



DS1051-047

Benutzer-Portal und -App für die Alarmanlage



Ungekürztes Handbuch

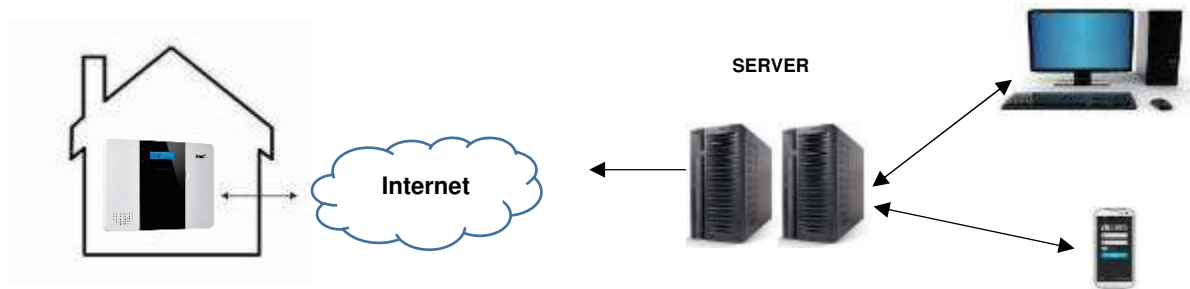
INHALT

1	EINLEITUNG	3
2	MINDESTANFORDERUNGEN UND KOMPATIBLE BROWSER.....	3
3	FERNVERWALTUNG DES SYSTEMS	4
3.1	Grundlegende Konfiguration der Zentrale.....	4
4	REGISTRIERUNG EINES NEUEN BENUTZERS ÜBER PORTAL UND APP	5
5	ZUGANG ZUM PORTAL	9
6	ANSICHT HOME	10
6.1	Bereich Systemstatus.....	10
6.1.1	Aktivierung bei Fehlern im System	12
6.2	BEREICH GERÄTE.....	14
6.3	BEREICH MENÜ UND BEREICH VERBINDUNG	15
6.4	BEREICH KAMERA	16
6.5	MENÜ EREIGNIS	17
7	KAMERA	19
8	MENÜ EINSTELLUNG	20
8.1	GERÄTE BEARBEITEN.....	21
8.2	HINZUFÜGEN UND BEARBEITEN VON CODES.....	22
9	ZUGANGSEINSTELLUNGEN DER BENUTZER	23
9.1	Benachrichtigung	25
9.2	VERLASSEN DES PORTALS	25
10	VERWENDUNG DER APP FÜR SMARTPHONES.....	26
10.1	TASTEN ZUM BEWEGEN IM INNEREN DER APP	30
11	ALLGEMEINE WARNHINWEISE ZUR VERWENDUNG VON PORTAL UND APP	31
11.1	AKTIVIERUNG MIT FEHLERN.....	31
11.2	Langsame oder kritische Internetverbindungen	32
11.3	Eingabe falscher Codes	32

1 EINLEITUNG

Urmel Zeno ist ein allumfassendes und zuverlässiges Sicherheitssystem zum Schutz und zur Überwachung Ihrer wichtigsten Lebens- und Arbeitsumgebungen. Verwaltung und Überwachung erfolgen über Internet und werden vom **Urmel-Server** garantiert, der für jeden autorisierten Benutzer die standortferne Kontrolle des Systemstatus, die Überwachung der Ereignisse und ihre Überprüfung im Bild- und Videoformat und den Empfang von Benachrichtigungen und Alarmen ermöglicht. Die verfügbaren Funktionen wurden für eine mühelose und intuitive Nutzung von jedem PC und Tablet aus auf dem **Multi-Browser-Portal Urmel** und von Ihrem **Smartphone mit Android** oder **iOS** über die dedizierte APP ausgelegt.

Das System ZENO schützt Ihr Zuhause, wo auch immer Sie sich befinden:



VERWENDETE TECHNOLOGIE

Die Drahtlostechnologie des Systems **ZENO** stützt sich auf die doppelte Konnektivität von ADSL und IP/4G.

Beide werden von einer dedizierten Plattform garantiert, mit der der Benutzer sich über sein Netzwerk zu Hause oder Fernzugriff mittels Handy verbinden und so die Steuer- und Überwachungsdienste in Anspruch nehmen kann.

- ☞ das ADSL-Netz gestattet bessere Leistungen beim Fernzugriff und beim Laden von Videos und Fotos;
- ☞ die doppelte Verbindung garantiert, dass im Fall des Ausfalls einer der beiden das System weiter und unter Verfügbarkeit aller Funktionen in Betrieb bleibt.

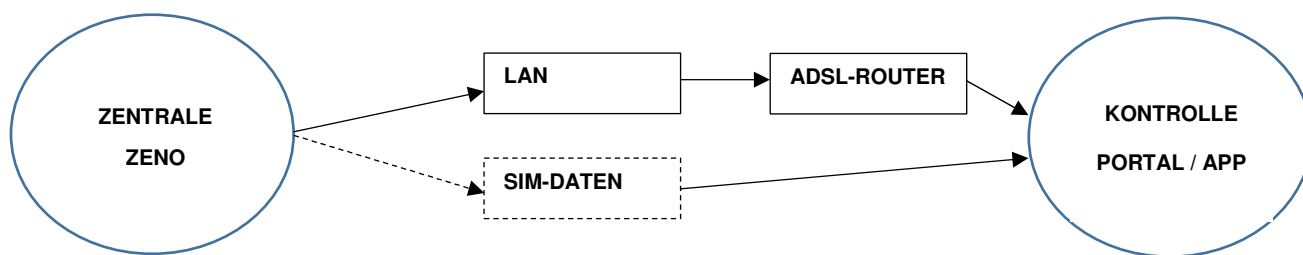
2 MINDESTANFORDERUNGEN UND KOMPATIBLE BROWSER

- Betriebssystem Microsoft Windows 98, ME, NT4.0, 2000, XP, Vista, 7, 8 oder 10.
- Microsoft Internet Explorer 5.x oder spätere oder Google Chrome (empfohlen).
- CPU: Intel Pentium II 266 MHz oder höher.
- Speicher: 64 MB oder mehr.
- VGA-Auflösung: 800x600 oder höher.

SYSTEMAUFBAU

Das Kommunikationssystem zwischen der Zentrale und den Geräten verwendet Funkfrequenzsignale bei 868 MHz und 2,4 GHz.

Die Funktechnologie und die Batterieversorgung der Geräte ZENO gestatten es, die bestehende elektrische Infrastruktur mit komplexen Verkabelungen nicht zu verändern.



Für weitere Einzelheiten siehe Installationshandbuch der Zentrale ZENO.

3 FERNVERWALTUNG DES SYSTEMS

Zugang zum Portal

Um Zugang zum Portal zu erhalten, muss nur über einen der angegebenen Internet-Browser die folgende Adresse eingegeben werden: <https://www.myzeno.urmet.com/home>

In den dem Portal gewidmeten Kapiteln dieses Handbuchs werden der Registrierungsvorgang auf dem Portal und seine Nutzung beschrieben.

Zugriff auf die APP

Die Applikation **MyZeno** ist auf Play Store oder APP Store für Smartphone und für Tablets mit Android und iOS erhältlich. Die erforderliche Mindestversion für Android-Geräte ist Android 5.0. Für iOS-Geräte ist es iOS 7.

Die beste Ansicht der Schnittstelle erhält man mit einem Display mit einer Größe von mehr als 4,5 Zoll.

In den der APP gewidmeten Kapiteln dieses Handbuchs wird ihre Nutzung beschrieben.

<HINWEIS>

Für den Zugriff auf die APP muss man bereits registriert sein. Die Registrierung als neuer Benutzer muss über das Portal oder die APP selbst erfolgen und das beim Registrierungsvorgang erhaltene Passwort gilt für den Zugang zum System ZENO sowohl mit APP als auch über das Portal.

3.1 GRUNDLEGENDE KONFIGURATION DER ZENTRALE

Dieses Handbuch bietet Ihnen eine Hilfestellung bei den Registrierungsvorgängen auf dem Portal und der Funktionsweise desselben und der Benutzer-APP: von der Kontrolle des Aktivierungs- und Deaktivierungsstatus der Anlage bis zur Verwaltung der einzelnen Geräte und dem Versand von Reports im Alarmfall.

Die Registrierung auf dem Portal setzt die vollständige Konfiguration von Seiten des Installateurs voraus. Zu diesem Zweck können die im Lieferumfang der Zentrale enthaltenen technischen Installations- und Programmierhandbücher als Bezug verwendet werden, indem die Netzwerkeinstellungen und der Status der aktiven Verbindung mit dem Server von Urmet überprüft werden.

4 REGISTRIERUNG EINES NEUEN BENUTZERS ÜBER PORTAL UND APP

Die Registrierung eines neuen Benutzers erfordert eingangs einige Vorgänge von Seiten des Installateurs auf der Zentrale, die mit dem Unterbrechen der Versorgung und dem Trennen der Batterie der Zentrale beginnen und mit der Eingabe der Identifizierungsdaten des Benutzers und der Zentrale von Seiten des Benutzers abgeschlossen werden. Dieser Vorgang muss in einem Zeitraum von 15 Minuten ab dem Moment der Stromversorgung der Zentrale abgeschlossen werden. Endet dieser Zeitraum, ohne dass der Vorgang beendet wurde, muss erneut die Stromversorgung zur Zentrale unterbrochen und der Zeitraum von 15 Minuten von vorn begonnen werden.

Schritt 1.

Über einen der angegebenen Browser die Adresse <https://www.myzeno.urmet.com/home> eingeben. Es erscheint die folgende Ansicht:

<HINWEIS>

Im Fall von Problemen beim Laden des Web-Portals muss das Schutzniveau des Browsers reguliert werden.

Schritt 2.

Klicken Sie auf **Neuer Benutzer**, um den Registrierungsvorgang zu starten, mit dem die Verknüpfung der Mac Address (eindeutige Identifizierungsadresse) Ihrer Zentrale mit Ihrem Account erfolgt (Master-Benutzer).

Um die Registrierungsvorgänge als neuer Benutzer abzuschließen, die Taste WEITER betätigen, um von einer Ansicht zur nächsten zu gelangen, und die Taste ZURÜCK, um die vorangegangene einzublenden. Wie folgt vorgehen:

- 1) Die Versorgung und die Batterie von der Zentrale und den Router von der Verbindung trennen.
- 2) Die Versorgung zur Zentrale wieder einschalten **und nicht vergessen, die Batterie wieder zu aktivieren**
- 3) Abwarten, bis die Led der Zentrale aufleuchtet.

Schritt 3.

Nach dem Abschluss der Vorgänge auf der Zentrale öffnet ein weiteres Anklicken der Taste WEITER die Ansicht zur Eingabe der vom Benutzer verlangten Zugangsinformationen.

In dieser Ansicht müssen ein Benutzername und ein Passwort für den Hauptbenutzer (Master) erstellt werden, die dazu dienen, normal sowohl zum Portal als auch zur APP Zugang zu erhalten.

The screenshot shows a registration form titled 'Account-Info' with a progress indicator at the top showing three steps: 'Account-Info' (active), 'Persönliche Info', and 'Register-Info'. The form contains the following fields:

- Benutzername
- Passwort
- Passwort bestätigen
- E-Mail
- Bestätige E-Mail
- Ländercode (dropdown menu showing 'Auswählen' and a text input field)
- Mobil
- Festnetz (dropdown menu showing 'Festnetz' and a text input field)

Below the fields is a checkbox labeled 'Ich habe die folg. Dokumentation gelesen und willige ein.' followed by a link to '[Geschäftsbedingungen](#)'. At the bottom are two buttons: 'Zurück' and 'Weiter'. At the very bottom, there is a 'Sprache' section with flags for USA, Italy, Germany, and France.

