Technische Projektakte

Austausch der Videosicherheitstechnik am Beispiel einer Bank

Version 1.2.

milestone

AXIS COMMUNICATIONS

Inhaltsverzeichnis

1. Aufgabenstellung

In einer Bank soll die bestehende Videosicherheitstechnik im Zuge des
> Auslaufs der Mietverträge und
> der Umbaumaßnahmen erneuert werden.

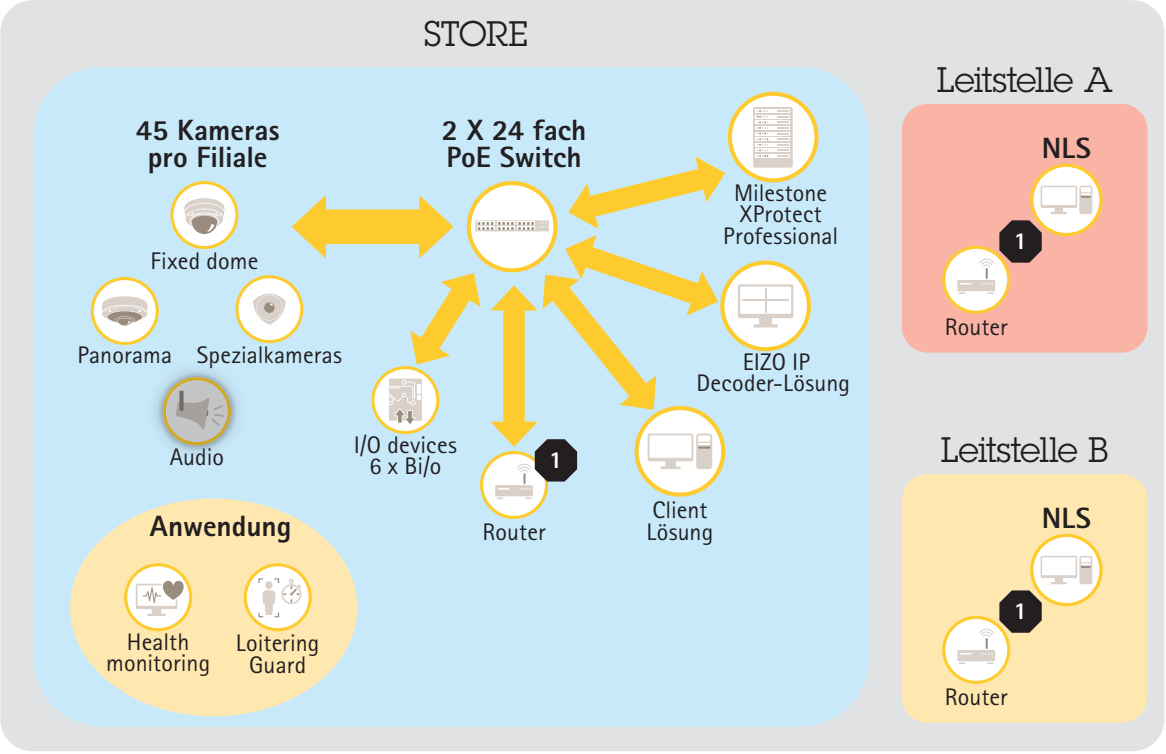
Die vorhandene Netzwerkverkabelung soll weiterverwendet werden.

Projektziele:
- Videoüberwachung auf dem aktuellen Stand der Technik
- Zentrale Verwaltung der Videotechnik

Dies ermöglicht eine schutzzielorientierte Sicherung. Die neue Technik wird so geplant, dass diese als betriebssicher gilt und entsprechend den Vorgaben ausfallsicher ist.

Die funktionale Leistungsbeschreibung basiert auf den Projektgesprächen und -unterlagen mit dem/der Sicherheitsverantwortlichen.

Dieses Dokument geht im weiteren Verlauf auf Details zur technischen Umsetzung ein.
Ziel des Dokuments ist es, Anbieter für Videosicherheitsanlagen in die Lage zu versetzen, ein konkretes Angebot zu erarbeiten, welches die Kosten für 5 Jahre für die Wartung und den Betrieb der Anlage berücksichtigt.



1 *Mindestanforderung DSL 16000 mindestens 2 Mbit/s up*

2. CSR - Corporate Social Responsibility / Code of Conduct

Auszug aus globalcompact.de:
Der United Nations Global Compact ist die weltweit größte und wichtigste Initiative für verantwortungsvolle Unternehmensführung. Auf der Grundlage 10 universeller Prinzipien und der Sustainable Development Goals verfolgt er die Vision einer inklusiven und nachhaltigen Weltwirtschaft zum Nutzen aller Menschen, Gemeinschaften und Märkte, heute und in Zukunft. Mit ihrem Beitritt zeigen bereits über 13.000 Unternehmen und Organisationen aus Zivilgesellschaft, Politik und Wissenschaft in 161 Ländern, dass sie diese Vision verwirklichen wollen.

Als Initiative der Vereinten Nationen bietet der UN Global Compact einen einzigartigen Rahmen, um über Branchen und Grenzen hinweg über eine gerechte Ausgestaltung der Globalisierung zu diskutieren und diese Vision mit geeigneten Strategien und Aktivitäten zu verwirklichen. Dabei versteht sich die Initiative nicht als zertifizierbarer Standard oder als Regulierungsinstrument, sondern als ein offenes Forum, um Veränderungsprozesse anzustoßen und Ideen zu teilen. In nationalen Netzwerken entwickeln die Teilnehmer konkrete Lösungsansätze und tragen damit zur globalen Vision des UN Global Compact bei.

Es wird erwartet, dass Zulieferer von technischer Ausstattung im Bereich der Videoüberwachung ebenfalls aktives Mitglied im UN Global Compact sind und seit mindestens 5 Jahren entsprechende Nachhaltigkeitsberichte veröffentlichen.

3. Planungsgrundlagen

Der Anspruch an die neue Videosicherheitsanlage ist zum einen die Beachtung der aktuell gültigen Gesetze und für die Videosicherheitstechnik geltenden Normen als auch eine den allgemein anerkannten Regeln der Technik entsprechende Ausführung der Videosicherheitstechnik. Nachfolgend eine Auswahl der berücksichtigten und weiterhin zu berücksichtigen Dokumente (Liste nicht abschließend):

> DIN EN 62676-1-1
> DIN EN 62676-1-2
> DIN EN 62676-4
> DIN EN 50518
> DSGVO (Datenschutz-Grundverordnung)

Sämtliche Planung basiert auf einer vorliegenden Dokumentation, Abstimmungen, Fotos, schriftlichen Informationen und Dokumenten, die vom Auftraggeber bereitgestellt worden sind und auf den Erkenntnissen einer durchgeführten Ortsbegehung.

