvollziehbarkeit. Sämtliche Prozessschritte sowie allfällige Entscheide oder Genehmigungen sollten demnach dokumentiert werden. Zur Minimierung von Bearbeitungsfehlern sowie zwecks Sicherstellung der Nachvollziehbarkeit über die einzelnen Bearbeitungsschritte hinweg wird daher empfohlen, die Verwaltungsprozesse soweit als möglich über einen toolgestützten Workflow abzuwickeln.

2.3 Risikomanagement

4.2.1 4.2.3

Relevante TOZ-Anforderungen

Das Risikomanagement hilft Risiken, welche die Vertraulichkeit, die Integrität, die Authentizität oder die Verfügbarkeit von EPD-relevanten Daten gefährden, zu identifizieren, systematisch zu bewerten, zu bearbeiten sowie allfällige verbleibende Restrisiken dem Risikoträger zu kommunizieren.

Ein Risikomanagementprozess ist ein Kreislauf und lässt sich in vier Phasen unterteilen:

- Identifikation der Risiken
- Analyse und Bewertung der Risiken
- Umsetzung der Massnahmen
- Überwachung

Um die Risiken steuern zu können, müssen diese zuerst identifiziert werden. Dazu müssen bei Änderungen – sowohl im Betrieb als auch im Rahmen eines Projekts – die Risiken identifiziert werden. Zudem wird empfohlen, mindestens jährlich einen dedizierten Risikomanagement-Workshop durchzuführen, der zum Ziel hat, bestehende Risiken zu aktualisieren sowie allfällige neue Risiken zu identifizieren. Nachdem die Risiken identifiziert wurden, müssen die Risiken bewertet werden. Hierzu sollte ein einheitliches Bewertungsschema für die Eintretenswahrscheinlichkeit sowie für die potentielle Auswirkung – sowohl auf die jeweilige Organisation wie auch auf die betroffenen Personen (Patienten) – zur Anwendung kommen. Bei der Beurteilung aus Sicht Patient sind sowohl die mögliche Persönlichkeitsverletzung als auch der Vertrauensverlust insgesamt zu berücksichtigen. Wichtig ist dabei, dass die Beurteilung nach einem einheitlichen Schema innerhalb der Organisation durchgeführt wird. Ebenfalls übergreifend sollten Kriterien der Risikoakzeptanz (bis zu welcher Bewertung kann ein Risiko unter welchen Umständen getragen werden) definiert werden.

Für die Bearbeitung der Risiken ist es vorteilhaft, die Einzelrisiken in thematischen Gruppen zusammenzufassen. Dadurch können mit Massnahmen ganze Risikogruppen adressiert werden. Die verbleibenden Restrisiken sollten abhängig von der Bewertung in regelmässigen Abständen durch den Risikoträger genehmigt werden. Die Kommunikation sollte dabei mindestens einmal pro Jahr oder bei grösseren Änderungen erfolgen.

Alle vorgenannten Verfahren und Arbeitsschritte sollten innerhalb der Organisation dokumentiert werden. Es wird empfohlen, für die Arbeitsschritte entsprechende Hilfsmittel in Form von Vorlagen oder Toolunterstützung vorzusehen.

2.4 Personalsensibilisierung

4.2.2

Relevante TOZ-Anforderungen

Um einen hohen Datenschutzstandard in einer Gemeinschaft nachhaltig zu sichern, bedarf es einer regelmässigen Information der Gesundheits-

Informierung der Mitarbeitenden

fachpersonen und deren Hilfspersonen über relevante technische und organisatorische Änderungen, über relevante Vorgaben sowie über zu beachtende Verfahren. Die Sensibilisierung der Mitarbeitenden kann über verschiedene Kanäle erfolgen.

Mögliche Kommunikationskanäle

- **Schulung beim Eintritt:** Beim Eintritt von Gesundheitsfachpersonen sollte eine Schulung über alle relevanten Vorgaben, Verfahren und Hilfsmittel durchgeführt werden. Zur Steigerung der Sichtbarkeit wird empfohlen, dass der Datenschutz- und Datensicherheitsverantwortliche diese Schulung durchführt.
- **Merkblatt:** Es wird empfohlen, ein Merkblatt zum Thema Datenschutz an alle neu in die Gemeinschaft eintretenden Gesundheitsfachpersonen auszuhändigen.
- **Vorgaben-Portal:** Alle relevanten Vorgaben im Zusammenhang mit dem Datenschutz und der Datensicherheit sollten in einem Vorgaben-Portal zentral zugänglich sein. Die Aufbereitung sollte dabei möglichst einfach und übersichtlich sein.
- **Ereigniskommunikation:** Sicherheitsrelevante Ereignisse sowie daraus resultierende Massnahmen sollten zeitnah nach dem Ereignis an die Mitarbeitenden kommuniziert werden (siehe Kapitel 0).
- **Mitarbeiterinformationen:** Werden grössere Änderungen zum Thema Datenschutz und Datensicherheit vorgenommen (z.B. Änderungen in Folge von Anpassungen der rechtlichen Vorgaben), sollten dedizierte Informationsschreiben an alle Mitarbeitenden verschickt werden. Damit soll sichergestellt werden, dass alle Gesundheitsfachpersonen die Information erhalten haben.
- **Weiterbildungsveranstaltungen:** Da Wiederholungen den Lernerfolg steigern, sollte in regelmässigen Abständen eine Schulung zum Thema Datenschutz und Datensicherheit stattfinden. Empfohlen wird mindestens eine Schulung jährlich. Dadurch bleibt den Mitarbeitenden das Thema präsenter und Neuerungen können zeitnah mitgeteilt werden.

Regelmässige Überprüfung der Sensibilisierung

Die Sensibilisierungsbestrebungen sollten regelmässig einer Erfolgskontrolle unterzogen werden. Hierzu können Simulationen und Tests eingesetzt werden; beispielsweise das Verschicken von fiktiven Phishing E-Mails an die Mitarbeitenden.

Nachweis über Sensibilisierungsaktivitäten

Die Durchführung von Sensibilisierungsmassnahmen sowie die Teilnahme der Gesundheitsfachpersonen sollte nachvollziehbar dokumentiert werden.

2.5 Umgang mit Sicherheitsschwachstellen

Relevante TOZ-Anforderungen

4.4.1, 4.4.2

Gemeinschaften müssen über ein Sicherheitsschwachstellenmanagement verfügen. Dieses soll Informationen über technische Sicherheitsschwachstellen von verwendeten Informationssystemen rechtzeitig einholen. Weiter ist die Aufgabe des Sicherheitsschwachstellenmanagements, dass es

Sicherheitsschwachstellen bewertet und dazu angemessene Massnahmen ergreift. Das Sicherheitsschwachstellenmanagement besteht grundsätzlich aus fünf Phasen, wie die folgende Abbildung zeigt:

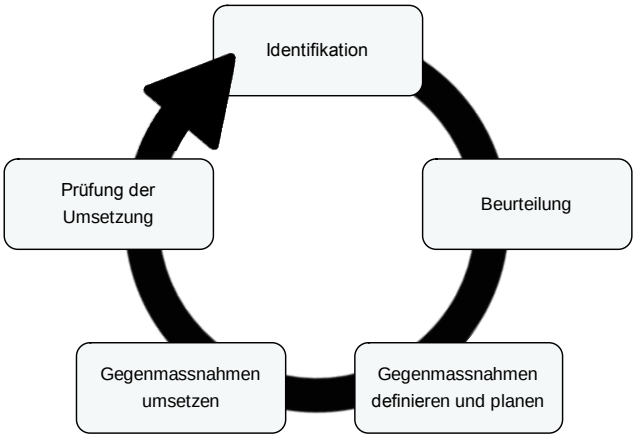

Abbildung 2: Phasen des Sicherheitsschwachstellenmanagements

Die Identifikation erfolgt mit Hilfe eines Vulnerability Scanners (manuell oder automatisiert), welcher alle internen und externen Systeme auf mögliche Schwachstellen überprüft. Typische Schwachstellen resultieren aus veralteter Software, Fehlkonfigurationen oder Fehlmanipulationen. Es wird empfohlen, einen solchen Scan jeweils einmal pro Monat vorzunehmen.

Die Beurteilung sollte anhand eines definierten Schemas vorgenommen werden. Grundsätzlich können die Schwachstellen in folgende vier Kategorien unterteilt werden:

- **Kritisch**: Die Vertraulichkeit, die Integrität der Verfügbarkeit der Daten ist sehr stark gefährdet. Eine sehr rasche Intervention ist zwingend notwendig. Dies ist beispielsweise der Fall, wenn eine kritische Schwachstelle mit automatisierten Tools ausgenutzt werden kann.
- **Hoch**: Es besteht eine hohe Gefährdung. Jedoch sind manuelle Tätigkeiten seitens des Angreifers notwendig. Trotzdem ist eine rasche Intervention gefragt.
- **Mittel**: Die Ausnutzung der Schwachstelle erfordert grossen Aufwand oder ist nur in Kombination mit mehreren grundsätzlich unabhängigen Schwachstellen möglich. Dies sollte mittelfristig behoben werden, jedoch ist keine unmittelbare Aktion notwendig.
- **Niedrig**: Kaum Auswirkung auf die Schutzziele der Daten oder Schwachstellen, welche es einem Angreifer ermöglichen, zusätzliche Informationen über die Systeme zu sammeln. Schwachstellen/Risiken mit der Bewertung „niedrig“ sollten allerdings, sofern sinnvoll, mittel- bis langfristig behoben werden.

Gegenmassnahmen müssen abhängig von der Kritikalität der Schwachstelle zeitnah definiert und geplant werden. Der allgemeine Gegenmassnahmenplan wird in folgende fünf Schritte aufgeteilt:

1. Einschätzung der Schwachstelle, basierend auf der Bewertung aus der Sicherheitsschwachstellenmanagement-Phase „Beurteilung“
2. Ermittlung von möglichen Gegenmassnahmen (auch kompensierende Massnahmen)
3. Beurteilung und Bewertung der Gegenmassnahmen
4. Funktionstest nach Umsetzung der Gegenmassnahme
5. Planung für die Umsetzung (Produktivschaltung)

Sollte auf die Umsetzung einer Gegenmassnahme verzichtet werden, müssen die entsprechenden Schwachstellen mit entsprechender Begründung, weshalb auf die Umsetzung verzichtet wird, in das Risikomanagement einfliessen. Sämtliche offenen, nicht bearbeiteten Schwachstellen sollen bekannt sein.

Die zuvor definierten, geplanten und getesteten Gegenmassnahmen werden basierend auf der vorhergehenden Planung umgesetzt.

Am Ende des Prozesses steht die Prüfung der Umsetzung. Durch die regelmässige Durchführung der Scans besitzt diese auch einen gewissen Prüfcharakter. Bei kritischen Schwachstellen ist jedoch eine zeitnahe Prüfung nach erfolgter Korrektur zu empfehlen.

Zusätzlich sollten mindestens einmal pro Jahr oder bei grösseren Änderungen Penetration Tests auf kritische Elemente durchgeführt werden. Sofern die Möglichkeit besteht, kann im Rahmen der Entwicklung auch ein Bug-Bounty-Programm etabliert werden. Dies sollte allerdings unter Berücksichtigung der jeweiligen organisationspezifischen Vorschriften und Richtlinien erfolgen.

Als zusätzliche Massnahme wird zudem empfohlen, die eingesetzten Produkte auch passiv zu überwachen. Hierzu können Feeds [CERT-Meldungen] mit Meldungen über neue Schwachstellen abonniert werden. Die entsprechenden Meldungen können dann im Anschluss mit den Angaben im Inventar verglichen werden.

2.6 Inventar der Informatikinfrastruktur

Relevante TOZ-Anforderungen

4.6.1, 4.6.2, 4.6.3, 4.6.2, 4.6.5

Inventarpflege

Alle schützenswerten Daten, Systeme und Einrichtungen (TOZ 4.6.1) des elektronischen Patientendossiers müssen von den Gemeinschaften identifiziert, klassifiziert und in einem „Inventar der Informatikstruktur“ erfasst und aktuell gehalten werden. Es wird empfohlen, das Inventar in einer entsprechenden Software zu pflegen. Dabei sollten mindestens die nachfolgenden Attribute eines Elements gepflegt werden:

- Name und Bezeichnung
- Verwendungszweck
- Klassifizierung
- Standort
- Physisches oder virtuelles System
- Verantwortlicher Eigentümer

- Zugriffsrechte auf das Element
- Identifikationsdaten (z.B. System-ID)
- Adressierungselemente
- Angaben zu Garantie und Wartung
- Eingesetzte Software-Versionen (Betriebssystem, Antivirus, Applikationen und relevante Libraries)
- Angaben zu den verwendeten Zertifikaten

Das „Inventar der Informatikstruktur“ muss vom Datenschutzbeauftragten mindestens jährlich überprüft werden.

Regelmässige Überprüfung

2.7 Disziplinarverfahren[1]

4.8.2

Relevante TOZ-Anforderungen

Sollten Gesundheitsfachpersonen, deren Hilfspersonen oder sonstige Personen im Zusammenhang mit EPD-relevanten Daten (z.B. Systemadministrator) gegen das Datenschutzgesetz (DSG) verstossen, muss dieses Verhalten sanktioniert werden. Zum einen können die Sanktionen vertraglich geregelt werden. Die Verträge sollten im Falle von Datenschutzverletzungen Kündigungsrechte, aber auch erhöhte Haftungsrisiken und Konventionalstrafen zur Folge haben. In diesem Fall wird das folgende Vorgehen empfohlen:

Verstoss gegen DSG

1. Identifikation des Verstosses
2. Beurteilung des Ausmasses des Verstosses
3. Definition der Sanktion basierend auf der Beurteilung des Verstosses
4. Umsetzung der Sanktion

Der Umfang der Sanktion liegt in diesem Fall im Ermessen der jeweiligen Gemeinschaft.

Zum anderen greift im Falle einer Verletzung der beruflichen Schweigepflicht der Artikel 35 des Datenschutzgesetzes: Wer vorsätzlich geheime, besonders schützenswerte Personendaten oder Persönlichkeitsprofile unbefugt bekannt gibt, von denen er bei der Ausübung seines Berufes, der die Kenntnis solcher Daten erfordert, erfahren hat, wird auf Antrag mit Busse bestraft.

Art. 35 Verletzung der beruflichen Schweigepflicht

Gleich wird bestraft, wer vorsätzlich geheime, besonders schützenswerte Personendaten oder Persönlichkeitsprofile unbefugt bekannt gibt, von denen er bei der Tätigkeit für den Geheimhaltungspflichtigen oder während der Ausbildung bei diesem erfahren hat.

Das unbefugte Bekanntgeben geheimer, besonders schützenswerter Personendaten oder Persönlichkeitsprofile ist auch nach Beendigung der Berufsausübung oder der Ausbildung strafbar.

[1] Entspricht dem Massregelungsprozess

2.8 Steuerung und Überwachung von Dritten

4.9.1, 4.9.2, 4.9.3, 4.9.4, 4.10	Relevante TOZ-Anforderungen
Die Auswahl des bestpassenden Angebots beinhaltet eine Evaluation und Bewertung des Anbieters und der Dienstleistungen. Folgende Aspekte sind daher zu prüfen: • Anforderungserfüllung • Bedeutung des Geschäftsbereichs • Geografische Datenverarbeitung • Gerichtsbarkeit • Referenzen • Unabhängige Beurteilungen (Lieferanten-Audits) Sämtliche Lieferanten, die unter Umständen auf Daten des elektronischen Patientendossiers zugreifen, sie verarbeiten, speichern, weitergeben oder Informatikinfrastruktur dafür bereitstellen, müssen systematisch erfasst und durch den Datenschutz- und Datensicherheitsverantwortlichen genehmigt werden.	Anbieter wählen
Die Leistungserbringung sollte dabei vertraglich festgelegt werden. Dabei sollten mindestens folgende Punkte abgedeckt sein: • Ort der Leistungserbringung • Ort der Datenhaltung (auch Sicherungen und Ausweichstandorte) • Definition von Kennzahlen und Reporting-Verfahren • Verfügbarkeitswerte (Messwerte) • Einhaltung von rechtlichen und regulatorischen Anforderungen (insbesondere EPDG und DSG) • Einhaltung von allgemeinen oder organisationsspezifischen Sicherheitsanforderungen • Einbezug und Verpflichtung von Unterlieferanten • Anforderungen an beteiligte Personen • Auflistung der beteiligten Personen • Änderungsmanagement • Mitteilung von organisatorischen oder technischen Änderungen • Kommunikations- und Eskalationswege • Vorgehen bei Sicherheitsvorfällen • Notfallvorsorge • Auditrecht • Haftungsfragen • Strafzahlungen bei nicht Erfüllung • Beendigung (vor allem Datenexport und -löschung)	Vertrag
Die Leistungserbringung sollte dabei laufend überwacht und bei Bedarf optimiert werden. Die Grundlagen dazu bilden definierte Messwerte der Leistungserbringung. Diese müssen durch die Gemeinschaft laufend überwacht	Steuerung und Überwachung

werden. Dazu müssen vom Lieferanten zugestellte oder gemessene Ist-Werte monatlich mit den definierten Soll-Werten verglichen werden. Werden Abweichungen festgestellt, sind angemessene Massnahmen umzusetzen. Zusätzlich zur Überwachung der Leistungserbringung sollten regelmässige Lieferanten-Audits durchgeführt werden. Dabei sollte die Einhaltung der festgelegten Bedingungen sowie die zweckmässige und vollständige Umsetzung der Vorgaben verifiziert werden. Die Regelmässigkeit sowie Prüftiefe der Lieferanten-Audits soll risikobasiert festgelegt werden. Für strategische Lieferanten oder Lieferanten mit umfangreichen Systemzugriffen soll ein jährliches Audit durchgeführt werden.

2.9 Änderungsmanagement

4.10

Relevante TOZ-Anforderungen

Das Änderungsmanagement steuert geplante Änderungen und Erweiterungen der ICT-Infrastruktur. Das Änderungsmanagement muss in Zusammenarbeit mit allen involvierten Organisationen erfolgen und daher organisationsübergreifend definiert und umgesetzt werden. Im Zusammenhang mit dem Änderungsmanagement sollten folgende Punkte beachtet werden:

- Änderungsmanagement sollte laufend erfolgen und in die Betriebsprozesse integriert sein. So sollten alle Änderungen den entsprechenden Prozess durchlaufen und systematisch beurteilt werden.
- Alle Änderungen an der ICT-Infrastruktur sollten kontrolliert werden und unter der Minimierung von Risiken für den laufenden Betrieb der betroffenen Geschäftsfelder durchgeführt werden können.
- Störungen infolge von Änderungen sollten vermieden und die Effizienz der Änderungen verbessert werden.
- Änderungen ohne Nutzen, die nicht gewünscht sind oder mangels Durchführbarkeit wieder rückgängig gemacht werden müssen, sollten komplett vermieden werden.
- Es sollte ein Rückfallverfahren (Fall-Back-Szenario) definiert werden.
- Das Änderungsmanagement muss ein Optimum zwischen Flexibilität und Stabilität der Verfahren herstellen.
- Sämtliche Änderungen sowie die einzelnen Bearbeitungs- und Genehmigungsschritte sollten nachvollziehbar dokumentiert werden.