Die unerlässlichen Informationen in dieser Ansicht betreffen **Benutzer**, **Passwort** und **E-Mail**. Nachdem die Felder ausgefüllt wurden, kann mit der Ansicht *Persönliche Info* fortgefahren werden.

The screenshot shows a registration form titled 'Persönliche Info' with a progress indicator at the top showing three steps: 'Account-Info', 'Persönliche Info' (active), and 'Register-Info'. The form contains the following fields:

- Vorname
- Nachname
- Str. Adresse
- Stadt
- Staat
- PLZ

At the bottom are two buttons: 'Zurück' and 'Weiter'.

Durch Anklicken von WEITER gelangt man für die Eingabe der Registrierungsinformationen der Zentrale in die Ansicht *Register-Info*:

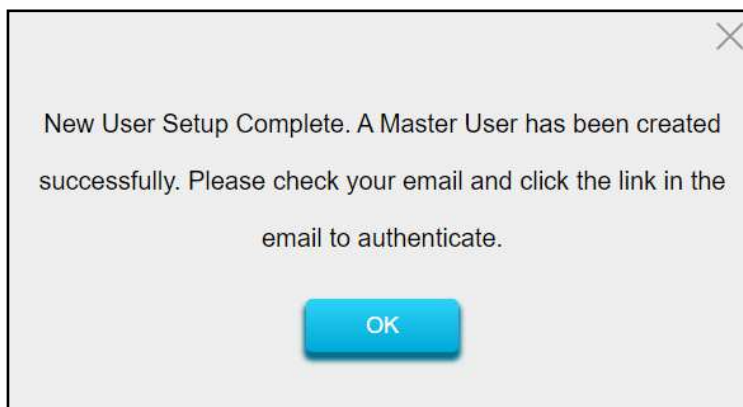
MAC: Die **Mac Address** ist auf dem hinteren Gehäusedeckel der Zentrale zu finden und gestattet es dem Server von Elkron, Ihre Zentrale mit Ihrem Account zu verknüpfen und so die Fernsteuerungsinstrumente sowohl vom Portal als auch von der APP aus zur Verfügung zu stellen.

ZENTRALE NAME: Der Name, den man an die Zentrale vergeben kann und der in den Benachrichtigungen und den E-Mails erscheint

SPRACHE: Auswahl unter Italienisch/Englisch/Französisch/Deutsch

Schritt 4.

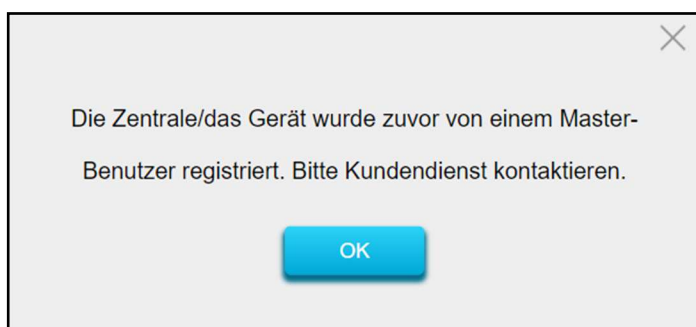
Durch Klicken auf die Taste OK wird der Registrierungsvorgang abgeschlossen. Die nachfolgende Bestätigungsnachricht wird eingeblendet und an die angegebene E-Mail-Adresse versandt. Durch Klicken auf OK kehrt man zur Startseite mit bereits eingegebenen Benutzernamen und Passwort zurück.



Der soeben beschriebene Registrierungsvorgang kann auch über die APP erfolgen (Version 1.8.31 oder höher).

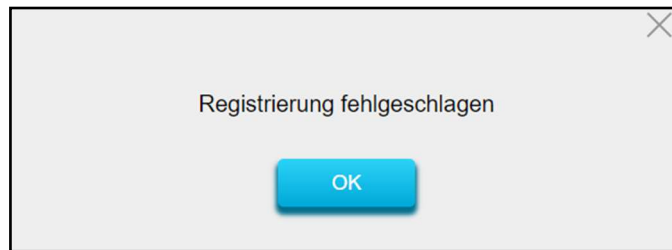
Durch Anklicken der Taste **VERBINDEN** (Taste **ZUGRIFF** von der APP aus) in der Startseite erhält man Zugang zu den Ansichten zur Verwaltung der Zentrale.

Wird eine Fehlermeldung wie die untenstehende eingeblendet, bedeutet dies, dass der Account bereits in der Urmet-Datenbank vorhanden ist. Man muss daher über die Zugangsdaten des Master-Benutzers verfügen, der als Erster die Registrierung durchgeführt hat.



Weitere Fehlermeldungen können die Unmöglichkeit der Verbindung mit der Zentrale betreffen, auf die die Empfehlung folgt, den Verbindungsstatus zu überprüfen.

In diesem Fall könnte die Zentrale nicht mit dem Server verbunden sein, zum Beispiel wegen fehlender Versorgung oder Problemen der Internetverbindung. Überprüfen Sie die Versorgung und den Verbindungsstatus. Kontrollieren Sie die Konfiguration des auf dem Router eingegebenen Filters der Mac Address und vergewissern Sie sich, dass die Mac Address der Zentrale autorisiert ist.



Die Registrierung der Zentrale wurde nicht innerhalb von 15 Minuten ab dem Moment der Versorgung der Zentrale abgeschlossen.

Sollte die Mac Address korrekt und die Zentrale verbunden sein, doch die Probleme bleiben bestehen, müssen Sie sich an eine Urmet-Kundendienststelle wenden.

5 ZUGANG ZUM PORTAL

Geben Sie, nachdem Sie sich auf dem Portal registriert haben, über den Link <https://www.myzeno.urmet.com/home> Ihren Benutzernamen und Ihr Passwort ein:



The image shows the login interface for the urmet zenO portal. On the left is the logo 'urmet zenO' in white and blue. To the right of the logo is a vertical line. To the right of the line are the login fields: a 'Benutzer-ID' field with a person icon, a 'Passwort' field with a lock icon, a 'Mich erinnern' checkbox, and a 'Passwort vergessen' link. Above the 'Benutzer-ID' field is a 'Neuer Benutzer' link. Below the login fields is a 'Verbinden' button. At the bottom center is a 'Sprache' section with four flags: USA, Italy, Germany (selected), and France.

In dieser ersten Ansicht ist es möglich, Zugangsdaten für spätere Zugriffe zu **speichern** und das eventuell vergessene Passwort **zurückzusetzen** (in diesem Fall löscht der Server das aktuelle und sendet Ihnen ein neues an Ihre E-Mail-Adresse).

Klicken Sie auf VERBINDEN, um zu den Ansichten zur Verwaltung Ihrer Zentrale zu gelangen.

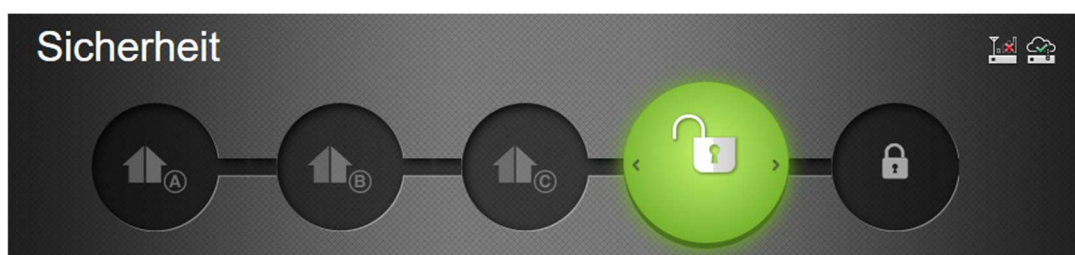
6 ANSICHT HOME

Diese erste Ansicht ist die Hauptseite Ihres Accounts. Von hier aus können Sie zu den anderen Bereichen des Portals gelangen und den Systemstatus und die Liste der die Alarmanlage (Sicherheit) betreffenden Geräte einblenden, die in Ihre Zentrale eingelernt wurden. Im Anschluss werden die verschiedenen Bereiche eingehender behandelt, aus denen sich die Ansicht zusammensetzt:



6.1 BEREICH SYSTEMSTATUS

Der Systemstatus wird von den 5 Symbolen im oberen Teil angegeben. Das hervorgehobene Symbol zeigt den aktuellen Systemstatus an. Im Beispiel gibt das grüne Symbol an, dass das System DEAKTIVIERT ist.



Jedes Mal, wenn der Status geändert werden soll, wird durch Anklicken des einzelnen Symbols die Eingabe des Benutzercodes verlangt (Standard 1234). Geben Sie die einzelnen 4 Ziffern Ihres Codes ein:

Bitte PIN eingeben

1

2

3

4

5

6

7

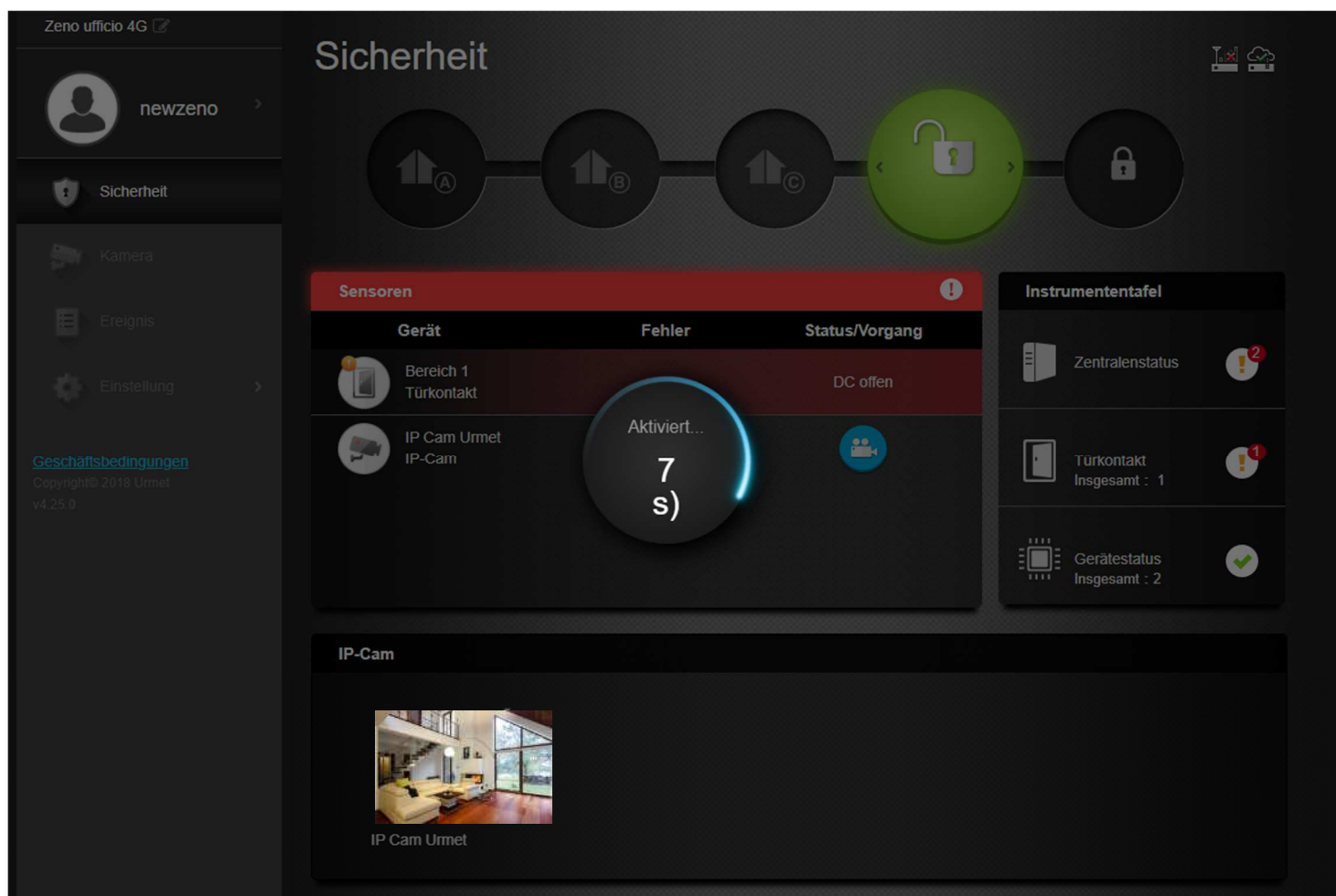
8

9

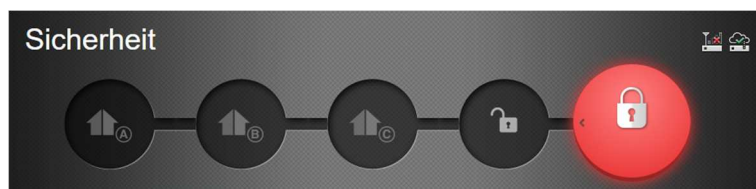
Zurück

0

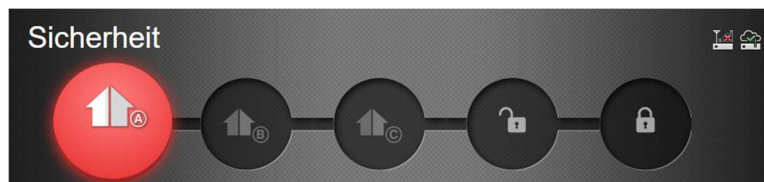
Nach Eingabe des korrekten Codes wechselt das System am Ende der Zählung der Ausgangszeit der Zentrale vom Status DEAKTIVIERT in den Status AKTIVIERT oder TEILAKTIVIERT, wenn vorgesehen:



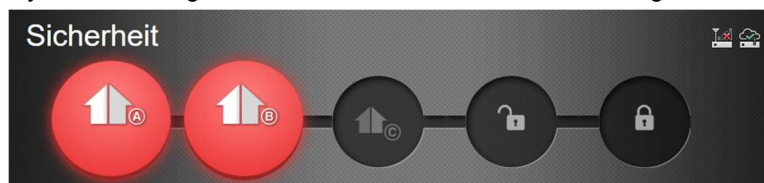
Der Status *VOLLAKTIVIERT* des Systems wird durch das Aufleuchten des entsprechenden Symbols angezeigt.



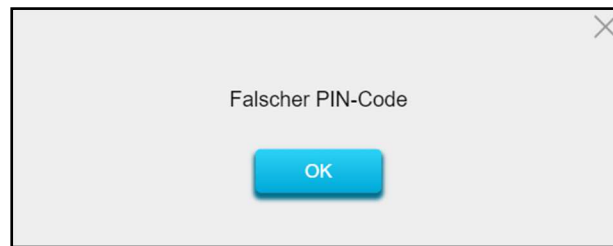
Der Status der *TEILAKTIVIERUNG* eines oder mehrerer Bereiche des Systems wird durch das Aufleuchten des entsprechenden Symbols angezeigt (zum Beispiel Bereich A):



Zum Aktivieren von mehr als einem Bereich, zum Beispiel A+B wie im untenstehenden Beispiel, müssen die einzelnen Symbole betätigt werden, doch Sie werden um die Eingabe des Codes für beide Bereiche gebeten.

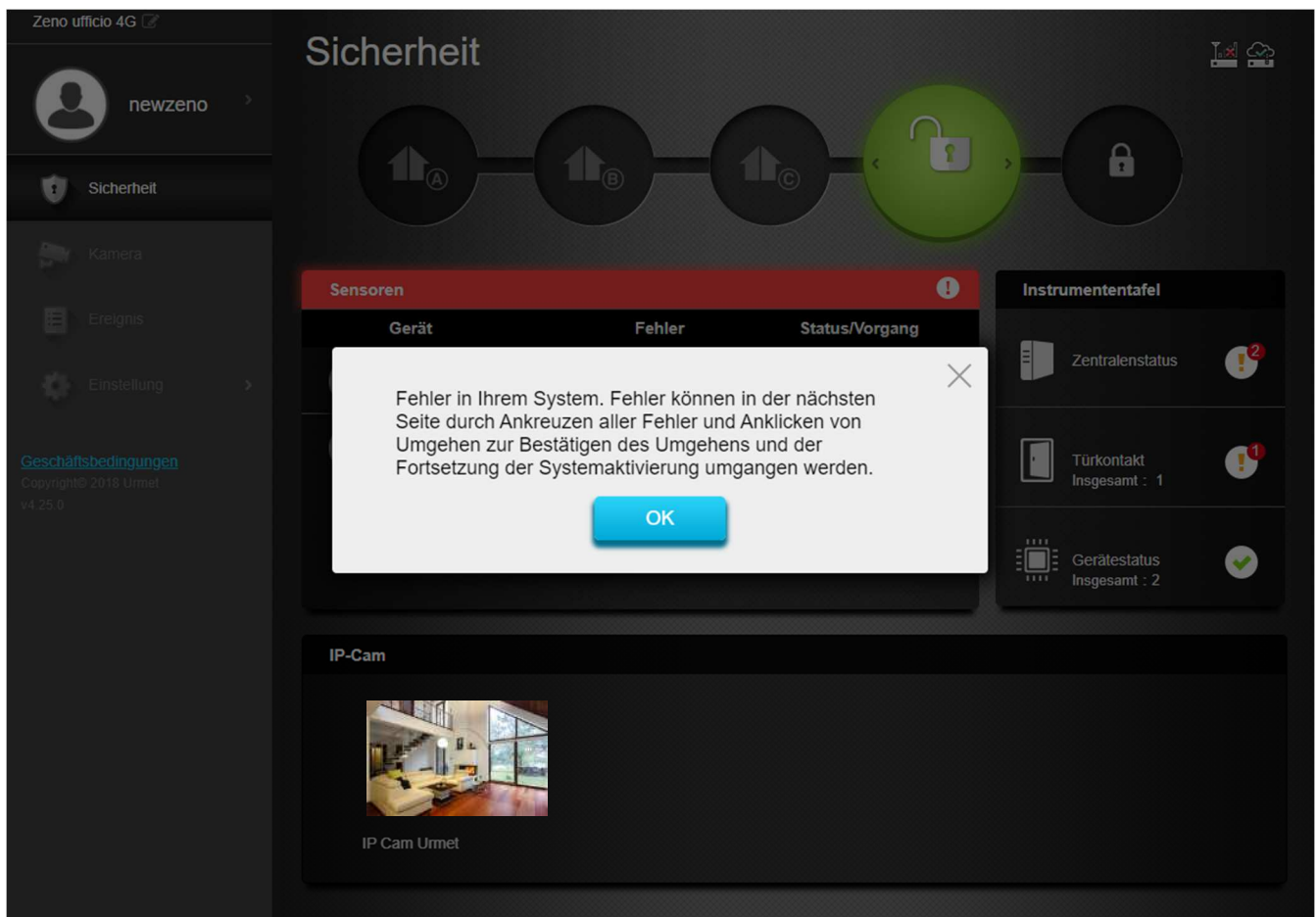


Die eventuelle Eingabe eines falschen Codes führt zum Einblenden der folgenden Meldung und der gewünschte Vorgang findet bis zum Eingeben eines korrekten Codes nicht statt:



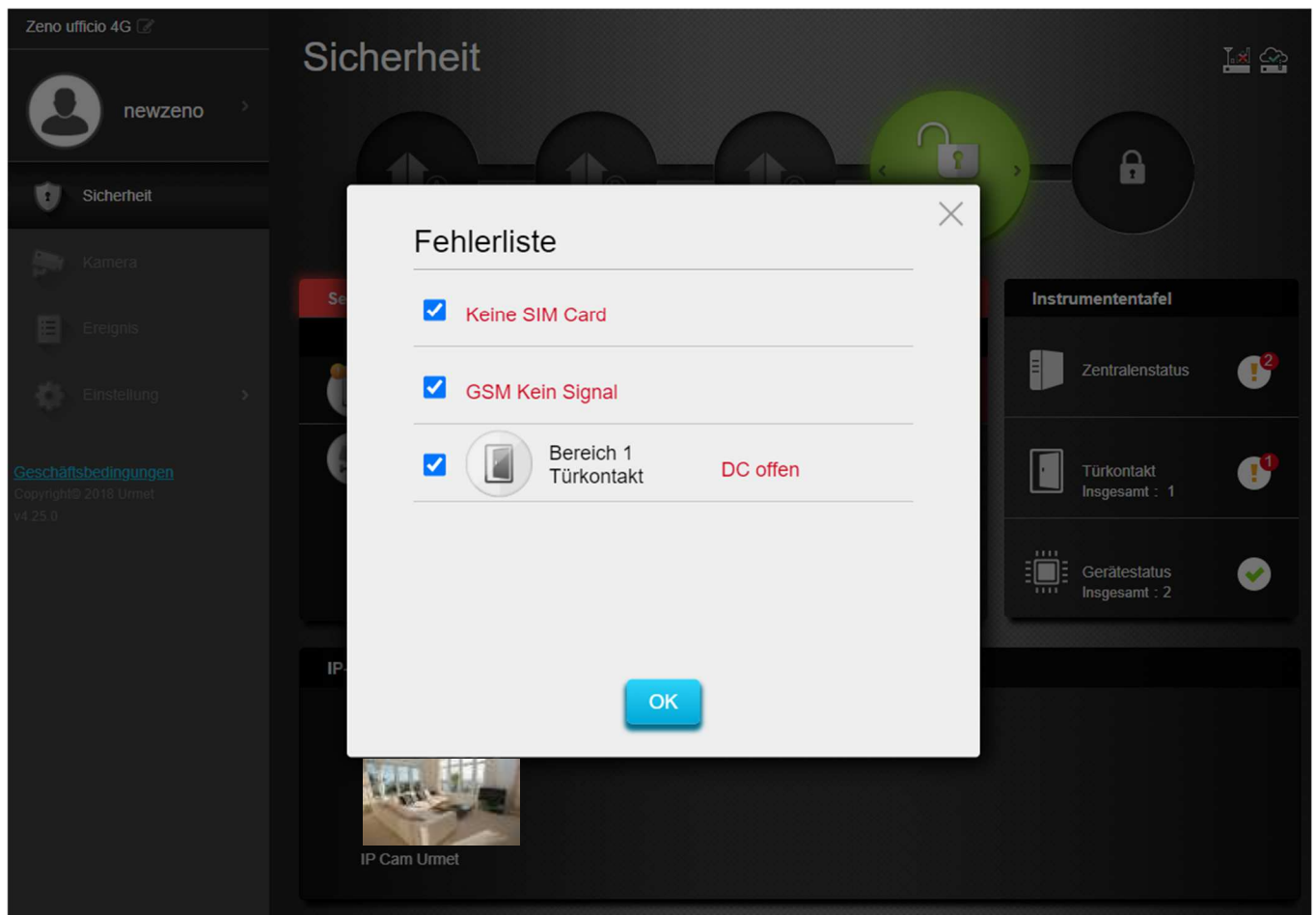
6.1.1 Aktivierung bei Fehlern im System

Während der Aktivierung der Anlage blendet das Portal beim Vorliegen eventueller Systemfehler (zum Beispiel ein offener Kontakt) die folgende Meldung ein:



Durch Betätigen der Taste OK zum Fortsetzen der Aktivierung blendet das Portal die Liste der im System vorliegenden Fehler ein.