4. DSGVO und der Schutz personenbezogener Daten

Um den Schutz der personenbezogenen Daten sicherstellen zu können, sind folgende Grundlagen bereitzustellen beziehungsweise in Zusammenarbeit mit dem Betreiber und Nutzer der Videosicherheitsanlage zu erarbeiten:

1. Vorlage für die Richtlinien zur Videoüberwachung
2. Anleitung zur Systemhärtung
3. Leitfaden zur DSGVO
4. Checkliste zur Sicherstellung der Integrität und Vertraulichkeit
5. Vorlage für kurzfristige Benachrichtigung
6. Vorlage für Anfragen von betroffenen Personen
7. Vorlage für die Benachrichtigung über Datenschutzverletzungen
8. Vorlage zur Verantwortlichkeit des Datenverarbeiters
9. Vorlage für die Aufzeichnung der Verarbeitungsaktivitäten
10. VMS (Video Management Software)
11. Schulung zum Thema Datenschutz
12. Security by Design
13. Security by Default

Jeder Anbieter hat für jede aktive Netzwerkkomponente, also jedes Gerät mit einem Netzwerk Port und ggf. einer IP-Adresse, zu bestätigen, dass die Entwicklung dieses Gerätes vollständig in der Verantwortung des Herstellers liegt unter dessen Marke das Produkt im Markt verkauft wird und dass es sich nicht um den Zukauf von Geräten handelt, die unter anderer Marke als die des Originalherstellers vertrieben werden.

Sogenannte OEM (Original Equipment Manufacturer, auf Deutsch: Originalgerätehersteller) oder ODM (Original Design Manufacturer) Geräte sind nicht zulässig, da der Nutzer keinerlei Risiko eingehen will, was den langfristigen Support dieser Geräte angeht.

Gleiches gilt auch für die Firmware auf den angebotenen Kamera Modellen, dies muss ebenfalls in der Verantwortung des Herstellers liegen, unter dessen Marke die Modelle angeboten werden.

Um die vielfältigen Anforderungen zum Schutz der Privatsphäre zu gewährleisten, muss bei den Kameras eine umfangreiche Möglichkeit der Maskierung von Bereichen gegeben sein.

1. Privatzonen
   Mindestens 30 unterschiedliche Bereiche müssen individuell maskiert werden können. Wahlweise können die Maskierungen als Verpixelung oder als Maskierung erfolgen:

   a. Verpixelung (grob):

   b. Verpixelung (fein):

   c. Vollständige Maskierung:

   d. Maskierung durch Overlays:

Mittels Overlays (über das Videobild gelegte Grafiken) können auch unterschiedliche Bildbereiche ausmaskiert werden.

5. Geräteverwaltungssoftware

Um das System in einem sicheren Zustand betreiben zu können, ist es unabdingbar, eine effiziente Geräteverwaltungssoftware (GVS) zu betreiben.
Es müssen mindestens die nachfolgenden Anforderungen erfüllt werden:

a) Information über verfügbare Firmware Updates
Alle in der Datenbank der GVS befindlichen Geräte werden mehrmals täglich auf verfügbare Firmware Updates hin überprüft. Auf verfügbare Updates ist entsprechend hinzuweisen.
Der Hinweis muss einfach erkennbar für den Anwender sein.

b) Individual- und Gruppen-Update
Die Geräte in der GVS müssen logisch gruppierbar sein, bspw. nach Bereich, Etage etc.
So soll sichergestellt werden, dass evtl. erforderliche Updates separiert nach Gruppen durchgeführt werden können.

Dies dient zum einen der Sicherstellung der Videoüberwachung im 24/7 Einsatz und zum anderen dazu, die Netzwerkinfrastruktur nicht über Gebühr zu belasten.
Updates müssen parallel oder sequenziell ausführbar sein.

c) Hardening Guide
Alle im Hardening Guide des Geräteherstellers empfohlenen Schritte zur Sicherstellung des Geräte Hardenings müssen vom GVS unterstützt werden. Auch hier muss eine effiziente Methode bereitgestellt werden, bspw. die Nutzung von Konfigurationsdateien etc., damit eine Vielzahl von Geräten (siehe Gruppen Update) entsprechend gleichzeitig konfiguriert werden können.

d) Software-Update und Lizenzen
Alle anfallenden einmaligen und sonstigen Kosten für Updates etc. sind entsprechend zu belegen. Die Kosten für Software Updates in den ersten 5 Jahren sind im Preis der GVS Lösung, in den Anschaffungskosten zu berücksichtigen.

Die Kosten für eine Gerätelizenz sind anzugeben. Sofern es Lizenz-Bundles, bspw. für 50 Geräte gibt, sind diese entsprechend einzutragen. Sofern es mehr als zwei Lizenz-Bundles gibt, sind diese in einem separaten Dokument zu hinterlegen. Der Auftraggeber behält sich vor, ggf. auf die Möglichkeit der Lizenz-Bundles zurückzugreifen, sofern diese wirtschaftlich sinnvoll sind.

6. Gliederung

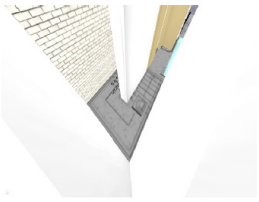
Zur Erinnerung an die Schutzziele gemäß EN 62676-4 hier eine Übersicht:

EN 62676- (Juli 2016)						
	Überwachen	Detektieren	Beobachten	Erkennen	Identifizieren	Begutachten
Szenenbreite (mm/Px)	80	40	16	8	4	1
Pixel / Meter*	12,5	25	62,5	125	250	1000

Bei der Aufgabenstellung Identifizieren ist auf den Blickwinkel der Kamera in die Szene zu achten.
Um optische Verzerrungen zu verhindern, müssen horizontale und vertikale Winkel zwischen Kamera und Prüftafel kleiner als 22,5° sein. Ziel sollte eine Montage der Kamera auf Kopfhöhe oder unwesentlich höher sein.

Im ersten Schritt wurde eine Gliederung der Szenen entwickelt, welche die einzelnen Sicherungsbereiche und Aufgaben gliedert und kategorisiert. Folgende Bereiche wurden gebildet:

1. Flurbereich/ Verkehrswege
   a. Kunden

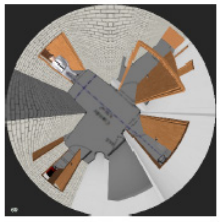


Onboard 1080p/3MP dome camera with WDR Dynamic Capture and AXIS Zip
Auflösung: 2016x1512
Sensorformat: 1/3 ; 4:3
Brennweite (mm): 1,8
Kamera Höhe: 2,5 m
Neigung: 58,8°
Blickwinkel [Grad]: 130°; 95°
Objekt Entfernung: 2,5 m
Objekt Breite: 7,4 m
Pixel/m am Objekt: 137 px/m

Aufgabenstellung ist das Erkennen von Personen

   b. Mitarbeiter und Warenempfang (Post, Pakete)

Vandal resistant indoor 1080p/2MP dome camera with WDR Forensic Capture, A
Auflösung: 1920x1080
Sensorformat: 1/3 ; 9:16
Brennweite (mm): 3,1
Kamera Höhe: 3 m
Neigung: 71,4°
Blickwinkel [Grad]: 48,8°; 89,6°
Objekt Entfernung: 2,8 m
Objekt Breite: 2 m
Pixel/m am Objekt: 259 px/m



Indoor 1080p/12MP dome camera with WDR Forensic Capture and AXIS
Auflösung: 2880x2880
Sensorformat: 1/1,7 ; 1:1
Brennweite (mm): 1,65
Kamera Höhe: 2,5 m
Neigung: 5,2°
Blickwinkel [Grad]: 360°; 180°
Objekt Entfernung: 2,2 m
Objekt Breite: 20,9 m
Pixel/m am Objekt: 432 px/m

Ziel ist es, im Laufweg eine Auflösung von >> 250 px/m, zur Dokumentation um Abläufe nachvollziehen zu können.

