UMSETZUNGSHILFE DATENSCHUTZ UND DATENSICHERHEIT

REDGUARD
SECURING YOUR ASSETS

28.06.2017 / RG-C0

REDGUARD
SECURING YOUR ASSETS

Agenda

1. **Vorstellung**
2. **Factsheet**
3. **Vorgehen**
4. **Themenübersicht**
5. **Fokusthemen**

VORSTELLUNG

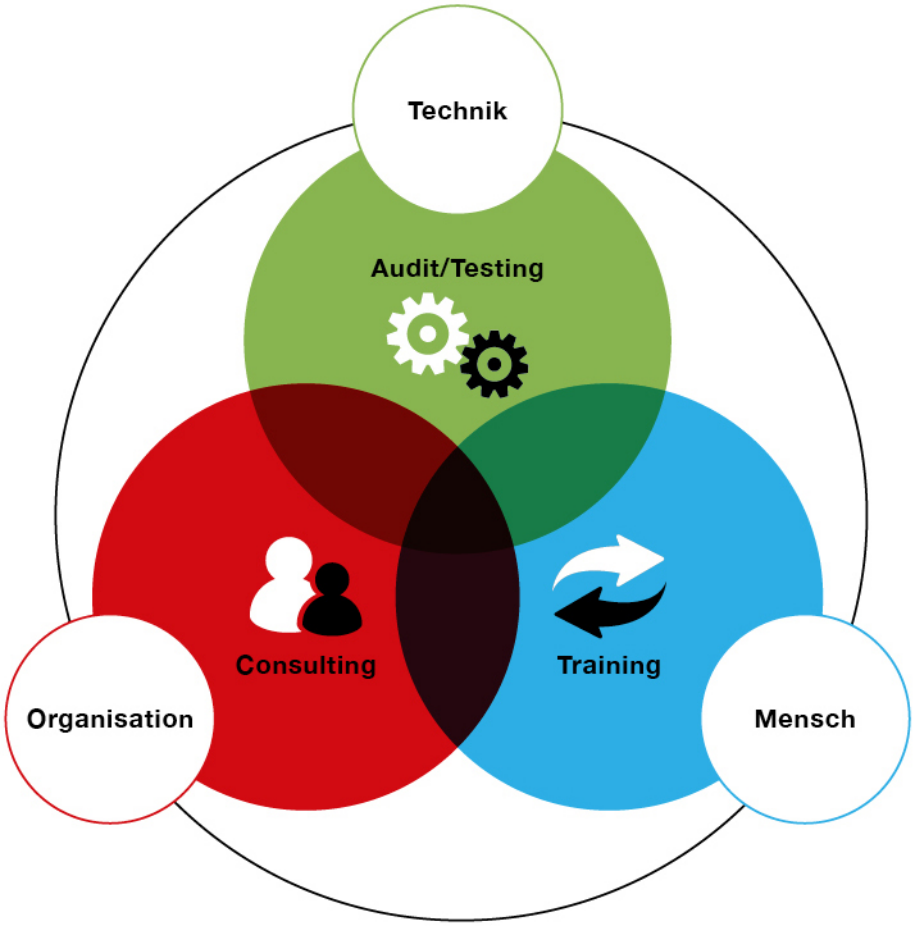
Redguard AG

Facts:

- Schweizer Beratungsunternehmen für Informationssicherheit
- Standorte Bern und Zürich
- 20 Mitarbeitende mit unterschiedlichen Schwerpunkte innerhalb der Informationssicherheit

Beratungsprinzipen:

- Wir beraten Sie unabhängig und neutral
- Unsere Beratung umfasst organisatorische, technische und menschliche Aspekte
- Unsere zentralen Werte sind: Fairness, Transparenz und Nachhaltigkeit
- Wir kommunizieren verständlich und für alle Stakeholder nachvollziehbar
- Unsere Beratung orientiert sich an Ihren Geschäftsprozessen



Wir verstehen die komplexen Zusammenhänge der Informationssicherheit.