Um die Aktivierung abschließen zu können, müssen alle Fehler markiert werden:

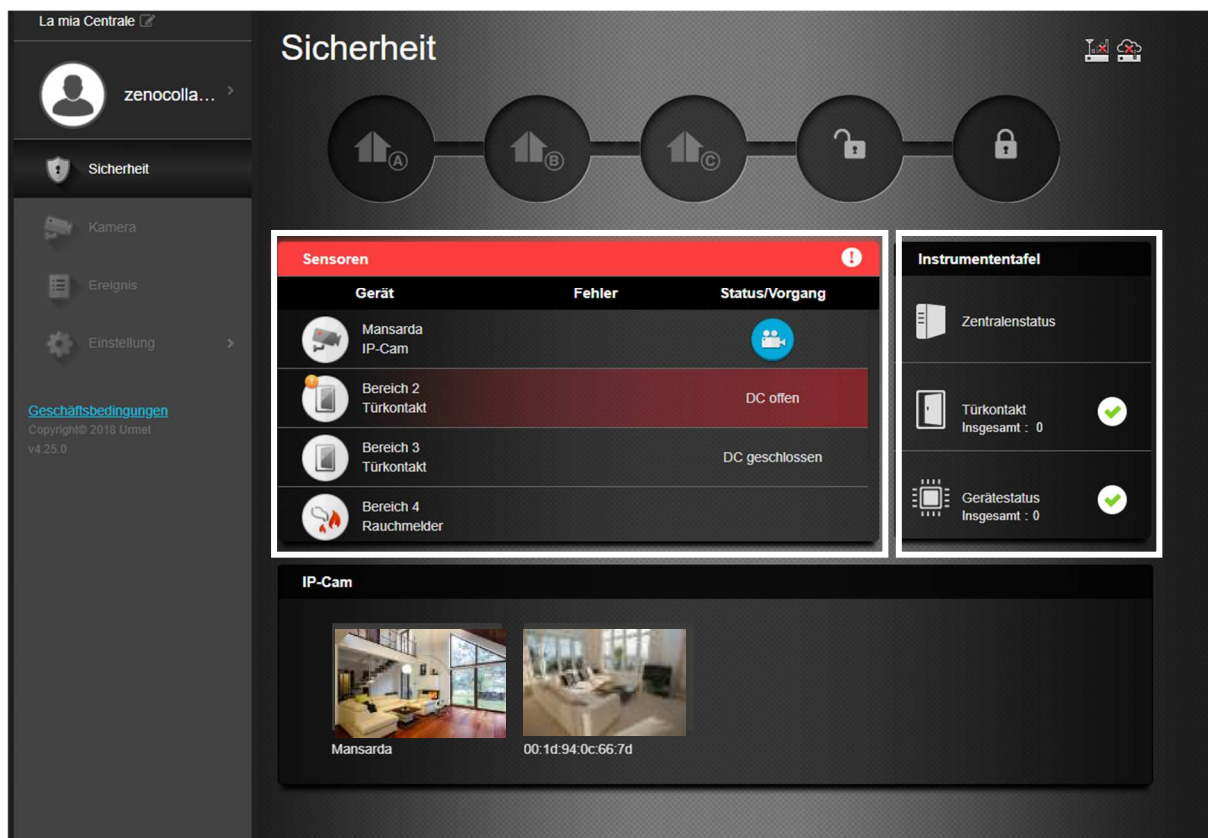


Beim Vorliegen von Fehlern empfehlen wir, den Absatz „Aktivierung mit Fehlern“ im Abschnitt *Hinweise* am Ende dieses Handbuchs aufmerksam zu lesen.

6.2 BEREICH GERÄTE

In den beiden von den Rechtecken hervorgehobenen Bereichen sind erkennbar:

1. die Details aller einzelnen **Geräte** des Bereichs Sicherheit;
2. der **Systemstatus**, d. h., die Anzeige eventueller Fehler der Zentrale, der Geräte, die den Zugang zu den Durchgängen steuern (Status geöffnet/geschlossen) und der Geräte, die Teil Ihres Systems sind.



Für jedes Gerät kann Folgendes eingeblendet werden:

- ☞ **Gerätetyp** (Türkontakt, Sirene, Tastatur, Fernsteuerung, Melder, Verstärker, usw.)
- ☞ **Vergebener Name** (kann vom Master-Benutzer geändert werden);
- ☞ **Fehler des Geräts**, und zwar:
 - Tamper geöffnet, entsprechendes Gehäuse eines Geräts beschädigt
 - Batterie entladen mit Anzeige des unzureichenden Batterieladestatus
 - außer Betrieb (zum Beispiel, wenn ein Melder auf die Anfrage nach Fotos/Videos nicht antwortet)
 - Überwachung (wenn die Zentrale über einen bestimmten Zeitraum keine Signale von einem Gerät erhält)

Das Vorliegen von Fehlern auf dem Gerät wird durch die rote Markierung der gesamten Zeile, die es beschreibt, angezeigt.

- ☞ **Status/Vorgang**, und zwar:
 - Geöffnet/geschlossen, wenn es sich um einen Türkontakt handelt, im Allgemeinen eine Schutzvorrichtung eines Durchgangs
 - der Vorgang, der ausgeführt werden kann, indem auf das entsprechende Symbol geklickt wird, wenn es sich um einen Melder mit Kamera oder Videokamera handelt
 -  „Ein Foto aufnehmen“
 -  „Eine Szene aufnehmen“

- ☞ **Umgangenes Gerät**. Sollte das Gerät umgangen worden sein.

Die Umgehung des Geräts wird durch die gelbe Markierung der gesamten Zeile, die es beschreibt, angezeigt.

6.3 BEREICH MENÜ UND BEREICH VERBINDUNG

Links in der Ansicht befindet sich der Zugangsbereich zu den anderen Menüs des Portals, während sich oben rechts der Bereich der Verbindung befindet.



BEREICH MENÜ

Von diesem Bereich aus ist es möglich, immer zur Ansicht **Home** zurückzukehren, indem das Menü **Sicherheit** angeklickt wird. In diesem Bereich stehen die folgenden Menüs zur Verfügung:

- ☞ **Kamera:** Verwaltung der mit der Zentrale verknüpften IP-Kameras
- ☞ **Ereignis:** hier werden die vollständige Liste der verschiedenen Interaktionen von Seiten des Benutzers mit der Zentrale und die eintretenden Alarmsituationen angezeigt.
- ☞ **Einstellung:** Der Konfiguration der Geräte, Benutzer und der Bedingungen für den Empfang der Reports gewidmeter Bereich. Außerdem kann von hier aus der vorübergehende Code für den Installateur generiert werden, der eine Systemwartung durchführen muss.

*HINWEIS. Das Menü **Einstellung** ist ausschließlich dem Master-Benutzer vorbehalten und ist für Nebenbenutzer nicht sichtbar.*

Auf den folgenden Seiten werden diese Menüs im Einzelnen beschrieben.

BEREICH VERBINDUNG

Die beiden Symbole rechts oben in der Ansicht **Home** erteilen Informationen zum Status der Verbindung.



die Zentrale ist mit dem Server verbunden (über Ethernet und Router oder Netzwerk 4G)



die Zentrale ist nicht mit dem Server verbunden



die SIM der Zentrale ist mit dem GSM-Mobilfunknetz verbunden und in der Lage, Sprachnachrichten und SMS zu versenden.

ACHTUNG! Diese Information bezieht sich nicht auf die tatsächliche Verbindung mit dem 4G-Datennetzwerk.

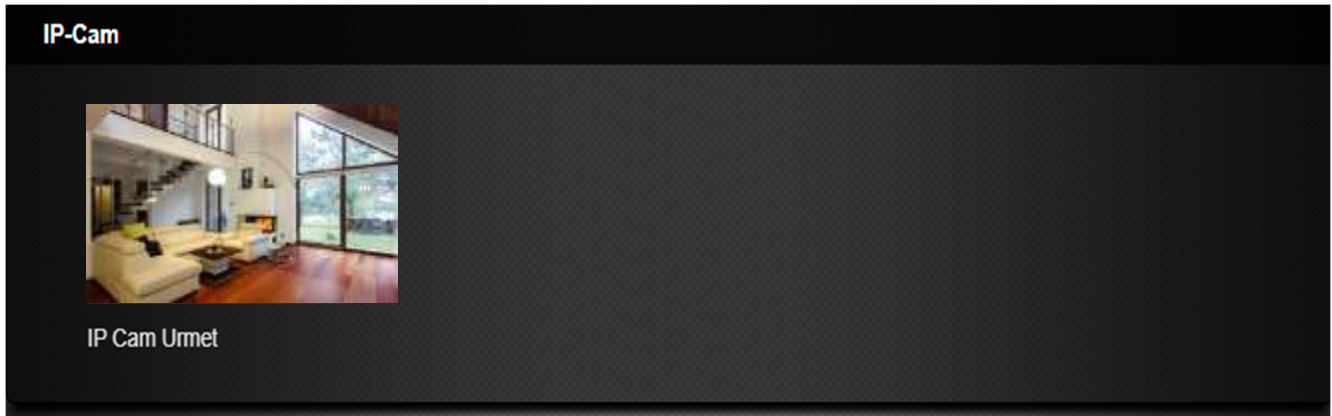


die SIM der Zentrale könnte fehlen oder nicht mit dem GSM-Mobilfunknetz verbunden sein oder eine kritische oder instabile Verbindung aufweisen.

ACHTUNG! In diesem Fall ist es unerlässlich, einen verkabelten Festanschluss über Ethernet zu garantieren.

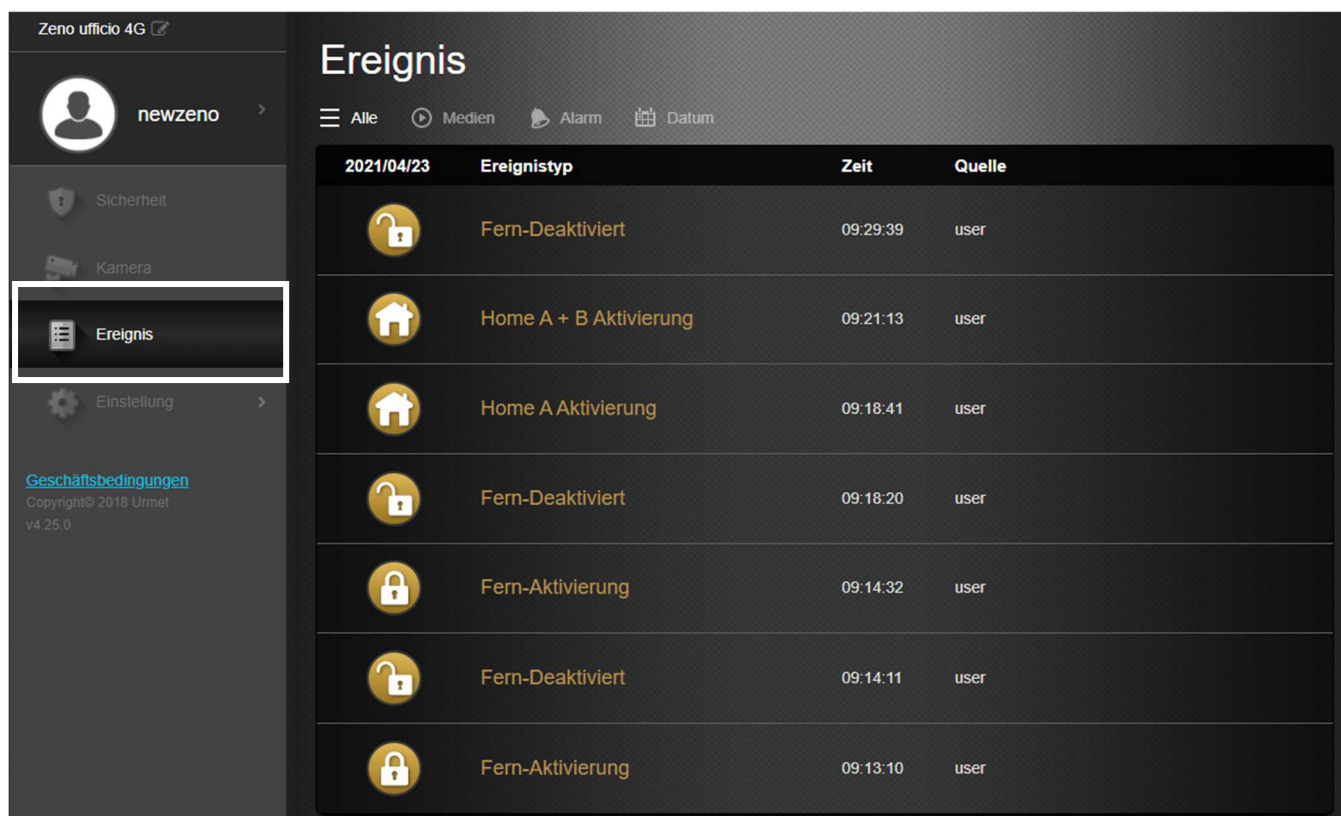
6.4 BEREICH KAMERA

Der Bereich der IP-Kameras zeigt die Bilder der mit der Zentrale verknüpften Kameras. Mit einem Doppelklick der Maus kann das Bild vergrößert und es kann die der Kontrolle gewidmete Seite geöffnet werden.