2. Personaleingang
Personen am Personaleingang bzw. in der Schleuse müssen identifiziert werden können.

3. Flur (Mitarbeiter mit oder ohne Kunden)
Erkennen von Personenbewegungen, um Abläufe nachvollziehen zu können.

Vandal resistant indoor 1080p/2MP dome camera with WDR Forensic Capture,
Auflösung: 1920x1080
Sensorformat: 1/3 ; 9:16
Brennweite (mm): 4
Kamera Höhe: 3 m
Neigung: 43,6°
Blickwinkel [Grad]: 40,1°; 72,9°
Objekt Entfernung: 8 m
Objekt Breite: 4,7 m
Pixel/m am Objekt: 165 px/m

4. Eingangsbereich der Bank – Kundenzutritt

Vandal resistant indoor 1080p/2MP dome camera with WDR Forensic Capture,
Auflösung: 1920x1080
Sensorformat: 1/3 ; 16:9
Brennweite (mm): 6,8
Kamera Höhe: 3 m
Neigung: 21,4°
Blickwinkel [Grad]: 48,8°; 27,7°
Objekt Entfernung: 7,5 m
Objekt Breite: 6,7 m
Pixel/m am Objekt: 262 px/m

Über diesen Kamerabereich müssen Kunden identifiziert werden können. Unter dem derzeitigen Aspekt der Maskentragepflicht bittet die Security um das Abnehmen der Maske im Eingangsbereich, um den Kunden identifizieren zu können.

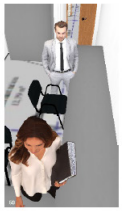
5. Wareneingang/Packtisch

Streamlined 4K fixed dome for any light conditions

Auflösung: 2160x3840
Sensorformat: 1/2,5 ; 9:16
Brennweite (mm): 5,3
Kamera Höhe: 3 m
Neigung: 57,1°
Blickwinkel [Grad]: 36,5°; 69°
Objekt Entfernung: 2,4 m
Objekt Breite: 1,4 m
Pixel/m am Objekt: 987 px/m
Totzone: -0,03 m (Breite: 0,54 m)

Die Auflösung in der Szene muss im Bereich der Warenbewegung die Bildqualität Begutachten haben.
> Lieferscheine müssen bei der Recherche zu lesen bzw.
> das Produkt eindeutig zu identifizieren sein.
Gleiches gilt für das Verpacken. Hierzu müssen in der Betriebsanleitung feste Plätze für
a. die Positionierung des Lieferscheins und des
b. Arbeitsplatzes definiert werden

6. Büro/Administration



Vandal resistant indoor 1080p/2MP dome camera with WDR Forensic Capture,
Auflösung: 1920x1080
Sensorformat: 1/3 ; 9:16
Brennweite (mm): 4,8
Kamera Höhe: 2,5 m
Neigung: 44,9°
Blickwinkel [Grad]: 34,9°; 62,9°
Objekt Entfernung: 2,5 m
Objekt Breite: 1,4 m
Pixel/m am Objekt: 444 px/m

Im BoH-Bereich (Back of House) geht es um das Erkennen von Geschäftsabläufen. Anlieferungen (z. B. von Frachtunternehmen oder der Post) werden hier im System erfasst und registriert.

7. Tresorraum

Vandal resistant outdoor/indoor 1080p/12MP dome camera with WDR Forensic Capture, AXIS Zipstream and Lightfinder

Auflösung: 2992x2992
Sensorformat: 1/1,7 ; 1:1
Brennweite (mm): 1,3
Kamera Höhe: 3 m
Neigung: 0°
Blickwinkel [Grad]: 360°; 180°
Objekt Entfernung: 2,6 m
Objekt Breite: 6,2 m
Pixel/m am Objekt: 377 px/m

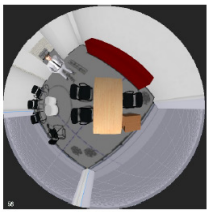
Lückenlose Dokumentation der Abläufe. Ware und Mitarbeiter müssen sehr gut erkennbar sein. Die Auflösung in der Szene muss im Bereich der Warenbewegung die Bildqualität Begutachten haben.

8. Technikräume

Vandal resistant indoor 1080p/2MP dome camera with WDR Forensic Capture,
Auflösung: 1920x1080
Sensorformat: 1/3 ; 9:16
Brennweite (mm): 3,3
Kamera Höhe: 3 m
Neigung: 63,7°
Blickwinkel [Grad]: 46,5°; 85,3°
Objekt Entfernung: 2,6 m
Objekt Breite: 1,8 m
Pixel/m am Objekt: 271 px/m

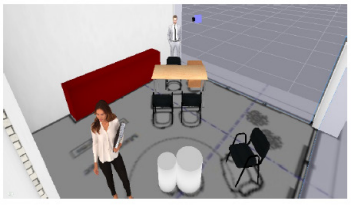
Ziel ist es, dass der Zugang zum Technikraum mittels VSS (Volume Shadow Copy Service) dokumentiert wird, um ein Bewegungsprofil erstellen zu können. Die Aufgabenstellung Erkennen ist gefordert.

9. Beratungsräume



12 MP mini dome with 360 panoramic view
Auflösung: 2880x2880
Sensorformat: 1/1,7 ; 1:1
Brennweite (mm): 1,65
Kamera Höhe: 2,5 m
Neigung: 5,2°
Blickwinkel [Grad]: 360°; 185°
Objekt Entfernung: 2,2 m
Objekt Breite: 20,9 m
Pixel/m am Objekt: 432 px/m

Vandal resistant indoor 1080p/2MP dome camera with WDR Forensic Capture,
Auflösung: 1920x1080
Sensorformat: 1/3 ; 16:9
Brennweite (mm): 3
Kamera Höhe: 3 m
Neigung: 33,1°
Blickwinkel [Grad]: 92°; 50°
Objekt Entfernung: 7 m
Objekt Breite: 13,3 m
Pixel/m am Objekt: 124 px/m

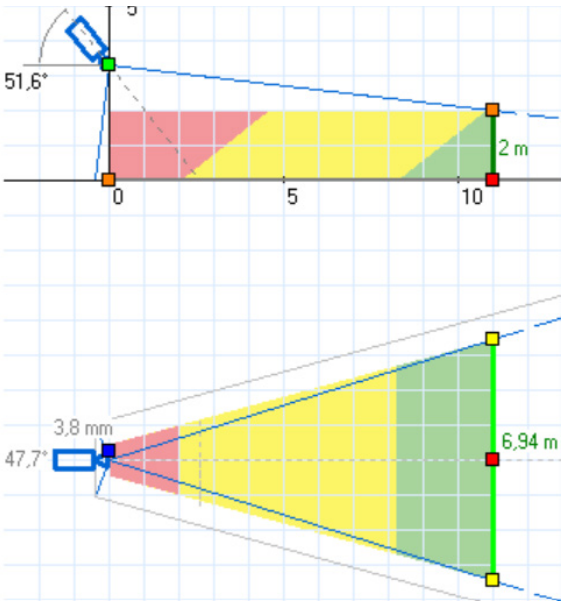


Vandal resistant indoor 1080p/2MP dome camera with WDR Forensic Capture,
Auflösung: 1920x1080
Sensorformat: 1/3 ; 16:9
Brennweite (mm): 3,2
Kamera Höhe: 3 m
Neigung: 32°
Blickwinkel [Grad]: 88°; 47,9°
Objekt Entfernung: 7,1 m
Objekt Breite: 12,7 m
Pixel/m am Objekt: 131 px/m

Alle Kundenbewegungen müssen aus unterschiedlichen Perspektiven nachvollziehbar sein, zur Identifizierung der Kunden kann die Kamera im Eingangsbereich herangezogen werden.