Alexander Hermann

Alexander Hermann

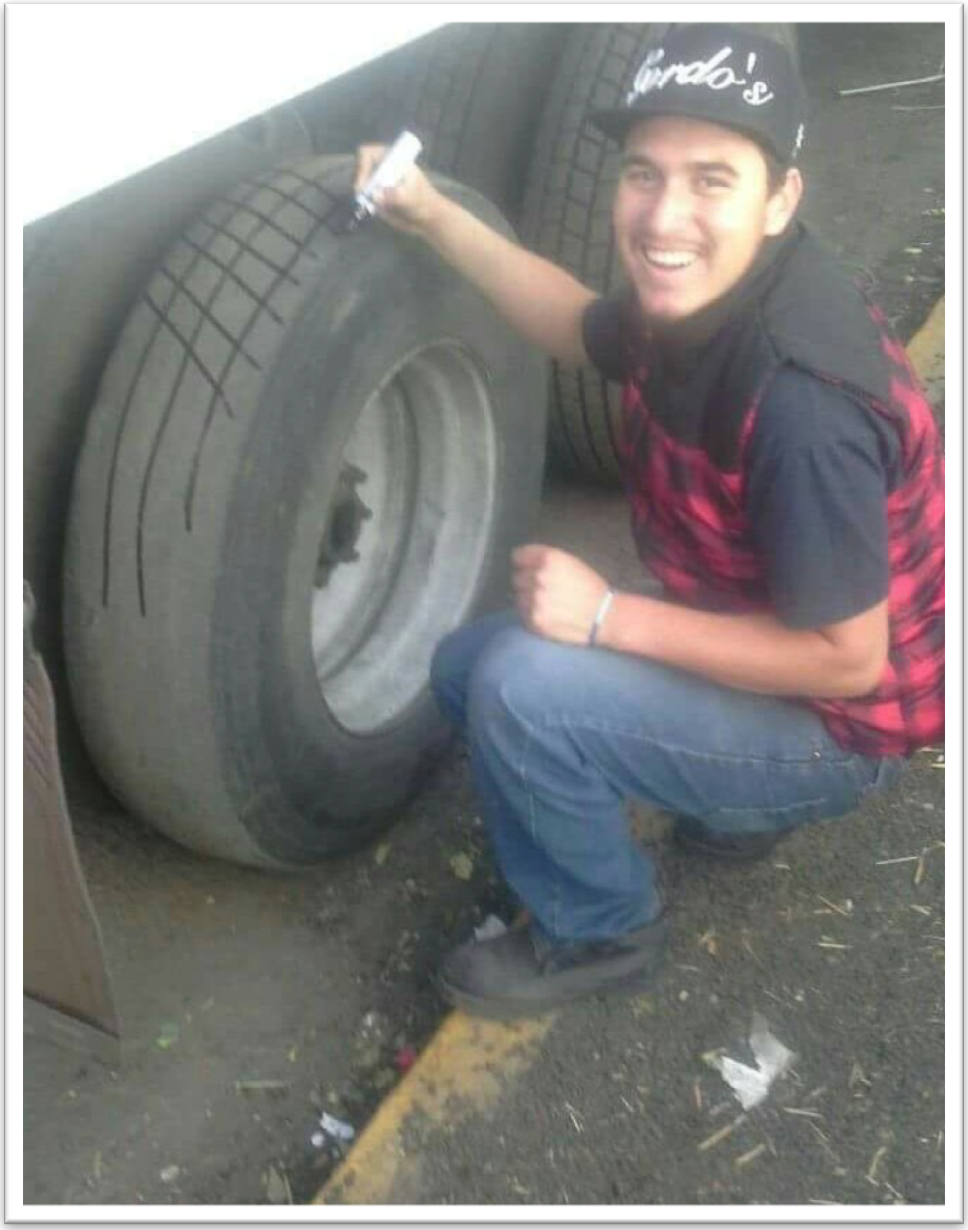
Seit 2012:
Managing Partner
Redguard AG

Seit über zehn Jahren als Berater im Bereich ICT- und Information Security unterwegs