2.10 Datenschutz- und Datensicherheitsverantwortlicher

4.11.1, 4.11.2

Relevante TOZ-Anforderungen

Die/der Datenschutz- und Datensicherheitsverantwortliche hat innerhalb der Gemeinschaft folgende Aufgaben:

Aufgabenprofil

- Aufbau, Unterhalt und laufende Optimierung des Datenschutz- und Datensicherheitsmanagementsystems
- Überwachung der Sicherheitsmassnahmen hinsichtlich der effektiven und effizienten Anforderungserfüllung
- Erarbeitung von organisationspezifischen Sicherheitsvorgaben, -richtlinien und Handlungsanweisungen
- Erheben, Einstufen, Beurteilen von Risiken im Umfeld der Schutzobjekte (Informationen, Daten, Anwendungen, Systeme und Prozesse)
- Bewerten und Überprüfen der Verträglichkeit von Vorhaben in Bezug auf den Datenschutz und die Datensicherheit
- Bearbeitung von Sicherheitsereignissen
- Information und Sensibilisierung der involvierten Personen in Bezug auf Sicherheitsbelange
- Ansprechpartner für sicherheitsrelevante Fragestellungen
- Zusammenarbeit mit Sicherheitsverantwortlichen von anderen Gemeinschaften, den Gesundheitseinrichtungen sowie involvierten Dritten (z.B. Lieferanten)

Unabhängigkeit der Funktion

Die Rolle beinhaltet seine Kontrollfunktion, wodurch eine Unabhängigkeit gegenüber Personen und Rollenträgern, die von der Sicherheit der Schutzobjekte abhängig sind, erforderlich ist. Es wird daher grundsätzlich empfohlen, die Rolle als Stabsfunktion anzusiedeln. Das regelmässige sowie situative Berichtwesen sollte dabei direkt an die Organisationsleitung gerichtet sein.

Wird die Rolle in der Personalunion wahrgenommen, muss einem Interessenskonflikt vorbeugt werden. Dabei sollten folgende Kombinationen explizit vermieden werden:

- Leitende Funktion innerhalb der Gemeinschaft/Stammgemeinschaft
- Leitende Funktion innerhalb der ICT
- Funktion mit ICT-Betriebsverantwortung
- Gesundheitsfachperson jeglicher Art

Die Rolle kann durch einen Mitarbeiter der Organisation oder durch einen beauftragten Dritten wahrgenommen werden. In diesem Fall gilt es anzumerken, dass die letztliche Verantwortung nicht von der Organisation wegdelegiert werden kann.

Erforderliche Kenntnisse

Vom Rollenträger werden sowohl breite als auch tiefgehende Fachkenntnisse sowie hohe Sozialkompetenzen verlangt.

Fachkompetenz:

- Technische, betriebswirtschaftliche oder juristische Grundausbildung mit zusätzlichen Ausbildungen in den jeweils anderen Fachbereichen
- Fundierte Kenntnisse und Erfahrung im medizinischen Umfeld

- Kenntnisse und Erfahrung in den Bereichen der Informations- und ICT-Sicherheit
- Kenntnisse des Schweizer Datenschutzgesetzes
- Kenntnisse der ISO/IEC-Standardreihe 2700x
- Erfahrung im Aufbau und Unterhalt eines Managementsystems (Informationssicherheit und Datenschutz)

Sozialkompetenz

- Von Vorteil: Führungserfahrung
- Hohe Eigenverantwortung und Zuverlässigkeit
- Die Fähigkeit, komplexe Sachverhalte einfach, verständlich und zielgerichtet mündlich und schriftlich zu kommunizieren
- Konfliktmanagement und Durchsetzungsvermögen

2.11 Backup- und Wiederherstellungsprozess

4.13.1

Relevante TOZ-Anforderungen

Die Datensicherung, auch Backup genannt, ist ein wichtiger Faktor um Daten zu schützen. Der Backupprozess muss jederzeit gewährleistet werden können, damit im Falle eines Datenverlusts oder bei sonstigen Fehlern eine rasche Wiederherstellung der betroffenen Daten erfolgen kann.

Die Sicherung sollte dabei zeitnah nach einer Änderung der Daten sowie – unabhängig von Änderungen – regelmässig erfolgen. Das Backup-Verfahren sollte definiert und in einem Backup-Konzept beschrieben werden. Der Backup-Mechanismus sollte dabei soweit als möglich automatisiert und mit geeigneten Tools und Alarmierungsverfahren überwacht werden.

Die Aufbewahrung der Backups soll getrennt vom Ursprungssystem und in verschlüsselter Form erfolgen. Hierbei ist darauf zu achten, dass Backups nachträglich nicht mehr verändert oder unbemerkt überschrieben werden können. Dies ist insbesondere im Zusammenhang mit den zurzeit geläufigen Ransomware-Attacken eine wichtige vorsorgliche Massnahme. Bei Backups ist darauf zu achten, dass diese ausschliesslich in der Schweiz und bei einem Anbieter, welcher dem Schweizer Recht untersteht, abgelegt werden.

Die Wiederherstellung von Backups sollte regelmässig testweise erfolgen. Dabei sollte alle drei Monate ein zufällig ausgewähltes Backup vollständig wiederhergestellt werden. Die korrekte Wiederherstellung sollte geprüft und dokumentiert werden.

2.12 Datenträgervernichtung

4.13.1

Relevante TOZ-Anforderungen

Werden Datenträger nicht mehr gebraucht, sollten diese sicher und unter Anwendung formeller Verfahrensanweisungen entsorgt werden.

Entsorgung

Die Datenträger des elektronischen Patientendossiers sollten nach DIN 66399 [DIN 66399] vernichtet werden. Da es sich bei Patientendaten um sensible Daten handelt, wird diesen Daten des elektronischen Patientendossiers nach DIN 66399 die Schutzklasse 3 zugewiesen. Diese Schutzklasse lässt nur Sicherheitsstufen von 4 bis 7 zu.

- 4: Besonders sensible Daten – Reproduktion mit aussergewöhnlichem Aufwand
- 5: Geheim zu haltende Daten – Reproduktion mit zweifelhaften Methoden
- 6: Geheime Hochsicherheitsdaten – Reproduktion technisch nicht möglich
- 7: Top-Secret Hochsicherheitsdaten – Reproduktion ausgeschlossen

Aufgrund der Datenzuweisung auf die höchste Schutzklasse nach DIN 66399 bedarf es Datenträgervernichtungen, welche eine Reproduktion nur mit aussergewöhnlichem Aufwand oder sicherer vernichten. Dies gilt für alle Arten von Datenträgern (inkl. Flash-Speicher und Solid-State Disks). Sämtliche Vernichtungen sollten nachweisbar dokumentiert werden.

2.13 Wiederanlaufplanung

4.18

Relevante TOZ-Anforderungen

Ein Wiederanlaufplan dient zur Planung der schnellstmöglichen Wiederherstellung der wichtigsten ICT-Infrastruktur. Ziel des Wiederanlaufplanes ist die genaue technische Beschreibung, wie eine Wiederherstellung nach einem grösseren Schadensfall zu erfolgen hat. Zum Wiederherstellungsplan gehören auch Wiederbeschaffungsmassnahmen und Ausweichmöglichkeiten auf andere Infrastrukturen, welche es erlauben, die Kontinuität des Betriebs beizubehalten.

Der Wiederanlaufplan muss auf zwei Komponenten aufgebaut sein:

- Maximale Ausfallzeit (RTO – Recovery Time Objectives)
- Maximal hinnehmbarer Datenverlust (RPO – Recovery Point Objectives)

Die Ausfallzeit muss aufgrund von Notfallsituationen, in welchen Daten über den Patienten überlebensentscheidend sind, sehr niedrig gehalten sein. Der hinnehmbare Datenverlust darf maximal die Menge an Daten sein, welche zwischen dem letzten Backup und dem Zwischenfall entstanden sind. Da das Backup kontinuierlich gemacht wird, ist auch diese Menge auf ein Minimum begrenzt.

Ein Wiederanlaufplan sollte mindestens die folgenden Punkte beinhalten:

- Aufbau, Installation und Konfiguration der erforderlichen Hardware-Komponenten
- Installation der Systemsoftware
- Installation der Anwendungssoftware
- Wiederherstellung der Daten einschliesslich der Konfigurationsdateien aus der Datensicherung
- Wiederanlauf des Systems
- Angaben zum Speicherplatzbedarf

- Liste aller erforderlichen Sicherungsdatenträger
- Kontrollen und Freigaben

Weiter ist ein essenzieller Bestandteil des Wiederanlaufplans, die Reihenfolge – unter Berücksichtigung der gegenseitigen Abhängigkeiten – für den Wiederanlauf der Systeme und Anwendungen festzuhalten. Es wird empfohlen, szenariobasierte Wiederanlaufpläne (z.B. nach Ransomware-Vorfall) zu erarbeiten.

Zur optimalen Vorsorge sollte ein Notfallhandbuch erarbeitet und abgelegt werden. Dabei sollten folgende Themen abgedeckt werden:

- Verfahren und Verantwortlichkeiten zur Bearbeitung von Notfällen
- Liste mit verantwortlichen Personen und deren Kontaktdaten
- Wiederanlaufpläne pro Szenario
- Kommunikationsmassnahmen

Das Notfallhandbuch sollte unabhängig von der EPD-Umgebung und idealerweise auch offline aufbewahrt werden. Dabei muss die regelmässige Aktualisierung sichergestellt sein. Ebenso der Zugriff für sämtliche involvierte Personen.

3 Schutz vor Schadsoftware

3.1 Einleitung

Antivirenprogramme

Computer-Schadsoftware sind Programme, deren Funktionalität darauf abzielt, dem rechtmässigen Betrieb zu schaden. Nach dem Installieren (Befall) versuchen diese zum Beispiel, sich zu vervielfältigen und auf dem Computer Daten zu sammeln, zu beschädigen oder gar zu löschen. Ohne Schutz vor Schadsoftware (je nach Funktionalität sogenannten Würmern, Viren oder trojanischen Pferden) besteht ein erhöhtes Risiko eines Schadsoftwarebefalls (auch Malware genannt). Um dies zu vermeiden, werden Antivirenprogramme eingesetzt. Die Antivirensoftware hat drei verschiedene Aufgaben. Zum einen schützt sie Systeme vor dem Befall von Malware. Dabei scannen die Antivirenprogramme die aufgerufenen Internetseiten, die empfangenen E-Mails, die angeschlossenen Datenträger oder Dateien nach Viren. Werden verdächtige Dateien gefunden oder Vorgänge registriert, die auf Schadsoftware hindeuten, wird verhindert, dass sie auf den eigenen Computer gelangen. Sofern sich diese bereits auf dem Computer befinden, wird der Zugriff und somit die schädliche Auswirkung eingeschränkt. Eine zweite Aufgabe der Antiviren-Lösungen besteht in der regelmässigen Durchsuchung von auf dem Computer befindlichen Dateien, welche zuvor von den Antivirenprogrammen nicht erkannt wurden. Die Antivirensoftware hat drittens die Aufgabe, die Verbreitung von Schadsoftware zu unterbinden. Wenn die Malware nicht entdeckt würde und den Computer befällt, stellen alle ausgehenden Interaktionen dieses Computers eine Gefahr für andere Endgeräte dar. Dabei ist zu beachten, dass Antivirenprogramme in ihrer Funktion beschränkt sind. Einerseits deshalb, weil die Erkennung mehrheitlich auf Signaturen basiert und somit die Schadsoftware zuvor bekannt sein muss, andererseits können die Mehrheit der Antivirenprogramme Dateien oder auch Netzwerkverbindungen, welche verschlüsselt sind, nicht auf schädliche Inhalte überprüfen. Der Einsatz von Antivirusprogrammen wird immer wieder kontrovers diskutiert. Ein Antivirusprogramm wird mit hohen Berechtigungen auf dem System ausgeführt und hat so Einsicht in alle Dateien und kann entsprechende Veränderungen auf dem System vornehmen. Verschärfend kommt noch hinzu, dass Antivirenprogramme durch die Anwendung der Signaturen in gewisser Weise ferngesteuert werden können. Daraus resultiert ein gewisses Restrisiko. Die Schlussfolgerung, vollständig und flächendeckend auf Antivirenprogramme zu verzichten, wäre allerdings falsch. Antivirenprogramme sind vor allem dann unerlässlich, wenn sehr viele Interaktionen von einem Gerät aus vorgenommen werden oder wenn von Benutzern direkt am Gerät gearbeitet wird. In diesem Fall ist ein ausgeprägter Virenschutz zu empfehlen.

Client, Server, Netzwerkperimeter

Antivirenprogramme können auf verschiedenen Ebenen zum Einsatz kommen. Grundsätzlich kann das Einsatzgebiet auf folgende Elemente eingeschränkt werden: Endgeräte/Clients, Server und Netzwerkelemente. Das organisationsspezifische Antivirenkonzept muss dabei alle Elemente unter Berücksichtigung der spezifischen Risikosituation in Betracht ziehen.

Da Endgeräte/Clients und Terminalserverumgebungen direkt mit dem Benutzer interagieren und häufig in Kontakt mit potentieller Schadsoftware kommen, sollten diese den höchsten Schutzgrad aufweisen. Bei Servern

kann, unter Berücksichtigung des jeweiligen Anwendungszwecks, der Einsatz von Antivirenprogrammen reduziert und mit anderen Massnahmen kompensiert werden.

Eingehende und ausgehende Netzwerkverbindungen sollten beim Eintritt in die Systemumgebung soweit als möglich auf schädliche Inhalte überprüft werden. Zudem sollten Webseiten, welche verseucht sind, temporär gesperrt oder unzugänglich gemacht werden. Die Prüfung auf Netzwerkebene erfolgt dabei typischerweise auf dem Netzwerkperimeter.

Anwendbarkeit

Die unter TOZ 4.5a und 4.6.2 aufgeführten Elemente müssen vor Schadsoftwarebefall geschützt sein. Das kann durch Installation eines Antivirenprogramms sowie durch die Umsetzung von alternativen Sicherheitsmassnahmen (z.B. Härtung, Netzwerkzonierung) erreicht werden.

Relevante TOZ-Anforderungen

4.5, 4.6.2

3.2 Empfehlungen

Verschiedene Produkte

Da jedes Antivirenprogramm nur einen Teil aller Schadsoftware entdeckt, empfehlen wir, auf dem Client und dem Server ein spezialisiertes Antivirenprogramm eines Herstellers und auf dem Perimeter ein dazu spezialisiertes Antivirenprogramm eines anderen Herstellers zu installieren. Dies erhöht die Wahrscheinlichkeit, eine Malware zu identifizieren.

Mehrstufiger Schutz

Antivirenprogramme auf Netzwerkperimetern haben die Aufgabe zu verhindern, dass Schadsoftware ins interne Netz gelangen kann. Der Netzwerkperimeter bildet dabei die erste Abwehrstufe und soll durch den Einsatz von zusätzlichen Antivirenprogrammen auf den Endgeräten/Clients unterstützt werden.

Aktualität der Software

Die zeitlichen Abstände der Aktualisierungen von Virenschutzprogrammen sowie Schadprogramm-Signaturen müssen konfigurierbar sein. Diese Aktualisierungsintervalle sollten möglichst kurzgehalten werden. Empfohlen wird hierbei eine stündliche Aktualisierung der Signaturen. Diese sollten aber mindestens täglich aktualisiert werden. Für die Virenschutzprogramme gilt, dass sie regelmässig aktualisiert werden sollen.

On Access Scanning

Unter On Access Scanning versteht man das Scannen nach Malware durch die Antivirenprogramme in Echtzeit. Alle Echtzeit-Aktivitäten, wie beispielsweise der Zugriff auf ein Dokument, werden beobachtet. Es wird empfohlen, das Verfahren so einzustellen, dass alle Interaktionen (auch lesende) vorgängig geprüft werden. Insbesondere sollten schreibende Zugriffe auf die Dokumentenablagen (Document Repositories) überprüft werden.

Heuristisches Verfahren

Trotz Antivirenprogrammen können Schadprogramme in das System gelangen. Dies liegt unter anderem daran, dass die Malware zum Zeitpunkt der Antiviren-Prüfung dem Antivirenprogramm noch unbekannt war. Um den Zeitraum bis zur Auslieferung der entsprechenden Signaturen für ein neues Schadprogramm zu überbrücken, sollten Viren-Suchprogramme zusätzlich über Mechanismen zur Erkennung noch nicht bekannter Schadprogramme verfügen. Diese Funktion wird „Heuristisches Suchen“ genannt und sollte beim Antiviren-Programm auf dem Endgerät/Client aktiviert sein. Mit dieser Funktion lassen sich auch noch unbekannte Schadprogramme aufspüren. Aufgrund des heuristischen Verfahrens ist es durchaus möglich, dass Fehlalarme ausgelöst werden. Für „False Positives“ wird ein Prozess zu deren Analyse und Bearbeitung empfohlen.

Full-Scan

Da Schadprogramme trotz Antiviren-Lösungen auf die Systeme gelangen können, wird ein regelmässiger Full-Scan empfohlen. Dabei sollen sämtliche bestehende Daten auf Malware geprüft werden. Da das Antivirenprogramm ständig aktualisiert wird und somit neue Schadprogramm-Signaturen erhält, kann durch einen Full-Scan bisher unentdeckte Malware gefunden werden. Aus Performance-Gründen sollte der Scan dann durchgeführt werden, wenn die Systemressourcen nicht stark beansprucht werden. Von Vorteil wäre, wenn die Software die Auslastung des Rechners kontrolliert und in Phasen, in welchen keine Rechenleistung vorgenommen wird, automatisch den Scan durchführt. Dieser Full-Scan sollte auf allen Elementen mit lokaler Datenablage wöchentlich durchgeführt werden.

Unveränderbare Konfigurationen

Die Konfiguration, insbesondere auf den Endgeräten/Clients, sollte so geschützt sein, dass die Benutzer keine sicherheitsrelevanten Änderungen an den Einstellungen der Antivirenprogramme vornehmen können. Insbesondere muss sichergestellt sein, dass die Benutzer die Viren-Schutzprogramme nicht komplett oder für bestimmte Verzeichnisse oder Dateien deaktivieren können.

Isolation von Schadsoftware

Entdeckt das Antivirenprogramm potentielle Schadsoftware oder besteht Verdacht auf infizierte Daten, sollte die Datei von den restlichen Daten isoliert werden. Im Anschluss daran sollte die Malware sofern möglich von der unter Quarantäne stehenden Datei entfernt werden. Sollte es nicht möglich sein, das Schadprogramm von der Datei zu trennen, muss die Datei gelöscht werden. Dabei ist der Benutzer über den Quarantäne- oder Löschvorgang zu informieren. Besteht Unsicherheit, ob die Schadsoftware vollständig entfernt werden konnte, wird empfohlen, das Betriebssystem neu zu installieren.