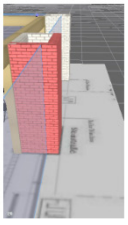
10. Bankschalter/Kasse

Complete, extremely discreet HDTV 1080p pinhole camera
Auflösung: 1920x1080
Sensorformat: 1/2.9 ; 16:9
Brennweite (mm): 3.7
Kamera Höhe: 3 m
Neigung: 78.8°
Blickwinkel [Grad]: 91°; 45°
Objekt Entfernung: 0.8 m
Objekt Breite: 2.8 m
Pixel/m am Objekt: 304 px/m
Totzone: -0.25 m (Breite: 2.38 m)



Die Abläufe müssen klar identifiziert werden, bspw. beim Zählen von Geldscheinen.

11. Schaufenster/Fassade öffentlicher Bereich



Streamlined outdoor-ready HDTV 1080p fixed dome for any light conditions

Auflösung: 1080x1920
Sensorformat: 1/2.8 ; 9:16
Brennweite (mm): 6.15
Kamera Höhe: 4 m
Neigung: 30.3°
Blickwinkel [Grad]: 29.6°; 54.5°
Objekt Entfernung: 10.9 m
Objekt Breite: 5.1 m
Pixel/m am Objekt: 179 px/m
Totzone: 2.54 m (Breite: 1.31 m)

Die Abläufe müssen klar identifiziert werden können. Bei einem Aufenthalt außerhalb der Geschäftszeiten von länger als 5 Minuten muss eine automatische Benachrichtigung an die Notruf- und Serviceleitstellen (NSL) erfolgen.

7. Betriebsanforderungen gemäß EN 62676-4

Die DIN EN 62676 ist als maßgebende Planungsgrundlage herangezogen worden. Aus dieser Normreihe sind die DIN EN 62676-4, die DIN EN 62676-1-1 und die EN 62676-1-2 für diese Planung berücksichtigt worden.

> Die DIN EN 62676-4 beschreibt die Anwendungsregeln, die den allgemein anerkannten Regeln der Technik entsprechen.
> Die DIN EN 62676-1-1 beschreibt die Systemanforderungen im Allgemeinen und
> die DIN EN 62676-1-1 beschreibt die Anforderungen an die Videoübertragung.

Die Normenreihe DIN EN 62676-1 gruppiert die Anforderungen aus der Risikoanalyse in 4 Bereiche, welche im weiteren Verlauf entsprechend der Anforderungen gesondert gekennzeichnet werden.

Ein wichtiger Baustein aus der DIN EN 62676-4 ist die Entwicklung und die Dokumentation der Betriebsanforderung. Dies ist eine formale schriftliche Erklärung der Notwendigkeit, der Begründung und des Zwecks der hier geplanten Videosicherheitsanlage.

Im Vorfeld der Planung sind die folgenden Punkte zu klären und näher zu beschreiben:

1. Grundlegende Ziele/Funktionalitäten
2. Festlegung von Überwachungsbeschränkungen
3. Festlegung des zu überwachenden Standortes
4. Festlegung der zu erfassenden Aktivitäten
5. System-/Bildqualität
6. Betriebsdauer
7. Bedingungen am Standort
8. Belastbarkeit
9. Überwachung und Bildspeicherung
10. Exportieren von Bildern
11. Routinemäßige Maßnahmen
12. Betriebliche Antwort
13. Arbeitsbelastung der Bedienpersonen
14. Schulung
15. Erweiterungen
16. Liste aller anderen besonderen und vorgenannt nicht abgedeckten Faktoren

7.1 Grundlegende Ziele/Funktionalitäten

1. Zweckbestimmung des Systems
   a. Objektüberwachung
   b. Detektion/Überwachung von Angriffen
   c. Aufzeichnung von Angriffen
   d. Angriffe gegen Individuen
   e. Angriffe gegen Eigentum
   f. Diebstahl
   g. Raubüberfälle
   h. Beschädigung
   i. Trickbetrug
   j. Kreditkartenbetrug
   k. Andere Bedrohungen wie zum Beispiel der Transport von Wertgegenständen von oder zu der Bank

In erster Linie dient das Videoüberwachungssystem dem Schutz der Mitarbeiter und der Produkte. Weiterhin geht es um die Dokumentation von Straftaten und deren Aufklärung.

2. Sicherungsgrad System gemäss DIN EN 62676
   a. 3 oder 4

7.2 Festlegung von Überwachungsbeschränkungen

Folgende Bereiche werden durch Festlegen des Blickwinkels oder durch Einsatz von elektronischer Maskierung in dem Kamerabild von der Einsicht in die Szene ausgenommen werden:

1. Tastenfeld des Geldautomaten
2. Tastenfeld Tresore
3. Arbeitsplatz Bankberater
4. Kundenberatungsplätze
5. Vorfeld Haupteingang max. 50 cm im öffentlichen Bereich.

6. Des Weiteren findet im Rahmen der DSGVO folgende Überwachungsbeschränkung statt:
   a. Sozialräume, diese im Einzelnen:
      i. Pausenraum,
      ii. Umkleideräume
      iii. Toiletten

7.3 Festlegung der (des) zu überwachenden Standorte(s)

Das nachfolgende Beispiel wird individuell anhand der Risikoanalyse auf jeden Standort angepasst. Dieser Vorgang ist auch ein dynamischer Prozess und kann noch während der Nutzungsphase geändert werden.
Die Bank ist ein Objekt mit 2 Etagen und seitlichem Zugang für Mitarbeiter und Lieferanten sowie einem Haupteingang im Erdgeschoss. Neben Beratungsfläche sowie Sozialräumen ist das teils öffentliche Treppenhaus Schwerpunkt der Videoüberwachung.

1. Gebäude
2. Innenbereiche
3. Außenhaut
4. Treppenhaus

7.4 Festlegung der zu erfassenden Aktivitäten

Die folgenden festgelegten Aktivitäten müssen abgedeckt werden

1. die vorgesehenen Ziele der Anlage in jedem Teil des Standortes
2. die erwartete Geschwindigkeit des vorgesehenen Ziels
3. die vorgesehene Beobachtungskategorie der Ziele aus Sicht der Bedienperson
4. ist externe Detektion erforderlich?

Personenbewegungen gilt es während der Geschäftszeiten zu dokumentieren. Weiterhin soll sich das Bank- sowie bei Bedarf das Sicherheitspersonal einen Überblick über die Situation an den Zugängen sowie vor der Bank verschaffen können.

Lfd. Nr.	Bereiche	FPS	24/7	LTS	SL	ST	Auflösung	IP/IK
1	Außen Personalkamera	15	X	X	V/A	X	I	>IP 65 >IK9
2	Personaleingang	12	X	X		X	I	>IP 65 >IK9
3	Nachtschalter	12	X	X		X	I	>IP 65 >IK9
4	Kunden Ein-/Ausgang	12	X	X		X	B	>IP 65 >IK9
5	Technikräume	12	X	X		X	E	
6	Beratungsbereiche	25	X	X		X	E	
7	Tresor (Nicht öffentlich)	25	X	X		X	Beg.	
8	Eingang Tresor	12	X	X		X	E	

Diese Tabelle ist als Beispiel zu sehen und individuell anzupassen.

