KANTON AARGAU

Beauftragte für
Öffentlichkeit und
Datenschutz

Merkblatt

26.05.2020 (Stand 07.07.2020)

Datensicherheit bei Videoüberwachungen mit Dokumentationsvorlage

1. Einleitung

Das vorliegende Merkblatt richtet sich an öffentliche Organe des Kantons Aargau, welche öffentlich zugängliche Räume mit optisch-elektronischen Anlagen (Videoüberwachung) beobachten oder beobachten möchten. Dafür ist eine Bewilligung der Beauftragten für Öffentlichkeit und Datenschutz erforderlich (§ 20 des Gesetzes über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen [IDAG][1]) erforderlich. Beim Betrieb von optisch-elektronischen Überwachungsanlagen muss die in § 12 IDAG statuierte und in den §§ 4 und 5 der Verordnung zum IDAG vom 26. September 2007 (VIDAG)[2] näher geregelte Datensicherheit gewährleistet sein. Personendaten müssen durch angemessene organisatorische und technische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. Das verantwortliche öffentliche Organ ist verpflichtet, die zur Gewährleistung der Datensicherheit getroffenen Massnahmen zu dokumentieren sowie deren Überprüfung und Aktualisierung sicherzustellen (§ 5 Abs. 1 VIDAG).

Der Nachweis, dass die einschlägigen Bestimmungen zur technischen und organisatorischen Datensicherheit eingehalten werden, ist von den öffentlichen Organen grundsätzlich zusammen mit dem Gesuch[3] um Bewilligung einer optisch-elektronischen Anlage i.S.v. § 20 IDAG und § 11 VIDAG einzureichen. Die Mustervorlage für ein mögliches Informations- und Datensicherheitskonzept (ISDS-Konzept) im Anhang zu diesem Merkblatt soll dazu beitragen, den geforderten Nachweis beim Betrieb einer optisch-elektronischen Überwachungsanlage durch öffentliche Organe zu vereinfachen. Aufgrund der unterschiedlichen Möglichkeiten der Ausgestaltung von optisch-elektronischen Überwachungssystemen müssen allenfalls zusätzliche Nachweise erbracht werden; diese sind bei der Verwendung der Vorlage entsprechend zu ergänzen.

2. Begrifflichkeiten

Nachfolgend werden die verwendeten Begrifflichkeiten näher erläutert. Zu beachten ist, dass nicht alles, was technisch möglich ist, beim Betrieb einer Videoüberwachungsanlage auch rechtlich zulässig ist. Dieser muss immer auf einer Rechtsgrundlage beruhen und der Eingriff in die Persönlichkeit betroffener Personen verhältnismässig sein.

2.1. IP-Kamera-Technik

In der zentralisierten IP-Kamera-Technik werden Kameras und Recorder ins Netzwerk eingebunden. Für eine reine Live-Ansicht kann zwischen einer IP-Kamera und einem

[1] SAR 150.700
[2] SAR 150.711
[3] https://www.ag.ch/media/kanton_aargau/dvi/dokumente_5/ges_1/organisation_8/idag/videoueberwachung/03_Formular_Gesuch_Stand_Mai_2019.pdf

Monitor ein IP-Videorecorder (NVR) geschaltet werden. Für eine Aufzeichnung mittels NVR muss dieser ebenfalls im Netzwerk integriert sein.

Der Zugriff auf die Livebilder und Aufnahmen erfolgt über den NVR, was das Einrichten (und den Support) stark erleichtern kann. Es kann lokal im Netzwerk sowie aus der Ferne (wenn eingerichtet) auf Livebilder und Einstellungen zugegriffen werden. Der Fernzugriff kann dann über einen PC mittels Software (oft via Browser) bzw. über Smartphone oder Tablet mittels App erfolgen.

Dezentralisierte IP-Kameras enthalten neben der eigentlichen Kamera-Komponente auch einen Rechner, der die Aufgaben des NVR übernimmt und die Bilddaten an jedes verbundene Speichermedium abgeben kann. Der Rechner besteht im Wesentlichen aus einer CPU, einem Flash-Speicher und einem DRAM-Speicher. Durch die Netzwerkkamera-Software wird es möglich, dass das Gerät im Netz als Webserver, FTP-Server sowie als FTP-Client und als E-Mail-Client auftritt.