Ausbildung: Wirtschaftsinformatiker (ICT-Management)

Zertifizierungen (Auswahl):
- Certified Information Security Manager (CISM)
- Certified Information System Auditor (CISA)
- Certified Information Systems Security Professional (CISSP)

Sonstiges:
- Vizepräsident bei der Information Security Society Switzerland (ISSS)



UMSETZUNGSHILFE DSDS – FACTSHEET

Factsheet

Name: Umsetzungshilfe Daten-schutz und Datensicherheit (DSDS)

Version: Entwurf

Zielgruppe:

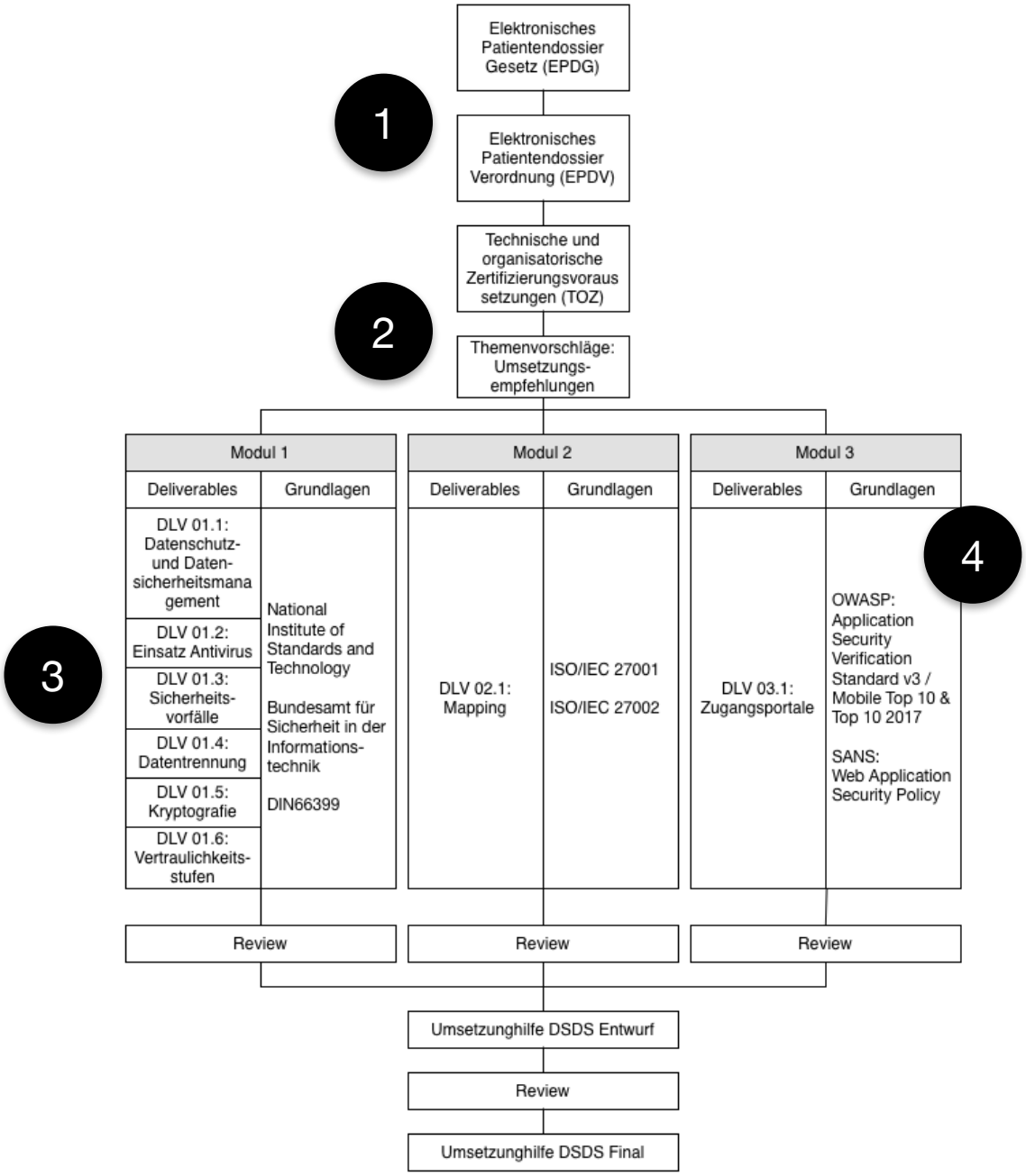
- Datenschutz- und Datensicherheitsverantwortliche der Gemeinschaften
- Lieferanten von Betriebsleistungen
- Hersteller von Produkten