> FPS Aufzeichnung in Bilder pro Sekunde
> 24/7 Betrieb (Kamera inkl. IR LED)
> LTS long-term support firmware track
> SL Sabotageüberwachung
  - Verdrehen
  - Abdecken
  - Out of Focus

> ST Störmeldung
  - Oberhalb oder unterhalb der Betriebstemperatur
  - Innerhalb der Betriebstemperatur

> V/A Verdrehen und Abdecke

Sabotageerkennung				
Das System muss folgendes erkennen können:	**Sicherheitsgrad**			
	1	**2**	**3**	**4**
Verbindungsverlust		X	X	X
Falls ein Bilderfassungsgerät mit festem Bildausschnitt nicht mehr den gesamten festgelegten Bildausschnitt enthält, muss die Kamera dies dem VMS melden und zur Anzeige gebracht werden.			X	X
Das absichtliche Verdecken oder Blenden des Bildaufnahmegerätes muss die Kamera dem VMS melden und zur Anzeige gebracht werden.			X	X
Das Ersetzen von Videodaten an der Bildquelle, bei Verbindungen oder bei der Bildhandhabung.				X
Eine signifikante Reduzierung des Bildkontrastes muss die Kamera dem VMS melden und zur Anzeige gebracht werden.				X

7.5 System-/Bildqualität

In den Eingangsbereichen sind die Personen nach DIN EN 62676-4 zu identifizieren, an den Bankschaltern und -automaten sind die Abläufe klar zu Identifizieren.

Die folgenden festgelegten Aktivitäten müssen abgedeckt werden

1. die wesentlichen Leistungsmerkmale des Systems und seiner angezeigten Bilder
2. der für den Zweck erforderliche Detaillierungsgrad des Bildes, welcher in jedem Live-Bild, aufgezeichneten und exportierten Bild beobachtet wird
3. eine Festlegung jeglicher Bildanalysefunktionalitäten zusammen mit der erwarteten Genauigkeit, und ob diese durch die Bedienperson oder automatisch durch das System erreicht wird.

Systemprotokolle				
Das System muss folgende Aktivitäten mit Zeitstempel (Datum und Zeit), Ereignis und Quelle protokollieren:	**Sicherheitsgrad**			
	1	**2**	**3**	**4**
Alarme		X	X	X
Sabotage			X	X
Videosignalstörung und Störungsbeseitigung (In Verbindung mit USV & Möglichkeit der USV Meldungen über TCP/UDP)			X	X
Stromausfall		X	X	X
Ausfall wesentlicher Funktionen und Wiederherstellung der Funktionalität			X	X
Störungsmeldungen, die dem Benutzer angezeigt werden			X	X
Systemrücksetzung (Reset), Systemstart, Systemstopp		X	X	X
* Diagnoseaktionen (Zustandsüberprüfung)			X	X
Export, Ausdruck einschließlich Bildquellenkennung und Zeitraum		X	X	X
Benutzeran- und -abmeldung bei der Arbeitsstation mit Zeitstempel, erfolgreiche und abgelehnte Anmeldungen (lokal/abgesetzt) einschließlich Grund für Ablehnung (falsches Passwort, unbekannter Benutzer, abgelaufenes Zugriffskonto)		X	X	X
Änderungen der Berechtigungscodes/ Benutzerpasswort			X	X
Steuerung von funktionellen Kameras				X
Bildsuche und -wiedergabe			X	X
Manuelle Änderungen der Aufzeichnungsparameter			X	X
Alarmbestätigung und -rücksetzung			X	X
Änderungen der Systemkonfiguration			X	X
Setzen und Ändern von Datum und Zeit einschließlich der aktuellen und der neuen Zeit			X	X

** System Monitor zum Anzeigen relevanter Daten der angeschlossenen System Komponenten – Bei VMS nur mit Expert und Corporate möglich*

7.6 Betriebsdauer

24 Stunden am Tag, 7 Tage in der Woche und 365 Tage im Jahr
Festlegung der System-Betriebsdauer

1. Werktags
2. Sonntags
3. Gesetzliche Feiertage
4. Werksferien
5. Kosten auf 5 Jahre für die Inspektion und den Betrieb der Videosicherheitsanlage sind anzugeben. Dies beinhaltet ebenfalls eine Herstellergewährleistung über 5 Jahre sowie eines ausgearbeiteten Konzeptes für die Inspektion. Hier ist ein besonderes Augenmerk auf die Geräteverwaltungssoftware und deren Funktionen zu richten.

7.7 Bedingungen am Standort

Festlegung von Umgebungsbedingungen, welche gelten und/oder während der Überwachungszeit variieren und welche für den Systementwurf maßgeblich sind

1. Minimale Beleuchtungsstärke (Lux) Innen
   Ist individuell zu bestimmen.
2. Minimale Beleuchtungsstärke (Lux) Außen
   Ist individuell zu bestimmen.
3. Potenzielle Hindernisse Kamerasicht
   Ist individuell zu bestimmen.
4. Temperaturbereich Innen
   Zwischen 19 und 22 Grad Celsius
5. Temperaturbereich Außen
   Zwischen -40 und + 50 Grad Celsius
6. Weitere Umgebungsbedingungen mit Einfluss?

7.8 Belastbarkeit

1. Notstromversorgung:
   Eine Notstromversorgung von allen Komponenten der Videoüberwachung mit 30 Minuten ist vorzusehen.

7.9 Überwachung und Bildspeicherung

Es ist sicherzustellen, dass die Bilder, Videosequenzen zu jeder Zeit ohne Verluste aufgezeichnet werden. Jegliche Störungen, welche die Aufzeichnung verhindern würden, sind mit einem „Back-Up System" abzusichern.

Die folgenden Speicherungsparameter müssen abgedeckt werden

1. Festlegung, wo und durch wen das System überwacht und betrieben werden soll
2. Festlegung, was aufzuzeichnen ist
3. Festlegung der Aufbewahrungszeit für Aufzeichnungen und Gegebenheiten, unter welchen sich dies ändert
4. Festlegung zusätzlicher (entfernter) Standorte, an denen die Bilder verfügbar sein sollen
5. Festlegung von Verfahren, die bei einer Entnahme, Speicherung und Verarbeitung von Bildern und Daten des Systems zu befolgen sind

Speicherung				
Die VSS muss über folgende Funktionen verfügen	**Sicherheitsgrad**			
	1	**2**	**3**	**4**
Datensicherung über RAID oder Speicher Cluster			X	X
Betrieb eines ausfallsicheren Speichers (z. B. RAID 5 oder fortlaufende Datenspiegelung) oder automatische Umschaltung von einem Speichermedium auf ein anderes im Fall eines Speicherausfalls.				X
Reaktion auf ein Ansteuersignal mit einer maximalen Latenzzeit von		1 s	500 ms	250 ms
Wiedergabe eines gespeicherten Bildes aus dem Speicher mit einer maximalen Zeit nach dem Vorfall oder der aktuellen Aufzeichnung von			2 s	1 s

Archivierung und Sicherung				
Die Archivierung muss folgende Funktionen bereitstellen	**Sicherheitsgrad**			
	1	**2**	**3**	**4**
Die Authentifizierung von jedem Einzelbild und der Bildfolge				X
Eine automatische, zeitgesteuerte Sicherung der Alarmbilddaten (Sonderentwicklung, PlugIn)				X
Eine Sicherung der Alarmbilddaten durch einen manuellen Request (Evidence Lock)			X	X
Manuelle Überprüfung der erfolgreichen Bildsicherung			X	X

7.10 Exportieren von Bildern

Die Videodaten müssen zu jeder Zeit durch den verantwortlichen Filialleiter oder einer vorgesagten Person eingesehen werden können. Die Sicherung der Daten auf ein externes Speichermedium obliegt dem Sicherheitsbeauftragten oder seinem Stellvertreter. Die Daten müssen gerichtsverwertbar und revisionssicher speicherbar sein.