6.5 MENÜ EREIGNIS

Durch Anklicken des Menüpunkts **Ereignis** im Bereich der Menüs gelangt man zu der Tabelle, in der alle im System aufgetretenen Ereignisse verfolgt und im Speicher archiviert werden.



2021/04/23	Ereignistyp	Zeit	Quelle
	Fern-Deaktiviert	09:29:39	user
	Home A + B Aktivierung	09:21:13	user
	Home A Aktivierung	09:18:41	user
	Fern-Deaktiviert	09:18:20	user
	Fern-Aktivierung	09:14:32	user
	Fern-Deaktiviert	09:14:11	user
	Fern-Aktivierung	09:13:10	user

Die Ereignisse werden nach Datum, Typ, Uhrzeit und Quelle des Ereignisses aufgezeichnet. Abhängig vom Typ des Ereignisses kann in der letzten Spalte „Quelle“ Folgendes angezeigt werden:

- ☞ die **Geräte**, die von dem Ereignis der Meldung und des Alarms oder dem Foto-/Videoabruf betroffen sind
- ☞ der **Benutzer**, der eine Statusänderung herbeigeführt hat
- ☞ das **System** für regelmäßige Tests, Tamper-Alarm der Zentrale, Überwachungsdefekte und Ausfall des Netzwerks oder der Batterie der Zentrale

Die Ereignisse können gemäß den verfügbaren Auswahlen gefiltert werden:

- ☞ **Alle**: es werden alle Ereignisse (die Alarmer rot, alle anderen gelb) und die aufgenommenen Bilder/Videos angezeigt
- ☞ **Medien**: es werden automatisch von den Sensoren mit Kamera und Videokamera im Alarmfall aufgenommene oder vom Benutzer im Bereich *Home* über die Symbole Kamera und Videokamera abgerufene Bilder angezeigt.

<HINWEIS>

Bilder und Videos stehen auf dem Server 30 Tage lang zur Verfügung und werden danach gelöscht.

- ☞ **Alarm**: es ergeht eine Benachrichtigung über Einbruch-, Panik- und Tamper-Alarm jeder beliebigen Sicherheitsvorrichtung. Die im Fall eines Einbruchs aufgezeichneten Bilder und Filmsequenzen können durch Auswahl von *Alle* oder *Medien* konsultiert werden.
- ☞ **Datum**: es kann ausgewählt werden, die Ereignisse eines spezifischen Tages anzuzeigen. Klicken Sie auf das Feld **Datum** und geben Sie den jeweiligen Tag im Format TT/MM/JJJJ (Tag, Monat und Jahr, z. B. 20.04.2020) ein.

Bei den Auswahlen *Alle* und *Medien* müssen zum Einblenden der Bilder oder Videos oder um sie zu löschen, die beim Gerät mit Kamera/Videokamera verfügbaren Symbole verwendet werden:



Löschen



Video anzeigen



Bild anzeigen

Beim Vorliegen eines Einbruchereignisses zeigt das Portal das Pop-up-Fenster **NEUES ALARMEREIGNIS** an. In der Liste **Ereignis** wird der Alarm umgehend aufgezeichnet und ist sofort zu sehen. Sollte auf einer Kamera/Videokamera ein Alarm DS1051-047

ausgelöst werden, benötigen die aufgenommenen Bilder oder Videos einige Minuten, bevor sie auf dem Portal eingesehen werden können. Diese Zeit benötigt der Server, um sie zu erfassen und an die Anwendung zu senden.

Beispiel einer Alarmbenachrichtigung auf dem Portal im Fall eines Einbruchs:

Zeno ufficio 4G

 newzeno

Sicherheit

Kamera

Ereignis

Einstellung

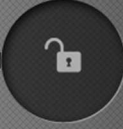
[Geschäftsbedingungen](#)
Copyright© 2018 Urmet
v4.25.0

Sicherheit











Sensoren

Gerät	Fehler	Status/Vorgang
 Bereich 1 Türkontakt		DC offen
 IP Cam Urmet IP-Cam		

IP Cam Urmet

IP Cam

Bereich 1

Neues Alarmereignis

Instrumententafel

Zentralenstatus



Türkontakt
Insgesamt : 1



Gerätestatus
Insgesamt : 2



IP-Cam



7 KAMERA

Diese Seite blendet das Bild der mit der Zentrale verknüpften IP-Kameras ein.



LISTE DER IP-KAMERAS

Der Bereich *Kamera* zeigt die Bilder der mit der Zentrale verknüpften Kameras. Mit einem Doppelklick der Maus kann das Bild vergrößert und es kann die der Kontrolle gewidmete Seite geöffnet werden.

Videoeinstellungen

-  Dieses Symbol gestattet das Öffnen des Menüs der Videoeinstellungen.

Videoaufzeichnungen

-  Durch Anklicken dieses Symbols kann die Aufzeichnung eines Videos angefordert werden. Die Aufzeichnungsparameter sind in der Konfiguration der Kamera festgelegt (siehe dedizierte Handbücher).

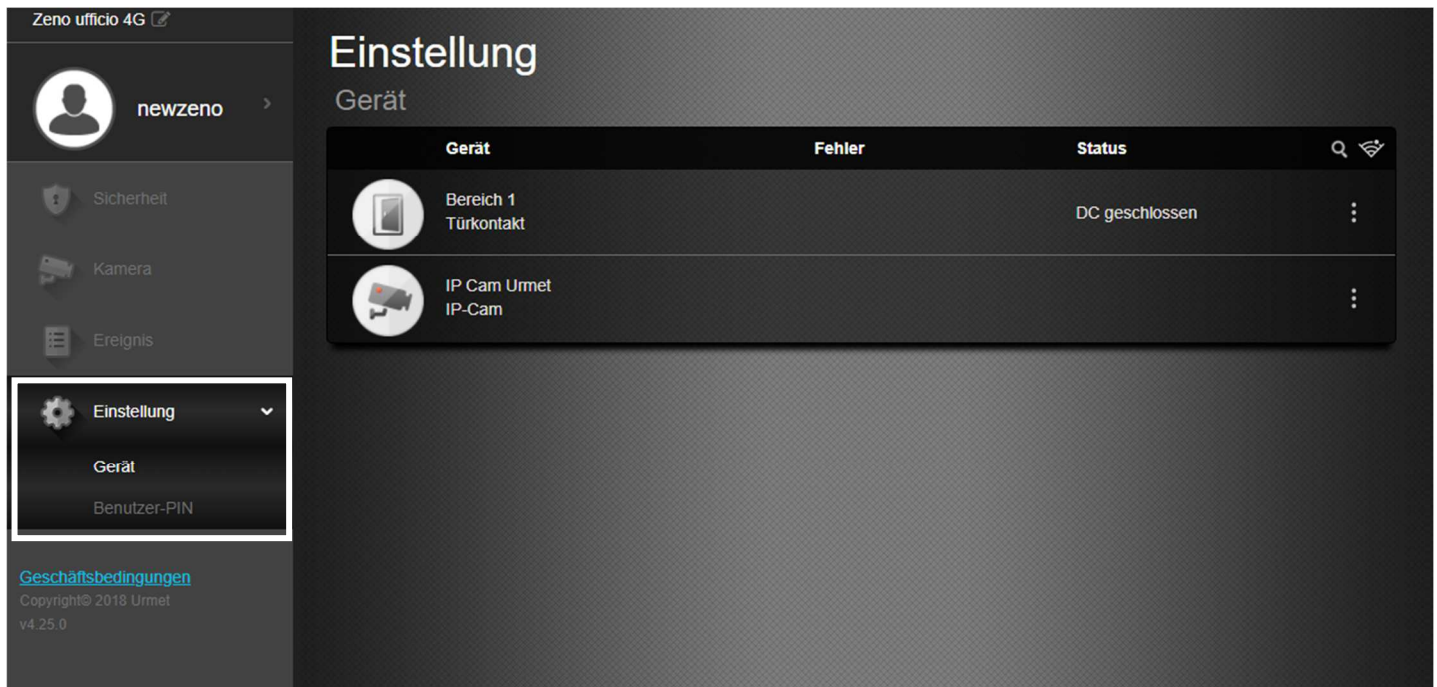
<HINWEIS>

-  Weitere die IP-Kameras betreffende Konfigurationen sind in den Menüs Einstellung/Gerät verfügbar. Für eingehendere Erklärungen zur Verwendung der die IP-Kameras betreffenden Programmierungen siehe Handbuch der jeweiligen Kamera.

8 MENÜ EINSTELLUNG

In diesem **ausschließlich dem Master-Benutzer vorbehaltenen und nur für diesen sichtbaren Bereich** ist es möglich, einige Eigenschaften der Geräte, die Codes zur Verwaltung der Zentrale, den Versand von Reports und den vorübergehenden Installateurcode einzugeben.

Klicken Sie zum Öffnen dieses Menüs auf **Einstellung** im rechten Menü.



Die Ansicht **Einstellung** erscheint mit der Liste der Geräte, die Teil des Systems sind, die dem Untermenü *Gerät* entspricht.

Die Spalten haben die folgende Bedeutung:

- 👉 **Gerät:** Sensortyp und vergebener Name.
- 👉 **Fehler:** erteilt eine zusammenfassende Erklärung des Fehlers.
- 👉 **Status:** gibt den Status Außer Betrieb oder Geöffneter Kontakt an (nur für Magnetkontakte).
- 👉  in diesem Bereich ist es möglich, den Walk Test auszuführen, um die Funkreichweite jedes einzelnen Geräts zu überprüfen. Durch Anklicken des Symbols bereitet sich die Zentrale auf den Empfang des Testcodes von Seiten des Geräts vor (siehe einzelne Anweisungen für den Versand).
- 👉  mit der Lupenfunktion kann ein spezifisches Gerät im Inneren der Liste gesucht werden.