Zusätzliche Härtungsmassnahmen

Da es sich im EPD um sensitive Daten handelt, sollten die Elemente zusätzlich – über den Antivirenschutz hinausgehend – geschützt werden. Dazu eignen sich unter anderem folgende Massnahmen, welche auf allen Elementen (Server, Client und Netzwerk) zum Einsatz kommen können:

- **Whitelisting von Anwendungen:** Mit dem Freigeben von Anwendungen ist gemeint, dass nur Anwendungen auf dem Endgerät oder Server verwendet werden können, welche zuvor explizit erlaubt wurden. Nicht erlaubte Anwendungen, somit auch potentielle Schadsoftware, werden nicht ausgeführt.
- **Host-basierte Firewalls:** Mittels host-basierter Firewall kann ein Gerät zusätzlich geschützt werden. Diese kann die eingehenden und ausgehenden Netzwerkaktivitäten nur für diesen Host beschränken und somit die Auswirkung eines Schadsoftwarebefalls reduzieren.
- **Aktualisierung der Software:** Die installierte Software sollte stets zeitnah, in der Regel innerhalb von wenigen Tagen, aktualisiert werden.
- **Deaktivieren von Services:** Indem Dienste und Anwendungen auf den Elementen soweit als möglich eingeschränkt werden, kann die Angriffsfläche für Schadsoftware reduziert werden. Das heisst, dass nicht benötigte Dienste und Anwendungen deaktiviert und wenn möglich deinstalliert werden sollen.
- **Minimale Rechte:** Das Ausführen von benötigten Services sollte mit den minimal möglichen Berechtigungen erfolgen.
- Zusätzliche Härtungsmassnahmen nach den gängigen Best-Practice-Empfehlungen, abhängig vom jeweiligen Betriebssystem. Siehe dazu die Zusammenstellung von möglichen Hilfsmitteln [Hardening-Guides].

4 Erkennung und Behandlung von Sicherheitsvorfällen

4.1 Einleitung

Reaktive Fähigkeiten sind von grosser Bedeutung

Sicherheitsvorfälle können trotz adäquaten Massnahmen in den Bereichen der eingesetzten Technologie, der vorhandenen Infrastruktur, der Organisation oder des Personals vorkommen. Ein rasches und zielgerichtetes Vorgehen in deren Behandlung sowie der vorhergehenden Erkennung dieser ist daher ein kritischer Erfolgsfaktor für die dauerhafte Aufrechterhaltung eines angemessenen Sicherheitsniveaus.

Eine Organisation kann mit präventiven Massnahmen vor schädlichen Ereignissen geschützt werden. Damit wird die Eintrittswahrscheinlichkeit oder die Schadensauswirkung und somit das Risiko insgesamt reduziert. Die Komplexität heutiger Strukturen lässt jedoch eine vollständige Risikoreduktion oftmals nicht zu. Sicherheitsverantwortliche müssen davon ausgehen, dass gewisse Risiken trotz aller präventiven Massnahmen eintreffen werden. Es braucht demnach organisatorische und technische Verfahren sowie dedizierte Hilfsmittel, um potentielle Sicherheitsvorfälle als solche zu erkennen, diese zeitnah zu bearbeiten und das Schadensausmass möglichst gering zu halten.

Ein Sicherheitsvorfall kann sich demnach in den folgenden Bereichen einer Gemeinschaft ereignen:

- Physische Sicherheit
- Vorhandene ICT-Umgebung
- Benutzer und Anspruchsgruppen
- Applikationen und Systeme

Für alle vorgenannten Bereiche müssen demnach Vorkehrungen und Massnahmen zur Erkennung und Behandlung von Sicherheitsvorfällen definiert und umgesetzt werden.

Die jeweiligen Schwerpunkte sind dabei risikobasiert und organisationsspezifisch festzulegen. Auf Grund der verschiedenen Gemeinschaften gibt es individuelle Lösungen zur Bereitstellung und Vernetzung des elektronischen Patientendossiers. Der Zugriff auf die Applikation und das sich dahinter befindende System wird durch viele unterschiedliche Benutzer eingesetzt, welche wiederum unterschiedliche Endgeräte verwenden. Es ist daher notwendig, den Umgang mit Sicherheitsvorfällen klar zu definieren und dem Einsatz einer kontinuierlichen Optimierung dieses Umgangs unter allen Beteiligten eine hohe Bedeutung zu verleihen.

Gesamtübersicht

Dieses Kapitel beschreibt die einzelnen Prozessschritte zur Erkennung und gezielten Behandlung von Sicherheitsvorfällen. Die Beschreibungen enthalten jeweils technische und organisatorische Elemente sowie empfohlene Hilfsmittel. Zur Erarbeitung der besagten Hilfen wird empfohlen, realistische Vorfälle zu ermitteln und zu diesem Szenario entsprechende Hilfsmittel zu erarbeiten. Es wird dabei empfohlen, mindestens nachfolgende Szenarien zu berücksichtigen:

- Phishing
- Kritische Schwachstellen in Hard- oder Software
- DDoS -Angriff auf ein Zugangsportal
- Schadsoftware (z.B. Ransomware)
- Unerlaubte Dateneinsicht
- Datenabfluss
- Kompromittierter kryptografischer Schlüssel

Der übergeordnete Prozess zur Erkennung und Behandlung von Sicherheitsvorfällen besteht aus den nachfolgenden fünf Phasen:

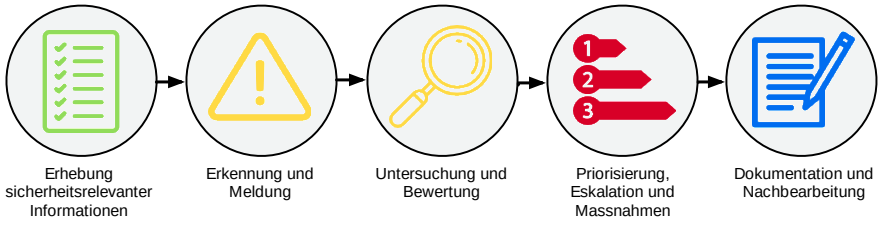

Abbildung 3: Prozess Erkennung und Behandlung Sicherheitsvorfälle

Ein möglicher Referenzprozess mit den jeweiligen Prozessschritten ist im Kapitel 4.7 ersichtlich.

4.2 Erhebung sicherheitsrelevanter Informationen

4.3.1, 4.3.2, 4.3.3, 4.6.1, 4.6.2

Relevante TOZ-Anforderungen

Um Sicherheitsvorfälle erkennen zu können, wird die tiefgehende Kenntnis der jeweiligen Umgebung vorausgesetzt. Die Strukturen, Schwachstellen und Risiken sowie die involvierten Anspruchsgruppen müssen vor Eintreten eines Vorfalls ermittelt und dokumentiert sein. Folgende Punkte sind im Sinne einer Vorbereitung einmalig und wiederkehrend zu erheben:

- Relevante bauliche Anlagen
- Struktur der relevanten Elemente, bestehend aus ICT-System- und Applikationslandschaft, und der Netzwerkumgebung (Gemäss TOZ 4.6.1 und TOZ 4.6.2)
- Verantwortlichkeiten der Elemente
- Informationswerte und Datenbestände sowie deren Kritikalität und Verteilung über die Systemlandschaft und die Klassifizierung der Informationen
- Benutzer und Anspruchsgruppen
- Bekannte Schwachstellen und Risiken

Sämtliche Angaben sind dabei mindestens jährlich oder nach grösseren Anpassungen auf ihre Vollständigkeit und Gültigkeit hin zu überprüfen.

Die Voraussetzungen auf technischer Ebene sind eine zentrale, vom Ursprungssystem getrennte Ablage der relevanten Protokolldaten sowie auto-

matisierte Verfahren zur laufenden Auswertung der Daten und die Erkennung von abnormalen Verhalten (Auffälligkeiten). Der Einsatz einer Logmanagement- oder Security-Incident-und-Event-Management-Lösung (SIEM) wird hierbei empfohlen.

4.3 Erkennung und Meldung

Relevante TOZ-Anforderungen

4.3.1, 4.3.2, 4.3.3

Erkennung durch automatisierte Überwachung

Auf der technischen Seite existieren eine Vielzahl von Möglichkeiten zur automatisierten Erkennung von potentiellen Sicherheitsvorfällen. Nachfolgende Massnahmen sollten im Umfeld des EPD umgesetzt sein:

- Verwendung von Antiviren-Software und automatische Alarmierung bei erkannter Schadsoftware (siehe Kapitel 3).
- Systematische Überwachung von Protokolldateien (Logfiles), Erkennung und Alarmierung von Auffälligkeiten (Logmanagement und SIEM).
- Auswertung der Netzwerkkommunikation durch den Einsatz von Firewalls und Intrusion Detection und Prevention Systeme (IDS/IPS).
- Überwachung sämtlicher EPD-bezogenen Zugriffe und Mutationen an relevanten Daten sowie aktive Alarmierung bei Auffälligkeiten.
- Überwachung von Berechtigungsmutationen sowie aktive Alarmierung bei Auffälligkeiten.
- Betriebliche Überwachung der relevanten Komponenten mit aktiver Alarmierung bei Fehlverhalten.

Zur gezielten Überwachung müssen vorgängig die relevanten und zu alarmierenden Ereignisse definiert werden (Events of Interest, EOI – Beispiele aus den TOZ sind Authentifizierungen am System, gemeinschaftsübergreifende Transaktionen über die Zugangspunkte der Gemeinschaften und die Suche nach Patienten). Diese Ereignisliste soll dabei regelmässig auf deren Aktualität geprüft werden. Ebenso soll geprüft werden, ob Ereignisse fehlen. Zudem müssen Umfang und Detailgrad der Protokolldaten über alle Elemente vereinheitlicht werden, damit im Bedarfsfall die notwendigen Informationen durchgängig ermittelt werden können.

Eine aktive Alarmierung der Betriebsorganisation sowie – im Falle eines sicherheitsrelevanten Ereignisses – eine direkte Meldung an den Datenschutz- und Datensicherheitsverantwortlichen wird empfohlen. Hierzu sollten soweit als möglich die bestehenden Betriebsprozesse sowie die dazugehörigen Betriebsmittel (z.B. Incident Management Tool, Ticketing-System usw.) zum Einsatz kommen.

Das Erkennen von potentiellen Sicherheitsvorfällen auf der Basis von Protokolldateien stellt hohe Anforderungen an die beteiligten Personen. Nebst fundierten und breiten technischen Fähigkeiten werden auch vertiefte Kenntnisse über das Systemumfeld benötigt. Zudem ist beim Inhaber dieser Rolle auf eine entsprechende Aufgabentrennung zu achten. So sollte die sicherheitsrelevante Überwachung getrennt von der eigentlichen Betriebsorganisation erfolgen.

Meldung durch Benutzende

Grundsätzlich kann jede/jeder Mitarbeitende die Meldung eines Sicherheitsvorfalls initiieren. Meldungen von Benutzern sind typischerweise Störungen, wie z.B. ein vermuteter oder tatsächlicher Virenbefall eines Endgerätes, Datenverluste oder Modifikationen von Informationen. Administratoren melden auch ihrerseits Störungen, welche sie im System feststellen. Es soll hierzu eine zentrale Anlaufstelle zur Meldung solcher potentiellen Sicherheitsvorfälle eingerichtet werden. Dies kann beispielsweise ein bestehender Help- oder Servicedesk der Betriebsorganisation sein.

Meldung aus einer anderen Organisation

Meldungen aus anderen beteiligten Organisationen (z.B. externer Betreiber, andere Gemeinschaften usw.), welche einen Vorfall bemerken und entsprechende Informationen zur Verfügung stellen, müssen zeitnah verarbeitet werden können. Es sollten daher entsprechende Informationsaustauschplattformen etabliert und genutzt werden. Frühzeitige Notifikationen sowie die Umsetzung der daraus resultierenden Erkenntnisse und Massnahmen können der Gemeinschaft einen wertvollen Zeitvorteil verschaffen.

Hilfsmittel

Der beschriebene Prozessschritt kann mit den nachfolgenden Hilfsmitteln unterstützt werden:

- Technische Überwachungs- und Monitoring-Instrumente
- Meldeprozess für sicherheitsrelevante Ereignisse
- Regelmässiger Austausch mit beteiligten Organisationen über Sicherheitsvorfälle und daraus resultierende Erkenntnisse

4.4 Untersuchung und Bewertung

Relevante TOZ-Anforderungen

4.4.1, 4.4.2, 4.5

Voraussetzungen

Ein potentieller Sicherheitsvorfall wurde erfolgreich detektiert und die Information liegt den verantwortlichen Personen vor. Zur gezielten Ergreifung von Massnahmen zur Eindämmung sowie zur Kommunikation des Vorfalls ist eine vorgängige Analyse der Einflussfaktoren notwendig. Die dazu notwendigen Hilfsmittel in Form von Checklisten oder Run-Books müssen vorgängig erarbeitet werden.

Erhebung der Einflussfaktoren

Zur Untersuchung und Bewertung des Sicherheitsvorfalls sind folgende Einflussfaktoren zu erheben:

- Welche Elemente sind von dem Sicherheitsvorfall betroffen?
- Wer hat den Vorfall bemerkt und gemeldet?
- Welcher Nutzerkreis / welche Daten sind von dem Sicherheitsvorfall betroffen (Grösse, Kritikalität usw.)?
- Müssen rechtliche Schritte eingeleitet werden?
- Welche Elemente können von dem Sicherheitsvorfall zusätzlich betroffen sein?

- Können Folgeschäden durch die Vernetzung der einzelnen ICT-Systeme der Gemeinschaften entstehen?
- Für welche Elemente können Folgeschäden ausgeschlossen werden?
- Wie hoch kann der durch den Sicherheitsvorfall verursachte direkte Schaden oder Folgeschade sein (Dabei ist insbesondere die Abhängigkeit der Elemente der einzelnen Gemeinschaften zu beachten)?
- Wodurch wurde der Sicherheitsvorfall ausgelöst (z.B. durch Unachtsamkeit, einen Angreifer, Ausfall der Sicherheitsinfrastruktur usw.)?
- Wann und an welcher Stelle hat sich der Sicherheitsvorfall ereignet?
- Sind durch den Sicherheitsvorfall nur interne Personen oder auch Patienten betroffen?
- Wie viele Informationen über den Sicherheitsvorfall sind bereits an die Öffentlichkeit gelangt?

Stellt sich bei dieser Untersuchung und Bewertung heraus, dass der Sicherheitsvorfall schwerwiegende Folgen nach sich ziehen kann, sollte eine unmittelbare organisationsinterne Eskalation erfolgen.

Nach der abgeschlossenen Erhebung der Einflussfaktoren sind als Nächstes die Handlungsoptionen zu erarbeiten, welche aus Sofortmassnahmen und ergänzenden Massnahmen bestehen. Die notwendige Zeitspanne für die Durchführung einzelner Massnahmen, deren Kosten und die benötigten Ressourcen für die Behebung und Wiederherstellung müssen im Prozess zwingend mitberücksichtigt werden.

Hilfsmittel

(siehe auch [Incident-Handling])

Der beschriebene Prozessschritt kann mit den nachfolgenden Hilfsmitteln unterstützt werden:

- Regelung der Verantwortlichkeiten
- Szenariobasierte Checklisten oder Run-Books zur systematischen Untersuchung und Bewertung von potentiellen Vorfällen
- Einheitliche Bewertungsskalen
- Definierte Kommunikationspfade

4.5 Priorisierung, Eskalation und Massnahmen

Relevante TOZ-Anforderungen

4.3.1, 4.3.2, 4.3.3

Voraussetzungen

In der Regel resultiert ein Sicherheitsvorfall aus einer Verkettung verschiedener Ursachen. Dabei sind meist mehrere verschiedene Geschäftsprozesse, Applikationen und Systeme betroffen. Es ist daher wichtig, dass die Prioritäten für die Problembeseitigung möglichst vorab festgelegt worden sind und somit eine Reihenfolge definiert werden kann, in welcher die erfassten Probleme und Schwierigkeiten behoben werden sollen.

Priorisierung vor der Behebung

Eine Prioritätensetzung ist organisationspezifisch und steht in Abhängigkeit zum Sicherheitsvorfall. Für die Prioritätensetzung sind demnach folgende Fragen zu bearbeiten:

- Welche Elemente sind betroffen und wie ist deren Schutzbedarf sowie die Kritikalität für das Gesamtsystem?
- Gibt es betriebliche Abhängigkeiten?
- Kann die Auswirkung des Vorfalls durch die Umsetzung von Sofortmassnahmen reduziert werden?
- Gibt es interne und externe Einflussfaktoren zur Priorisierung?
- Müssen Beweise gesichert werden?

Hilfestellung für die Beantwortung dieser Fragen bietet die Risikoanalyse zum elektronischen Patientendossier [EPD-RA], in welcher potentielle Schäden abgebildet und entsprechend ihres Schutzbedarfs kategorisiert sind. Es wird empfohlen, vorgängig anhand der Szenarien eine Priorisierung zu erarbeiten.

Definition und Umsetzung von Massnahmen

Es gibt Massnahmen, welche durchgeführt werden können, bevor detaillierte Resultate aus den laufenden Analysen vorliegen. Dies sind die sogenannten Sofortmassnahmen. Dazu gehören beispielsweise das Isolieren oder die Ausserbetriebnahme von einzelnen Diensten oder Systemen. Das Ergreifen beziehungsweise die Auslösung dieser oftmals bereits vordefinierten Abläufe soll die Eindämmung des Sicherheitsvorfalles weitgehend sicherstellen sowie das Fundament für erweiterte Massnahmen legen. Diese werden dann aus den Erkenntnissen der Analysen und Entscheidungen der verantwortlichen Personen generiert.

Pro erarbeitetes Szenario aus der Erhebung sicherheitsrelevanter Informationen soll eine vorgefertigte (nicht abschliessende) Massnahmenliste erarbeitet werden. Damit wird ein rasches und adäquates Handeln im Ereignisfall massgeblich unterstützt.

Eskalation und Meldewesen

Die bestehende Eskalationshierarchie mit den entsprechenden Voraussetzungen und Kommunikationskanälen innerhalb einer Organisation soll klar definiert, dokumentiert und mindestens einmal pro Jahr oder bei Organisationsanpassungen auf ihre Aktualität hin überprüft und gegebenenfalls angepasst werden. Weiter sollen diese Informationen allen Mitarbeitenden der Organisation in einfacher und rasch auffindbarer Form zur Verfügung gestellt werden.

Je nach Ausmass eines Sicherheitsvorfalles müssen zusätzlich beteiligte Dritte oder sonstige externe Organisationen informiert werden. Hierbei ist es wichtig, innerhalb der erarbeiteten Eskalationshierarchie klare Ebenen aufzuzeigen, wann ein Vorfall kommuniziert werden kann und welche Informationen in einem solchen Fall mit den beteiligten Organisationen geteilt werden.

Es muss ein Meldewesen für sicherheitsrelevante Vorfälle an die Zertifizierungsstelle sowie an das Bundesamt für Gesundheit etabliert werden. Dazu sind organisationsspezifische Kriterien zu definieren, bei welchen Vorfällen eine Meldung erfolgt und wie das Meldewesen prozessual abgewickelt wird.

Bei Verletzung der Persönlichkeitsrechte (z.B. unerlaubte Dateneinsicht) ist zudem die betroffene Person über den Vorfall in Kenntnis zu setzen.

Darüber hinaus wird empfohlen, bei Sicherheitsvorfällen mit grosser Trageweite (z.B. Dateneinsicht/-abfluss) die Öffentlichkeit über den Vorfall sowie die eingeleiteten Massnahmen zu informieren. Dazu sollten Stellungnahmen zur Verfügung stehen, damit die Information zeitnah, präzise und inhaltlich korrekt erfolgen kann.