Die folgenden Speicherungsparameter müssen abgedeckt werden

1. Festlegung, wie Bilder für kurze Sequenzen exportiert werden
2. Festlegung, wie Bilder für lange Sequenzen exportiert werden
3. Festlegung der benötigten Kompatibilität des exportierten Mediums

7.11 Routinemäßige Maßnahmen

Das Videosicherheitssystem wird jeden Morgen durch den Filialleiter oder seinen Stellvertreter auf die Live- und Aufzeichnungsfunktion per Sichtprüfung kontrolliert. Außerdem „prüft es sich" fortlaufend selbst und meldet jegliche Störung an die Leitstelle.

Festlegung von Maßnahmen, welche im Rahmen der bestimmungsgemäßen Routine erforderlich sind

1. Routinemäßige Maßnahmen notwendig.

Überwachung der Verbindungen				
Das System muss:	**Sicherheitsgrad**			
	1	**2**	**3**	**4**
die Verbindungen wiederholt in regelmäßigen Zeitabständen überprüfen, mit einem maximalen zeitlichen Abstand von			30 s	< 10 s
mit der folgenden Anzahl von Wiederholungen versuchen, eine Verbindung wiederherzustellen, bevor eine Benachrichtigung erfolgt			5	2
die maximal zulässige Zeit von der Benachrichtigung eines Bedieners über eine Verbindungsunterbrechung einhalten			180 s	30 s

7.12 Betriebliche Antwort:

Die folgenden Antwortmaßnahmen müssen abgedeckt werden:

> Festlegung der für die Antwort verantwortlichen Person
Wird seitens der Sicherheitsabteilung der Bank festgelegt

> Festlegung der Art der Antwort, welche für ein potenzielles Ereignis erforderlich ist.
Wird seitens der Sicherheitsabteilung der Bank festgelegt

> Festlegung von Zielzeiten für jede Antwort
Wird seitens der Sicherheitsabteilung der Bank festgelegt

7.13 Arbeitsbelastung der Bedienpersonen

Es ist davon auszugehen, dass außer der Kontrolle vor Öffnung der Bank und einer Recherche pro Quartal keine weiteren Bedienungen stattfinden.

7.14 Schulungen

Der Filialleiter und sein Stellvertreter sind so zu schulen, dass das Videoüberwachungssystem jederzeit sicher bedient werden kann. Entsprechende Schulungsunterlagen sowie ein *Quick Guide* sind zur Verfügung zu stellen.

Festlegung erforderlicher Schulungen für jede in der Verwaltung und im Betrieb der Anlage beteiligten Rolle

7.15 Erweiterung

Die folgenden Systemerweiterungen müssen abgedeckt werden:

> Es muss eine geplante Erweiterung des Systems von 10 % bei der Planung berücksichtigt werden.

7.16 Liste aller anderen besonderen und vorgenannt nicht abgedeckten Faktoren

Wenn die Betriebsanforderungen mit derzeitiger Technologie oder Ressourcen nicht erfüllt werden können, wird dies im Angebot des Integrators/Facherrichters gesondert vermerkt.

Zugangsebenen

Funktion	Zugangsebenen			
	1	2	3	4
Systemkonfiguration	NE	NE	E	E
einzelne Berechtigungscodes ändern	NE	E	E	E
Zuweisen und Löschen von Benutzern der Zugangsebene 2 sowie von Berechtigungscodes	NE	NE	E	E
Zurücksetzen auf Werkseinstellungen	NE	NE	E	E
Aufrüsten des Systems	NE	NE	E	E
Start/Stopp der VSS oder einzelner Komponenten	NE	NE	E	E

Legende
E Erlaubt
NE Nicht erlaubt

Ergänzung zu den Zugangsebenen:
Die Benutzerrollendefinitionen ermöglicht es, strikte und granulare Benutzerrechte auf bestimmte Rollen (einzelne oder Gruppen von Benutzern) anzuwenden, und zwar in Bezug auf:

> Client-Schnittstellen, die der Benutzer verwenden kann sowie
> Kameras und andere
> Sicherheitseinrichtungen und
> Gerätefunktionen, auf die der Benutzer zugreifen kann.
> Systemfunktionen, zu deren Verwendung der Benutzer berechtigt ist
> Systemkonfigurationsdaten, die der Benutzer abfragen/bearbeiten kann.

Die Benutzerrechte können sowohl statisch als auch zeitabhängig definiert werden. So ist es z. B. möglich, einem Benutzer den Zugriff auf das System außerhalb der normalen Arbeitszeiten zu sperren oder die Zugriffsrechte auf Kameras und Funktionen während bestimmter Zeiträume einzuschränken. Mit den zeitabhängigen Benutzerrechten ist es auch möglich, den Zugriff auf Aufzeichnungen zu sperren, die älter als eine bestimmte Zeit sind.

Anforderungen an den Berechtigungscode

Anforderungen an den Berechtigungscode	Sicherheitsgrad			
	1	2	3	4
Anzahl möglicher logischer Berechtigungsschlüssel		> 10.000	> 100.000	> 1.000.000
Anzahl möglicher physischer Berechtigungsschlüssel		> 3.000	> 15.000	> 50.000

Datenzugriff

Funktion	Zugangsebenen			
	1	2	3	4
Anzeige von Live-Bildern und Daten	E	E	E	E
Anzeige von gespeicherten Bildern und Daten, wenn Aufzeichnungen verfügbar sind	NE	E	E	E
Anzeige von Speicherinformationen, wenn ein Speicher Bestandteil der VSS ist	NE	E	E	E
Drucken und Speichern von Videodaten	NE	E	E	E
Exportieren von Bildern und Daten	NE	E	E	E
Löschen von Bildern und Daten (nur mit Bestätigung)	NE	NE	NE	NE

Legende
E Erlaubt
NE Nicht erlaubt

Zugriff auf Systemprotokolle

Funktion	Zugangsebenen			
	1	2	3	4
Anzeige von Systemprotokollen	NE	E	E	E
Exportieren von Protokollen	NE	NE	E	E
Löschen von Protokollen	NE	NE	NE	NE

Legende
E Erlaubt
NE Nicht erlaubt

Zugriff auf die Systemkonfiguration

Schutz des Zugriffs auf die Systemkonfiguration	Zugangsebenen			
	1	2	3	4
Konfiguration und Einrichtung	NE	NE	E	E
Wiederherstellung nach einem Systemausfall	NE	E	E	E
Wiederinbetriebnahme nach Sabotage	NE	E	E	E

Legende
E Erlaubt
NE Nicht erlaubt

Datenkennzeichnung

Die VSS muss Daten durch Folgendes eindeutig kennzeichnen	Sicherungsgrad			
	1	2	3	4
Speicherort (z. B. Name des Standortes)		X	X	X
Quelle (z. B. Bildaufnahmegerät mit Kameranummer als Kennzeichnung)		X	X	X
Datum und Uhrzeit	X	X	X	X
Datum und Uhrzeit in koordinierter Weltzeit (UTC) einschließlich Verschiebung für die lokale Zeit				X

Genauigkeit des Zeitdienstes für den Videotransportstrom

Klasse	T1	T2	T3	T4
Genauigkeit des Zeitdienstes für den Transportstrom via NTP	80 ms	40 ms	5 ms	1 ms