Umfang: ca. 75 Seiten

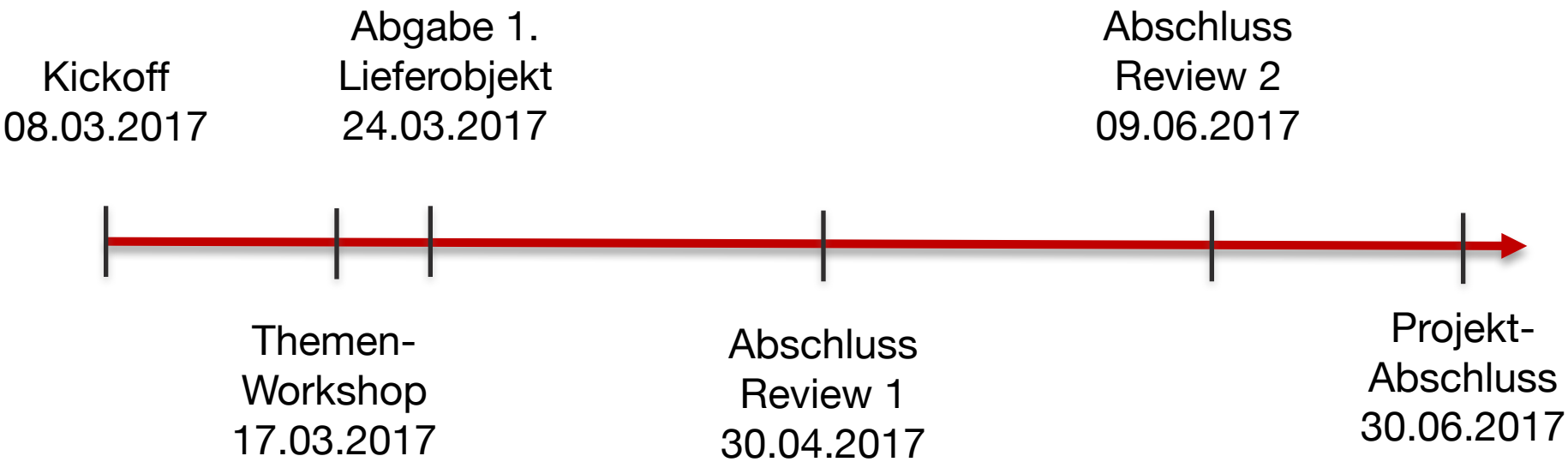
Abgrenzungen

- Beschränkt auf ausgewählte Themen im Bereich Datenschutz und Datensicherheit
- Die Ausführungen sind als Empfehlung zu verstehen
- “Kann“-Ausführung
- Inhaltlich nicht vollständig – weder in der Breite noch in der Tiefe
- Keine Garantie zum Bestehen der Zertifizierung

