

EWS Dokumente

Kundendokumentation zum Einbruchwarnsystem (EWS): Fact-Sheet, FAQ, Anleitungen

- [Einbruchwarnsystem \(EWS\) Fact-Sheet](#)
- [Fragen und Antworten zum Einbruchwarnsystem \(EWS\)](#)

Einbruchwarnsystem (EWS) Fact-Sheet

KI-gestütztes Einbruchwarnsystem mit physischem Datenschutz

1. Einleitung

Das **Einbruchwarnsystem (EWS)** überwacht Außen- und Innenbereiche von Gebäuden über IP-Kameras mit eingebauter **KI-Personenerkennung**. Bei unberechtigtem Zutritt löst das System eine vollständige Alarmkette aus – wahlweise lautstark mit Sirene und Strahler oder als stiller Alarm an Leitstellen und Alarmdienste wie DIVERA 24/7, Alamos, GroupAlarm oder per E-Mail. Jeder Alarm enthält einen zeitlich begrenzten Link zum Beweisbild zur Fernbeurteilung.

Das EWS ist ein **eigenständiges Produkt** der dexa group und vom Brandwarnsystem Safe Fire House getrennt. Es nutzt jedoch dieselbe bewährte Plattform und Zentralen-Hardware, sodass beide Systeme auf einer Anlage betrieben werden können. Das EWS ist ein lizenzpflichtiges Modul (MAC-gebundene Lizenz).

Datenschutz by Design: Im unscharfen Zustand sind alle Kameras physisch stromlos – nicht nur per Software deaktiviert, sondern physisch vom Strom getrennt. Kein Bild, kein Stream, keine Daten.

2. Das Problem

Klassische Einbruchmeldeanlagen arbeiten mit Bewegungsmeldern und erzeugen häufig Fehlalarme durch Tiere, Fahrzeuge, Schatten oder Witterung. Kamerasysteme wiederum stehen unter Datenschutz-Vorbehalt: Eine dauerhaft laufende Kamera in einem Feuerwehrhaus, einem Bauhof oder einer Liegenschaft ist gegenüber Personal und Besuchern kaum vermittelbar – und ein attraktives Ziel für Manipulation.

Behörden und Organisationen mit Sicherheitsaufgaben benötigen eine Lösung, die **zuverlässig zwischen Mensch und Störquelle unterscheidet, Bildbeweise** für die schnelle Lagebeurteilung liefert und gleichzeitig **datenschutzkonform** ist, weil sie nur dann sieht, wenn sie sehen soll.

3. Die Lösung – und die zentrale Innovation

Im Unterschied zu klassischen Einbruchmeldeanlagen sind die Sensoren des EWS keine Bewegungsmelder, sondern **KI-Kameras**, die menschliche Personen, Linienüberschreitungen und Bereichsverletzungen selbst klassifizieren. Das reduziert Fehlalarme deutlich und ermöglicht eine **Bildbeweis-Quittierung** im Alarmfall.

Das Problem, das bisher jede Kameralösung ausbremst

Kameras in Feuerwehrhäusern, Bauhöfen, Liegenschaften oder Betrieben scheitern selten an der Technik – sie scheitern am **Datenschutz und an der Akzeptanz**. Eine dauerhaft laufende Kamera überwacht potenziell auch das eigene Personal. Personalrat, Betriebsrat und Mitarbeitende lehnen das zu Recht ab, und der Betreiber trägt das volle datenschutzrechtliche Risiko.

Die Lösung ist physisch, nicht nur Software

Genau hier liegt die Innovation des EWS: **Solange die Anlage unscharf ist, sind die Kameras physisch vom Strom getrennt** – die PoE-Ports am Switch sind abgeschaltet. Keine laufende Kamera, kein Bild, kein Stream, keine Aufzeichnung. Es gibt schlicht nichts, was jemand abgreifen, einsehen oder missbrauchen könnte. Erst beim **Scharfschalten** wird PoE aktiviert, die Kameras booten und überwachen; beim

Unscharfschalten werden sie sofort wieder stromlos.

Das entschärft die Datenschutz-Frage **an der Wurzel** und macht die Anlage gegenüber Personal und Gremien überhaupt erst vermittelbar – mit zwei Effekten:

- **Datenschutz & Akzeptanz:** Im Normalbetrieb (Personal anwesend, Anlage unscharf) ist Überwachung technisch unmöglich. Das schafft Vertrauen statt Widerstand.
- **Sabotageschutz:** An stromlosen Kameras lässt sich nichts manipulieren; beim Scharfschalten werden die Erkennungsfunktionen ohnehin frisch konfiguriert.