Hilfsmittel

Der beschriebene Prozessschritt kann mit den nachfolgenden Hilfsmitteln unterstützt werden:

- Szenariobasierte Checklisten oder Run-Books zur Priorisierung von Sicherheitsvorfällen
- Szenariobasierte Massnahmenlisten (Sofortmassnahmen und ergänzende Massnahmen)
- Definierte Eskalationspfade und Meldeprozesse
- Regelungen zum Informationsaustausch (welche Informationen dürfen mit welchen Organisationen ausgetauscht werden)
- Kommunikationsregelungen zur Information der Öffentlichkeit

(siehe auch [Incident-Handling])

4.6 Dokumentation und Nachbearbeitung

Relevante TOZ-Anforderungen

4.3.1, 4.3.2, 4.3.3

Voraussetzungen

Nach der Bewältigung eines Sicherheitsvorfalls erfolgt die Dokumentation und Nachbearbeitung. Dabei gilt es, die wesentlichen Eigenschaften des Vorfalls (Ursache, Auswirkung, Betroffene, eingeleitete Massnahmen, Erkenntnisse, erfolgte Kommunikation) zu dokumentieren. Gleichzeitig muss geprüft werden, ob die bestehenden Prozesse und Hilfsmittel aufgrund der bewältigen Ereignisse aktualisiert oder erweitert werden müssen. Ebenso gilt es, die erstellte Risikoanalyse und allfällige Vorgaben und Richtlinien aufgrund von neuen Erkenntnissen anzupassen

Um sicherzustellen, dass die Nachbearbeitung die notwendige Priorität und Aufmerksamkeit erhält, muss hierbei auf klare Verantwortlichkeiten geachtet werden.

Lessons Learned

Das Lessons Learned definiert sich durch das Festhalten gewonnener Erkenntnisse, neuen Wissens oder neuer Erfahrungen. Sie können sowohl aus negativen wie auch aus positiven Erfahrungen abgeleitet werden und beschreiben ein mögliches Optimierungspotential zur jeweiligen Situation.

Im Rahmen des Gesamtprozesses zum Umgang mit Sicherheitsvorfällen müssen folgende Schritte durchlaufen werden, damit der erhoffte Nutzen generiert werden kann:

1. Erfahrungswerte sollen mit Beteiligung der involvierten Personen erfasst und zusammengetragen werden.
2. Die Erfahrungen sollen analysiert, bewertet und mit Angaben zu ihrem Gültigkeitsbereich dokumentiert werden.
3. Die dokumentierten Erfahrungswerte sollen den relevanten Anspruchsgruppen in leicht recherchierbarer Form zugänglich gemacht werden.

Auswertung

Folgende Informationen gilt es als Erstes zusammenzutragen und die erarbeiteten Resultate dann in einem Bericht zusammenzufassen:

- Was genau ist passiert und zu welchen Zeiten?
- Wie wurde in der betroffenen Organisation das Ereignis angegangen? Wurden dokumentierte Prozesse beigezogen? Waren diese angebracht/passend?
- Welche Informationen hätte man früher benötigt?
- Wurden Schritte unternommen und/oder Aktionen ergriffen, welche die Wiederherstellung behinderten?
- Was sollte in Zukunft anders gemacht werden?
- Wie kann der Informationsfluss mit anderen Organisationen verbessert werden?
- Welche Massnahmen können einen ähnlichen Vorfall in Zukunft verhindern?
- Welche neuen Abhängigkeiten wurden festgestellt?
- Welche Abläufe oder Indikatoren sollten in Zukunft besser überwacht werden, um ähnliche Vorfälle frühzeitig zu erkennen (z.B. Aktualisierung Events of Interest)?

- Welche zusätzlichen Ressourcen oder Instrumente werden benötigt, um das Erkennen, die Analyse und die Bewältigung von Sicherheitsvorfällen zu verbessern?

Aktualisierung von Checklisten und Vorgaben

Entscheidungen, welche aus dem Lessons Learned resultieren und zu Anpassungen in Prozessen, Checklisten und Weisungen führen, sollen auch in bestehenden Dokumentationen ergänzt werden. Die aktualisierten Unterlagen müssen anschliessend neu publiziert und kommuniziert werden.

Kommunikation

Die abschliessende Kommunikation sollte proaktiv an die Anspruchsgruppen erfolgen. Art und Umfang der Information sollten auf die Bedürfnisse der jeweiligen Anspruchsgruppen ausgerichtet sein. So sollte die Information an andere Gemeinschaften einen wesentlich höheren Detailgrad aufweisen als die Mitteilung an die Öffentlichkeit.

Hilfsmittel

(siehe auch [Incident-Handling])

Der beschriebene Prozessschritt kann mit den nachfolgenden Hilfsmitteln unterstützt werden:

- Regelung der Verantwortlichkeiten
- Szenariobasierte Checklisten oder Run-Books zur Dokumentation und Nachbearbeitung von Vorfällen
- Vorlagen und Anleitungen
- Regelungen zum Informationsaustausch (Welche Informationen dürfen mit welchen Organisationen ausgetauscht werden)
- Kommunikationsregelungen zur Information der Öffentlichkeit

4.7 Referenzprozess

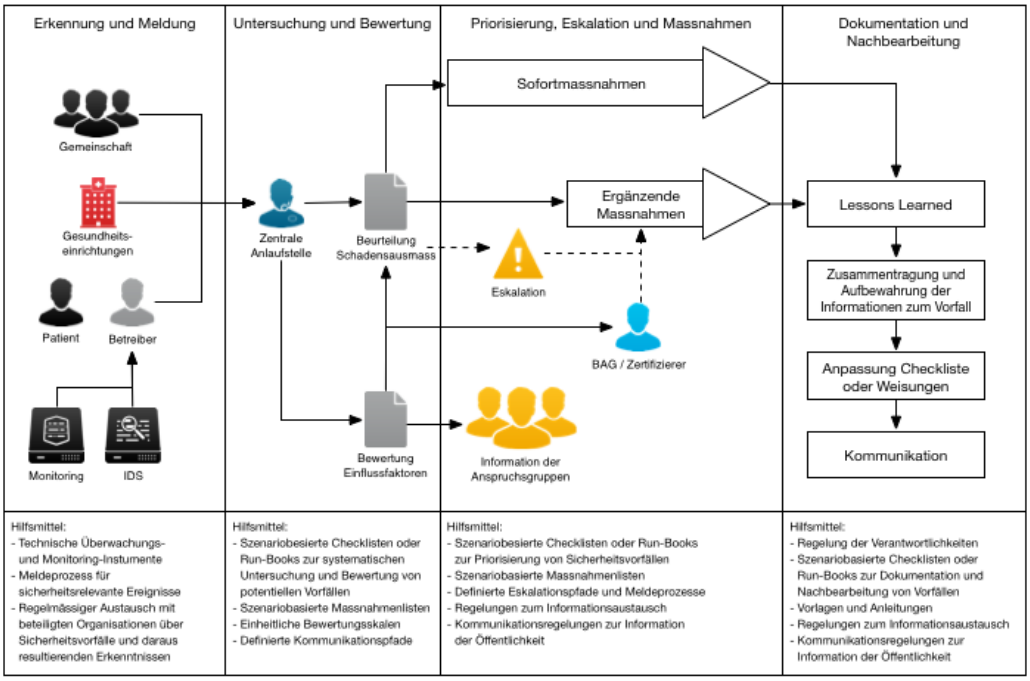

Abbildung 4: Referenzprozess

5 Datentrennung

5.1 Einleitung

Ausgangslage

Ausgehend von der gesetzlichen Vorgabe für das elektronische Patientendossier (EPDV Artikel 9, Absatz 1, Buchstabe c) und den technischen und organisatorischen Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften (TOZ 2.4b) müssen Gemeinschaften sicherstellen, dass die medizinischen Daten des elektronischen Patientendossiers (EPD) in den Dokumentenablagen so von anderen Datenbeständen getrennt gespeichert werden, dass sie gegen unzulässige Verwendung geschützt sind. Daraus ergibt sich eine Datentrennung, welche die Datenbestände separieren und die EPD-relevanten Daten isolieren soll.

Datentrennung

Der reine Begriff der Datentrennung kann verschieden genutzt werden. In diesem Dokument wird unterschieden zwischen der getrennten Datenhaltung, sprich der Ablage der Daten, und der getrennten Datenverarbeitung, welche das Bearbeiten der Daten nur getrennt ermöglichen soll. Die Vorgaben an das EPDV zielen einzig auf eine getrennte Datenhaltung und erlauben explizit die Bearbeitung der Daten mit einer gemeinsam genutzten Oberfläche. Damit sind auch hybride Nutzungen von Dokumentenablagen auf der gleichen Hardware, dem gleichen Betriebssystem und mit den gleichen Datenbanken möglich.

Datenbestände

Zu den bestehenden Datenbeständen, welche vom EPD separiert werden sollen, gehören unter anderem Daten aus Systemen wie dem Klinikinformationssystem (KIS) oder dem Praxisinformationssystem (PIS). In der EPD-Lösung sollen nur EPD-relevante Daten abgelegt oder verarbeitet werden. Diese getrennte Datenhaltung ist auf allen Ebenen der Lösung zu implementieren und betrifft sowohl das Primärsystem als auch Sekundärsysteme wie Archiv, Backup, Ablage- und Austauschplattformen.

Vorteile der Datentrennung

Die Datenbestände müssen separiert behandelt werden, damit die Verantwortung zwischen dem EPD und den Einrichtungen, welche an eine EPD-Gemeinschaft angebunden werden, klar definiert sind. Folgende Punkte werden dabei erreicht:

- Die **Hoheit** über die Daten in den Systemen einer Einrichtung liegt bei der jeweiligen Einrichtung. Die Hoheit über die Daten im EPD liegt jedoch beim Patienten. Der Patient kann insbesondere die Erfassung spezifischer Dokumente untersagen oder die Vernichtung bereits erfasster Daten verlangen.
- Die **Verantwortung** für eine angemessene Datensicherheit und den Datenschutz für die Systeme einer Einrichtung liegt bei der jeweiligen Einrichtung und erfolgt gemäss deren Policies und Standards. Die im EPD abgelegten Dokumente hingegen sind dem Datenschutz- und Datensicherheitsmanagementsystem der Gemeinschaft unterworfen, das den Anforderungen aus EPDV und TOZ genügen muss.

- Die **Aufsicht** über die Einrichtungen mit ihren Systemen und Daten obliegt den Kantonen oder – bei privaten Einrichtungen – dem Bund. Die Aufsicht über die Systeme und Daten des EPD obliegt dem Bund, der die EPD-Gemeinschaften gemäss den Vorgaben von EPDG, EPDV und TOZ zertifiziert.

Neben der klaren Verantwortlichkeit gibt es weitere Vorteile einer Separierung:

- **Datenschutz und Datensicherheit des elektronischen Patientendossiers**: Durch die Isolation der Datenbestände kann (besser) verhindert werden, dass über die Systeme einer Einrichtung (z.B. KIS oder PIS) direkt und unter Umgehung der EPD-Zugriffskontrolle auf Daten im EPD zugegriffen wird.
- **Datenschutz und Datensicherheit der Systeme einer Einrichtung**: Durch die Isolation der Datenbestände kann (besser) verhindert werden, dass Zugriffe auf die EPD Repositories aus dem Internet oder aus anderen Einrichtungen und Gemeinschaften die Verfügbarkeit und die Datensicherheit der Primärsysteme beeinträchtigen.
- **Fehlertoleranz**: Durch einen geordneten Replikationsprozess kann die Wahrscheinlichkeit dafür, dass nicht behandlungsrelevante Dokumente irrtümlich im elektronischen Patientendossier erfasst und von aussen zugreifbar werden, reduziert werden.
- **Datenlebenszyklus**: Die unterschiedlichen Aufbewahrungs- und Löschpflichten für Daten im EPD und Daten von Einrichtungen können einfacher erfüllt werden.
- **Zertifizierungsaufwand**: Die Zertifizierung einer EPD-Gemeinschaft kann auf isolierte Bereiche der angebundenen Einrichtungen eingegrenzt und damit effizienter durchgeführt werden.

Möglichkeiten der Datentrennung

Grundsätzlich gilt es bei der getrennten Datenhaltung zu unterscheiden zwischen einer physischen Trennung, bei welcher unterschiedliche Hardware für den jeweiligen Einsatzzweck verwendet wird, und der logischen Trennung, welche Hardware-unabhängig eine Trennung der Daten erzwingen soll. Die aktuellen Rahmenbedingungen lassen beide Möglichkeiten oder gegebenenfalls auch eine Kombination davon zu.

5.2 Erläuterung zur Datentrennung

Verhindern von Isolationsversagen

Aufgabe der Trennung ist es, eine Isolation der EPD-Dokumente von den sonstigen Datenbeständen zu erreichen. Diese Abschottung soll eine unbeabsichtigte „Durchlässigkeit“ (sogenanntes „Isolationsversagen“) mit technischen Mitteln verhindern. Unabhängig davon, ob die Trennung physikalisch oder logisch (z.B. durch getrennte Datenbanken, virtuelle Maschinen, Mandantentrennung etc.) vollzogen wird, muss die Isolation der „sekundären“ Dokumentenablagen von den „primären“ Daten der Primärsysteme eine sichere Abschottung erlauben und eine unbeabsichtigte „Durchlässigkeit“ mit technischen Mitteln sicher verhindern.

Ebenen der Datentrennung

Die aufgeführte Visualisierung zeigt einen vereinfachten Ablauf einer Datenverarbeitung bis zur Datenhaltung. Der Endnutzer (z.B. Patient oder Gesundheitsfachperson) editiert oder erfasst Daten innerhalb einer Applikation. Die Anwendung speichert die Daten in einer dafür vorgesehenen Datenbank. Die vorgenannten Elemente werden auf einem oder mehreren Betriebssystemen (OS) betrieben, wie beispielweise Windows oder Linux. Das OS wiederum kann sowohl virtuell, auf Basis einer Virtualisierungsplattform, oder auf einem physischen Server betrieben werden. Die Ablage sämtlicher Daten erfolgt dann auf einem Storage-System. In jeder Ebene können EPD- oder sonstige Daten verarbeitet werden. Die getrennte Datenhaltung kann dabei sowohl physisch als auch logisch von jeder Ebene aus erreicht werden. Im Falle einer logischen Trennung braucht es Sicherheitsmassnahmen, um ein Isolationsversagen zu vermeiden. Eine Trennung der Datenbestände auf einer möglichst hohen Ebene (Endnutzer, Anwendung) kann die Sicherheit der Daten erhöhen. Ab der Trennung dürfen die Daten auf den darunterliegenden Ebenen nicht mehr gemeinsam verarbeitet werden.

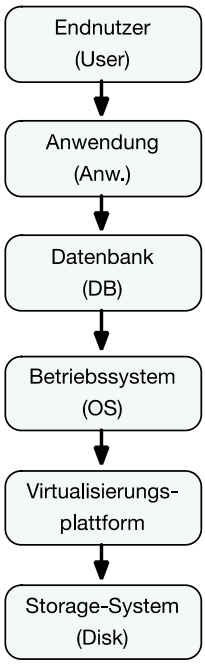

Abbildung 5: Ebenen der Datentrennung

Physische Datentrennung

Bei der physischen Trennung wird für EPD-bezogene Daten eine dedizierte Umgebung aufgebaut. Sämtliche Elemente werden ausschliesslich zur Verarbeitung von EPD-Daten verwendet. Die physische Datentrennung stellt die Maximalvariante dar und ermöglicht eine weitgehende Isolation der EPD-Daten. Eine komplette physische Trennung auf allen Ebenen erreicht zugleich eine getrennte Datenverarbeitung, welche dadurch zu einem erhöhten administrativen Aufwand führt, da Datensätze im EPD wie auch in den sonstigen Datenbeständen geführt und aktuell gehalten werden müssen.

Logische Datentrennung

Die logische Datentrennung setzt keine physische Trennung voraus, das heisst, vorhandene Hardware-Ressourcen können geteilt werden. Stattdessen wird die Trennung auf einer logischen Ebene durch Isolation und Virtualisierung vollzogen. Die logische Trennung ist grundsätzlich anfälliger auf ein Isolationsversagen. Die daraus resultierenden Risiken müssen getragen oder mit zusätzlichen Sicherheitsmassnahmen kompensiert werden. Mögliche nicht abschliessende Massnahmen können technisches Ursprungs sein (ein umfangreiches Hardening der Plattform oder eine Auditierung der Umgebung) oder durch organisatorische Massnahmen, wie beispielsweise der Segregation of Duties, kompensiert werden.

Visualisierung Logische Trennung

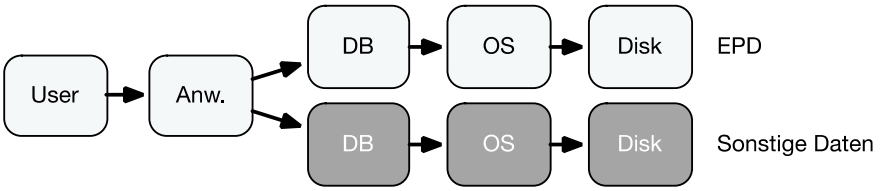

Abbildung 6: Logische Trennung

Kryptografische Trennung

Die Trennung der Daten kann grundsätzlich oder ergänzend kryptografisch erfolgen. Kryptografische Massnahmen können dabei auf sämtlichen Elementen zum Einsatz kommen. Damit eine sinnvolle Trennung vorliegt, müssen die Massnahmen mindestens auf Ebene der Applikation oder noch besser auf Ebene des Endbenutzers (User) zum Einsatz kommen. Eine Verschlüsselung durch den Endnutzer, welche nur durch ihn oder von ihm autorisierte Personen entschlüsselt werden kann, entspricht einer End-zu-End-Verschlüsselung. Es empfiehlt sich, die Datenbestände bereits beim Ablegen in der Applikation zu verschlüsseln. Damit können diese nur durch den Applikationsschlüssel wieder entschlüsselt werden. Dies erlaubt es, die Daten vor Zugriffen auf den Ebenen des Betriebssystems, der Datenbank und des Speichers zu schützen.

Visualisierung Kryptografische Trennung

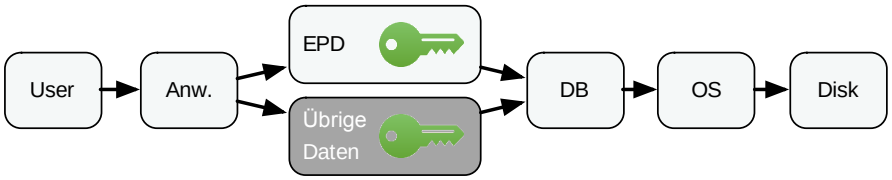

Abbildung 7: Kryptografische Trennung

Gegenüberstellung/Bewertung der Lösungen

Die drei Möglichkeiten der getrennten Datenhaltung sind unterschiedlich aufwendig umzusetzen und bieten nicht durchgängig denselben Schutz der Daten. Wird die grundsätzliche Trennung der Datenbestände durch eine logische oder physische Trennung genauer betrachtet, stellt sich die physische Trennung als Maximalvariante dar. Eine logische Trennung bietet mindere Hardware-Kosten durch geteilte Infrastruktur. Jedoch muss bei dieser Lösung sichergestellt werden, dass das Risiko eines Isolationsversagens reduziert wird. Die kryptografischen Massnahmen bieten den grössten Schutz der Daten, da sie die Daten ab der Verschlüsselung vor Isolationsversagen auf jeder unterliegenden Ebene schützen. Der höhere Aufwand, welcher mit einer solchen Implementation verbunden ist, wird durch einen hohen Schutz der Daten belohnt. Eine Kombination der physischen oder logischen Trennung mit zusätzlichen kryptografischen Massnahmen erhöht den Schutz der Daten zusätzlich. Gesetzlich sind alle drei Variationen oder eine Kombination möglich. Um dem hohen Schutzbedarf der Daten gerecht zu werden, empfiehlt sich die kryptografische Variante mit einer Verschlüsselung auf mindestens Ebene Applikation.