VORGEHEN


1
Elektronisches Patientendossier Gesetz (EPDG)
Elektronisches Patientendossier Verordnung (EPDV)
2
Technische und organisatorische Zertifizierungsvoraussetzungen (TOZ)
Themenvorschläge: Umsetzungs-empfehlungen
3
4
Modul 1
Deliverables
Grundlagen
DLV 01.1: Datenschutz- und Datensicherheitsmanagement
DLV 01.2: Einsatz Antivirus
DLV 01.3: Sicherheitsvorfälle
DLV 01.4: Datentrennung
DLV 01.5: Kryptografie
DLV 01.6: Vertraulichkeitsstufen
National Institute of Standards and Technology
Bundesamt für Sicherheit in der Informationstechnik
DIN66399
Modul 2
Deliverables
Grundlagen
DLV 02.1: Mapping
ISO/IEC 27001
ISO/IEC 27002
Modul 3
Deliverables
Grundlagen
DLV 03.1: Zugangsportale
OWASP: Application Security Verification Standard v3 / Mobile Top 10 & Top 10 2017
SANS: Web Application Security Policy
Review
Review
Review
Umsetzunghilfe DSDS Entwurf
Review
Umsetzunghilfe DSDS Final

Zeitplan


Kickoff
08.03.2017
Abgabe 1.
Lieferobjekt
24.03.2017
Abschluss
Review 2
09.06.2017
Themen-
Workshop
17.03.2017
Abschluss
Review 1
30.04.2017
Projekt-
Abschluss
30.06.2017

THEMENÜBERSICHT


Empfehlungen
Schutz vor Schadsoftware
Erkennung & Meldung
Erhebung sicherheitsrelevanter Informationen
Untersuchung und Bewertung
Erkennung & Behandlung von Sicherheitsvorfällen
Priorisierung, Eskalation & Massnahmen
Referenzprozess
Dokumentation und Nachbearbeitung
Erläuterung zur Datentrennung
Datentrennung
Ausgestaltung der Datentrennung
Sicht Gemeinschaft
Sicht Outsourcing-Provider
Umsetzungshilfe
Disziplinarverfahren
Wiederanlaufplanung
Personalsensibilisierung
Umgang mit Sicherheitsschwachstellen
Datenschutz & Datensicherheitsmanagementsystem
Datenschutz- & Datensicherheitsverantwortlicher
Backup und Wiederherstellungsprozess
Datenträgervernichtung
Änderungsmanagement
Risikomanagement
Verwaltung Gesundheitsfachperson und deren Hilfspersonen
Steuerung und Überwachung von Dritten
Inventar der Informatikinfrastruktur
Schutz vor Manipulation der Vertraulichkeitsstufen
Sicherheitsmassnahmen
Kryptographie
Konfiguration & Wartung
Web-Services
Transport von Daten
Dateien und Ressourcen
Speicherverschlüsselung
Kryptografische Grundsätze
Einsatz von Kryptografie
Kryptografische Verfahren
Ersatz von Verfahren mit bekannten Schwachstellen
Hashing
Transportverschlüsselung
Kompromittierung & Wiederherstellung von kompromittierten Dateien
Schlüsselverwaltung
Schlüssel Verantwortlichkeiten und Audit
Verwendung von Transport Layer Security (TLS)
Session Management
Sicherung der Zugangsportale
Zugriffskontrolle / Managemen
Fehlermanagement und Logging
Architektur, Design & Bedrohungsmodelle
Validierung von Eingaben
HTTP Sicherheitskonfiguration
Authentifikation und Verifikation
Schutz von sensiblen Daten
Mobile Applikationen (Apps)

FOKUS 1: DATENSCHUTZ- UND DATENSICHERHEITS-MANAGEMENTSYSTEM

Rolle DSDS-Verantwortlicher

TOZ-Vorgabe (4.11)

Für das Führen des DSDS Managementsystems der Gemeinschaft ist ein/eine DSDS-Verantwortliche(r) zu benennen und sein Aufgabenprofil zu definieren

Unabhängigkeit der Funktion

Bei Personalunion muss einem Interessenkonflikt vorgebeugt werden. Folgende Kombinationen sollten vermieden werden:

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

Aufgaben

- 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
- Zusammenarbeit mit Sicherheitsverantwortlichen anderer Organisationen

Steuerung und Überwachung von Dritten

TOZ-Vorgabe (4.10)

Die von Dritten (inkl. Unterlieferanten) gelieferten Dienstleistungen, Berichte und Aufzeichnungen müssen regelmässig überwacht und überprüft werden.