Software-Lösungen, die Kameras „nur deaktivieren“, können das nicht leisten – eine deaktivierte Kamera bleibt am Netz und ist eine Vertrauens- und Angriffsfläche. Eine **stromlose Kamera nicht**.

4. Kernfeatures

Feature	Beschreibung
KI-Personenerkennung	Klassifizierung direkt in der Kamera (Smart Events: FieldDetection, LineCrossing, RegionEntrance/-Exit). Tiere, Fahrzeuge und Schatten werden zuverlässig von Personen unterschieden – nur menschliche Ziele lösen einen Voralarm aus.
Kameras stromlos im Ruhezustand	Im unscharfen Zustand sind alle Kameras physisch vom Strom getrennt (PoE-Port aus). Echter Datenschutz statt Software-Versprechen.
Adaptive Bildsteuerung	Tag-, Dämmerung- und Nachtprofile werden automatisch nach Sonnenstand umgeschaltet (WDR, HLC, Belichtung, IR-Strahler je Profil). Optimale Erkennung rund um die Uhr.
Multi-Kamera-Korrelation	Erkennen mehrere Kameras innerhalb von 30 s dieselbe Person, fasst der Korrelator dies zu einem Aggregatalarm zusammen.
Stiller Alarm + Strahler	Pro Kamera einstellbar. Ohne stillen Alarm: WhiteLight-Strahler und Sirene. Mit stillem Alarm: nur Schnittstellen-Dispatch ohne Aufschrecken.
Snapshot mit Public-Link	Pro Alarm ein Kurzlink zum Beweisbild zur Fernbeurteilung – ohne Login. Nach 15 Minuten automatisch ungültig, danach automatische Löschung nach Datenschutzkriterien.
Automatische Bildlöschung	Erfasste Bilder werden nach konfigurierbarer Frist automatisch gelöscht. DSGVO-konform ohne manuellen Eingriff.
NFC + PIN am Kiosk	Schnelle Authentifizierung per NFC-Token oder PIN am Touchscreen. Optional zusätzliche Anlagen-PIN für mehrstufige Absicherung. 3 Fehlversuche ? 5 Minuten Sperre.
Schließanlagen-Integration	Beim Unscharfschalten öffnet die Tür, beim Scharfschalten wird verriegelt – ein Vorgang, kein Medienbruch.
Aufnahmen-Aufbewahrung	Konfigurierbar bis 180 Tage (Default 30). Kalender-Ansicht, Filter nach Kamera und Typ.
MAC-gebundene Lizenz	Kryptographisch an die Hardware gebunden (HMAC-SHA256). Ein Klon der SD-Karte auf andere Hardware startet nicht.
Port-Mismatch-Erkennung	Bei unterstützten Switches wird die MAC-Tabelle (FDB) gegen die erwartete Belegung geprüft. Fremde Geräte oder Umverkabelung werden erkannt und im Dashboard gemeldet.

5. Bedienung und Zustände

Die webbasierte Oberfläche signalisiert den Anlagenzustand eindeutig – kein Rätselraten:

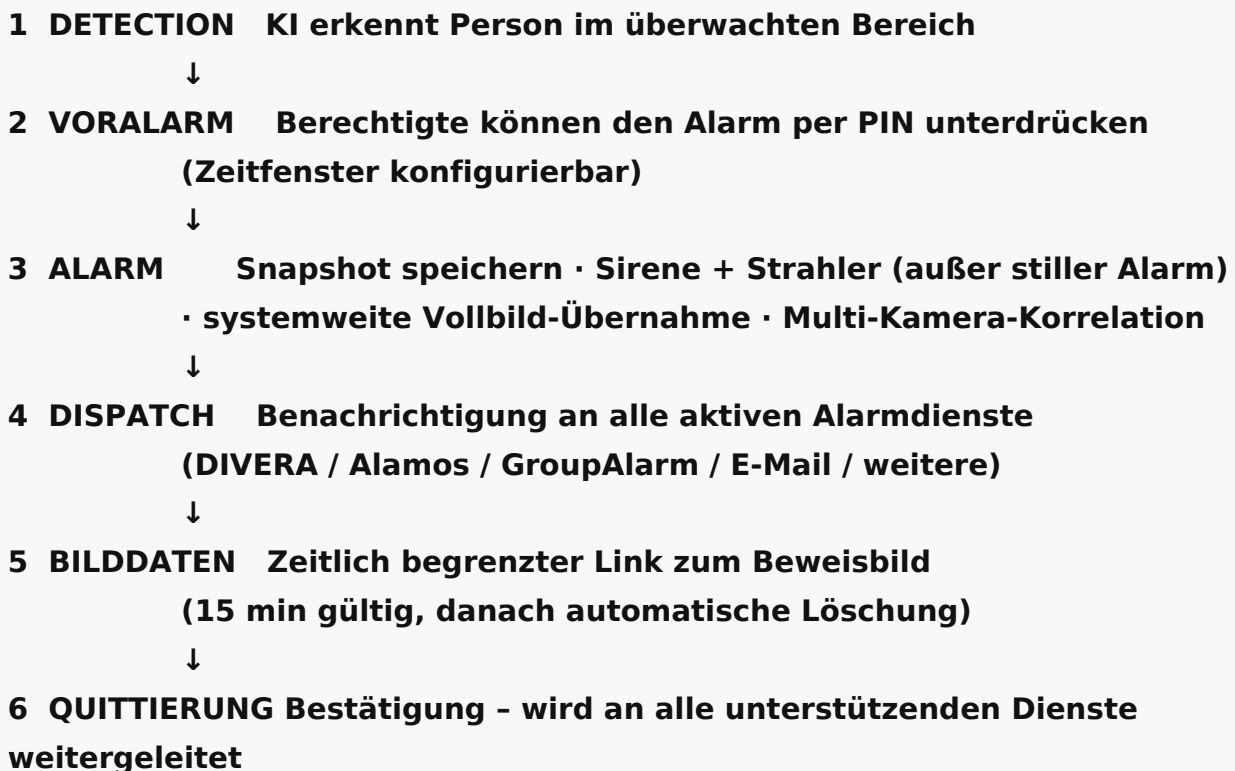
- **Unscharf** (grün): Kameras stromlos, kein Monitoring.
- **Scharfschaltung** (blau): Countdown läuft, Kameras booten, Zeit, das Gebäude zu verlassen.
- **Scharf / Alarm** (rot): Kameras aktiv, Vollüberwachung; bei Erkennung sofortige Alarmkette.

Scharfschalten per dexa PoE-Display mit NFC (Eigenprodukt)

Das Scharf- und Unscharfschalten erfolgt komfortabel direkt am **dexa PoE-Display** – einem **Eigenprodukt der dexa group**, das auch im Brandwarnsystem eingesetzt wird. Ein kurzes Vorhalten eines **NFC-Tokens** genügt (optional zusätzlich mit PIN). Kein Fremdsystem, kein Medienbruch: **eine Hardware für Bedienung, Zustandsanzeige und – in Kombination mit dem Schaltkontakt – die Türfreigabe**. Das Display ist PoE-versorgt (nur ein Kabel) und als Aufbau-, Wand- oder Einbauvariante erhältlich. Drei Fehlversuche sperren die Eingabe für 5 Minuten.

Live-Streams werden als WebRTC im 1×1- oder 2×2-Grid angezeigt – nur bei scharfer Anlage oder im Wartungsmodus verfügbar. Bei kombiniertem Brand- und Einbruchbetrieb auf einer Anlage hat ein **Brandalarm stets Vorrang** vor einem Einbruchalarm.

6. So funktioniert die Alarmkette



7. Systemkomponenten

EWS PoE KI-Kamera (DXO-SFH-CM-XX-01)

- Hikvision 8-MP-IP-Kamera (4K) mit integrierter KI-Personenerkennung

- Smart Events: FieldDetection, LineCrossing, RegionEntrance/-Exit
- IR-Nachtsicht, WhiteLight-Strahler als optische Alarmierung
- PoE-Versorgung (IEEE 802.3af/at), max. 16 Kameras pro Lizenz

SFH PoE-Zentrale / Server

- Standard-Serie **DXO-SFH-CU-B-02** (kompakte Wandzentrale) oder Pro-Serie **DXO-SFH-CU-P-01** (19"-Server) – dieselbe Plattform wie das Brandwarnsystem
- Betreibt den EWS-Broker, die Streaming- und Korrelationslogik sowie die Alarm-Schnittstellen