5.3 Ausgestaltung der Datentrennung Sicht Gemeinschaft

Bei der Datenregistrierung

Bereits bei der Erfassung (Registrierung) von Daten sollte die Ablage getrennt erfolgen. Dies kann auf Applikationsebene oder organisatorisch gelöst werden. Für die Benutzenden muss aufgrund von Hinweisen oder bedingt durch die Arbeitsschritte deutlich gemacht werden, dass EPD-relevante Daten verarbeitet werden. Es darf neben den für die Gesundheitsfachpersonen vorgesehenen Verfahren (Erfassen, Herunterladen) lediglich eine weitere Rolle mit entsprechenden Systemprivilegien geben. Um unzulässige Datenübertragung zu vermindern, sind die entsprechenden Zugänge oder Applikationsschlüssel geeignet abzusichern und beispielsweise durch weitergehende organisatorische Massnahmen („segregation of duties“, „Vier-Augen-Prinzip“) zu schützen. Allfällige Importprozeduren oder sonstige automatisierten Verfahren sollten dediziert bereitgestellt und überwacht werden.

In der Anwendung

Eine getrennte Datenhaltung schliesst grundsätzlich nicht aus, dass beide Datenarten in derselben Anwendung verarbeitet werden. Die Datenbearbeitung ist jedoch soweit als möglich zu trennen.

Arbeitsschritte, welche eine Zusammenführung der beiden Datenarten bedingen, müssen abschliessend bekannt und minimal gehalten sein. Die entsprechenden Arbeitsschritte dürfen nur von einem ausgewählten Benutzerkreis (EPD-GFPs) ausgeführt werden. Eine dauerhafte Ablage von zusammengeführten Datensätzen muss unterbunden werden.

Bei der Datenhaltung

Bei der Datenhaltung ist mindestens eine logische Trennung auf Ebene Betriebssystem vorzunehmen. Ein bestehendes Storage-System oder eine Virtualisierungsplattform können demnach weiterverwendet werden. Dabei sind in Bezug auf die EPD-relevanten Daten folgende Aspekte zu berücksichtigen:

- Auf der Ebene des Storage-Systems besteht eine logisch getrennte Ablage. Der getrennte Bereich verfügt über eine eigene EPD-konforme Berechtigungsdomäne für Systemadministratoren.
- Das Betriebssystem wird als eigenständige virtuelle Maschine bereitgestellt. Die Interaktion mit anderen Maschinen sowie der darunterliegenden Virtualisierungsplattform ist so weit wie möglich eingeschränkt. Um das Risiko eines möglichen Isolationsversagens auf der Ebene der Virtualisierung möglichst klein zu halten, soll nur bewährte und aktuell gehaltene Virtualisierungssoftware eingesetzt werden. Die virtuelle Disk ist dabei vollständig verschlüsselt. Alternativ besteht auch die Möglichkeit, die Ablage auf Ebene Storage-System zu verschlüsseln.

Bei der Archivierung

Die Archivierung der Daten muss mindestens eine logische Trennung vorweisen. Ein bestehendes Archiv-System kann demnach weiterverwendet werden. Auf der Ebene des Storage-Systems besteht eine logisch getrennte Ablage. Der getrennte Bereich muss über eine eigene EPD-konforme Berechtigungsdomäne für Systemadministratoren verfügen. Die virtuelle Disk ist vollständig zu verschlüsseln. Alternativ besteht auch die Möglichkeit, die logisch getrennte Ablage des EPD-Bereichs zu verschlüsseln.

5.4 Ausgestaltung der Datentrennung Sicht Outsourcing-Provider

Grundsatz

Werden bei einem Outsourcing-Provider EPD-bezogene Datenbestände von unterschiedlichen Gemeinschaften oder Einrichtungen verarbeitet, sind diese grundsätzlich getrennt zu bearbeiten und zu speichern. Dies gilt sowohl in Bezug auf die verschiedenen Gemeinschaften als auch in Bezug auf Daten weiterer Kunden des Outsourcing-Providers. Die notwendige Trennung auf Anwendungsebene kann am besten durch eine logische Massnahme erreicht werden.

Mandantenfähigkeit der Anwendung

Die Anwendung muss verschiedene voneinander getrennte Mandanten unterstützen. Unter Mandantenfähigkeit sind folgende Punkte zu verstehen:

- Getrennte Datenablage und somit keine Möglichkeit für einen Mandanten-übergreifenden Datenaustausch oder Isolationsversagen.
- Dedizierte Berechtigungsdomäne pro Mandant.
- Transaktionen werden innerhalb eines Mandats geschlossen abwickelt.
- Mandantenspezifische Konfiguration der Anwendung.
- Mandantenspezifische Protokollierung sowie Ablage der Protokolldateien.
- Mandantenspezifische Löschung von Daten (auch Backups und Protokolldaten).

Kryptografische Trennung

Zusätzlich zur Mandantenfähigkeit ist eine kryptografische Trennung der verschiedenen Datenbestände notwendig. Dies soll durch eine mandantenspezifische Verschlüsselung auf der Ebene der Anwendung erreicht werden. Alle Daten eines Mandats werden demnach mit einem spezifischen Schlüssel verschlüsselt und abgelegt. Im Falle eines Isolationsversagens auf der Ebene der Anwendung verfügen die Daten über einen zusätzlichen Schutz. Zudem sind Daten gegen unerlaubte Einsichtnahme auf der Ebene der Infrastruktur durch die Systemadministratoren geschützt.

Physische Trennung

Eine vollständige physische Trennung der EPD-bezogenen Datenbestände bei einem Outsourcing-Provider ist ebenfalls möglich und würde die Anforderungen an die Mandantenfähigkeit erfüllen. Die Daten müssen zudem mindestens auf Ebene Datenträger verschlüsselt sein. Empfohlen ist eine Verschlüsselung der Daten auf Ebene Anwendung.

6 Einsatz von Kryptografie

6.1 Einleitung

2.5, 4.12	Relevante TOZ-Anforderungen
Die Kryptografie ist ein wichtiger Bestandteil der Informationssicherheit. Es geht im Wesentlichen darum, Daten, Nachrichten und die Kommunikation zu verschlüsseln. Diese Verschlüsselung dient dazu, dass die Informationen vor der Einsicht und der Manipulation geschützt sind. Die generellen Ziele der Kryptografie lassen sich demnach wie folgt beschreiben:	Einleitung
Durch die Verschlüsselung einer Datei oder Nachricht bleibt deren Inhalt für eine nicht autorisierte Person trotz Besitz der Datei oder Nachricht ohne den passenden Schlüssel (Key) unbekannt.	Vertraulichkeit
Durch Anwendung von kryptografischen Massnahmen werden unautorisierte Änderungen an den Daten verhindert respektive nachweisbar gemacht. Die Integrität kann dadurch sichergestellt werden, dass unerlaubte Veränderungen sichtbar sind.	Integrität
Durch die qualifizierte persönliche elektronische Signatur von Informationen ist der Absender einer Nachricht oder der Ersteller einer Datei eindeutig nachweisbar.	Authentizität
Die im vorliegenden Dokument empfohlenen kryptografischen Verfahren können gemäss dem aktuellen Stand heute und in naher Zukunft als sicher betrachtet werden. Die Entwicklung ist jedoch mit Unsicherheit behaftet (z.B. Quanten-Computing). Entsprechend können die Empfehlungen durch aktuelle Entwicklungen übersteuert werden. Bei der Auswahl der Verfahren sowie der dazugehörigen Systemparameter (z.B. Schlüssellänge) wurde im vorliegenden Dokument eine Sicherheitsreserve vorgesehen, wodurch der Einsatzzeitraum – vorbehaltlich neuer, unvorhersehbarer Entwicklungen – über rund zehn Jahre sichergestellt sein sollte.	Gültigkeit und Einsatzdauer

6.2 Kryptografische Grundsätze

Auf Eigenentwicklungen oder Adaptionen von Algorithmen oder Verfahren muss verzichtet werden. Die eingesetzten Algorithmen und deren Implementation müssen durch eine möglichst breite Expertengruppe überprüft worden sein, um das Risiko von Schwachstellen zu minimieren.	Keine Eigenentwicklung
Der Kerckoffs'sche Grundsatz besagt, dass die Sicherheit eines Verfahrens darauf beruht, dass der Schlüssel und nicht der Verschlüsselungsalgorithmus geheim ist. Ein öffentlich bekannter Algorithmus bietet den Vorteil, dass dieser breitflächig und unabhängig auf mögliche Schwachstellen hin geprüft werden kann. Dadurch können sich zahlreiche Experten an der Entwicklung und Weiterentwicklung beteiligen. Im Kontext des EPD sollen deshalb offene Verfahren bevorzugt werden.	Verwendung von offenen Verfahren
Auf dem Markt gibt es viele unterschiedliche Verfahren, welche den ersten beiden bereits genannten Grundsätzen nicht widersprechen und daher eingesetzt werden können.	Zugelassene Verfahren

Sofern Verfahren zum Einsatz kommen, welche von den vorliegenden Empfehlungen abweichen, sollten die Empfehlungen von FIPS [FIPS140.0] berücksichtigt werden.

6.3 Speicherverschlüsselung

2.5	Relevante TOZ-Anforderungen
EPD-relevante Daten müssen immer in verschlüsselter Form aufbewahrt werden.	Beschreibung

6.4 Transportverschlüsselung

2.5, 4.15.3, 4.15.4	Relevante TOZ-Anforderungen
EPD-relevante Daten müssen nicht nur während deren Aufbewahrung im EPD-Kontext geschützt werden, sondern auch beim Transport. Eine typische Angriffsform auf Datentransporte ist die sogenannte Man-In-The-Middle-Attacke. Dabei steht ein Angreifer zwischen den beiden Kommunikationspartnern und kontrolliert somit den Datenverkehr. Wenn ein Angreifer in einem solchen Fall aber nur verschlüsselte Daten abfängt, kann er damit nichts anfangen, wenn er den entsprechenden Schlüssel nicht kennt. Für diese Verschlüsselung des Datenverkehrs wird die sogenannte Transport-Layer-Security-Verschlüsselung eingesetzt (TLS). Siehe dazu die Empfehlungen im Kapitel 6.11.	Beschreibung

6.5 Kryptografische Verfahren

Erläuterung

Unter dem Begriff „Kryptografische Verfahren“ versteht man Algorithmen, Mechanismen und Verfahren, welche der Verschlüsselung von Informationen dienen. Es wird unterschieden zwischen symmetrischen und asymmetrischen Verfahren sowie hybriden Verfahren, welche eine Kombination dieser beiden Verfahren darstellen. Im Rahmen des elektronischen Patientendossiers (EPD) werden beide Verfahren verwendet. Daher werden diese nachfolgend kurz erläutert.

Symmetrische Verfahren

Das symmetrische Verfahren arbeitet mit einem einzigen Schlüssel für Ver- und Entschlüsselung von Informationen. Dieses Verfahren ist Ressourcenschonend und verhältnismässig einfach zu implementieren.

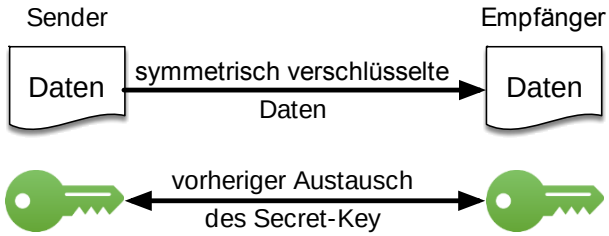

Abbildung 8: Symmetrische Verschlüsselung

Symmetrischer Verschlüsselungsprozess

Das Verfahren arbeitet mit einem einzigen Schlüssel (Secret-Key), welcher beim Sender und beim Empfänger vorhanden sein muss. Es ist demnach rasch in seiner Ausführung und bietet bei einer entsprechenden Länge des Schlüssels auch einen angemessenen Sicherheitsstand. Die Schwierigkeit liegt bei der vorhergehenden Schlüsselübergabe der beiden kommunizierenden Gemeinschaften. Wird die Kommunikation von einem Angreifer bei der Schlüsselübergabe abgefangen, so sind die verschlüsselten Informationen auch nicht mehr geschützt, da der Angreifer diese selbst auch entschlüsseln kann. Weiter kann sich ein Angreifer auch eines Schlüssels bemächtigen, wenn dieser bei einem der kommunizierenden Gemeinschaften nicht entsprechend geschützt abgespeichert ist.

Schlüsselaustausch

Beim Schlüsselaustausch ist darauf zu achten, dass dieser über eine gesicherte Verbindung oder in verschlüsselter Form (z.B. durch Anwendung von asymmetrischen Verfahren) übertragen wird.

siehe Kapitel 6.8

Advanced Encryption Standard (AES)

Als symmetrisches Verschlüsselungsverfahren wird AES empfohlen. AES kann mit unterschiedlichem Betriebsmodus und Systemparameter verwendet werden.

Betriebsmodus

Der Betriebsmodus sollte wie folgt ausgewählt werden:

- Bei einer Blockverschlüsselung wird empfohlen, Cipher-Block Chaining (CBC) einzusetzen.
- Ist neben der Verschlüsselung auch eine Authentifizierung der Daten erforderlich, sollte der Galois Counter Mode (GCM) verwendet werden.
- Für eine Stromverschlüsselung wird der Counter Mode (CTR) empfohlen.
- Im Falle, dass ein Initialisierungsvektor (IV) benötigt wird, muss dieser für jede Verschlüsselung neu generiert werden. Es ist essentiell,

dass sich dieser IV innerhalb einer Schlüsselwechselperiode nicht wiederholt und dass er nicht voraussehbar ist.

AES kann mit unterschiedlicher Schlüssellänge verwendet werden. Es wird empfohlen, mindestens AES-256 mit einer Schlüssellänge von 256 Bit zu verwenden.

Minimale Schlüssellänge

Es wird empfohlen, AES-256 mit dem Cipher-Block Chaining (CBC) oder im Falle von TLS mit dem Verfahren Galois Counter Mode (GCM) einzusetzen.

Empfehlung zum symmetrischen Verfahren

Beim asymmetrischen Verfahren werden zwei unterschiedliche, von einander abhängige Schlüssel eingesetzt. Dieses Schlüsselpaar besteht aus einem öffentlichen (Public Key) und einem privaten (Private Key) Schlüssel. Das asymmetrische Verfahren wird auch Public-Key-Verschlüsselung genannt.

Asymmetrische Verfahren

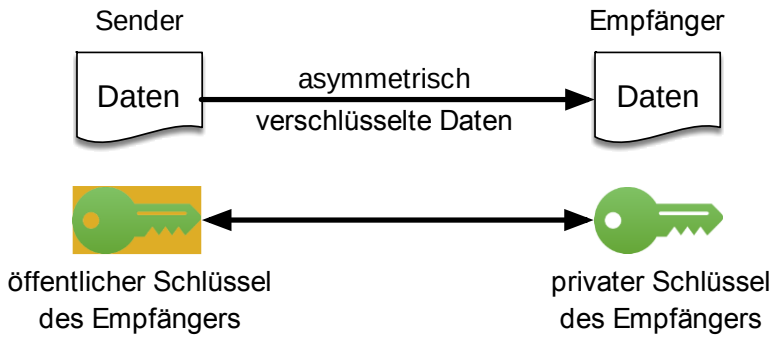

Abbildung 9: Asymmetrische Verschlüsselung

Informationen, welche mit einem öffentlichen Schlüssel verschlüsselt werden, können nur mit dem privaten Schlüssel entschlüsselt werden. Deshalb muss der private Schlüssel vom Besitzer des Schlüsselpaares geheim gehalten werden. Will der Sender eine verschlüsselte Nachricht an den Empfänger senden, so benötigt er den öffentlichen Schlüssel des Empfängers. Mit dem öffentlichen Schlüssel wird die Nachricht verschlüsselt, kann aber nicht mehr mit diesem entschlüsselt werden (Einwegfunktion). Für die Entschlüsselung benötigt es den privaten Schlüssel des Empfängers. Wichtig bei diesem Verfahren ist, dass der private Schlüssel (Private Key) geheim gehalten wird. Kommt ein Angreifer an den privaten Schlüssel, kann dieser auf die verschlüsselten Erzeugnisse zugreifen und diese entschlüsseln.

Asymmetrischer Verschlüsselungsprozess

Im Gegensatz zum symmetrischen Verfahren ist die Schlüsselverteilung hier einfacher. Jedoch benötigt dieses Verfahren mehr Rechenleistung als das symmetrische Verfahren. Aus diesem Grund wird das asymmetrische Verfahren in der Praxis häufig dazu verwendet, die Schlüssel für das symmetrische Verfahren zu übermitteln.

Schlüsselverteilung

siehe Kapitel 6.8

Es wird empfohlen, RSA mit einer Schlüssellänge von 4096 Bit (oder höher) für die asymmetrische Verschlüsselung zu verwenden.

Empfehlung zum asymmetrischen Verfahren

6.6 Hashing

Relevante TOZ-Anforderungen

2.10, 4.3.1, 4.13.1, 10.2.3

Einleitung

Hash-Verfahren bilden einen eigenen Bereich der Kryptografie und sind ein wichtiges Instrument zum Schutz von Informationen. Die Länge des Hash-Wertes wird in Bit angegeben. Der Datensatz kann dabei aus einem einzelnen Zeichen, einem Satz oder einer komplexen Datei bestehen. Die erzeugte Zeichenkette wird als digitaler Fingerabdruck (Fingerprint), kryptografische Prüfsumme, Message Digest (MD) oder Message Authentication Code (MAC) bezeichnet. Diese Bezeichnungen sind auch als der Hash-Wert oder nur Hash bekannt. Die Bildung dieses Wertes hat in erster Linie nichts mit einem kryptografischen Verfahren zu tun. Das bedeutet, dass nicht jedes Hash-Verfahren ein kryptografisches Hash-Verfahren ist.

Voraussetzungen für ein Hash-Verfahren

Ein Hash-Verfahren gilt als kryptografisches Hash-Verfahren, wenn folgende Punkte erfüllt sind:

1. Eindeutigkeit:
   Eine identische Zeichenfolge muss zum selben Hash-Wert führen.
2. Reversibilität:
   Der Hash-Wert darf nicht in die ursprüngliche Zeichenfolge zurückberechnet werden können.
3. Kollisionsresistenz:
   Zwei unterschiedliche Zeichenfolgen dürfen nicht absichtlich den gleichen Hash-Wert ergeben.

Empfehlung zum Hashing

Es wird empfohlen, für das Hashing zum Speichern von Passwörtern die Algorithmen ARAGON2 respektive PBKDF2 mit Salz einzusetzen. Für Einsatzzwecke, bei denen die Geschwindigkeit hoch sein muss, wie zum Beispiel bei TLS, sind die Verfahren SHA-512 oder SHA3-512 zu verwenden

6.7 Ersatz von Verfahren mit bekannten Schwachstellen

Ersatz von Verfahren

Sollten bei einem verwendeten Verfahren neue Schwachstellen bekannt werden, welche dazu führen, dass die definierten Ziele aus dem Sicherheitskonzept (siehe Kapitel 6.1) nicht mehr vollständig erfüllt werden können, so muss der zeitnahe Ersatz eines Verfahrens angestrebt werden.