2.2. Analoge-Kamera-Technik

Analoge-Kameras (HDCVI/HDTVi-Kameras) werden für eine reine Live-Ansicht mittels Koaxialverkabelung an einen Monitor mit BNC-Eingang angeschlossen. Für eine Aufzeichnung ist die Verwendung eines Digitalvideorecorders (DVR) notwendig. Über diesen kann das Videosystem auch in ein Netzwerk integriert werden. So ist auch die Möglichkeit eines Fernzugriffs über einen PC mittels Browser oder Software bzw. über Smartphone oder Tablet mittels App gegeben. Inzwischen können auch IP-Kameras an einen DVR angeschlossen bzw. integriert werden.

2.3. Video-Management-Software (VMS)

Die Video-Management-Software (oft frei verfügbar) erlaubt die Verwaltung aller Recorder und Kameras im System. Nicht nur die klassischen Grundfunktionen wie Vorschau, Aufnahme, Wiedergabe, Exportieren, Foto- und Sofortwiedergabe stehen zur Verfügung, auch sogenannte intelligente Funktionen[4] (Video-Content-Analyse) können mittels dieser Software genutzt werden (z.B. Personenzählungen, smarte Verfolgung, Gesichtserkennung usw.).

2.4. Video-Content-Analyse

Bei der Video-Content-Analyse wird versucht, Objekte im Bild vom Hintergrund zu unterscheiden, um diese anschliessend zu analysieren. Dadurch kann ein zum Voraus definierter Event (z.B. eine E-Mail, eine SMS oder ein Alarm auf einen Anzeigemonitor) ausgelöst werden. Dies kann auf intelligenten Kameras oder auf einem Aufzeichnungsserver erfolgen.

2.5. Life Cycle Management

Moderne Videosysteme sind komplexe IT-Systeme, die für einen sicheren Betrieb eine kontinuierliche fachgerechte Wartung erfordern. Dazu gehört, dass sämtliche Systemkomponenten regelmässig mit Updates auf den neusten Stand gebracht werden. Das Updaten von Software und Firmware ist ein wichtiger Prozess der Cybersecurity. Angreifer werden oft versuchen, übliche (bekannte) Schwachstellen auszunutzen. Wenn Angreifer Netzwerkzugriff auf einen ungepatchten Service erhalten, können sie damit

[4] Intelligente Funktionen sind im Gesuch um Bewilligung einer optisch-elektronischen Anlage gesondert auszuweisen. Je nach Art der intelligenten Funktion wird für deren Einsatz eine gesetzliche Grundlage vorausgesetzt. Das Fehlen einer gesetzlichen Grundlage kann zur Nichterteilung einer Bewilligung führen.

Erfolg haben. Der Life-Cycle Managementprozessbeauftragte stellt immer die neueste Firmware und Sicherheitspatches für die sämtlichen Systemkomponenten für bekannte Schwachstellen sicher und beschreibt den Prozess.

3. Datensicherheit

3.1. Verantwortlichkeit

Öffentliche Organe sind verpflichtet, Personendaten durch organisatorische und technische Massnahmen gegen unbefugtes Bearbeiten zu schützen (§ 12 IDAG i.V.m. §§ 4 und 5 VIDAG). Dabei haben sie bei der elektronischen Bearbeitung von Personendaten insbesondere die Vertraulichkeit (Verhinderung unrechtmässiger Kenntnisnahme von Informationen), die Integrität (Gewährleistung der Richtigkeit und Vollständigkeit), die Authentizität (Zurechenbarkeit der Informationsbearbeitungen) sowie die Verfügbarkeit (Speicherkontrolle, Wiederherstellung und Festlegung der Löschfristen) zu gewährleisten.

Die Personendaten müssen also vor dem Zugriff Unberechtigter mit physischen und technischen Massnahmen geschützt sein. Die Daten sind sicher aufzubewahren und der Zugriff muss beschränkt und protokolliert sein. Das verantwortliche öffentliche Organ hat sicherzustellen, dass aufgezeichnete Daten nicht verändert werden können. Die Aufnahmen sind spätestens nach 7 Tagen zu löschen oder zu überschreiben, wenn keine Widerhandlung im Sinne des im Anhang zum Reglement über die Videoüberwachung festgelegten Zwecks vorliegt.