Managed PoE-Switch

- Managed PoE+-Switch als zentrales Bindeglied; Steuerung der Kamera-Ports (Arm/Disarm = PoE on/off) über **SNMPv3 mit AES-256**, Reaktionszeit < 100 ms
- Erkennt über die FDB-Tabelle fremde Geräte oder Umverkabelung am Kameraport

SFH PoE-Display (DXO-DX-DP-F-01)

- Netzwerkdisplay/Bedienpanel zur Anzeige und Steuerung, PoE-versorgt
- PIN-Eingabe und NFC-Anmeldung direkt am Gerät; Varianten Aufbau/Tisch, Wand oder Einbau

SFH Alarmsirene (DXO-SFH-AS-XX-01)

- Signalisiert Einbruchalarme optisch (LED) und akustisch (bis 100 dB)
- Solar-/USB-C-Betrieb, IP44, für den Außenbereich – nahezu überall installierbar

8. Schließanlagen-Integration

Das EWS lässt sich mit bestehender Infrastruktur verbinden – diese wird genutzt, nicht ersetzt. Beim Unscharfschalten öffnet die Tür, beim Scharfschalten wird verriegelt. Neben fertigen Integrationen gibt es mit dem Schaltkontakt eine **universelle Rückfallebene für jedes Gebäude**.

- **Potenzialfreier Schaltkontakt (universell)** – der SFH Schaltkontakt (DXO-SFH-SC-1-01 / DXO-SFH-SC-4-01) schaltet beim Scharf-/Unscharfschalten einen **potenzialfreien Kontakt**. Damit lässt sich **praktisch jede** elektrische Türöffnung, jeder Türöffner, jedes Motorschloss, Tor oder Relais ansteuern – herstellerunabhängig, auch dort, wo keine fertige Integration existiert.
- **dexa PoE-Display** – PIN-Eingabe und NFC-Anmeldung direkt am Display, ohne zusätzliche Hardware (Eigenprodukt)
- **NFC-Tags** – generische Token für schnelles Entsperren ohne Hersteller-Bindung
- **ABUS** – professionelle Schließzylinder und Zutrittskontrolle
- **Salto** – Zutrittslösungen für Gebäude und Liegenschaften
- **dormakaba** – Schließanlagen und digitale Zylinder
- **ASSA ABLOY** – Zutrittssysteme und Aperio-Komponenten
- **Consumer-Systeme** – Nuki, SwitchBot und weitere smarte Türschlösser

9. Schnittstellen

Bei jedem Alarm werden **alle aktiven Schnittstellen gleichzeitig** angesprochen; eine fehlgeschlagene Zustellung blockiert die übrigen nicht (automatischer Backoff mit Wiederholung).

Einsatzbereit:

- **DIVERA 24/7** – Alarm mit Snapshot-Anhang und Rückmeldung/Quittierung
- **Alamos FE2 / aPager Pro** – Alarm mit Snapshot-Link im Alarmtext
- **GroupAlarm** – Alarm mit Snapshot-Anhang und Quittierung
- **E-Mail (SMTP)** – Alarm mit Snapshot als E-Mail-Anhang

Erweiterbar:

- Offene **BaseInterface**-Schicht für eigene Integrationen; über die dexa-Plattform (BOS Data Broker) an **30+ Alarm- und Leitstellensysteme** anbindbar.

10. Sicherheit auf mehreren Ebenen

- **Kameras physisch stromlos:** Im unscharfen Zustand ist PoE abgeschaltet. Kein Live-Bild, keine Manipulation. Steuerung über SNMPv3 mit AES-256, Reaktionszeit < 100 ms.
- **MAC-gebundene Lizenz:** Lizenzdatei kryptographisch an die Hardware gebunden; ein Klon auf andere Hardware startet nicht.
- **Snapshot-Token-Härtung:** Kurzlinks für Alarmbilder mit ~71 Bit Entropie, wenige Minuten gültig, In-Memory. Nach Ablauf forensisch wertlos, anschließend automatische Löschung.
- **Port-Mismatch-Erkennung:** FDB-Abgleich am Switch erkennt fremde Geräte oder Umverkabelung und meldet sie im Dashboard.
- **Zwei Authentifizierungs-Ebenen:** Web-GUI über zentrale Anmeldung; EWS-Bedienung am Kiosk unabhängig davon per NFC + PIN.