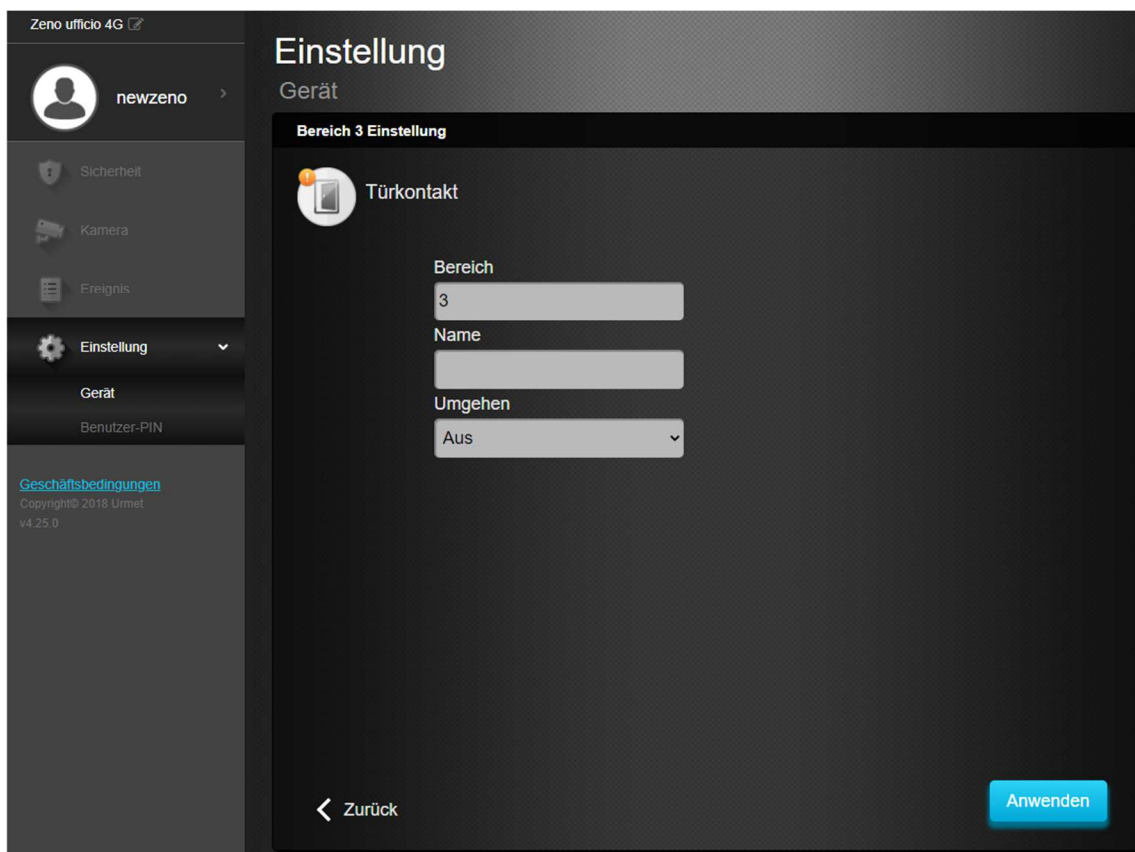
Walk Test-Beispiel

Im untenstehenden Beispiel werden die zu der Zentrale, auf der der Walk Test ausgeführt wurde, gehörenden Geräte angezeigt. Die Antwort der Zentrale erscheint in der Spalte **RSSI** und gibt den Wert der Funkreichweite an (max. 9):

Walk Test		
Typ	Bereich	Gerätename
 Türkontakt	3	
		RSSI
		9
OK		

8.1 GERÄTE BEARBEITEN

Klicken Sie, um in die Einstellungen eines Geräts zu gelangen, auf das Symbol  am Ende der Zeile des jeweiligen Geräts. Es erscheinen der Gerätetyp, die eindeutige Nummer, mit der es im Inneren des Systems erkannt wird, der daran vergebene Name und die Auswahl *Umgehen*.



The screenshot shows the 'Einstellung' (Settings) screen for a device named 'Türkontakt'. The screen is divided into a left sidebar and a main content area. The sidebar contains a user profile 'newzeno' and a list of settings: 'Sicherheit', 'Kamera', 'Ereignis', 'Einstellung' (selected), 'Gerät', and 'Benutzer-PIN'. The main content area is titled 'Einstellung' and 'Gerät'. It shows the device name 'Türkontakt' with a door contact icon. Below this, there are four input fields: 'Bereich' (set to 3), 'Name' (empty), 'Umgehen' (set to 'Aus'), and a dropdown menu. At the bottom, there are two buttons: 'Zurück' (Back) and 'Anwenden' (Apply).

Das Umgehen deaktiviert ein Gerät dauerhaft. Nachdem das Umgehen ausgewählt und die Zentrale mit der Taste **ANWENDEN** aktualisiert wurde, werden alle Einbruchalarme ignoriert. Eventuelle Situationen von entladener Batterie und unerlaubten Eingriffen werden dagegen stets von dem umgangehenen Gerät gemeldet.

ACHTUNG! Was das Gerät „Sirene“ betrifft, deaktiviert die Umgehungsfunktion diese nicht vollständig, sondern unterbindet den Versand der Reports zu ihren Fehlern.

Um die erfolgte Programmierung zu bestätigen und die Daten in der Zentrale zu aktualisieren, die Taste OK, andernfalls **ZURÜCK** betätigen, um zur Tabelle **Gerät** zurückzukehren.

8.2 HINZUFÜGEN UND BEARBEITEN VON CODES

Im Inneren dieses Untermenüs des Bereichs **Einstellung**, in das man durch Anklicken von **Benutzer-PIN** gelangt, können bis zu sechs Benutzer verwaltet werden, die mit den jeweiligen Codes auf das System zugreifen können. Der Master-Benutzer, der in der ersten Zeile erscheint, kann nicht gelöscht werden, jedoch die von ihm erstellten Nebenbenutzer löschen. Die Auswahl des Felds „*Sperre*“ gibt an, dass die Zugriffe auf das System in der Liste der Ereignisse verzeichnet werden. Sollten aus Datenschutzgründen diese Ereignisse nicht aufgezeichnet werden, muss das Feld abgewählt werden.

Benutzer-PIN		
user		☒ Sperre
prova		☒ Sperre
io		☒ Sperre

Zum Aktualisieren der Zentrale mit den erfolgten Änderungen auf **Anwenden** klicken.

HINWEIS: Die Verwendung des Werts 1111 für den Benutzercode ist nicht zulässig.

9 ZUGANGSEINSTELLUNGEN DER BENUTZER

Durch Anklicken des Namens der Zentrale oben links gelangt man in die Ansicht unten, die dem Bereich *Benutzer-Info* entspricht. Von hier aus ist es möglich, auch in den Bereich *Benachrichtigung* zu gelangen.

Zeno ufficio 4G

newzeno

Account

Benachrichtigung

Sicherheit

Kamera

Ereignis

Einstellung

Geschäftsbedingungen

Copyright© 2018 Urmet v4.25.0

Account

Basic

newzeno

Avatar ändern Passwort ändern Account-Info

Benutzer-Info

Account-Nr.	9097		
Vorname	Nachname		
Ländercode	Festnetz		
Mobil	E-Mail	federicoperrachio@gmail.com	
Str. Adresse	Stadt		
Staat	PLZ		

Sprache

Deutsch

Datumsformat

YYYY-MM-DD

In dieser Ansicht können die folgenden Parameter individuell angepasst werden:

- **Avatar ändern**, gestattet das jeweilige Account mit einem Bild persönlich zu gestalten. Dazu eine Datei durch Anklicken der von dem Rechteck markierten Stelle auswählen und durch Betätigen der Taste Upload bestätigen.

Speicherort

Empfohlen wird das Hochladen eines rechteckigen Bildes mit 250 x 250 Pixeln oder mehr und einer Dateigröße unter 2 MB.

Erfolgt kein Hochladen, wird das Standardbild des Systems verwendet.

Upload

Passwort ändern: zum Ändern des Zugangspassworts zum Portal. Geben Sie dieses in die entsprechenden Felder ein und betätigen Sie Anwenden.



- **Account-Info:** in diesem Pop-up-Fenster werden die MAC Address und die Parameter eingeblendet, mit denen die Zentrale in der Datenbank des Servers identifiziert wird. Die Taste gestattet das erneute Senden der auf dem Server gespeicherten Netzkonfigurationsdaten an die Zentrale:



Und schließlich kann unten in der Ansicht die für das Portal zu verwendende Sprache verwaltet und das Datenformat eingegeben werden. Wählen Sie für Deutschland DD-MM-YYYY.

Um die im Menü **Benutzer-Info** angezeigten Benutzerdaten zu ändern, das Symbol  anklicken.

Im mittleren Teil der Ansicht steht dem Master-Benutzer ein Bereich zur Verfügung, in den er **Andere Benutzer** eingeben kann, die befugt sind, mit dem System **Zeno** zu interagieren. Die neuen Benutzer können auf das System zugreifen doch nicht auf die Funktionen der Konfiguration der Geräte.

Zum Eingeben eines neuen Benutzers auf **+** klicken, zum Löschen auf . Zum Ändern der Daten des einzelnen Benutzers das Symbol  neben dem Namen betätigen.

9.1 BENACHRICHTIGUNG

Die Seite **Benachrichtigung** gestattet die Auswahl der mit der auf dem jeweiligen Smartphone installierten APP verbundenen *Push*-Nachrichten.

Benachrichtigung

Push

Alle

Mobile Device Management

Benutzer-ID	Model	Name	Last Login
newzeno	iPhone 7	iPhone	2021/04/23 08:56:24
newzeno	iPhone 7	iPhone (2)	2021/02/17 16:24:51
newzeno	a50eea	SM-A505FN	2021/02/16 10:04:53
newzeno	dreamltxx	SM-G950F	2020/10/06 14:56:21

E-Mail

newzeno federico@gmail.com Benachrichtigung: Alle

Liste

Keine Daten verfügbar.

Extraempfänger

Keine Daten verfügbar.

Abbrechen Anwenden

Die in den Dropdown-Menüs für die Benachrichtigungen und die E-Mails erfolgte Auswahl gilt für alle Benutzer, die die App installiert haben und sich mindestens einmal mit dem Account des Portals verbunden haben. Folgende Optionen sind verfügbar:

- ☞ **Alle**, alle Benachrichtigungen und Ereignisse
- ☞ **Alarme und Fehler**, sowohl die Alarm- als auch die Fehlerbenachrichtigungen
- ☞ **Alarme**, nur die Alarmbenachrichtigungen
- ☞ **Keine**, um keine Push-Nachrichten zu erhalten.

9.2 VERLASSEN DES PORTALS

Auf das Symbol  klicken, um das Portal zu verlassen.

10 VERWENDUNG DER APP FÜR SMARTPHONES

Suchen Sie die Applikation **MyZeno** im Inneren des von Ihrem Smartphone verwendeten Stores (Play Store oder App Store).

Nehmen Sie die Installation vor und gestatten Sie dazu den Zugang zu den Bereichen Ihres Smartphones, die zur Verwaltung Ihres Zeno-Systems über die APP unerlässlich sind.

Öffnen Sie die Applikation, um die Installation auf Ihrem Smartphone abzuschließen.