Transparenz über die eingesetzten Komponenten

Es wird empfohlen, die eingesetzten Software-Komponenten und Verschlüsselungsverfahren kontinuierlich auf mögliche Schwachstellen hin zu überwachen. Dazu müssen die notwendigen Informationen (z.B. verwendete Software-Versionen) bekannt und im Inventar erfasst sein (siehe Kapitel 2.6). Folgende Hilfsmittel können dazu in einer Entwicklungsumgebung verwendet werden:

- OWASP Dependency Check
- Versions-Plugin für Maven

Zusätzlich sollten Meldungen von CERTs sowie bekannte Verwundbarkeitsdatenbanken regelmässig geprüft werden. Eine Liste mit Informationsquellen ist den [CERT-Meldungen] zu entnehmen.

6.8 Schlüsselverwaltung

Schlüsselgenerierung

Bei der Generierung von Schlüsselmaterial gilt es zu beachten, dass die verwendeten kryptografischen Module, wenn möglich kompatibel sind mit FIPS 140.0-2 [FIPS140.0] und entsprechend konfiguriert wurden. Jegliches Schlüsselmaterial muss in diesem Modul generiert werden. Generell sind Hardwaremodule Softwaremodulen vorzuziehen.

Schlüsselverteilung

Beim Schlüsselaustausch ist darauf zu achten, dass dieser über eine gesicherte Verbindung oder in verschlüsselter Form (z.B. durch Anwendung von asymmetrischen Verfahren) übertragen wird.

Schlüsselspeicherung

Folgende Punkte sollen für die Speicherung von Schlüsseln beachtet werden:

1. Der Speicherort (innerhalb der Applikation sowie auf den Datenträgern) von kryptografischem Schlüsselmaterial soll dem notwendigen Personenkreis bekannt sein.
2. Die Schlüssel sollen durch kryptografische Module geschützt sein, unabhängig davon, ob sich diese auf dem eigentlichen Datenträger der Aufbewahrung oder in einem vorübergehenden Zwischenspeicher befinden.
3. Auf die Aufbewahrung von Schlüsselmaterial in Klartext muss verzichtet werden.
4. Soweit möglich sollten alle Schlüssel in einem kryptografischen Tresor wie einem Hardware-Sicherheits-Modul (HSM) oder einem isolierten kryptografischen Service aufbewahrt werden.
5. Wenn Schlüssel in einer Datenbank aufbewahrt werden sollen, soll sichergestellt sein, dass die Schlüssel vor dem Transport auf den Datenträger mit Key Encryption Keys (KEK) verschlüsselt werden. Diese müssen mindestens die gleiche Stärke aufweisen wie die Schlüssel selbst.
6. Es soll sichergestellt sein, dass Schlüssel in einer Datenbank über Integrity Proctection verfügen. Dies kann durch die Verwendung eines Dual-Purpose-Algorithmus umgesetzt werden, welcher Verschlüsselung und Message Code Authentication (MAC) unterstützt.
7. Es soll sichergestellt sein, dass der Standard Applikationscode keine kryptografischen Schlüssel, sondern Key Management Libraries verwendet.
8. Es soll sichergestellt sein, dass Schlüssel- und kryptografische Operationen immer innerhalb eines geschützten Tresors ausgeführt werden. Dies betrifft den Schlüssel-Zugriff, die Ver- und Entschlüsselung sowie das Signieren.

Backup von Schlüsseln

Verschlüsselte Dateien können bei Verlust des dazu verwendeten Schlüssels nicht mehr wiederhergestellt werden. Daher ist ein adäquates Backup-Management der Schlüssel von hoher Wichtigkeit. Unter gewissen Voraussetzungen müssen Daten aus dem EPD wiederhergestellt werden können.

Wenn eine Backup-Datei von Schlüsseln erstellt wird, muss diese mit einem kryptografischen Modul von mindestens FIPS 140.0-2 [FIPS.140.0] versehen werden.

6.9 Schlüssel Verantwortlichkeiten und Audit

Identifikation

Die Verantwortlichkeit beinhaltet die Identifikation aller Anwender und Systemadministratoren im Rahmen der Systementwicklung und des Betriebs des EPD mit Zugang oder Kontrolle über die kryptografischen Schlüssel während deren Lebenszyklus. Mit Hilfe von klar definierten Verantwortlichkeiten kann dem generellen Missbrauch von Schlüsseln vorgebeugt sowie auch das Ausmass bei einem Missbrauch eingedämmt werden.

Resultierende Vorteile

Geregelte Verantwortungen für die Zugriffe auf sämtliches Schlüsselmaterial ergeben die folgenden Vorteile für eine Gemeinschaft im EPD:

1. Bei einem erkannten Missbrauch lässt sich durch die Verantwortlichkeit über den betroffenen Schlüssel rasch erkennen, welche Individuen im Sicherheitsvorfall involviert sind und wie dieser zustande gekommen ist.
2. Eine klare Verantwortung schützt den Schlüssel zusätzlich, da betroffene Anwender darüber informiert sind, dass sie bei einem Vorfall Rechenschaft darüber ablegen müssen, was die Sensibilisierung zum Umgang damit erhöht.
3. Das Wissen darüber, welche Daten durch einen missbrauchten Schlüssel geschützt waren, hilft beim Prozess im Sicherheitsvorfall für die Wiederherstellung der Daten, da durch den Vorfall ein möglicher Integritätsverlust entstanden ist.

Prinzipien

Um diese Vorteile zu gewährleisten, sollen die folgenden Prinzipien der Verantwortung bezüglich der Schlüssel eingehalten werden:

1. Alle Schlüssel müssen eindeutig identifizierbar sein.
2. Der Benutzer eines Schlüssels muss eindeutig identifizierbar sein.
3. Jeder Einsatz eines Schlüssels muss aufgezeichnet werden (Datum, Zeitpunkt, Benutzer, Zugriff auf welche Daten).

Audit Voraussetzungen

Für die Auditierung müssen zwei unterschiedliche, sich ergänzende Ansätze durchgeführt werden. Zum einen werden regelmässige Audits im Bereich der eingesetzten Prozeduren und der generellen Schlüsselverwaltung [NIST-SP-800-57] benötigt, zum anderen müssen auch die konkreten Schutzmechanismen regelmässig auditiert und in Bezug auf die Daten, welche von ihnen geschützt werden, hinterfragt werden. Es handelt sich hierbei um eine zusätzliche Auditempfehlung, unabhängig vom Zertifizierungsaudit sowie von allfälligen Lieferanten-Audits.

Kontinuierliche Anpassungen

Neue Formen von Technologien und Angriffen müssen stets bei der Auditierung mitbedacht werden, um frühzeitig auf mögliche Bedrohungen reagieren zu können. Weiter ist zu berücksichtigen, dass die Sicherheit der aktuell eingesetzten Technologie stark von den menschlichen Einflussfaktoren abhängig ist. Die involvierten Personen sollten deshalb regelmässig geschult und sensibilisiert werden (siehe Kapitel 2.4).

6.10 Kompromittierung von Schlüsseln und Wiederherstellung von kompromittierten Dateien

Ein kompromittierter Schlüssel muss so rasch wie möglich gesperrt werden. Das bedeutet, dass die Daten, zu welchen der Schlüssel den Zugang eröffnet, mit einem neuen Schlüssel versehen werden müssen, um den unberechtigten Zugang zu verhindern. Weiter muss auch davon ausgegangen werden, dass Dateien, zu welchen es einen kompromittierten Schlüssel gab, veränderte Inhalte enthalten können.

Präventive Prozeduren

Folgende Prozeduren müssen von einer Gemeinschaft im EPD sichergestellt werden, damit die Möglichkeiten zur Kompromittierung eines Schlüssels minimiert und das mögliche Schadensausmass eingedämmt werden kann:

1. Es muss eine zeitliche Limitierung geben, in welcher ein symmetrischer Schlüssel in Klartext vorhanden ist. Und zwar unabhängig davon, ob sich dieser in einer Datenbank oder einem Zwischenspeicher befindet.
2. Benutzern und Systemadministratoren sollte es soweit als möglich verunmöglicht sein, Schlüssel in Klartext-Form einsehen zu können.
3. Einführung und Einhaltung eines Verantwortlichkeitssystems inkl. Aufzeichnung sämtlicher Verwendungen und Zugriffen von Schlüsseln.
4. Einsatz einer Integritätsprüfung bei den Schlüsseln (MAC oder digitale Signaturen).
5. Einsatz von vertrauenswürdigen Timestamps (Zeitnachweisen). Es ist dazu die gesetzliche Zeit der METAS zu verwenden (siehe TOZ 2.9.30).
6. Entwicklung eines Musterschemas für die Wiederherstellung von kompromittierten Dateien im System der eigenen EPD-Gemeinschaft.

Run-Book als Hilfsmittel

Als abschliessenden Punkt wird der Einsatz eines Run-Books innerhalb der eigenen EPD-Gemeinschaft genannt. Ein solches Hilfsmittel ist von hoher Wichtigkeit, um im Falle eines Sicherheitsvorfalls entsprechend und rasch reagieren zu können. Um ein solches Hilfsmittel entwickeln zu können, müssen die folgenden Punkte gewährleistet sein:

1. Identifikation und Kontaktdaten von Personal, welches bei einem Vorfall informiert werden muss.
2. Identifikation und Kontaktdaten von Personal, welches für die Wiederherstellung der Dateien benötigt wird.
3. Definition der verwendeten Re-Key-Methode.
4. Führung eines Inventars aller Schlüssel sowie deren Einsatzzwecke (z.B. Standort aller Zertifikats-Systeme).
5. Eine Ausbildung des Personals zum Kompromittierungs- und Wiederherstellungsprozess.
6. Implementierung einer Policy zum Einsatz der einzelnen Prozeduren beim Widerruf von Schlüsseln.
7. Überwachung aller Re-Keying-Operationen, um sicherzustellen, dass alle betroffenen Schlüssel widerrufen und die Dateien wiederhergestellt wurden.

8. Auflistung aller weiteren gemeinschaftsabhängigen Prozeduren im Rahmen des Widerrufs und der Wiederherstellung:
    a. Physische Inspektion von Geräten und Hardware.
    b. Identifikation aller Informationen, welche möglicherweise kompromittiert wurden.
    c. Identifikation aller Signaturen, welche möglicherweise kompromittiert wurden.
    d. Verteilung der neuen Schlüssel.

Siehe dazu auch Kapitel 4.

6.11 Verwendung von Transport Layer Security (TLS)

Relevante TOZ-Anforderungen

4.15.3, 4.15.4

Anwendbarkeit

Gemäss den TOZ soll zur Sicherung die Datenübertragung über HTTPS TLS zum Einsatz kommen. TLS erlaubt es, Daten gegen unerlaubtes Einsehen und Verändern zu schützen, wenn sie zwischen zwei Systemen ausgetauscht werden.

Generelle Empfehlungen

Generelle Empfehlungen:

- TLS soll in der jeweils aktuellsten Version verwendet werden.
- Das Schlüsselaustauschverfahren soll auf Diffie-Hellman Ephemeral (DHE) basieren.
- Einsatz von Perfect Forward Secrecy (PFS).
- Der Einsatz von CBC sollte vermieden werden.
- Alle Seiten und ihre Ressourcen müssen über HTTPS angeboten werden.
- Der HTTP Strict Transport Security Header (HSTS) muss jederzeit verwendet werden.
- Cookies müssen mit dem Secure Flag versehen sein.
- Caching von Daten soll unterbunden sein.
- Die TLS-Einstellungen entsprechen den aktuell geltenden Empfehlungen von OWASP [OWASP-TLS-CS].

Server-Zertifikate

Empfehlungen zum Einsatz von Server-Zertifikaten:

- Es werden mindestens öffentliche Extended-Validation-Zertifikate eingesetzt.
- Es sollten Zertifikate verwendet werden, welche alle benötigten Domain-Namen unterstützen (z.B. https://www.example.ch und https://example.ch).
- Es sollten nur Fully Qualified Names in Zertifikaten verwendet werden.
- Es sollten keine Wildcards in Zertifikaten verwendet werden.
- Es sollten keine privaten IP-Adressen (RFC 1918 Adressbereich) in Zertifikaten verwendet werden.
- Es sollten nur bekannte und vertrauenswürdige Certification Authorities (CAs) verwendet werden.

Nach der Einrichtung und Konfiguration wird empfohlen, das TLS-Setup gemäss dem OWASP Testing Guide [OWASP-TLS-TG] zu überprüfen.

7 Schutz vor Manipulation der Vertraulichkeitsstufen

7.1 Einleitung

Vertraulichkeitsstufen

Dem Patienten ist es frei überlassen, ob er oder sie dem elektronischen Patientendossier (EPD) beitreten möchte. Entscheidet sich jemand dafür, hat diese Person die volle Entscheidungsmacht, aber auch die Verantwortung über seine Patientendaten. Grundsätzlich können die medizinischen Daten einer der folgenden drei Vertraulichkeitsstufen zugeordnet werden:

- normal zugänglich
- eingeschränkt zugänglich
- geheim.

Sollte der Patient die Daten nicht zuordnen, so werden die neu erstellten Daten automatisch der Vertraulichkeitsstufe „normal zugänglich“ zugeordnet. Es ist jedoch auch möglich, dass Gesundheitsfachpersonen medizinische Daten, welche nicht explizit vom Patienten zugeordnet wurden, als sensibel betrachten und die Daten der Vertraulichkeitsstufe „eingeschränkt zugänglich“ zuordnen.

Zugriffsrechte

Der Patient kann die Zugriffsrechte einer Gesundheitsfachperson oder einer Gruppe von Gesundheitsfachpersonen zuweisen. Die Zugriffsrechte gelten so lange, bis der Patient die Rechte wieder entzieht. Eine gesetzliche Befristung ist nicht vorgesehen. Es besteht aber die Option, Zugriffsrechte zeitlich zu beschränken. Hingegen müssen Zugriffsrechte für Gruppen zeitlich beschränkt werden. Damit kann sichergestellt werden, dass Gesundheitsfachpersonen, die voraussichtlich nur einmal oder nur für kurze Zeit in die Behandlung involviert werden, nicht unbeschränkt lange auf das elektronische Patientendossier zugreifen können. Damit verringert sich auch die Gefahr, dass Zugriffsrechte vergessen werden.

Gruppenberechtigung

Werden die Zugriffsrechte einer Gruppe zugeteilt, so erhalten alle Gesundheitsfachpersonen automatisch die Zugriffsrechte, welche der Gruppe zugesprochen wurden, wenn sie der Gruppe beitreten. Verlässt eine Gesundheitsfachperson die Gruppe, verliert sie automatisch auch die durch den Beitritt zur Gruppe erhaltenen Zugriffsrechte. Der Patient kann festlegen, dass er über den Eintritt von Gesundheitsfachpersonen in Gruppen, denen er ein Zugriffsrecht erteilt hat, informiert wird.

Notfallsituation

In medizinischen Notfallsituationen gibt es für Gesundheitsfachpersonen die Möglichkeit, auf die Vertraulichkeitsstufe „normal zugänglich“ zuzugreifen. Als Sicherungsmassnahme gegen eine missbräuchliche Verwendung des Notfallzugriffs, beispielsweise aufgrund automatisierter Angriffe auf ein Endgerät, wird empfohlen, dass der Notfallzugriff von der Gesundheitsfachperson anhand einer nicht automatisierten, reproduzierbaren und manuellen Interaktion bestätigt werden muss (Ziff. 2.2 Bst. a Anhang 2 EPDV-EDI). Denkbar sind hier zusätzliche Sicherungselemente, wie beispielsweise der Erhalt eines Einmalpasswortes oder die erneute Eingabe eines sonstigen Sicherheitsmerkmals. Der Patient muss über einen solchen Notfallzugriff in einer angemessenen Frist informiert werden. Die Verantwortlichkeit der Informierung liegt diesbezüglich bei der Gemeinschaft. Diese wiederum darf die

Pflicht aber an die Gesundheitseinrichtungen delegieren oder den Patienten per SMS, Brief oder E-Mail benachrichtigen.

Berechtigte Gesundheitsfachperson / Stellvertretung

Der Patient hat die Möglichkeit, eine Gesundheitsfachperson seiner Stammgemeinschaft zu ermächtigen, dass sie das Zugriffsrecht an weitere Gesundheitsfachpersonen weitergibt. In diesem Fall gilt jedoch, dass das Zugriffsrecht höchstens im gleichen Masse weitergegeben werden kann, wie es die Gesundheitsfachperson selber besitzt. Weiter ist es möglich, dass der Patient eine oder mehrere Stellvertretungen benennen kann. Die Stellvertretung hat das Recht, auf das elektronische Patientendossier zuzugreifen und Vertraulichkeitsstufen sowie Zugriffsrechte zuzuweisen. Wichtig ist, dass die Stellvertretung mit einem eigenen Identifikationsmittel auf das EPD zugreift. Empfohlen werden Stellvertretungen für die Vertretung eines Kindes oder einer betagten Person durch Angehörige oder andere Vertrauenspersonen.

Ausschlussliste

Patienten können einzelnen Gesundheitsfachpersonen nicht nur Zugriffsrechte auf Vertraulichkeitsstufen entziehen, sondern es ist auch möglich, einzelne Gesundheitsfachpersonen vom Zugriff auf die Daten vollständig auszuschliessen. Die ausgeschlossenen Gesundheitsfachpersonen kommen auf eine „Ausschlussliste“. Diese Ausschlussliste geht in jedem Fall vor – auch in medizinischen Notfallsituationen.

Sensibilisierung der Patienten

Die Patienten müssen bei der Registrierung des elektronischen Patientendossiers darauf aufmerksam gemacht werden, dass die vollständige Verantwortlichkeit bei ihnen liegt. Es muss deutlich gemacht werden, dass der Patient die vollständige Macht über seine Daten besitzt, insbesondere darüber, wer Zugriff auf seine Daten hat. Gleichzeitig muss der Patient darüber informiert werden, dass bei einer fehlenden manuellen Einstellung des elektronischen Patientendossiers eine automatische Einteilung der Daten auf die Vertraulichkeitsstufe „normal zugänglich“ stattfindet und dementsprechend ein potentiell grosser Benutzerkreis besteht.

7.2 Sicherheitsmassnahmen

Verwendung von Benutzeraccounts überwachen

Es wird empfohlen, ein Verfahren zu implementieren, welches die Verwendung der Benutzeraccounts überwacht. Das heisst, es wird überprüft, wann, wo, wie oft und von welchem Endgerät aus ein Patient oder eine Gesundheitsfachperson auf ein elektronisches Patientendossier zugreift. Bei Auffälligkeiten wie einer Anmeldung aus dem Ausland oder Mehrfachsessions wird die zu behandelnde Person per E-Mail (oder eine sonstige Nachricht) alarmiert.

Aufzeichnung und Auswertung von Mutationen

Weiter sollte ein System aktiv sein, welches alle Mutationen von Daten des EPD aufzeichnet und auswertet. Gibt es in der Auswertung Auffälligkeiten, wie beispielsweise eine statistisch signifikante Anzahl an Patientendaten, bei welchen in einem kurzen Zeitraum die Vertraulichkeitsstufe heruntergesetzt wurde, wird der Datenschutz- und Datensicherheitsverantwortliche der Gesundheitseinrichtung oder der (Stamm-)Gemeinschaft alarmiert. Es ist danach Aufgabe der Gesundheitsinstitution, der Auffälligkeit nachzugehen.