11. Datenschutz (DSGVO)

Anders als das Brandwarnsystem verarbeitet das EWS **personenbezogene Daten** (Bildaufnahmen), da es dem Zweck der Einbruchüberwachung dient. Das System ist auf Datenschutzkonformität ausgelegt:

- Kameras nur im scharfen Zustand aktiv (physische Stromtrennung im Ruhezustand)
- Beweisbild-Links nur wenige Minuten gültig, danach automatische Löschung
- Aufnahmen-Aufbewahrung konfigurierbar, automatische Löschung nach Frist
- Zugriff geschützt (NFC/PIN, Rollen, Audit-Log)

Für den Betrieb stellt die Dexa Solutions GmbH einen **Auftragsverarbeitungsvertrag nach Art. 28 DSGVO** bereit (siehe Buch „Dokumente“ ? Datenschutz).

12. Technische Spezifikationen (Zusammenfassung)

Parameter	Wert
Erkennung	KI-Personenerkennung in der Kamera (Smart Events)
Kamera	Hikvision 8 MP (4K), IR-Nachtsicht, WhiteLight-Strahler
Max. Kameras	16 (lizenzabhängig)
Stromversorgung Kameras	PoE (IEEE 802.3af/at), im Ruhezustand abgeschaltet
Switch-Steuerung	SNMPv3, AES-256, < 100 ms Reaktionszeit
Streaming	WebRTC (1×1 / 2×2 Grid), nur bei scharfer Anlage

Parameter	Wert
Alarm-Schnittstellen	DIVERA 24/7, Alamos FE2/aPager Pro, GroupAlarm, E-Mail + offene Schnittstelle (30+ über Plattform)
Beweisbild-Link	~71 Bit Entropie, 15 min gültig, automatische Löschung
Aufbewahrung	bis 180 Tage (konfigurierbar, Default 30)
Lizenz	MAC-gebunden (HMAC-SHA256)
Authentifizierung	NFC-Token + PIN, Rollen, Audit-Log
Schließanlagen	potenzialfreier Schaltkontakt (universell), NFC, ABUS, Salto, dormakaba, ASSA ABLOY, Nuki, SwitchBot u. a.
Plattform	gemeinsame Zentrale mit Safe Fire House (CU-B-02 / CU-P-01)
Datenschutz	DSGVO-konform ausgelegt, AVV nach Art. 28 verfügbar

13. Status und Verfügbarkeit

Das EWS wurde zur **INTERSCHUTZ 2026** in Hannover vorgestellt. Für Pilotprojekte und frühen Zugang sprechen Sie uns an.

Hersteller

Dexa Solutions GmbH Möhnestraße 2 · 59519 Möhnesee · Germany Tel: +49 2924 496 937-0 · Web: dexa.gmbh

Stand: Juni 2026

Fragen und Antworten zum Einbruchwarnsystem (EWS)

Fragen und Antworten zum Einbruchwarnsystem (EWS)

Das Einbruchwarnsystem (EWS) ist ein eigenständiges Produkt der dexa group, getrennt vom Brandwarnsystem Safe Fire House, nutzt aber dieselbe Zentralen-Plattform. Diese Seite beantwortet die häufigsten Fragen.

Grundlagen

Was ist das EWS?

Das Einbruchwarnsystem (EWS) überwacht Außen- und Innenbereiche von Gebäuden mit **KI-Kameras**, die menschliche Personen erkennen. Bei unberechtigtem Zutritt löst es eine Alarmkette über alle gängigen Alarmdienste aus und liefert ein Beweisbild zur Fernbeurteilung.

Wie unterscheidet sich das EWS von einer klassischen Einbruchmeldeanlage?

Statt Bewegungsmeldern nutzt das EWS KI-Kameras, die **Personen von Tieren, Fahrzeugen und Schatten unterscheiden**. Das reduziert Fehlalarme deutlich. Zusätzlich liefert jeder Alarm ein Bild, sodass sich aus der Ferne sofort beurteilen lässt, ob es sich um einen echten Einbruch oder einen Fehlalarm handelt.

Gehört das EWS zu Safe Fire House?

Es ist ein **eigenständiges Produkt**, läuft aber als Modul auf derselben Zentralen-Hardware wie das Brandwarnsystem. Beide Systeme können gemeinsam auf einer Anlage betrieben werden. Bei kombiniertem Betrieb hat ein **Brandalarm immer Vorrang** vor einem Einbruchalarm.