3.2. Informationstechnologie

Aus IT-/Netzwerk-Perspektive ist die Kamera ein Netzwerk-Endpunkt – ähnlich wie Laptops, Desktops und mobile Geräte in der Organisation. Im Gegensatz zu einem Laptop in einer Organisation ist eine Netzwerk-Kamera nicht der häufigen Bedrohung durch Benutzer ausgesetzt, die eventuell schädliche Websites besuchen, gefährliche E-Mail-Anhänge öffnen oder nicht vertrauenswürdige Anwendungen installieren. Die Kamera und ihre Komponenten sind jedoch Netzwerkgeräte mit Schnittstellen, durch die das System Risiken ausgesetzt ist. Diese Massnahmen konzentrieren sich darauf, den Einwirkungsbereich dieser Risiken zu reduzieren.

Ein Massnahmenplan wird erarbeitet, sobald dies sinnvollerweise möglich ist (i.d.R. nach einem Beschaffungsentscheid, damit zusammen mit dem Lieferanten die Umsetzung der bekannten Massnahmen geplant werden kann).

4. Bemerkungen zur Mustervorlage

Planung, Konfiguration und Administration derart komplexer Netze und der dazu nötigen aktiven Netzwerkkomponenten erfordern solides und aktuelles Fachwissen auf diesem Gebiet, damit nicht durch Unkenntnis Sicherheitslücken entstehen. Als Herangehensweise für das Ausfüllen der nachfolgenden Vorlage empfehlen wir dringend, entsprechendes technisches Fachpersonal heranzuziehen.

Angaben zur Datensicherheit bei der Überwachung mit optisch-elektronischen Anlagen an *[Standort(e) eintragen]*

Rechtliche Grundlage

☐ Reglement über die Videoüberwachung *[Benennung des öffentlichen Organs]* vom *[TT.MM.JJJJ]*

Art der Auswertung und Art der technischen Auswertung

☐ **Ereignisfallbezogene Auswertung**

☐ Nur Auswertung der gespeicherten Daten im Ereignisfall
Ereignisse: *[Nennung der Ereignisse, welche zu einer Auswertung führen]*

☐ Video-Content-Analyse[5]
Auslösendes Element: *[Nennung der Elemente, welche zu einer Aufzeichnung führen]*

☐ **Ereignisfallbezogene Auswertung mit der Möglichkeit einer ereignisfallbezogenen Echtzeitüberwachung**

☐ Auswertung der gespeicherten Daten im Ereignisfall
Ereignisse: *[Nennung der Ereignisse, welche zu einer Auswertung führen]*

☐ Echtzeitüberwachung bei folgenden Ereignissen
Ereignisse: *[Nennung der Ereignisse, welche zu einer Auswertung führen]*

☐ Ereignisfallbezogene Auswertung

☐ Video-Content-Analyse
Auslösendes Element: *[Nennung der Elemente, welche zu einer Aufzeichnung führen]*

☐ **Ereignisfallbezogene Auswertung mit dauernder Echtzeitüberwachung[6]**

☐ Auswertung der gespeicherten Daten im Ereignisfall
Ereignisse: *[Nennung der Ereignisse, welche zu einer Auswertung führen]*

☐ Video-Content-Analyse
Auslösendes Element: *[Nennung der Elemente, welche zu einer Aufzeichnung führen]*

☐ **Echtzeitüberwachung ohne Aufzeichnung**

☐ Video-Content-Analyse
Auslösendes Element: *[Nennung der Elemente, welche zu einer Aufzeichnung führen]*

☐ **Videokamera-Attrappe (unzulässig)**

☐ **Mobile Videokamera (zulässig nur für bewilligte Perimeter im Reglement)**

Video-System besteht aus

☐ zentrale / ☐ dezentrale IP-Kamera[7]	Anzahl: [ ]	☐ Ethernet-Verkabelung / ☐ WLAN
☐ HDCVI/HDTVi-Kameras	Anzahl: [ ]	☐ Koaxial-Verkabelung
☐ Netzwerkvideorecorder (NVR)	Anzahl: [ ]	
☐ Digitalvideorecorder (DVR)	Anzahl: [ ]	IP-Netzwerk Anbindung ☐Ja / ☐ Nein