Steuerung und Überwachung

Empfehlungen zur Steuerung und Überwachung:

- Monatlicher Vergleich der Messwerte (Soll- / Ist Vergleich)
- Durchführung von regelmässigen Lieferanten-Audits (bei strategischen Lieferanten jährlich)
- Massnahmen bei festgestellten Abweichungen definieren und umsetzen

Vertrag

Die Leistungserbringung muss schriftlich definiert sein (Vertrag). Unter anderem müssen folgende Punkte abgedeckt sein:

- Ort der Leistungserbringung und Datenhaltung
- Definition der Kennzahlen und Reporting-Verfahren
- Verpflichtung zur Einhaltung der rechtlichen Vorgaben und den daraus resultierenden Anforderungen
- Einbezug von Unterlieferanten
- Kommunikations- und Eskalationswege
- Vorgehen bei Sicherheitsvorfällen
- Auditrecht
- Beendigung (vor allem Datenexport und –löschung)

Inventar

TOZ-Vorgaben (4.6.1 und 4.6.2)

Gemeinschaften müssen sicherstellen, dass alle schützenswerten Daten, Systeme und EPD Einrichtungen identifiziert, klassifiziert und in einem Inventar der Informatikinfrastruktur erfasst und aktuell gehalten werden

Bedeutung des Inventars

Ein vollständiges und aktuelles Inventar ist eine wichtige Grundlage für spätere Aktivitäten. Es unterstützt unter anderem nachfolgende Prozesse:

- Risikomanagement
- Schwachstellen-Management
- Erkennung und Behandlung von Sicherheitsvorfällen
- Ersatz von kryptografischem Schlüsselmaterial

Relevante Attribute

Folgende Attribute eines Elements sollten mindestens gepflegt werden:

- Name und Bezeichnung
- Verwendungszweck
- Klassifizierung
- Standort
- Physisch oder virtuell
- Verantwortlicher Eigentümer
- Zugriffsrechte
- Identifikationsdaten (z.B. System-ID)
- Adressierungselemente
- Angaben zu Garantie und Wartung
- Eingesetzte Software-Versionen

Es wird empfohlen für die Verwaltung des Inventars ein entsprechendes Tool einzusetzen. Dieses kann auch die jährliche Überprüfung massgeblich unterstützen.

Umgang mit Sicherheitsschwachstellen

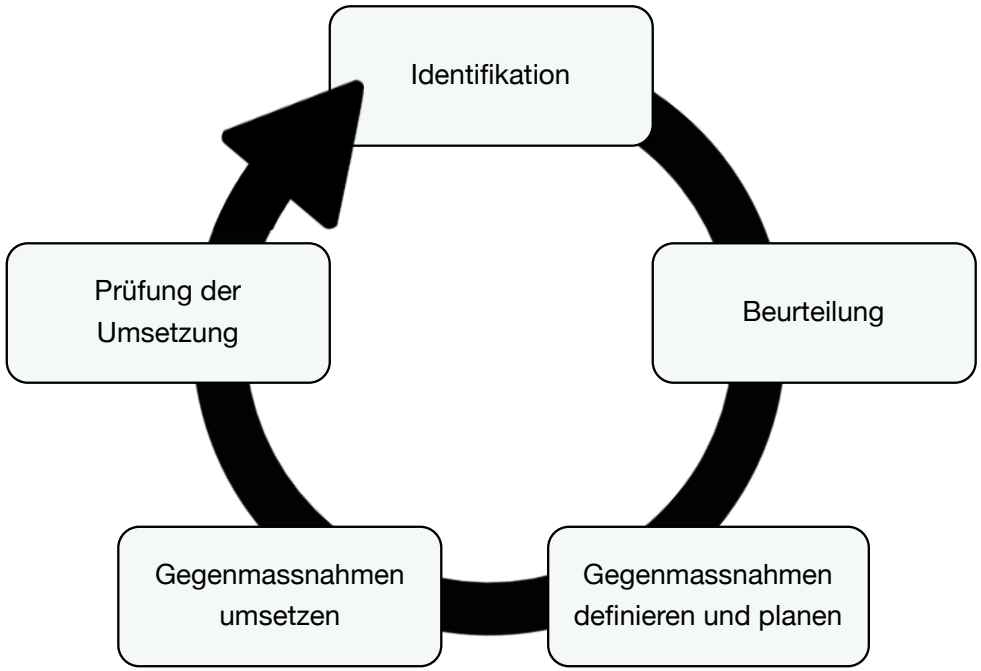
TOZ-Vorgaben (4.4.1 und 4.4.2)