Datenschutz

Wie ist das mit dem Datenschutz bei Kameras?

Das ist der **Kern der Innovation** – und der Grund, warum das EWS dort funktioniert, wo klassische Kameralösungen am Datenschutz scheitern. Kameras in Feuerwehrhäusern, Bauhöfen oder Betrieben scheitern selten an der Technik, sondern an der **Akzeptanz**: Eine dauerhaft laufende Kamera überwacht potenziell auch das eigene Personal – Personalrat und Mitarbeitende lehnen das zu Recht ab.

Das EWS löst das **physisch, nicht per Software**: Solange die Anlage unscharf ist (Normalbetrieb, Personal anwesend), sind **alle Kameras über den PoE-Switch physisch vom Strom getrennt**. Keine laufende Kamera, kein Bild, kein Stream, keine Aufzeichnung – es gibt schlicht nichts, was jemand einsehen oder missbrauchen könnte. Eine softwareseitig „nur deaktivierte“ Kamera bleibt dagegen am Netz und ist eine Vertrauens- und Angriffsfläche; eine **stromlose Kamera nicht**. Das entschärft die Datenschutz-Frage an der Wurzel und macht die Anlage gegenüber Personal und Gremien überhaupt erst vermittelbar.

Wann sehen die Kameras überhaupt etwas?

Erst beim **Scharfschalten** wird die Stromversorgung der Kameras aktiviert; sie booten und beginnen mit der Überwachung. Beim Unscharfschalten werden sie sofort wieder stromlos.

Was passiert mit den aufgenommenen Bildern?

Beweisbild-Links sind nur **wenige Minuten gültig** (15 min) und werden danach automatisch gelöscht. Aufnahmen werden für eine konfigurierbare Frist (bis 180 Tage, Standard 30 Tage) aufbewahrt und danach **automatisch gelöscht** – ohne manuellen Eingriff.

Verarbeitet das EWS personenbezogene Daten?

Ja – anders als das Brandwarnsystem verarbeitet das EWS Bildaufnahmen und damit personenbezogene Daten. Es ist auf DSGVO-Konformität ausgelegt (physische Stromtrennung im Ruhezustand, kurze Link-Gültigkeit, automatische Löschung, geschützter Zugriff). dexa stellt einen **Auftragsverarbeitungsvertrag nach Art. 28 DSGVO** bereit.

Technik & Erkennung

Welche Kameras kommen zum Einsatz?

Hikvision-IP-Kameras mit **8 MP (4K)**, IR-Nachtsicht und integrierter KI-Personenerkennung (Smart Events: FieldDetection, LineCrossing, RegionEntrance/-Exit). Je Lizenz sind bis zu **16 Kameras** möglich.

Wie funktioniert die Personenerkennung?

Die Klassifizierung läuft **direkt in der Kamera**. Nur wenn ein menschliches Ziel erkannt wird, wird ein Voralarm ausgelöst. Bewegungen durch Tiere, Fahrzeuge oder Lichtwechsel führen nicht zum Alarm.

Funktioniert das auch nachts?

Ja. Die Kameras haben IR-Nachtsicht, und das System schaltet automatisch zwischen **Tag-, Dämmerung- und Nachtprofilen** nach Sonnenstand um (Belichtung, WDR, IR-Strahler je Profil).

Was ist der WhiteLight-Strahler?

Ein in der Kamera integrierter Strahler, der bei Erkennung als **optische Abschreckung/Alarmierung** ausgelöst wird. Im **stillen Alarm** lässt er sich pro Kamera deaktivieren – dann erfolgt nur die Benachrichtigung der Schnittstellen, ohne Aufschrecken.

Wie werden mehrere gleichzeitige Erkennungen behandelt?

Erkennen mehrere Kameras innerhalb von 30 Sekunden dieselbe Person, fasst der Korrelator dies zu **einem Aggregatalarm** zusammen – statt mehrerer Einzelmeldungen.

Bedienung

Wie schalte ich die Anlage scharf/unscharf?