Netzwerk Segmentierung: ☐ Ja / ☐ Nein (z.B. Videoüberwachung separiert von der Büroautomation)

☐ Zugriff	☐ PC via lokalem Netzwerk / ☐ via Internet mittels (PC, App, Smartphone)
☐ Fernzugriff	☐ Ja für Supportzwecke / ☐ Ja für Support und Ansicht / ☐ Nein

[5] Für Begriffsdefinition siehe 2.4.
[6] Darunter wird eine Live-Ansicht von Bildmaterial auf einem Monitor verstanden.
[7] Risiko: Wie bei jeder Netzwerkkomponente besteht auch bei Netzwerkkameras die Gefahr, dass es zu Zugriffen von nicht autorisierten Personen kommt. Die meisten modernen Kameras verfügen über einen Passwortschutz und ähnliche Sicherheitsmechanismen. Zudem müssen die Bilddaten per SSLv3-Verschlüsselung übertragen werden und die Kameras müssen mit regelmässigen, aktuellen Sicherheitsupdates versorgt sein.

Sprach-Aufzeichnung: ☐Ja / ☐ Deaktiviert

Video-Systemarchitektur-Skizze

[Architektur-Skizze einfügen]

Dauer der Überwachung (Technische Umsetzung)

☐ während der Dienst- / Publikumszeiten

☐ ausserhalb der Dienst-/ Publikumszeiten

☐ täglich in der Zeit

von [ ] bis [ ] Uhr

von [ ] bis [ ] Uhr

☐ Wochenenden / Feiertage

Freitag, [ ] Uhr bis Montag [ ] Uhr

[ ] Uhr des Vortages bis [ ] Uhr des folgenden Tages

☐ 24 Stunden

☐ sonstige Beobachtungs-/Aufnahmezeiten

Beschreibung:

Löschfristen (Technische Umsetzung)

☐ Aufnahmedaten werden nach […. h] automatisch gelöscht

☐ Aufnahmedaten werden nach […. h] überschrieben

☐ Zugang-/Zugriffs-Protokolldaten werden […. Monaten] automatisch gelöscht oder überschrieben

☐ Es ist ein Backup der Aufnahmedaten vorhanden, Aufnahmedaten sind [….Tagen] rekonstruierbar

☐ Es ist ein Backup der Zugang-/ Zugriffs-Protokolldaten vorhanden, Protokolldaten sind [….Tagen] rekonstruierbar

☐ Es besteht eine andere Regelung

Beschreibung:

! Ergibt die Auswertung, dass die Aufzeichnungen geeignet sind, zur Ahndung von im Reglement genannten Widerhandlungen (*z.B. groben Sachbeschädigungen, Körperverletzungen, erheblichen Verunreinigungen, Einbrüchen oder von Verstössen gegen das Abfallbeseitigungsreglement [hier die im Reglement festgelegten Widerhandlungen aufführen]*) beizutragen, sind diese aufzubewahren, bis sie nicht mehr zu Aufklärungs- und Beweiszwecken benötigt werden.

Kontrolle und Aufzeichnungs-Protokollierung (kein unbefugter Zugriff)

Für die Vertraulichkeit der Videodaten werden alle technisch-organisatorischen Massnahmen aufgelistet, die sicherstellen sollen, dass die Video- und Protokolldaten ausschliesslich einem bestimmten Personenkreis zugänglich sind. Dazu gehören regelmässig Zutritts-/Zugangs-/Zugriffskontrollen zu den jeweiligen System-Komponenten.

☐ Kontrolle/Protokollierung des Zutritts zum Videoüberwachungssystem.

Beschreibung: *[Wie wird Kontrolle durchgeführt?]*

☐ Protokollanalyse: Verdächtigter Datenverkehr zu den Videoüberwachungssystemen wird automatisch erkannt. Wie und wem werden die Systemmeldungen zugesandt?

Beschreibung:

☐ Protokollierung für Beweiszwecke: Übergabeprotokolle zwecks Beweissicherung sind vorhanden. Ein dokumentierter Übergabeprozess wird gelebt?

Beschreibung:

☐ Kontrolle/Protokollierung des Zutritts zum Videoüberwachungssystem. Wie und durch Wen?

Beschreibung [Beschreibung]

☐ Kontrolle/Protokollierung des Zugangs zum Videoüberwachungssystem. Wie und durch Wen?