Gemeinschaften müssen über ein Sicherheitsschwachstellenmanagement verfügen, das Informationen über technische Sicherheitsschwachstellen der verwendeten Informatikmittel rechtzeitig einholt.

Hilfsmittel

- Vulnerability Scanner
- Penetration Tests
- Prozessbeschreibung
- Beurteilungsschema
- Passive Überwachung mittels laufender Auswertung von bekannten Schwachstellen

Ablauf



FOKUS 2: SCHUTZ VOR SCHADSOFTWARE

Schutz vor Schadsoftware

TOZ-Vorgabe (4.5)

Massnahmen zum Schutz insbesondere der schützenswerten Elemente der Informatikinfrastruktur vor Schadsoftware müssen getroffen werden.

Zusätzliche Härtung

Zusätzlich zum klassischen Antivirenprogramm empfehlen wir zusätzliche Härtungsmassnahmen:

- Whitelisting von Anwendungen
- Host-basierte Firewalls
- Aktualisierung der Software
- Deaktivieren von Services
- Minimale Rechte
- Hardening gemäss Herstellerempfehlungen

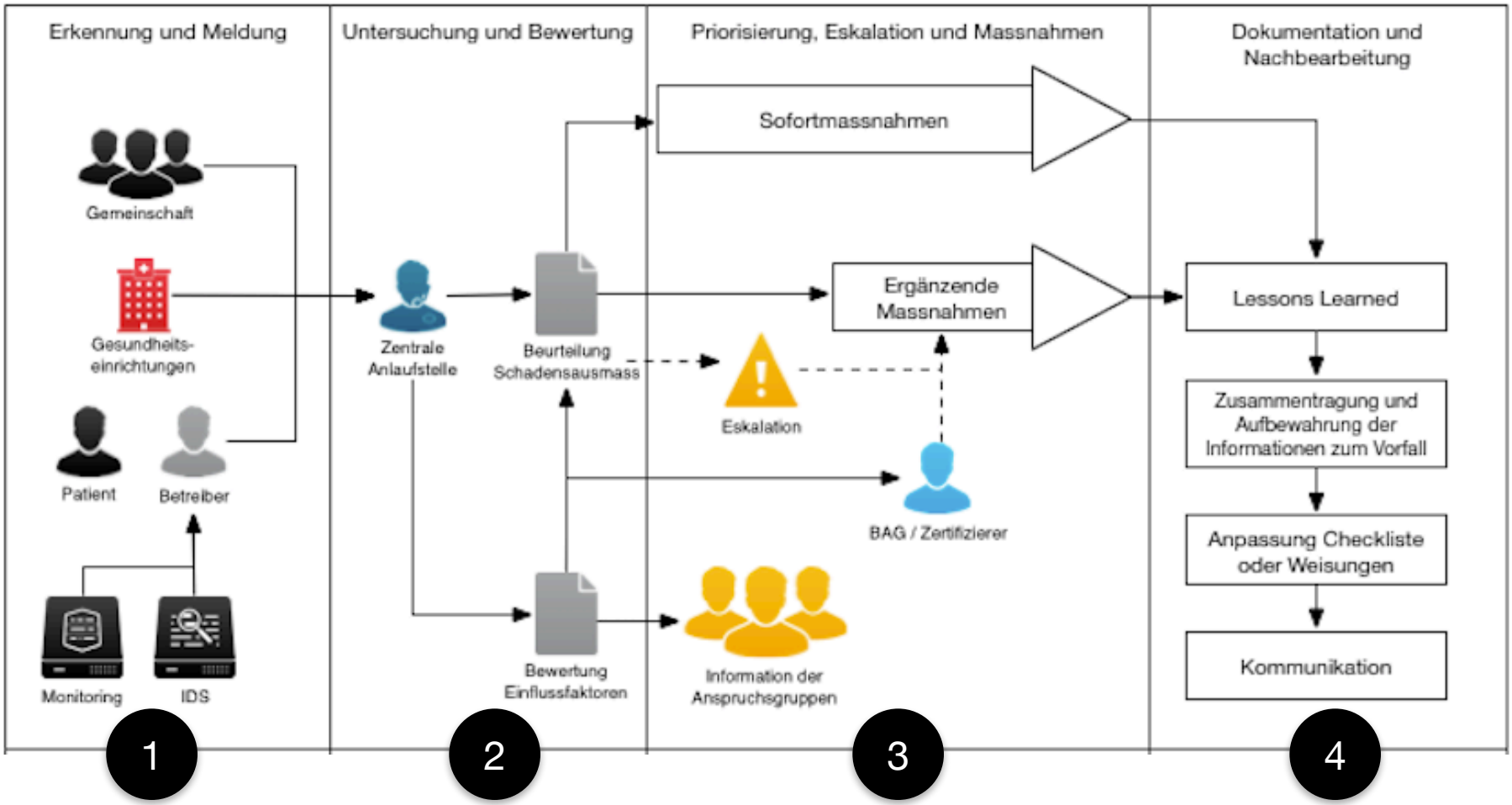
Empfehlungen

Im Zusammenhang mit dem Schutz vor Schadsoftware wurden folgende Empfehlungen formuliert:

- Unterschiedliche Produkte auf Ebene Element und Netzwerkperimeter
- Aktualisierung der Software und Signaturen