Komfortabel direkt am **dexa PoE-Display** – einem **Eigenprodukt der dexa group**, das auch im Brandwarnsystem eingesetzt wird. Ein kurzes Vorhalten eines **NFC-Tokens** genügt; optional zusätzlich mit **PIN** (Anlagen-PIN für mehrstufige Absicherung). Beim Scharfschalten läuft ein Countdown (Zeit, das Gebäude zu verlassen), danach ist die Anlage scharf. Ein Gerät für Bedienung, Zustandsanzeige und – mit dem Schaltkontakt kombiniert – die Türfreigabe; PoE-versorgt, also nur ein Kabel. Drei Fehlversuche sperren die Eingabe für 5 Minuten.

Wie erkenne ich den Anlagenzustand?

Über eine eindeutige Farbsignalisierung: **grün = unscharf** (Kameras stromlos), **blau = Scharfschaltung läuft** (Countdown), **rot = scharf/Alarm**.

Was passiert bei einem Alarm?

Detection ? Voralarm (Berechtigte können per PIN unterdrücken) ? Alarm (Snapshot, Sirene + Strahler, systemweite Vollbild-Anzeige) ? Dispatch an alle Dienste ? Beweisbild-Link ? Quittierung. Die Quittierung wird an alle unterstützenden Dienste weitergeleitet.

Kann ich die Kameras live sehen?

Ja, als WebRTC-Stream im 1×1- oder 2×2-Grid – allerdings **nur bei scharfer Anlage** oder im Wartungsmodus, da die Kameras sonst stromlos sind.

Kann ich die Anlage mit der Schließanlage verbinden?

Ja. Beim Unscharfschalten öffnet die Tür, beim Scharfschalten wird verriegelt – ein Vorgang, kein Medienbruch. Die **universelle Möglichkeit** ist der **potenzialfreie Schaltkontakt** (DXO-SFH-SC-1-01 / SC-4-01): Damit lässt sich praktisch **jede** elektrische Türöffnung, jeder Türöffner, jedes Motorschloss oder Relais ansteuern – herstellerunabhängig, auch ohne fertige Integration. Daneben gibt es fertige Integrationen für **ABUS, Salto, dormakaba, ASSA ABLOY**, generische **NFC-Tags**, Consumer-Schlösser wie **Nuki** und **SwitchBot** sowie die PIN-/NFC-Freigabe direkt am **dexa PoE-Display**.

Schnittstellen

Über welche Dienste alarmiert das EWS?

Einsatzbereit sind **DIVERA 24/7, Alamos FE2 / aPager Pro, GroupAlarm und E-Mail (SMTP)**. Über die offene BaseInterface-Schicht und die dexa-Plattform sind **30+ weitere Alarm- und Leitstellensysteme** anbindbar. Bei jedem Alarm werden alle aktiven Dienste gleichzeitig benachrichtigt.

Wird ein Bild mitgeschickt?

Ja – je nach Dienst als Anhang oder als **zeitlich begrenzter Public-Link** (ohne Login aufrufbar, nach 15 Minuten ungültig). So lässt sich aus der Ferne sofort beurteilen, ob ein echter Einbruch vorliegt.

Sicherheit

Kann jemand die Kameras manipulieren?

Im Ruhezustand sind die Kameras stromlos – Manipulation ist sinnlos. Zusätzlich erkennt die **Port-Mismatch-Erkennung** über die MAC-Tabelle des Switches fremde Geräte oder Umverkabelung am Kameraport und meldet sie im Dashboard.

Was passiert, wenn jemand die Hardware kopiert?

Die Lizenz ist **kryptographisch an die Hardware gebunden** (MAC-gebunden). Ein Klon der SD-Karte auf andere Hardware startet nicht.

Wie sind die Beweisbild-Links abgesichert?

Sie haben ~71 Bit Entropie, sind nur wenige Minuten gültig und werden nur im Arbeitsspeicher gehalten. Nach Ablauf sind sie forensisch wertlos; anschließend erfolgt die automatische Löschung.

Verfügbarkeit & Rahmen

Ist das EWS schon verfügbar?

Das EWS wurde zur **INTERSCHUTZ 2026** vorgestellt. Für Pilotprojekte und frühen Zugang sprechen Sie uns an.

Wer ist Ansprechpartner und welche Rolle hat dexa?

dexa nimmt – wie beim Brandwarnsystem – die Rolle des **Systemintegrators** ein: Beratung, Planung, Konfiguration, Inbetriebnahme und Dokumentation. Bei externen Schnittstellen (z. B. Alarmdiensten) hängt

die Funktion auch vom jeweiligen Anbieter ab.

Stand: Juni 2026