Beschreibung [Beschreibung]

☐ Kontrolle/Protokollierung des Zugriffs zum Videoüberwachungssystem. Wie?

☐ Protokollanalyse: Verdächtigter Datenverkehr zu den Videoüberwachungssystemen wird automatisch erkannt. Wie und wem werden die Systemmeldungen zugesandt?

Beschreibung [Beschreibung]

☐ Protokollierung für Beweiszwecke: Übergabeprotokolle zwecks Beweissicherung sind vorhanden. Ein dokumentierter Übergabeprozess wird gelebt?

Beschreibung [Beschreibung]

Personenkreis mit Zugang zu den durch die Videoüberwachung erhobenen Bilddaten

Personenkreis	**Beschreibung / Bemerkung / Anzahl Personen**[8]
☐ Empfang	[Aufgabenbeschreibung / Bemerkung / Anzahl Personen]
☐ Mitarbeitende mit besonderen Funktionen (Administratoren, externe Mitarbeitende eines Dienstleisters per Fernwartung)	[Aufgabenbeschreibung / Bemerkung / Anzahl Personen]
☐ Mitarbeitende im Sicherheitsdienst	[Aufgabenbeschreibung / Bemerkung / Anzahl Personen]
☐ Dienststellenleitung	[Aufgabenbeschreibung / Bemerkung / Anzahl Personen]
☐ Sonstige Zugriffsberechtigte	[Aufgabenbeschreibung / Bemerkung / Anzahl Personen]

Datensicherheit-Empfehlung zur Freigabe von IP-Kameras in einer Netzwerkumgebung

Authentifizierung (Standard-Passwörter)

[8] Verweise auf bestehendes Benutzerberechtigungskonzept mit den aufgeführten Rollen möglich.

Es muss damit gerechnet werden, dass Angreifer und Schadsoftware die Standard-Passwörter (Default Password) vieler Produkte kennen, denn Listen dieser Passwörter sind im Internet frei zugänglich**. Unmittelbar bei der Erstinbetriebnahme müssen deshalb dringend auf jedem Gerät eigene "starke" Passwörter konfiguriert und die vom Hersteller vorkonfigurierten Benutzerkonten gelöscht werden.**

Freigabe ins Internet

Es ist **nicht gestattet**, die Kamera als **öffentlichen Webserver freizugeben** und dadurch unbekannten Clients einen Netzwerkzugriff auf die Kamera zu ermöglichen.

Freigabe im lokalen Netzwerk begrenzen

In einer VMS-Umgebung greifen die Clients über den VMS-Server (oft gleich auch Aufnahmegerät) auf die Live-Videos und Aufzeichnungen zu**.** Die Platzierung des VMS-Server und der Kameras in einem isolierten Netzwerk, entweder durch physikalische oder durch virtuelle Isolation, ist eine übliche und empfohlene Massnahme, um Gefahren und Risiken zu reduzieren.

Art der Geräte, Standort und Überwachungsbereiche

Art der Geräte

Art	Beschreibung / Verweise
Kamera Hersteller, Typenbezeichnung sowie Darstellung der Leistungsmerkmale wie anlog/digital, Lichtempfindlichkeit, Bildauflösung, Erfassungswinkel, interne Speicher, Schwenk/Neigefunktion (mechanisch bzw. digital), Signalverarbeitung, Alarmfunktion, mit/ohne Fernsteuerung etc.	[Beschreibung / Verweise]
Netz[9] Darstellung der Netzverbindungen (z.B. Funk-, Kabelverbindung) und der Einbindung in vorhandene Netze und deren Schnittstellen: WLAN, ISDN/DSL, Intranet, Internet, verschlüsselt/unverschlüsselte Datenübertragung	[Beschreibung / Verweise]
Aufnahmegeräte Analoger/digitaler Rekorder, PC, Server, …., Hersteller, Typenbezeichnung und/bzw. Darstellung spez. Leistungsmerkmale wie Speicherkapazität, Netzeinbindung, Zugriffsschutz, eingesetzte Videomanagementsoftware	[Beschreibung / Verweise]
Kodierer (Encoder)[10] -> Einbindung analoger Geräte	[Beschreibung / Verweise]

[9] Grosse Netze sollten in separate Teilnetze aufgeteilt werden (subnetting) und zwischen diesen Teilnetzen sollten gezielt nur die erwünschten Verbindungen zugelassen werden, damit beispielsweise sensible Organisationsdaten vor Zugriffen aus dem Videosystem geschützt bleiben.