Klicken Sie auf das soeben erstellte Symbol, um die Zugangsseite aufzurufen, in die das zuvor auf dem Portal registrierte Passwort eingegeben werden muss:

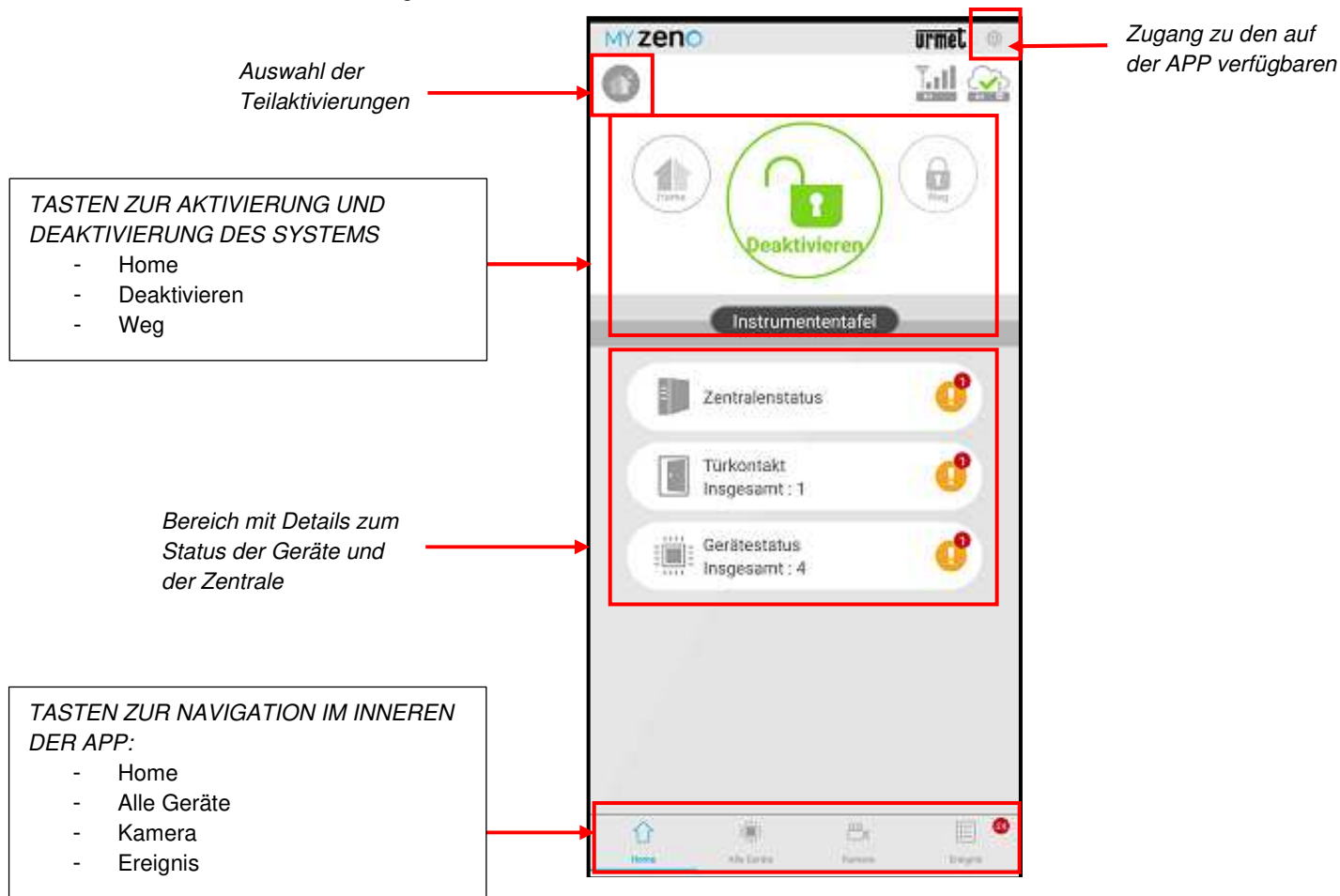
A screenshot of the MyZeno login interface. At the top, the 'urmet' logo is above the 'MY zeno' logo. Below this are two input fields: the first contains the username 'newzeno' and the second contains a masked password '*****'. There is a checked checkbox labeled 'Mich erinnern' and a link 'Passwort vergessen'. A large blue button labeled 'LOGIN' is below the inputs, followed by a button labeled 'Neuer Benutzer'. At the bottom, it says 'Copyright© 2018 Urmet' and 'Version 1.8.60'.

Wird die Funktion **Mich erinnern** aktiviert, ist es nicht mehr erforderlich, bei jeder Verwendung der App die Zugangsdaten einzugeben.

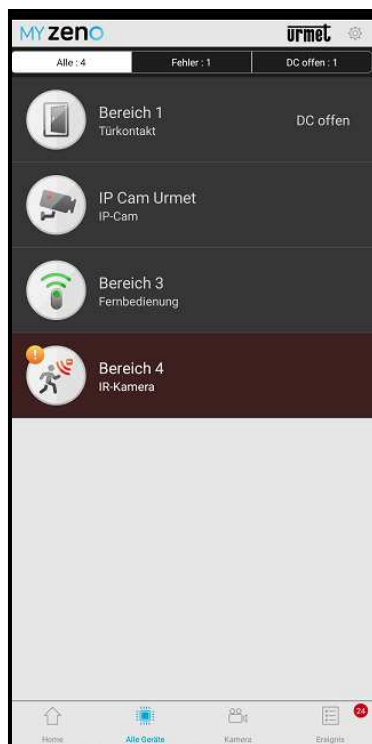
In dieser Seite kann die erste Registrierung vorgenommen werden. Der Vorgang ist dem für das Portal in Kapitel 4 dieses Handbuchs beschriebenen sehr ähnlich.

HAUPTANSICHT

Nachdem die registrierten Zugangsdaten eingegeben wurden, öffnet sich durch Anklicken der Taste **ZUGANG** die Hauptansicht, als Standard **Sicherheit**, die sich wie folgt zusammensetzt:

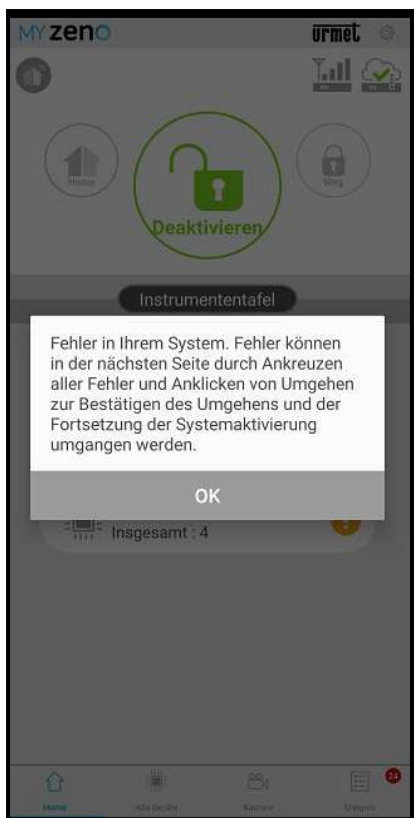


Durch Anklicken von **Alle Geräte** wird die Liste der in Ihrem System vorhandenen Geräte eingeblendet:



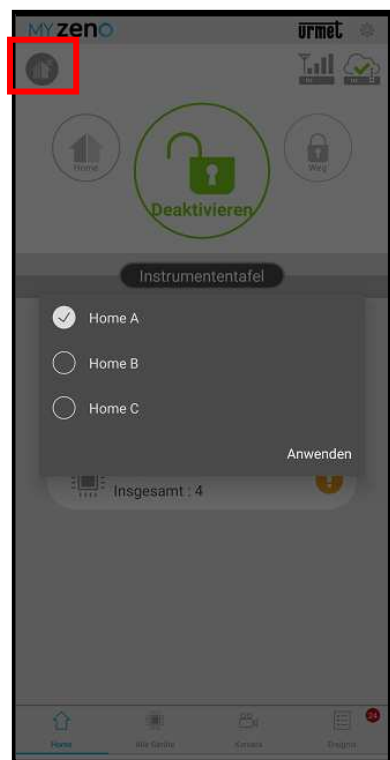
Liegen Melder mit Kamera oder Videokamera vor, kann in dieser Geräteliste ein Bild oder ein Video abgerufen werden. Durch Betätigen der entsprechenden seitlichen Taste wird der Abruf in der Liste der Ereignisse aufgezeichnet. Nach der erforderlichen Zeit für den Upload-/Download vom Server können die jeweiligen Medien eingeblendet werden.

Das Vorliegen von Fehlern wird in der Ansicht **Home** im **Bereich mit Details zum Status der Zentrale und der Geräte** angezeigt und mit einem Ausrufezeichen und einer Nummer hervorgehoben. Durch Anklicken erscheint eine zusammenfassende Beschreibung der erfassten Problematiken:



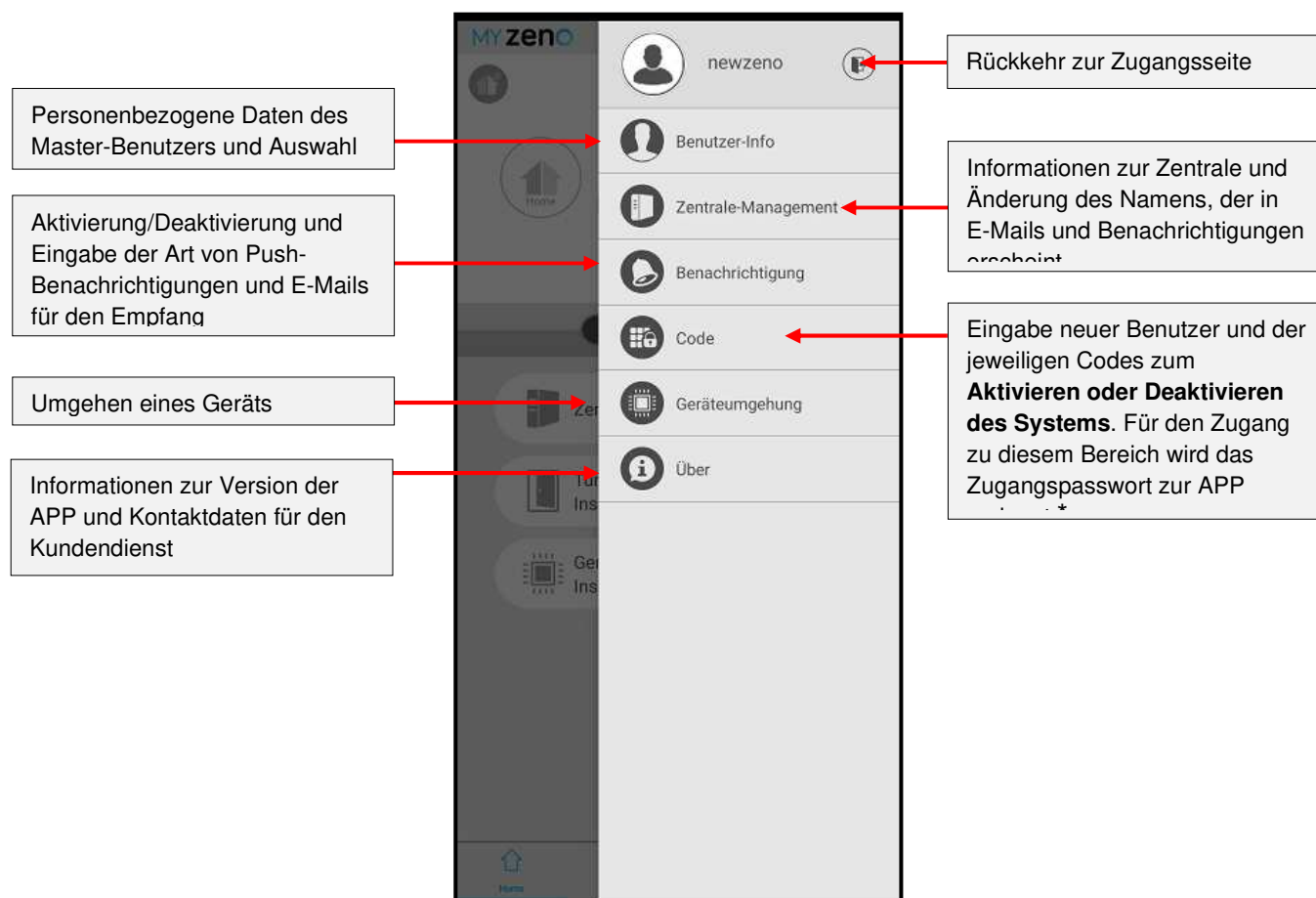
AUSWAHL DER TEILAKTIVIERUNGEN

Durch Anklicken der hervorgehobenen Taste oben links werden die drei im System **ZENO** verfügbaren Teilaktivierungen angezeigt. Es kann mehr als eine ausgewählt werden und durch Anklicken der Taste **Anwenden** wird die Auswahl in der Zentrale registriert. Wird anschließend die Taste **Weg** betätigt, werden nur der Sektor oder die Sektoren aktiviert, die in diesem Bereich ausgewählt sind.