- On Access Scanning (auch lesende Zugriffe)
- Heuristisches Verfahren auf exponierten Systemen

Beim Einsatz von Antivirenprogrammen gilt: Je mehr Interaktionen eines Endbenutzers am Gerät (Clients, Terminalserver usw.), je ausgeprägter muss der Schutz sein.

FOKUS 3: ERKENNUNG UND BEHANDLUNG VON SICHERHEITSVORFÄLLEN


Erkennung und Meldung
Untersuchung und Bewertung
Priorisierung, Eskalation und Massnahmen
Dokumentation und Nachbearbeitung
Gemeinschaft
Gesundheits-einrichtungen
Patient
Betreiber
Monitoring
IDS
Zentrale Anlaufstelle
Beurteilung Schadensausmass
Bewertung Einflussfaktoren
Sofortmassnahmen
Ergänzende Massnahmen
Eskalation
BAG / Zertifizierer
Information der Anspruchsgruppen
Lessons Learned
Zusammentragung und Aufbewahrung der Informationen zum Vorfall
Anpassung Checkliste oder Weisungen
Kommunikation
1
2
3
4

Herzlichen Dank

BERN
Redguard AG
Eigerstrasse 60
CH-3007 Bern

ZÜRICH
Redguard AG
Hardturmstrasse 103
CH-8005 Zürich

Phone: +41 (0)31 511 37 50
contact@redguard.ch
www.redguard.ch

Kontaktdaten

Alexander Hermann

Managing Partner
+41 79 619 56 37
alexander.hermann@redguard.ch