[10] Der Kodierer (Encoder) ist ein System, das die aus der Videokamera übermittelten Daten in ein anderes Datenformat umwandelt, um Videodaten für eine schnelle Übertragbarkeit zu komprimieren.

Hersteller, Typenbezeichnung, besondere Leistungsmerkmale	
Kreuzschiene (Umschaltbox)[11] Hersteller, Typenbezeichnung, besondere Leistungsmerkmale	[Beschreibung / Verweise]
Monitor Hersteller, Typenbezeichnung, besondere Leistungsmerkmale	[Beschreibung / Verweise]
Drucker Hersteller, Typenbezeichnung, besondere Leistungsmerkmale	[Beschreibung / Verweise]
Weitere Geräte	[Beschreibung / Verweise]

Standort der Geräte

(Beschreibung der Installationsorte der Kameras und sonstiger eingesetzter Systemkomponenten)

Systemkomponente	Standort / Installationsorte
Kamera	[Standort / Installationsorte]
Aufnahmegeräte	[Standort / Installationsorte]
Monitor	[Standort / Installationsorte]
Drucker	[Standort / Installationsorte]
Weitere Geräte	[Standort / Installationsorte]

Räumlicher Überwachungsbereich

(bildliche Darstellung des Überwachungsbereiches: bei mechanischer oder digitaler Schwenk-/Neige-/Zoom-Funktion und ähnlicher Darstellung der max. Werte: Erfassungswinkel, Zoom etc.)

Kamera	Beschreibung / Werte
Kamera 1	[Beschreibung / Werte]
Kamera 2	[Beschreibung / Werte]
Kamera 3	[Beschreibung / Werte]
Kamera 4	[Beschreibung / Werte]
Kamera 5	[Beschreibung / Werte]
Kamera x	[Beschreibung / Werte]

Massnahmenplan zur Abwendung von Bedrohungen auf Systeme

! Zum Massnahmenplan können auch die Bausteine und deren Massnahmenbeschreibungen vom deutschen Bundesamt für Sicherheit in der Informatik (BSI) und ihrem IT-Grundschutz herangezogen werden (siehe dazu "Allianz für Cyber-Sicherheit" mit der BSI-Empfehlung "Sicherheit von IP-basierten Überwachungskameras"

[11] Eine Kreuzschiene (Umschaltbox) ist ein Steuergerät, mit dem bei Videoüberwachungsanlagen verschiedene Kamerapositionen in beliebiger Folge und Dauer an mehreren Monitorplätzen gleichzeitig angezeigt werden können.

in der Version 1.1 vom 08.11.2016 oder in der Version 2 mit dem Titel "Sicherheit von Geräten im Internet der Dinge"). Insbesondere wird der Baustein B3.407 "Eingebettetes System[12]" für die Anwendung erwähnt. Darüber hinaus liefern die zusätzlich aufgeführten Bausteine und Massnahmen weitere Informationen. Sie beschreiben zusätzliche Umsetzungsempfehlungen von zuvor genannten Massnahmen auf die Bedrohungen.

Siehe dazu:

- B 3.407 Eingebettetes System
- B 4.6 WLAN
- M2.8 Vergabe von Zugriffsrechten
- M 2.11 Regelung des Passwortgebrauchs
- M2.109 Rechtevergabe für den Fernzugriff
- M 2.273 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
- M 2.384 Auswahl geeigneter Kryptoverfahren für WLAN
- M2.417 Planung der technischen VPN-Realisierung
- M2.555 Entwicklung eines Authentisierungskonzeptes für Anwendungen
- M 4.7 Änderung voreingestellter Passwörter
- M 4.488 Deaktivieren nicht benutzter Schnittstellen und Dienste bei eingebetteten Systemen
- M 5.61 Geeignete physische Segmentierung
- M 5.62 Geeignete logische Segmentierung
- M 5.77 Bildung von Teilnetzen