Zusätzliche Authentifizierung für kritische Aktionen

Damit die Vertraulichkeitsstufen von Patientendaten nur erschwert heruntergestuft werden können und somit ein vermindertes Risiko darstellen, wird empfohlen, dass die zu behandelnden Personen bei der Herabstufung ihrer Patientendaten eine zusätzliche Authentifizierung vornehmen müssen. Mit

anderen Worten: Sobald eine zu behandelnde Person ihre Patientendaten von der Vertraulichkeitsstufe „geheim“ auf „normal“ zugänglich stellt, erhält diese eine E-Mail (oder eine sonstige Nachricht), in welcher sie die vorzunehmende Änderung im elektronischen Patientendossier bestätigen muss. Bei einem temporären Verlust des jeweiligen Benutzeraccounts können dadurch keine Anpassungen an den Vertraulichkeitsstufen oder sonstigen sicherheitsrelevanten Einstellungen und Daten vorgenommen werden. Hierbei muss allerdings beachtet werden, dass Dokumente bis zur Bestätigung nicht zugänglich sind.

Regelmässige Kontrolle durch den Patienten

Regelmässig, mindestens einmal jährlich, soll die zu behandelnde Person eine E-Mail (oder eine sonstige Nachricht) erhalten, in welcher steht, dass die Vertraulichkeitsstufen in ihrem elektronischen Patientendossier überprüft werden sollen. Der Zweck der Erinnerungsmail besteht darin, dass die zu behandelnde Person die Zugriffsrechte ihrer Patientendaten selber (auf Auffälligkeiten) überprüft und dass sie den Überblick über allfällige Veränderungen ihrer berechtigten Gruppen, wie beispielsweise beim Zuwachs oder Abgang einer Gesundheitsfachperson, hat.

Zusätzliche Information bei sicherheitsrelevanten Änderungen durch den Patienten

Aufgrund der Eigenverantwortung der zu behandelnden Personen für ihr elektronisches Patientendossier entstehen auch Risiken. Personen, welche ungenügend über das EPD aufgeklärt sind, können ihre Patientendaten den falschen Vertraulichkeitsstufen zuweisen. Daher muss eine gewisse Grundsicherheit gewährleistet werden. Da es legitim ist, seine Patientendaten von Beginn weg auf „normal zugänglich“ zu stellen, kann hier kein automatischer Systemmechanismus greifen, welcher diese Aktion blockiert. Aus diesem Grund wird vorgeschlagen, dass drei bis fünf Kontrollfragen bezüglich der Nutzungsbedingungen gestellt werden, die prüfen sollen, ob die zu behandelnde Person die Nutzung des EPDs verstanden hat. Zudem soll bei der Herabstufung der Vertraulichkeitsstufe immer ein Browserfenster erscheinen, welches kurz zusammenfasst, was die Folgen dieser Tätigkeit sind. Beispiel: „Sind Sie sicher, dass Sie die ausgewählten Daten auf die Vertrauensstufe ‚normal zugänglich’ herabstufen möchten, womit alle Gesundheitsfachpersonen Einsicht auf diese Daten haben?“ Mit diesen Massnahmen sollen das Bewusstsein der Eigenverantwortung sowie die Verständlichkeit des elektronischen Patientendossiers unterstützt werden. Dabei muss darauf geachtet werden, dass keine sensitiven Informationen über unsichere Kanäle verschickt werden.

8 Sicherung der Zugangsportale

8.1 Einleitung

Risiken von Zugangsportalen

Für die Sicherheit des Gesamtsystems EPD sind die Zugangsportale ein sicherheitskritisches Element. Die Portale, bestehend aus Web- sowie Mobileapplikationen, sind exponiert und erlauben den Zugriff auf sensible Daten. Ein aktiver Angriff auf ein Zugangsportal kann die Vertraulichkeit, die Integrität der Daten des EPD oder die Verfügbarkeit des Zugangsportals insgesamt nachhaltig beeinträchtigen. Die OWASP Top 10 inklusive Mobile [OWASP-Top10] und [OWASP-MobileTop10] beinhalten die wesentlichen Risiken, welche mit geeigneten Massnahmen reduziert werden sollen.

Das vorliegende Dokument umfasst die wichtigsten Massnahmen zur Reduktion der Risiken. Die Massnahmen umfassen dabei Aspekte der Architektur und des Designs, der Entwicklung sowie der Anwendungsbereitstellung.

Anwendbarkeit

Die hier aufgeführten Empfehlungen können teilweise auch für andere Elemente der ICT-Infrastruktur zur Anwendung kommen. Zur übersichtlichen Darstellung werden diese jedoch fortfolgend unter dem Thema Zugangsportale gesamthaft ausgewiesen.

Abgrenzung

Der Scope liegt auf dem sicheren Datentransfer und den zu übertragenden Daten zwischen der EPD-Datensammlung zum Benutzer (Gesundheitsfachperson oder Patient) via Zugangsportal.

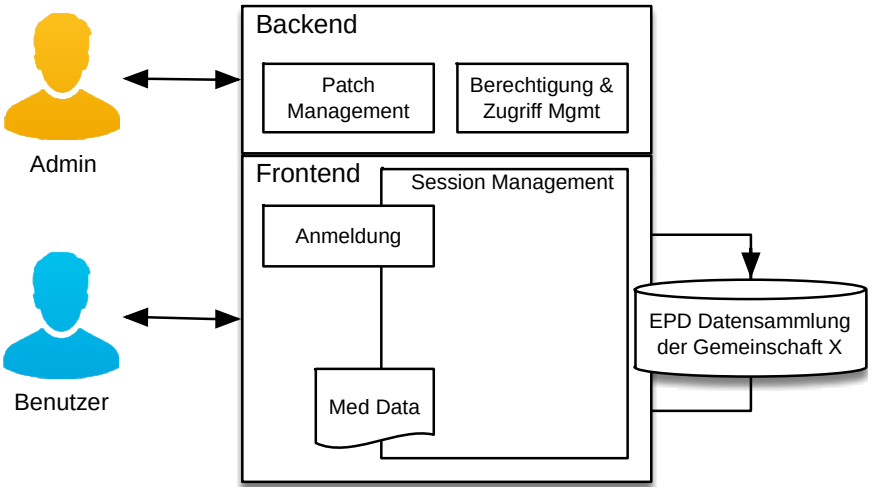

Abbildung 10: Scope der Zugangsportale

Die Endgeräte der Benutzenden tragen zur Sicherheit der Daten massgebend bei. Endgeräte, welche via Zugangsportale auf die Daten des EPD zugreifen, sollten demnach mindestens folgende Voraussetzungen erfüllen:

- Das verwendete Betriebssystem sowie mindestens der Web-Browser, der PDF-Leser, die Antivirensoftware sowie Komponenten zur Darstellung von Inhalten, welche aus dem Internet bezogen werden, müssen laufend aktualisiert werden.

- Die Signaturen der installierten Antivirensoftware werden laufend aktualisiert.
- Die Datenträger sollten verschlüsselt sein.
- Die Einstellungen des eingesetzten Web-Browsers sollten entsprechend der gegebenen Möglichkeiten des Browsers und des eingesetzten Umfeldes möglichst sicher und restriktiv gewählt werden. Soweit als möglich und durchsetzbar sollten vorkonfigurierte und gehärtete Browser zum Einsatz kommen.

8.2 Themenbereich Architektur, Design und Bedrohungsmodelle

Zielsetzung

Um die Angriffsfläche möglichst klein zu halten, sollten nur Komponenten eingesetzt werden, welche für den Betrieb notwendig sind. Die Architektur und der Code müssen in einem wirtschaftlich sinnvollen Rahmen aufeinander abgestimmt sein.

Relevante TOZ-Anforderungen

3.1, 3.2, 3.3, 9.1, 9.2, 9.3, 9.4, 9.5, 14.4.2

Sichere Entwicklung und laufende Risikobeurteilung

Im Rahmen des Entwicklungsprozesses soll sichergestellt sein, dass:

- Leitlinien zur sicheren Softwareentwicklung über den ganzen Lifecycle des Produkts zum Einsatz kommen.
- der Quellcode (Source Code) zentral verwaltet und der Zugriff beschränkt, kontrolliert und protokolliert ist.
- ein Bedrohungsmodell und eine Risikoanalyse für die Anwendung existiert und laufend gepflegt wird. Mindestens folgende Risiken müssen dabei gemäss den TOZ aktiv bearbeitet werden: Manipulation von Daten, Verlust der Integrität (Tampering), Vortäuschen einer Identität (Spoofing), Abstreiten einer Handlung (Repudiation), Verlust der Vertraulichkeit (Information Disclosure) und Erweiterung der Rechte einer Rolle oder der Identität (Elevation of privilege).
- sich in Entwicklungs- und Testumgebungen keine produktiven Daten befinden.
- sämtliche verwendeten Komponenten (z.B. Libraries) bekannt und dokumentiert sind, aus vertrauenswürdigen Quellen stammen und zur Nutzung freigegeben sind. Siehe auch Kapitel 6.7.
- keine Tracking-Dienste oder Technologien (z.B. Google Analytics usw.) eingesetzt oder eingebunden werden.

Design und Architektur

Die Architektur und das Design der Anwendung sollen sicherstellen, dass:

- die Anwendung eine klare Trennung zwischen dem Daten-Layer, dem Kontroll-Layer und dem Display-Layer vornimmt.
- alle Sicherheitskontrollen (einschliesslich Bibliotheken, welche externe Sicherheitsdienste aufrufen) zentral implementiert sind.
- keine sensiblen Informationen, geheime Schlüssel oder urheberrechtlich geschützte Informationen im clientseitigen Code vorhanden sind.
- die Geschäftslogik der Anwendung und somit die einzelnen Arbeitsschritte gemäss Geschäftsprozess sequentiell erfolgen, wobei alle Schritte in der korrekten Abfolge und in realistischen Zeitabständen verarbeitet werden müssen.

8.3 Themenbereich Authentifikation und Verifikation

Zielsetzung

Die Identität jedes Benutzers soll verifiziert werden und Zugriffe sind nur autorisierten Personen zu ermöglichen.

Relevante TOZ-Anforderungen

1.4.1, 1.4.2, 1.4.3, 1.6.2, 8.2.2, 8.3.1, 8.4.1, 8.4.2

Ausgestaltung der Authentifizierung

Bei der Ausgestaltung der Authentifizierungskontrollen soll berücksichtigt werden, dass:

- die eingesetzten Identifikationsmittel die Vertrauensstufe LoA 3 der Norm ISO/IEC 29115:2013(E) erfüllen. Siehe dazu auch Art. 23 bis 27 EPDV.
- alle Seiten und Ressourcen (sofern diese nicht öffentlich zugänglich sein müssen) standardmässig eine gültige Authentifizierung verlangen, welche ausschliesslich serverseitig erzwungen wird.
- alle Anmeldeinformationen nur verschlüsselt transportiert werden und dass alle Seiten und Funktionen, welche nur für eingeschränkte Benutzerkreise verfügbar sein sollen, nur über verschlüsselte Kanäle aufgerufen werden können.
- diese über ein solides Error-Handling verfügen und beim Versagen in einen sicheren Zustand übergehen (fail-safe).
- die Anzahl der Requests zeitlich begrenzt ist (Throttling).
- alle Authentifizierungsversuche, ob erfolgreich oder fehlgeschlagen, in der gleichen durchschnittlichen Reaktionszeit reagieren.
- sämtliche Anmeldeversuche (erfolgreich und nicht erfolgreich) protokolliert werden.
- alle Funktionalitäten zur Kontoverwaltung den gleichen Schutz aufweisen wie die Authentifizierung an sich.

Passwort eingeben

Im Zusammenhang mit einem allfälligen Passworthandling soll Folgendes berücksichtigt werden:

- Bei der Eingabe wird das Passwort nicht in Klartext dargestellt.
- Die Eingabefelder sollen die Verwendung von langen und komplexen Passwörtern unterstützen (mindestens 50 Zeichen ohne Einschränkung auf spezifische Zeichen).
- Passwörter dürfen nicht im Klartext abgespeichert werden und müssen durch sichere Hashing-Verfahren (siehe Kapitel 6.6) geschützt sein.
- Nur starke und komplexe Passwörter (mindestens 10 Zeichen, mit Gross-/Kleinbuchstaben und Sonderzeichen sowie Unterdrückung von Trivialwörtern) sollen verwendet werden.

Passwort zurücksetzen oder ändern

Hat ein Benutzer sein persönliches Passwort vergessen oder möchte er dieses ändern, sollen im Vorfeld der Rücksetzung oder Änderung folgende Punkte beachtet werden:

- Allfällig verwendete Geheim-/Sicherheitsfragen sollen nicht aufgrund von öffentlich verfügbaren Informationen zu beantworten sein. Die Fragen müssen dem Benutzer demnach vorgegeben werden (z.B. via Dropdown).

- Es soll sichergestellt sein, dass die Funktion der Passwort-Wiederherstellung sowie andere Wiederherstellungspfade einen Soft-Token-, Mobile-Push- oder einen Offline-Wiederherstellungsmechanismus verwenden.
- Die Passwortrücksetzung soll keine Rückschlüsse auf das aktuelle Passwort zulassen.
- Das neue Passwort soll dem Benutzer nicht im Klartext zugestellt werden.
- Die Wiederverwendung von alten Passwörtern soll beim Wechsel nicht zugelassen sein.

Ablage von Authentifizierungsmerkmalen

Bei der Ablage (Speicherung) von Authentifizierungsmerkmalen ist zu berücksichtigten, dass:

- alle Authentifizierungsanmeldeinformationen für den Zugriff auf Dienste ausserhalb der Anwendung verschlüsselt und an einem geschützten Speicherort hinterlegt sind.
- API-Schlüssel und Passwörter nicht in den Quellcode- oder Online-Quellcode-Repositories enthalten sind.

Anti-Enumeration

Bei sämtlichen Funktionen (speziell bei Anmeldung, Login, Passwortwiederherstellung) soll keine Informationsenumaration möglich sein.

Das bedeutet, dass dem Benutzer jeweils die gleiche Fehlermeldung angezeigt wird, unabhängig davon, ob dieser über einen Account verfügt oder ob nur die Authentifizierung fehlgeschlagen ist.

8.4 Themenbereich Session-Management

Sessions müssen für jeden Zugriff auf das EPD-Portal neu generiert werden und dürfen nicht erraten oder geteilt werden können. Zudem sind diese nach Gebrauch vollständig zu schliessen.	Zielsetzung
4.16.1, 4.16.2	Relevante TOZ-Anforderungen
Folgende Punkte sind bei der Ausgestaltung des Session-Handlings zu berücksichtigen: • Es soll ein bekannter, erprobter Session Manager eingesetzt werden (nach Möglichkeit keine Eigenentwicklung). • Bei einer Abmeldung durch den Benutzer oder beim Erreichen eines Timeouts muss die Session vollständig beendet werden. • Die Anzahl der gleichzeitig aktiven Sessions soll beschränkt sein.	Session-Handling
Die Handhabung der Session-ID soll unter Berücksichtigung folgender Punkte erfolgen: • Die Session-IDs müssen so generiert werden, dass diese nicht erraten werden können. • Es soll sichergestellt sein, dass die Session-ID nicht in einer URL, einer Fehlermeldung oder einem Protokoll angezeigt wird. Zudem darf URL-Rewriting bei Session Cookies nicht möglich sein. • Alle erfolgreichen Authentifizierungen und Re-Authentifizierungen müssen eine neue Session sowie eine neue Session-ID generieren. • Werden Session-IDs in Cookies abgespeichert, muss ihr Gültigkeitspfad möglichst restriktiv gesetzt sein. • Bei Authentifizierungs-Tokens müssen die Attribute „HttpOnly“ und „secure“ gesetzt werden.	Session-ID
Dem Benutzer sollen die folgenden Punkte ermöglicht werden: • Alle Seiten, welche eine Authentifikation benötigen, sollen über eine einfache und für den Benutzer gut sichtbare Abmeldefunktion verfügen. • Eine aktive Auflistung der eigenen Sessions im Kontoprofil oder dergleichen soll bei jedem Benutzer angezeigt werden. Der Benutzer sollte in der Lage sein, jede aktive Session beenden zu können. • Anzeigen eines Hinweis über die letzte Anmeldung „Letzte Anmeldung am tt.mm.jj um hh:mm“).	Benutzerkontrolle über Sessions

8.5 Themenbereich Zugriffskontrolle/-management

Benutzer benötigen gültige Anmeldedaten für den Zugriff auf die Zugangsportale. Die Verwaltung der Berechtigung erfolgt anhand der Rollenzugehörigkeit des Benutzers und ist auf die dafür notwendigen Funktionen und Daten eingeschränkt.	Zielsetzung
1.3.4, 1.3.5, 1.4.1, 1.6.2, 2.2, 2.3.2, 4.8.1, 4.8.2, 4.8.3, 4.13.1	Relevante TOZ-Anforderungen
Alle Zugangsportale unterliegen den spezifischen Regeln für Berechtigungs- und Vertraulichkeitsstufen sowie den Datenabruf. Die Zugriffskontrolle muss diese Anforderungen in der Anwendung implementieren. Dies gilt für alle Funktionen, Dateien, URLs, Controller, Dienste sowie für alle anderen Ressourcen der Anwendung.	Zugriffsmanagement
Es soll sichergestellt sein, dass das Durchsuchen von Verzeichnissen auf dem Webserver nicht möglich ist. Darüber hinaus sollten Anwendungen keine Einsicht von Datei- oder Verzeichnis-Metadaten ermöglichen.	Durchsuchen von Verzeichnissen
Sämtliche Zugriffe sollen kontrolliert erfolgen. Um dies zu ermöglichen sind folgende Punkte umzusetzen: • Die Zugriffskontrollen verfügen über ein solides Error-Handling (fail-safe). • Die Regeln für die Zugriffssteuerung werden auf der Serverseite erzwungen. • Es gibt einen zentralen Mechanismus zur Zugriffskontrolle (Policy Decision Point und Policy Enforcement Point). • Alle Zugriffssteuerungsentscheidungen (inkl. fehlgeschlagene Entscheidungen) müssen protokolliert werden.	Zugriffskontrolle
Um die Daten vor ungewollter Manipulation zu schützen, sind folgende Punkte zu berücksichtigen: • Benutzer- und Datenattribute sowie Zugriffsrichtlinien dürfen nicht durch die Benutzer mutiert werden können. • Sämtliche Zugriffe und Anfragen müssen anhand der geltenden Berechtigungen des eingeloggten Benutzers verifiziert werden.	Manipulationsschutz
Es soll sichergestellt sein, dass die Anwendung oder das Framework einen starken Transaktionsschutzmechanismus verwenden (z.B. zufällige Anti-CSRF-Tokens).	Transaktionsschutz