Verbindungen - Zeitliche Anforderungen

Videoübertragungsgeräte dürfen höchstens	Klasse			
	I1	I2	I3	I4
eine initiale Verbindungszeit für jede neue Anforderung eines Videodatenstroms haben von	2 000 ms	1 000 ms	500 ms	250 ms

Anforderungen an das Videoübertragungsnetzwerk

Videoübertragungsgeräte in einem gemeinsam genutzten Netzwerk müssen Mittel bereitstellen für die Konfiguration	Klasse			
	C1	C2	C3	C4
der maximalen Datenrate von Videodatenströmen für jeden Videokanal			X	X
der maximalen Datenrate für alle verfügbaren Videodatenströme eines einzelnen Gerätes			X	X
der maximalen Datenrate oder Anzahl der Videodatenströme für alle Client-Geräte im Netzwerk			X	X

Anforderungen an das Videoübertragungsnetzwerk

Videoübertragungsgeräte in einem gemeinsam genutzten Netzwerk müssen Mittel bereitstellen für	Klasse			
	P1	P2	P3	P4
die Priorisierung bestimmter Datenströme gegenüber anderen, z. B. Datenströme für die Aufzeichnung oder Alarmmeldungen gegenüber Live-Bilddatenströmen			X	X *
die Priorisierung bestimmter Benutzer gegenüber anderen, z.B. für die PTZ-Steuerung			X	X

** Keine Priorisierung der Datenströme, da nur ein Video-Stream abgerufen wird*

Leistungsanforderungen an das Video-Streaming und die Wiedergabe des Videodatenstroms				
Klasse	**S1**	**S2**	**S3**	**S4**
Maximaler Verlust	240 ppm	120 ppm	60 ppm	30 ppm
Maximale Einweg-Latenzzeit des Live- Videodatenstroms (einschließlich Kodierung, Vernetzung, Dekodierung, Wiedergabe)	600 ms	400 ms	200 ms	100 ms
Maximale Reaktionszeit bei Abspielbetrieb (Pause, Einzelschritt, usw.)	400 ms	200 ms	200 ms	100 ms
Umlauf-Latenzzeit einschließlich Visualisierung und Steuerung, z. B. PTZ	700 ms	500 ms	300 ms	200 ms
*Umlauf-Latenzzeit einschließlich Visualisierung und Steuerung, z. B. PTZ, bei der Überwachung und Verfolgung beweglicher Objekte.	650 ms	450 ms	250 ms	150 ms

** kommt nicht zum Tragen, da ausschließlich fix Kameras verbaut werden*

Paket-Jitter des Videodatenstroms im Netzwerk					
Klasse	**M0 ms**	**M1 ms**	**M2 ms**	**M3 ms**	**M4 ms**
Maximaler Spitze-Spitze-Paket-Jitter	-	160	80	40	<20

Überwachung von Verbindungen				
Das System muss sicherstellen für	**Sicherheitsgrad**			
	1	**2**	**3**	**4**
eine maximal zulässige Dauer der Nichtverfügbarkeit des Gerätes			180 s	30 s
eine maximale Zeit für die Erkennung des Verlusts des Live-Signals		8 s	4 s	2 s
Die oben stehende Anforderung dient der Feststellung, ob eine Kommunikation möglich ist, indem die Videoübertragung überwacht wird, um sicherzustellen, dass sie für die Übertragung eines Signals oder einer Nachricht verfügbar ist. Die Überwachung kann in Form einer Suche nach Störungen erfolgen, wenn das Videoübertragungsgerät über gemeinsam genutzte Verbindungen mit anderen Geräten oder Anwendungen kommuniziert.				

8. Einstellungen in den Kameras

Je nach Anwendungszweck und Einsatzbereich sind in den Kameras unterschiedliche Einstellungen erforderlich bzw. möglich. Die hier aufgeführten Einstellungen sind Empfehlungen und jeweils vor Ort in den einzelnen Filialen auf ihren Nutzen hin zu prüfen.

8.1 Verschlusszeiten (Shutter)

Die Shutterzeiten der Kameras sollen sich vollautomatisch den jeweiligen Helligkeitsbedingungen im Store anpassen. Feste Shutterzeiten sind nicht zulässig.

In den Bereichen, in denen schnelle Bewegungen in kurzer Distanz zur Kamera zu erwarten sind, ist es empfehlenswert, die Shutterzeit zu begrenzen.

Welche genauen Werte erforderlich sind, richtet sich nach

- der Helligkeit in der Filiale
- der Pixeldichte pro Meter und
- dem Überwachungszweck.

Je mehr Details gefordert sind und höher die Auflösung in Pixeln/Meter ist, desto kürzer muss die gewählte Shutterzeit in den Kameraeinstellungen angepasst werden.

8.2 WDR (Wide Dynamic Range)

Die Performance der WDR Eigenschaften der Kameras hängt von einer Vielzahl von Faktoren ab und unterscheidet sich teils deutlich zwischen den unterschiedlichen Kameratypen.

Ob die WDR Funktion einen Mehrwert für den Anwendungszweck bietet, ist entsprechend zu prüfen.

Um Bewegungsartefakte zu verhindern/minimieren, muss ggf. auch hier die Verschlusszeit angepasst werden.

9. Vorgeschriebene Switche:

Um einen reibungslosen Service des Netzwerkes gewährleisten zu können, müssen folgende Funktionen sichergestellt werden:

- Kennwortschutz
- IP-Adressfilter
- HTTPS-Verschlüsselung
- IEEE 802.1X-Netzwerkzugriffskontrolle
- ACL
- Private VLANs
- DHCP-Snooping

sowie folgende Protokolle unterstützt werden:
IPv4, IPv6, HTTP, HTTPS, QoS, Bonjour, UPnP, SNMP v1/v2c/v3, DNS, NTP, TCP, UDP, IGMP, ICMP, DHCP, ARP, SSH, STP, RSTP, MSTP, LLDP, LLDP-MED, TFTP, SMTP, BPDU.

Bei der Belegung der Switche ist die Leistungsberechnung gemäß der angeschlossenen und zu versorgenden Komponenten entsprechend zu berücksichtigen. Ziel sollte eine symmetrische Auslastung und eine Risikoverteilung der angeschlossenen Geräte sein.

10. Vorgeschriebene Router

Um einen reibungslosen Service des Netzwerkes gewährleisten zu können, werden ausschließlich Cisco Integrated Services Router in das Netzwerk integriert.
Zurzeit sind nachfolgende Komponenten geprüft und zugelassen:

- ISR4351/K9*
- ISR4451-X/K9*

**oder Nachfolgemodell*

11. VPN Anbindung/Zugriff der Hauptverwaltung nach dem IT-Grundschutz des BSI (Bundesamt für Sicherheit in der Informationstechnik)

Basis-Anforderungen
Die folgenden Anforderungen MÜSSEN für den Baustein VPN (Virtual Private Network) vorrangig umgesetzt werden:

11.1 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein VPN. Sie MÜSSEN grundsätzlich umgesetzt werden

11.1.1 Planung des VPN-Einsatzes

Die Einführung eines VPN MUSS sorgfältig geplant werden. Dabei MÜSSEN die Verantwortlichkeiten für den VPN-Betrieb festgelegt werden. Es MÜSSEN für das VPN zudem Benutzergruppen und deren Berechtigungen geplant werden. Ebenso MUSS definiert werden, wie erteilte, geänderte oder entzogene Zugriffsberechtigungen zu dokumentieren sind.