System-komponente	Schutzziel	Bedrohungen	Massnahmen13	Wie?
Kamera	Vertraulichkeit	[Bedrohungen]	[Massnahmen]	[Beschreibung]
	Integrität	[Bedrohungen]	[Massnahmen]	[Beschreibung]
	Verfügbarkeit	[Bedrohungen]	[Massnahmen]	[Beschreibung]
	Authentizität	[Bedrohungen]	[Massnahmen]	[Beschreibung]
	Revisionsfähigkeit	[Bedrohungen]	[Massnahmen]	[Beschreibung]
Netz	Vertraulichkeit	[Bedrohungen]	[Massnahmen]	[Beschreibung]
	Integrität	[Bedrohungen]	[Massnahmen]	[Beschreibung]
	Verfügbarkeit	[Bedrohungen]	[Massnahmen]	[Beschreibung]
	Authentizität	[Bedrohungen]	[Massnahmen]	[Beschreibung]
	Revisionsfähigkeit	[Bedrohungen]	[Massnahmen]	[Beschreibung]
Aufnahmegerät (z.B. Videoserver/Videorekorder)[14]	Vertraulichkeit	[Bedrohungen]	[Massnahmen]	[Beschreibung]
	Integrität	[Bedrohungen]	[Massnahmen]	[Beschreibung]
	Verfügbarkeit	[Bedrohungen]	[Massnahmen]	[Beschreibung]

[12] Embedded Systems (eingebettete Systeme) sind Computer, die für einen bestimmten technischen Zweck in ein Gerät eingebaut werden und dort – für den Anwender oft unsichtbar – ihren Dienst tun. Meist Produkte wie, "intelligente" Lautsprecher, Alarmanlagen und auch IP-Kameras.

[13] Massnahmen sind grundsätzlich als Eignungskriterien für das beschaffene System und deren Bedrohungen zu verstehen, soweit dies möglich ist. Es muss auf jeden Fall ein schriftliches Benutzerberechtigungskonzept erarbeitet werden, welches von der systemverantwortlichen Stelle unterzeichnet ist. Dieses beinhaltet abschliessend die vorgesehenen Rollen inkl. den Zugriffsberechtigungen der zugeteilten einzelnen Mitarbeitenden bzw. Externen.

[14] Sollten Videodaten im Internet übertragen oder gespeichert werden (z.B. "Cloud-Lösung), ist eine zuverlässige durchgehende Verschlüsselung gefordert. Zu den Voraussetzungen für den Einsatz von Cloud-Lösungen vgl. Merkblatt Auslagerung von Datenbearbeitungen; Besonderheiten des Cloud Computing.

	Authentizität	[Bedrohungen]	[Massnahmen]	[Beschreibung]
	Revisionsfähigkeit	[Bedrohungen]	[Massnahmen]	[Beschreibung]
Monitor / PC	Vertraulichkeit	[Bedrohungen]	[Massnahmen]	[Beschreibung]
	Integrität	[Bedrohungen]	[Massnahmen]	[Beschreibung]
	Verfügbarkeit	[Bedrohungen]	[Massnahmen]	[Beschreibung]
	Authentizität	[Bedrohungen]	[Massnahmen]	[Beschreibung]
	Revisionsfähigkeit	[Bedrohungen]	[Massnahmen]	[Beschreibung]
Sonstige Geräte	Vertraulichkeit	[Bedrohungen]	[Massnahmen]	[Beschreibung]
	Integrität	[Bedrohungen]	[Massnahmen]	[Beschreibung]
	Verfügbarkeit	[Bedrohungen]	[Massnahmen]	[Beschreibung]
	Authentizität	[Bedrohungen]	[Massnahmen]	[Beschreibung]
	Revisionsfähigkeit	[Bedrohungen]	[Massnahmen]	[Beschreibung]

Beispiel Kamera

Bei einer Kamera könnten die technischen und organisatorischen Massnahmen beispielweise wie folgt beschrieben werden:

System-Komponente	Schutzziel	Mögliche Bedrohungen	Beispiel Massnahmen	Wie?
Kamera	Vertraulichkeit	Diebstahl, unberechtigter Zugriff, unberechtigtes mitsehen…	Zugangssicherung, Zugriffsschutz, Berechtigungssystem	HTTPS verschlüsselt den Datenaustausch zwischen dem Client und der Kamera (Achtung! Aktivierung von HTTPS werden nicht automatisch Video verschlüsselt, das über RTP/TTSP gesendet wird. Hinweis: Ein selbstsigniertes Zertifikat bietet eine angemessene Verschlüsselung, schützt aber nicht von einem Man-in-the-Middle-Angriff. Clients (z.B. Webbrowser) werden davor warnen, dass das Zertifikat nicht vertrauenswürdig ist.
	Integrität	Unberechtigte Eingriffe, Veränderungen, Bildbearbeitung	Protokollierung, Zugriffschutz	Aus Sicherheitsperspektive ist es wichtig, dass das Datum und die Uhrzeit korrekt sind, damit zum Beispiel die Zeitstempel der System-Logs die richtigen Informationen haben. Ein Syslog-Server sammelt alle Log-Meldungen der Kameras. Dies vereinfacht Audits und verhindert, dass Log-Meldungen in der Kamera entweder absichtlich /heimtückisch oder unbeabsichtigt (z.B. durch einen Neustart einer Kamera, der durch das Erreichen einer maximalen Log-Grösse verursacht wird) verloren gehen..
	Verfügbarkeit	Vandalismus, Witterungseinflüsse, Diebstahl, Stromausfall	Vandalismusschutz, Alarmfunktionen bei Ausfall	Die offensichtlichsten Bedrohungen für eine Netzwerk-Kamera sind physikalische Sabotagen, Vandalismus und Manipulation. Um das Produkt vor diesen Bedrohungen zu schützen, ist es wichtig, ein Vandalismus geschütztes Model

				oder Gehäuse auszuwählen, es auf die empfohlene Weise zu montieren und die Kabel zu schützen.
	Authentizität	Unzulässige Eingriffe	Erstellen eines schwer zu erratenden Admin Kennwortes mit mindestens 12 Zeichen, bestehend aus Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen[15] (evtl. Verwendung eines Kennwortgenerators[16]).	Das Kennwort ist die wichtigste Schutzmassnahme für eine Netzwerk-Kamera. Es ist wichtig ein starkes Kennwort einzusetzen und es geschützt zu halten. Bei einer Installation mit mehreren Kameras können die Kameras dasselbe Kennwort oder eigene Kennwörter haben. Die Verwendung desselben Kennworts vereinfacht die Verwaltung, erhöht aber das Risiko, wenn die Sicherheit einer Kamera gefährdet ist.
	Revisionsfähigkeit	Unkontrollierbare Auswertung/ Nutzung der Bilddaten für andere Zwecke	Zugriffsschutz, Zugriffsprotokollierung	Der zentrale Syslog-Server sammelt alle Log-Meldungen der Kameras. Dies vereinfacht Audits und verhindert, dass Log-Meldungen in der Kamera verloren gehen.

Life Cycle Management

Prozessbeschreibung für die sämtlichen Systemkomponenten	***[Beschreibung]***
Life Cycle Manager für die sämtlichen Systemkomponenten	*[Name des Prozessbetriebsbeauftragten / Anschrift datenverarbeitender Stelle / Hauptfunktion]*
Leistungserbringer / Systemintegratoren zu den verschiedenen Systemkomponenten	*[Leistungserbringer Systemkomponente / Firma / Adresse / Kontaktperson]*

Gültigkeitsdauer des ISDS-Konzepts und Aktualisierungen

Das vorliegende ISDS-Konzept ist für die Dauer von [*Gültigkeitsdauer angeben]* gültig und wird von der verantwortlichen Person oder Fachstelle für die Informatik- und Informationssicherheit periodisch alle *[Dauer angeben]* überprüft und bei Bedarf angepasst.

[15] Siehe BSI-Empfehlung Passwörter

[16] Siehe BSI-Empfehlung Umgang mit Passwörter

Änderungskontrolle

Datum	Verantwortlicher	Änderungen

Ort / Datum: [Ort / Datum]

Unterschrift: [Unterschrift / elektronische Signatur]

Datum, Unterschrift der internen verantwortlichen Person für die Informatik-/Informationssicherheit

Ort / Datum: [Ort / Datum]

Unterschrift: [Unterschrift / elektronische Signatur]

Datum, Unterschrift für das verantwortliche öffentliche Organ[17]

[17] Unterschriftsberechtigte Person auf Führungsebene.