8.6 Themenbereich Validierung von Eingaben

Jeglicher Input wird validiert und auf seine Korrektheit überprüft. Im Grundsatz darf Daten von externen Quellen nicht vertraut werden und erkannte bösartige Aktivitäten müssen entsprechend behandelt werden.	Zielsetzung
4.5, 4.7.3	Relevante TOZ-Anforderungen
Damit die Daten sicher und korrekt in der Applikation abgelegt werden, sind folgende Punkte der Validierung zu berücksichtigen: • Fehlerhaft oder nicht validierte Eingaben (Input) dürfen nicht verarbeitet werden. • Die Input-Validierung muss auf der Serverseite erzwungen werden. • Für alle Datentypen soll eine Input-Validierung erfolgen. • Alle Eingabedaten sind zu validieren. Dies bezieht sich nicht nur auf HTML-Formularfelder, sondern auf alle Eingabequellen wie REST-Aufrufe, Abfrageparameter, HTTP-Header, Cookies, Batchdateien, RSS-Feeds usw.	Validierung
Um Injection-Angriffe auf die Umgebung zu verhindern, sind unter anderem folgende Punkte zu beachten: • Alle SQL-Queries, HQL, OSQL, NOSQL sowie die gespeicherten Prozeduren und deren Aufrufe sind durch die Verwendung von Anweisungen oder Abfrage-Parametrisierung geschützt (Verhinderung von SQL-Injektion). • Es sind keine LDAP-Injektionen oder OS-Command-Injektionen möglich. • Es besteht keine Anfälligkeit für Remote File Inclusion (RFI) oder Local File Inclusion (LFI). • Die Anwendung ist nicht anfällig auf gängige XML-Angriffe wie XPath-Abfrage-Manipulationen, XML-External-Entity- und XML-Injection-Angriffe.	Schutz vor Injection-Angriffen
Alle String-Variablen, die in HTML oder anderen Web-Client-Codes verwendet werden, sollen korrekt encodiert sein.	Schutz vor Cross-Site-Scripting-Angriffen
Es soll sichergestellt sein, dass die Laufzeitumgebung (Interpreter, JVM usw.) nicht anfällig auf Buffer-Overflows ist.	Schutz vor Buffer-Overflow
Es ist darauf zu achten, dass ausschliesslich sichere JavaScript-Methoden, wie zum Beispiel „.innerText“ und „.val.“ zum Einsatz kommen, um Daten von einem DOM-Kontext zu einem anderen zu übertragen.	Umgang im DOM-Kontext
Es soll sichergestellt sein, dass authentifizierte Daten aus dem Client-Speicher gelöscht werden, z.B. der Browser-DOM, nachdem die Session beendet wurde.	Löschung von Daten bei Beendigung der Session

8.7 Themenbereich Kryptographie

Kryptografische Module sind sicher anzuwenden und gemäss den geltenden Empfehlungen einzubinden.	Zielsetzung
2.5.1, 4.12	Relevante TOZ-Anforderungen
Die eingesetzten kryptografischen Verfahren sowie deren Verwendung soll gemäss Kapitel 5 erfolgen.	Sichere Kryptografie

8.8 Themenbereich Fehlermanagement und Logging

Sicherheitsrelevante Systeminteraktionen müssen zur Sicherung der Nachvollziehbarkeit protokolliert werden. Fehler und auffällige Abweichungen sind gemäss einem definierten Verfahren zu bearbeiten.	Zielsetzung
2.10, 4.13.1, 4.13.3	Relevante TOZ-Anforderungen
Es muss sichergestellt sein, dass die Anwendung keine Fehlermeldungen ausgibt oder Logeinträge generiert, welche sensible Daten enthalten. Dazu gehören die Session-ID, Software, Framework-Versionen, Informationen zum Betriebssystem sowie persönliche Informationen oder medizinische Daten.	Sensible Daten (Medizinische Daten)
Im Zusammenhang mit der Protokollierung sind folgende Punkte zu beachten: • Es müssen sämtliche in den TOZ geforderten Ereignisse mit den jeweils notwendigen Angaben und Informationen protokolliert werden. • Es soll sichergestellt sein, dass alle nicht druckbaren Symbole und Trennzeichen in Logeinträgen ordnungsgemäss codiert sind.	Protokollierung
Zum Schutz von Protokolldaten sind folgende Massnahmen umzusetzen: • Alle Protokolldaten müssen vor unbefugtem Zugriff und Veränderungen geschützt sein. Nachträgliche Änderungen müssen sichtbar und nachvollziehbar sein. • Protokolldaten, insbesondere die darin enthaltenen Daten, dürfen in der Log-Viewing Software nicht ausgeführt werden. • Die Speicherung der Logs erfolgt auf einer anderen Partition, als die Anwendung ausgeführt wird. Empfohlen wird zudem eine zentrale und vom Ursprungssystem unabhängige Logablage. Die dazu verwendete Ablage sollte vor unerlaubter Löschung sowie Veränderung geschützt sein. Zur Sicherstellung der Integrität ist ein Hashing-Verfahren zu verwenden.	Schutz der Protokolldaten (Logs)

8.9 Themenbereich Schutz von sensiblen Daten

Daten müssen entsprechend ihrer Sensibilität geschützt werden und dürfen lediglich einem definierten Benutzerkreis zur Verfügung stehen. Alle Daten müssen vor unerlaubter Einsichtnahme und Veränderung geschützt sein.	Zielsetzung
2.1, 4.17, 10.2.1, 10.2.2, 10.2.3	Relevante TOZ-Anforderungen
Es soll sichergestellt sein, dass die sensiblen Daten (personenidentifizierende sowie medizinische Daten) innerhalb der Anwendung ordnungsgemäss identifiziert und entsprechend geschützt sind.	Identifikation von sensiblen Daten
Die folgenden Punkte sollen erfüllt werden, um sensible Daten vor unberechtigten Zugriffen zu schützen: • Alle sensiblen Daten werden im HTTP Message Body oder Header gesendet (URL-Parameter werden nicht zum Versand von sensiblen Informationen genutzt). • Sensible Daten sollen clientseitig nicht temporär oder dauerhaft gespeichert werden. • Der Anti-Caching-Header soll bei sensiblen Daten eingesetzt werden. • Sensible Daten, welche temporär zwischengespeichert werden, sollen vor unbefugtem Zugriff geschützt sein und gelöscht werden, sobald die Transaktion abgeschlossen ist. • Werden Daten aus der Anwendung heruntergeladen (Export), soll der Benutzer darauf hingewiesen werden, dass diese Daten den geschützten Kontext verlassen.	Schutz von sensiblen Daten
Übermässige Zugriffe auf sensible Daten sowie eine ungewöhnliche Anzahl von Anfragen zur Datenerfassung sollten erkannt und alarmiert werden.	Erkennen von ungewöhnlichen Zugriffen

8.10 Themenbereich Transport von Daten

Bei sämtlichen Datenübermittlungen muss das TLS-Protokoll verwendet werden. Dabei müssen eine bewährte und sichere Konfiguration und ein starkes Verschlüsselungsverfahren eingesetzt werden.	Zielsetzung
2.5, 4.15.3, 4.15.4, 4.15.6	Relevante TOZ-Anforderungen
Um sensitive Daten (z.B. medizinische Daten) beim Transport ausreichend zu schützen, sind folgende Punkte zu berücksichtigten: • Für alle Verbindungen ist TLS zu verwenden (einschliesslich Backend-Verbindungen). • Alle Verbindungen müssen authentifiziert erfolgen.	Transportverschlüsselung (Siehe dazu auch Kapitel 6.11)
Im Umgang mit Zertifikaten sind die Punkte aus dem Kapitel 6.11 zu berücksichtigen.	Umgang mit Zertifikaten

8.11 Themenbereich HTTP-Sicherheitskonfiguration

Das HTTP-Protokoll wird auf die notwendigen Methoden reduziert und gehärtet.	Zielsetzung
Keine direkte Zuordnung	Relevante TOZ-Anforderungen
Im Zusammenhang mit der HTTP-Sicherheitskonfiguration sind folgende Punkte zu berücksichtigen: • Die Anwendung akzeptiert die definierten HTTP-Request-Methoden (z.B. GET und POST), und unbenutzte Methoden (z.B. TRACE, PUT und DELETE) werden explizit nicht zugelassen. • Im HTTP-Header muss der Zeichensatz definiert werden. • HTTP-Header, welche von einem vertrauenswürdigen Proxy- oder SSO-Gerät hinzugefügt werden, sollen ebenfalls von der Anwendung authentifiziert werden. • Die HTTP-Header enthalten keine Informationen über das System sowie über eingesetzte Versionen. • Es soll die Content Security Policy (V2 – CSP) im Einsatz sein. Dabei soll Inline JavaScript vollständig deaktiviert werden oder es muss eine Integritätsprüfung auf Inline JavaScript in Form von „CSP Noncing“ oder „Hashing“ durchgeführt werden. • Der Header „X-XSS-Protection: 1; mode = block“ wird mitgeschickt.	HTTP-Sicherheitskonfiguration

8.12 Themenbereich Dateien und Ressourcen

Zielsetzung

Nicht vertrauenswürdige Dateien müssen in geschützter Umgebung behandelt werden. Dateien von nicht vertrauenswürdigen Quellen werden ausserhalb des webroot aufbewahrt.

Relevante TOZ-Anforderungen

3.3, 9.4.2

Umgang mit Dateien und Ressourcen

Im Zusammenhang mit Dateien und Ressourcen, welche eingebunden werden, sind folgende Aspekte zu berücksichtigen:

- Es soll sichergestellt sein, dass URL-Umleitungen und Forwards nur auf explizit freigegebene Ziele zugelassen sind oder dass eine Warnung anzeigt wird, wenn auf potentiell nicht vertrauenswürdige Inhalte umgeleitet wird.
- Es sollen nur die in der TOZ definierten Dateiformate im System verarbeitet werden.
- Alle eingehenden Dateien sollen validiert und auf Schadsoftware hin geprüft werden.
- Dateien sind getrennt von der Applikation, z.B. ausserhalb des Verzeichnisses „webroot“, aufzubewahren.
- Der Zugriff auf entfernte Ressourcen oder Systeme ausserhalb des Web- respektive Anwendungsservers soll minimal gehalten sein.
- Auf die Verwendung von Flash-, Active-X-, Silverlight-, NACL- oder Client-Side-Technologien, die nicht nativ über W3C-Browser-Standards unterstützt werden, ist zu verzichten.

8.13 Themenbereich Mobile Applikationen (Apps)

Die Daten, welche über mobile Applikationen verarbeitet werden, müssen den gleichen Schutz aufweisen wie jene in klassischen Webapplikationen. Allfällige Speicherungen (temporär oder dauerhaft) müssen eingeschränkt sein. Die Kommunikation muss vollständig verschlüsselt sein.	Zielsetzung
Keine direkte Zuordnung	Relevante TOZ-Anforderungen
Im Zusammenhang mit mobilen Applikationen, sogenannten Apps, sind zusätzlich folgende Aspekte zu berücksichtigen: • ID-Werte, die auf dem Gerät gespeichert und von anderen Anwendungen abgerufen werden, wie die UDID- oder IMEI-Nummer, sollen nicht als Authentifizierungs-Token verwendet werden. • Daten des EPG sollen nicht unverschlüsselt auf dem Gerät gespeichert werden. • Alle zwischengespeicherten Inhalte sollen geschützt werden.	Mobile Applikationen (Apps)

8.14 Themenbereich Web-Services

Sämtliche Web-Services benötigen ein adäquates Authentisierungssystem und Session-Management. Zudem müssen sämtliche Parameter vollständig validiert werden.	Zielsetzung
2.5, 2.9.26, 4.15.3, 4.15.4, 4.15.6	Relevante TOZ-Anforderungen
Im Zusammenhang mit Web-Services sind folgende Punkte zu berücksichtigen: • Es soll sichergestellt sein, dass zwischen dem Client und dem Server das gleiche Encoding (UTF-8) verwendet wird. • Der Zugriff auf Administration- und Verwaltungsfunktionen ist beschränkt. • Es soll ein XML- oder JSON-Schema verwendet werden. Sämtliche Eingaben sollen darauf basierend geprüft werden. • Alle Eingaben sollen validiert werden und über entsprechende Grössenbeschränkungen verfügen. • SOAP-basierte Web-Services sind kompatibel mit der Web-Services-Interoperabilität (WS-I) und unterstützen die TLS-basierte Verschlüsselung. • Jede Session wird authentifiziert. Der Gebrauch von statischen API-Keys oder Ähnlichem ist zu vermeiden. • Die Integrität von eingehenden Meldungen sollte überprüft werden.	Web-Services

8.15 Themenbereich Konfiguration und Wartung

Libraries und Plattformen müssen stets aktuell gehalten werden. Dazu muss ein Patch-Management-Prozess definiert und umgesetzt sein. Es ist eine Grundkonfigurierung nach dem Grundsatz „Secure by Default“ für alle eingesetzten Komponenten und Konfigurationen anzustreben.	Zielsetzung
Keine Zuordnung	Relevante TOZ-Anforderungen
Bei der Konfiguration von Komponenten sind folgende Punkte zu berücksichtigen: • Es wird jeweils die aktuelle Version und Konfiguration eingesetzt; dies nach der vorgängigen Prüfung, dass der aktuelle Sicherheitsstand nicht gesenkt wird. • Nicht benötige Konfigurationen, Dateien, Beispielanwendungen und Standardbenutzer sind gelöscht. • Die Kommunikation der Komponenten erfolgt authentifiziert und verschlüsselt. • Durch den Einsatz von Sandboxing- oder Container-Verfahren erfolgt die Anwendungsbereitstellung von anderen Anwendungen getrennt.	Konfiguration
Es sollte sichergestellt sein, dass autorisierte Administratoren die Möglichkeit haben, die Integrität aller sicherheitsrelevanten Konfigurationen zu überprüfen, um sicherzustellen, dass sie nicht manipuliert wurden.	Integrität der Konfiguration
Alle Anwendungskomponenten sind signiert.	Verwendung von signierten Komponenten

9 Anhang

9.1 Übersicht Autoren

Redguard AG
Eigerstrasse 60
CH-3007 Bern

+41 (0)31 511 37 50
https://www.redguard.ch

Projektverantwortlicher:

Alexander Hermann, Managing Partner

9.2 Übersicht Mitglieder Begleitgruppe

Name	**Organisation**
Cedric Michelet	Hôpital du Valais
Damiano Boppart	CCC-ZH
Frank Calcavecchia	Hôpitaux Universitaires de Genève
Heinz Schütz	BINT GmbH
Hernani Marquez	CCC-ZH
Jan Zbinden	Kanton Basel-Stadt
Johannes Gnägi	eHealth Suisse
Klaus Pirker	-
Lucas Schult	Health Info Net (HIN) AG
Martin Bruderer	Universitätsspital Basel
Martin Smock	Swisscom Health AG
Mauro Rudi	Kanton Basel-Stadt
Reto Schnellmann	Swisscom Health AG
Stefan Beyeler	Spital Emmental
Thomas Menet	Kanton Aargau
Volker Birk	CCC-ZH
Walid Ahmed	Bundesamt für Gesundheit

Tabelle 1: Begleitgruppe

9.3 Verwendete Abkürzungen

Abkürzung/Begriff	Bedeutung
AES	Advanced Encryption Standard
API	Application programming interface (Anwendungsprogrammierschnittstelle)
ASLR	Adress space layout randomization (Zufallsgestaltung des Adressraum-Aufbaus)
ASVS	Application Security Verification Standard
CAs	Certification Authorities
CBC	Cipher-Block Chaining
CERTs	Computer emergency response team (Computersicherheits-Ereignis- und Reaktionsteam)
CORS	Cross-Origin Ressource Sharing
CSP	Content Security Policy
CSRF	Cross-Site Request Forgery (Website-übergreifende Anfragenfälschung)
CTR	Counter Mode
DEP	Data Execution Prevention (Datenausführungsverhinderung)
DOM	Document Object Model
DHE	Diffie-Hellman Ephermal
DSMS	Datenschutzmanagement
FIPS	Federal Information Processing Standard (Bundesstandard für Informationsverarbeitung)
GCM	Galois Counter Mode
HTML	Hypertext Markup Language (Hypertext Auszeichnungssprache)
HTTP	Hypertext Transfer Protocol (Hypertext Übertragungsprotokoll)
HQL	Hibernate Query Language
HSM	Hardware Sicherheits Modul
HSTS	HTTP Strict Security Header
ID	Identifier (Identifikator)
IDS	Instrusion Detection System (Angriffserkennungssystem)
ICT	Information and Communication Technology (Informations- und Kommunikations-Technologie)
IMEI	International Mobile Equipment Identity
Inkl.	Inklusive
IPS	Instrusion Prevention Systeme
ISMS	Informationssicherheitsmanagementsystem
IV	Initialisierungsvektor
JSON	JavaScript Object Notation
JVM	Java Virtual Machine
KEK	Key Encryption Keys
LDAP	Lightweight Directory Access Protocol (Leichtgewichtiges Verzeichniszugriffsprotokoll)
LFI	Local File Inclusion
MAC	Message Authentification Code (Nachrichtenauthentifizierungscode)
MD	Message Digest (Nachrichten-Kurzfassung)

Abkür-zung/Begriff	Bedeutung
NACL	Eine Programmbibliothek
Noncing	Anwendung von Nonce → „used only once“
NOSQL	Not only SQL
OS	Operating System (Betriebssystem)
OSCP	Online Certificate Status Protocol
OSQL	Object-Structured Query Language
OWASP	Open Web Application Security Project
PFS	Perfect Forward Secrecy
REST	Representational State Transfer
RFC	Request for Comments (Bitte um Kommentare)
RFI	Request for Information (Bitte um Information)
RPO	Recovery Objectives (Maximal hinnehmbarer Datenverlust)
RSA	Rivest, Shamir und Adleman – Asymmetrisches kryptografisches Verfahren
RSS	Rich Site Summary / Really Simple Syndication → Web-Feed (Sehr einfache Zusammenfassung)
RTO	Recovery Time Objectives (Maximale Ausfallzeit)
SHA	Secure Hash Algorithm (Sicherer Hash-Algorithmus)
SOAP	Simple Object Access Protocol
SQL	Structured Query Language (Strukturierte Abfrage-Sprache)
SSO	Single Sign-on (Einmalanmeldung)
TLS	Transport Layer Security (Transportschichtsicherheit)
U-DID	Unique Device-ID
URLs	Uniform Resource Locator (Einheitlicher Ressourcenanzeiger)
Usw.	Und so weiter
W3C	Gremium zur Standardisierung der Techniken im Internet (World Wide Web Consortium)
WS-I	Web Services Interoperability
XML	Extensible Markup Language (Erweiterte Auszeichnungssprache)
X-Path	Abfragesprache zur Auswertung von Teilen eines XML-Dokumentes
XSS	Cross-Site-Scripting (Webseitenübergreifendes Skripting)

Tabelle 2: Verwendete Abkürzungen

9.4 Mapping TOZ/ISO

Siehe Beilage1_TOZ-ISO_Mapping_v1.00.xlsx

9.5 Pendenzen

Folgende Themen sind als offene Punkte und somit als Pendenzen für kommende Überarbeitungen zu berücksichtigen:

Nr.	Beschreibung
P1	Die Zuordnung der Rolle Datenschutz- und Datensicherheitsverantwortlicher wird in der Praxis vermutlich an bestehende Rollen angeknüpft. Gemachte Praxiserfahrungen sollten zu einem späteren Zeitpunkt ebenfalls in die vorliegende Umsetzungshilfe eingearbeitet werden.
P2	Inwiefern ist ein automatisches Entfernen oder Sperren von Dokumenten (z.B. bei Verdacht auf Schadsoftware) aus einem Repository möglich? Es können im Einzelfall lebenswichtige medizinische Informationen nicht zugänglich sein oder gelöscht werden. Diese Frage sollte aus juristischer Sicht beurteilt werden.
P3	Prüfung von alternativen Authentifizierungsverfahren
P4	Anwendbarkeit der Bestimmungen (insbesondere in Bezug auf die Zugangsportale) auf Primärsysteme mit hoher EPD-Integration.