11.1.2 Auswahl eines VPN-Dienstleisters [Informationssicherheitsbeauftragter (ISB)]

Mit einem VPN-Dienstleister MÜSSEN Service Level Agreements (SLAs) ausgehandelt und schriftlich dokumentiert werden. Es MUSS regelmäßig kontrolliert werden, ob der VPN-Dienstleister die vereinbarten SLAs einhält.

11.1.3 Sichere Installation von VPN-Endgeräten

Das zugrundeliegende Betriebssystem der VPN-Plattform MUSS sicher konfiguriert werden. Wird eine Appliance eingesetzt, MUSS es dafür einen gültigen Wartungsvertrag geben. Es MUSS sichergestellt werden, dass nur qualifiziertes Personal VPN-Komponenten installiert. Die Installation der VPN-Komponenten sowie eventuelle Abweichungen von den Planungsvorgaben MÜSSEN dokumentiert werden. Die Funktionalität und die gewählten Sicherheitsmechanismen des VPN MÜSSEN vor Inbetriebnahme geprüft werden.

11.1.4 Sichere Konfiguration eines VPN

Für alle VPN-Komponenten MUSS eine sichere Konfiguration festgelegt werden. Diese SOLLTE geeignet dokumentiert werden. Auch MUSS der zuständige Administrator regelmäßig kontrollieren, ob die Konfiguration noch sicher ist und sie eventuell für alle IT-Systeme anpassen.

11.1.5 Sperrung nicht mehr benötigter VPN-Zugänge

Es MUSS regelmäßig geprüft werden, ob ausschließlich berechtigte IT-Systeme und Benutzer auf das VPN zugreifen können. Nicht mehr benötigte VPN-Zugänge MÜSSEN zeitnah deaktiviert werden. Der VPN-Zugriff MUSS auf die benötigten Benutzungszeiten beschränkt werden.

11.1.6 Durchführung einer VPN-Anforderungsanalyse

Es SOLLTE eine Anforderungsanalyse durchgeführt werden, um für das jeweilige VPN die Einsatzszenarien zu bestimmen und daraus Anforderungen an die benötigten Hard- und Software-Komponenten ableiten zu können. In der Anforderungsanalyse MÜSSEN folgende Punkte betrachtet werden:

- Geschäftsprozesse beziehungsweise Fachaufgaben
- Zugriffswege
- Identifikations- und Authentisierungsverfahren
- Benutzer und Benutzerberechtigungen
- Zuständigkeiten und Meldewege

11.1.7 Planung der technischen VPN-Realisierung

Neben der allgemeinen Planung (siehe NET.3.3.A1 Planung des VPN-Einsatzes) MÜSSEN die technischen Aspekte eines VPN sorgfältig geplant werden. So MÜSSEN für das VPN die Verschlüsselungsverfahren, VPN-Endpunkte, erlaubten Zugangsprotokolle, Dienste und Ressourcen festgelegt werden. Zudem MÜSSEN die Teilnetze definiert werden, die über das VPN erreichbar sind (siehe NET.1.1 Netzarchitektur und -design).

11.1.8 Erstellung einer Sicherheitsrichtlinie zur VPN-Nutzung

Es SOLLTE eine Sicherheitsrichtlinie zur VPN-Nutzung erstellt werden. Diese SOLLTE allen Mitarbeitern bekannt gegeben werden. Die in der Sicherheitsrichtlinie beschriebenen Sicherheitsmaßnahmen MÜSSEN

im Rahmen von Schulungen erläutert werden. Wird einem Mitarbeiter ein VPN-Zugang eingerichtet, SOLLTE ihm ein Merkblatt mit den wichtigsten VPN-Sicherheitsmechanismen ausgehändigt werden. Alle VPN-Benutzer MÜSSEN verpflichtet werden, die Sicherheitsrichtlinien einzuhalten.

11.1.9 Geeignete Auswahl von VPN-Produkten

Bei der Auswahl von VPN-Produkten MÜSSEN die Anforderungen der Institutionen an die Vernetzung unterschiedlicher Standorte und die Anbindung mobiler Mitarbeiter oder Telearbeiter berücksichtigt werden.

11.1.10 Sicherer Betrieb eines VPN

Für VPNs MUSS ein Betriebskonzept erstellt werden. Darin MÜSSEN die Aspekte Qualitätsmanagement, Überwachung, Wartung, Schulung und Autorisierung beachtet werden.

11.1.11 Sichere Anbindung eines externen Netzes

Wird ein VPN benutzt, um ein externes Netz anzubinden, MÜSSEN dabei als sicher geltende Authentisierungs- und Verschlüsselungsverfahren mit ausreichender Schlüssellänge verwendet werden. Auch das gewählte Verfahren zum Schlüsselaustausch SOLLTE als sicher gelten. Es SOLLTE sichergestellt werden, dass VPN-Verbindungen NUR zwischen den dafür vorgesehenen IT-Systemen und Diensten aufgebaut werden. Die dabei eingesetzten Tunnel-Protokolle MÜSSEN für den Einsatz geeignet sein.

11.1.12 Benutzer- und Zugriffsverwaltung bei Fernzugriff-VPNs

Für Fernzugriff-VPNs SOLLTE eine zentrale und konsistente Benutzer- und Zugriffsverwaltung gewährleistet werden. Die genutzten Authentisierungsverfahren MÜSSEN die Anforderungen des Bausteins ORP.4 Identitäts- und Berechtigungsmanagement erfüllen.

Werden eigenständige Server für die Benutzer- und Zugriffsverwaltung eingesetzt, MÜSSEN sichergestellt sein, dass diese sicher und konsistent zu den Anforderungen des Bausteins ORP.4 Identitäts- und Berechtigungsmanagement eingerichtet und betrieben werden. Weiterhin MÜSSEN die eingesetzten Server vor unbefugten Zugriffen geschützt sein.

11.1.13 Integration von VPN-Komponenten in eine Firewall

Die VPN-Komponenten MÜSSEN in die Firewall integriert werden. Es MUSS dokumentiert werden, wie die VPN-Komponenten in die Firewall integriert sind.

11.1.14 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein VPN exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden MÜSSEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

12. Sonstige Anforderungen

1. Es muss möglich sein, die Kameras in der gewünschten RAL Farbe umlackieren zu können, ohne die Gewährleistung zu verlieren.

Dies muss ein standardisierter Prozess vom Lieferant des Kameraherstellers sein.

2. Der Integrator muss mindestens ein vergleichbares Projekt, vom Umfang und der Aufgabenstellung her, nachweisen können.

Die grün markierten Werte entsprechen den Anforderungen an dieses Projekt.

DE/R1/2202

Über Axis Communications

Axis ermöglicht eine smarte und sichere Welt durch die Entwicklung von Netzwerk-Lösungen. Diese bieten Erkenntnisse, um die Sicherheit und Geschäftsmethoden zu verbessern. Als Technologieführer im Bereich Netzwerk-Video bietet Axis Produkte und Dienstleistungen für die Videosicherheit/-analyse und Zutrittskontrolle sowie Intercoms und Audiosysteme. Das 1984 gegründete schwedische Unternehmen beschäftigt mehr als 3.800 engagierte Mitarbeiter in über 50 Ländern. Gemeinsam mit seinen Partnern auf der ganzen Welt bietet das Unternehmen kundenspezifische Lösungen an.

Weitere Informationen über Axis finden Sie unter www.axis.com

AXIS COMMUNICATIONS