ZUGRIFF AUF DIE VERFÜGBAREN FUNKTIONEN

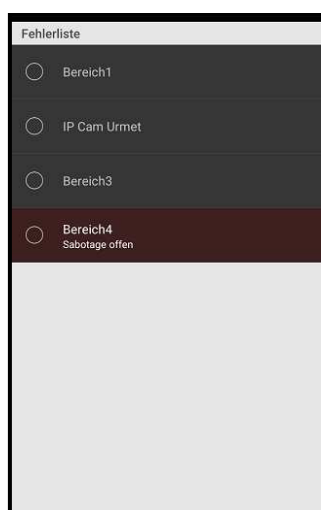
Durch Anklicken des Symbols oben rechts in jeder Ansicht wechselt man auf die Seite zur Verwaltung der verfügbaren Funktionen:



*** Die Verwendung der Werte 1111 und 7982 als Benutzercode ist nicht gestattet, da diese bereits vom System verwendet werden.**

BEREICH UMGEHUNGEN

Im Bereich der verfügbaren Funktionen den Menüpunkt **Geräteumgehung** auswählen. Das Umgehen deaktiviert eine Sicherheitsvorrichtung dauerhaft. Nachdem das zu umgehende Gerät ausgewählt wurde, wird dieses unmittelbar vom System ignoriert.



Eventuelle Situationen von entladener Batterie und unerlaubten Eingriffen werden weiter von dem umgangeenen Gerät gemeldet.

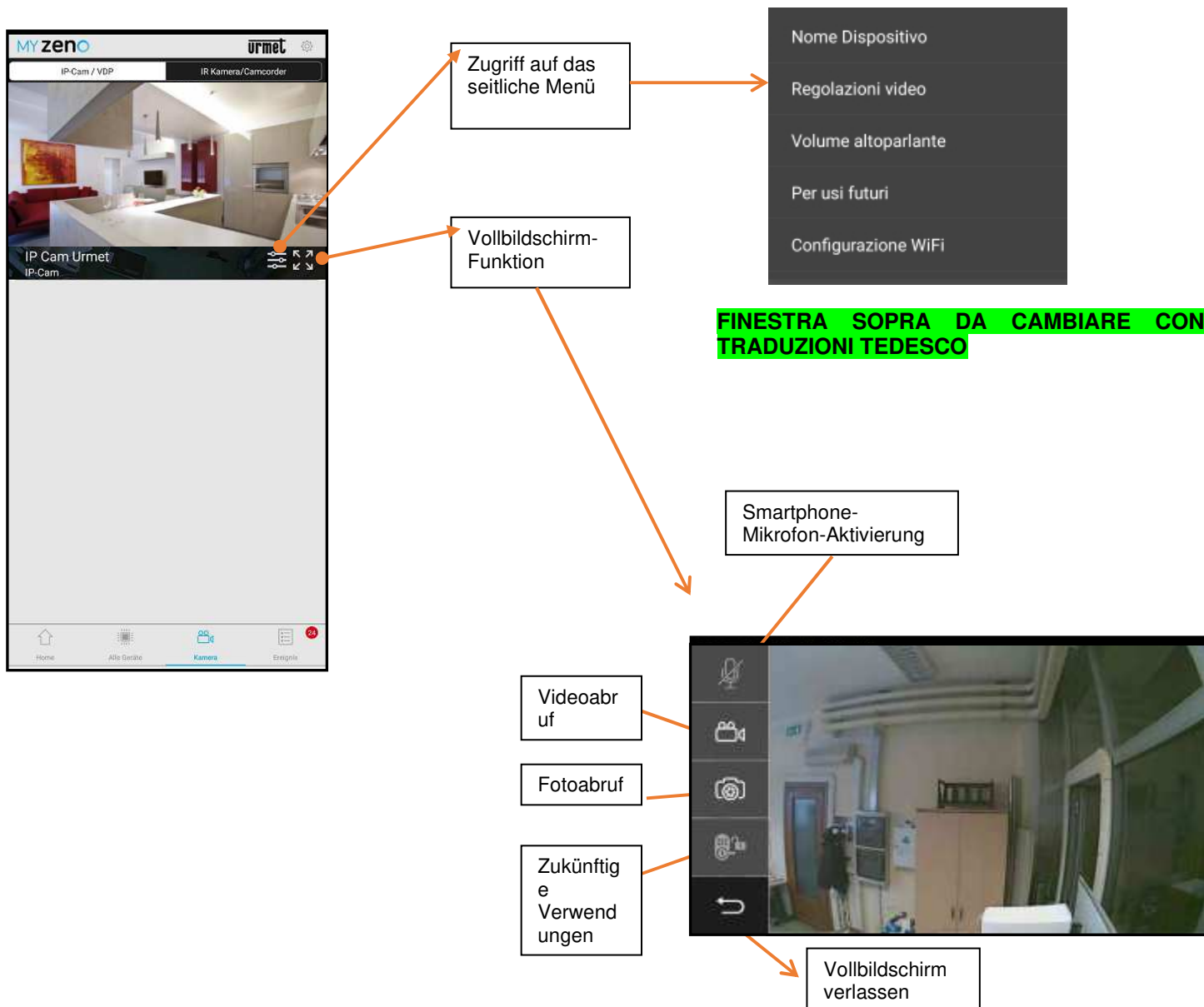
ACHTUNG! Was das Gerät „Sirene“ betrifft, deaktiviert die Umgehungsfunktion diese nicht vollständig, sondern unterbindet den Versand der Reports zu ihren Fehlern.

<HINWEIS>

Um ein Gerät erneut in das System einzubinden, muss die Kennzeichnung **Umgehung** vom Gerät entfernt werden. Es wird empfohlen, die APP zu verlassen und den Zugang erneut auszuführen, um korrekte Informationen zu dem wieder aktivierten Gerät zu erhalten.

MENÜ KAMERA

Dieses Menü wurde mit der Version **1.8.50 der APP von Android** und der Version **1.45 der APP von iOS** eingeführt. In diesem Bereich werden die Bilder aller Kameras und die Sensoren mit Fotos oder Videos angezeigt, die mit der Zentrale verknüpft sind. Unten wird im Einzelnen die Verwendung der Steuertasten in der Multi-Screen- oder Vollbildschirm-Konfiguration dargestellt.



10.1 TASTEN ZUM BEWEGEN IM INNEREN DER APP

Zum Bewegen zwischen den verschiedenen Bereichen im Inneren der APP stehen spezielle Tasten und Symbole zur Verfügung. Um zur vorigen Seite zurückzukehren, die Taste ZURÜCK des jeweiligen Smartphones verwenden.

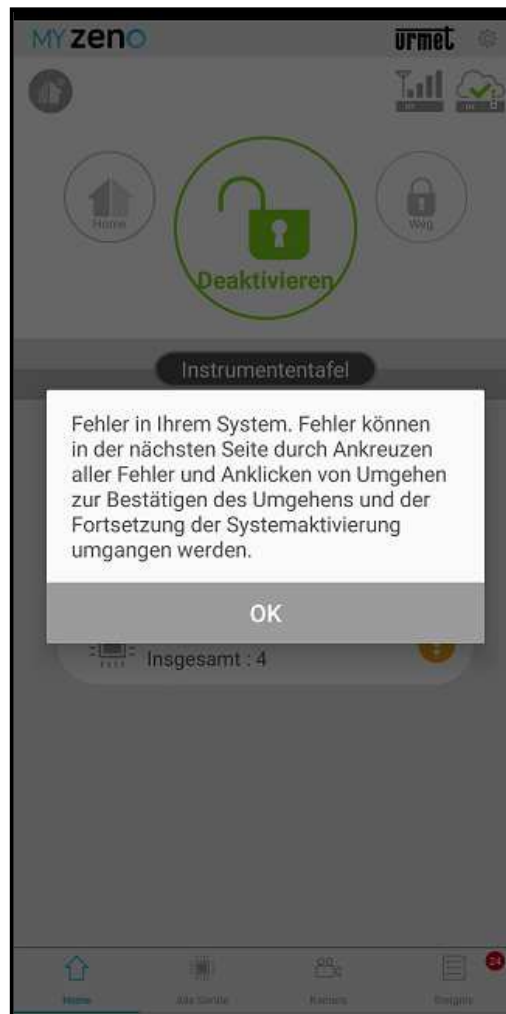
<HINWEIS>

☞ Im System Android die Funktionstaste ZURÜCK verwenden, um die virtuelle Tastatur zu verbergen.

11 ALLGEMEINE WARNHINWEISE ZUR VERWENDUNG VON PORTAL UND APP

11.1 AKTIVIERUNG MIT FEHLERN

Sollte das System im Moment der **Voll- oder Teilaktivierung** Fehler aufweisen, erscheint nach der Eingabe des Benutzer-PINs im Display die folgende Meldung:



Durch Betätigen der Taste Anwenden zum Fortsetzen der Aktivierung wird die Liste der im System vorliegenden Fehler eingeblendet. Um die Aktivierung abschließen zu können, müssen alle angekreuzt werden. Nur in diesem Fall ist die Taste Anwenden verfügbar und kann angeklickt werden.

Folgende Fehler können vorliegen:

- Der **Status geöffneter Kontakt**, zum Beispiel für ein Fenster, das nur angelehnt ist. Diese Informationen werden in der Liste der Geräte des Portals und der APP und im Bereich **Sicherheit** des Portals und der APP rot hervorgehoben.
- Der **Status der Geräte des Systems, an denen unerlaubte Eingriffe erfolgt sind** (Tamper-Alarme), bei **fast entladener Batterie**, außer Betrieb, usw. Auch diese Informationen sind rot hervorgehoben.
- Der Fehlerstatus der Zentrale sowie unerlaubte Eingriffe daran (Tamperalarm), der Ausfall des Stromnetzes und das Fehler der Datenverbindung (Internet oder 4G) sind Informationen, die nicht zu den Geräten gehören, sondern im Bereich **Sicherheit** zu finden sind

<HINWEIS>

Die Zentrale kann so konfiguriert werden, dass sie die Fehler während der Aktivierungen ignoriert. Dies kann auf zwei Arten erfolgen: 1) indem eine direkte Aktivierung vorgesehen wird (siehe „Systemparameter - Aktivieren mit Fehlern“ im Installationshandbuch der Zentrale); 2) durch Umgehen der Kontrolle jedes Fehlers (siehe „Info - Systemfehler“ im Installationshandbuch der Zentrale).

11.2 LANGSAME ODER KRITISCHE INTERNETVERBINDUNGEN

Im Fall von langsamen Internetverbindungen (zum Beispiel, wenn die verfügbare Verbindung nur in 3G oder mit GPRS erfolgt) ist es, sobald man sich im Portal oder der APP befindet, empfehlenswert, vor Eingriffen im System einige Sekunden abzuwarten, um es der Verbindung zu gestatten, sich zu stabilisieren.

Der Verbindungsstatus kann über das Symbol  überprüft werden, das in Absatz 6.3 dieses Handbuchs beschrieben wird.

11.3 EINGABE FALSCHER CODES

Nachdem fünf Mal nacheinander ein *falscher Benutzercode* auf dem Portal oder in die APP eingegeben wurde, wird das System gesperrt und bleibt ca. 9 Minuten lang in diesem Zustand. Während dieser Zeit ist es auch bei Eingabe des korrekten Codes nicht möglich, das System zu entsperren und die Tastatur ist nicht verwendbar. Das System kann den Status nur mittels Fernbedienung oder nach Ablauf der Sperrzeit ändern und zurückgesetzt werden.

In der Annahme, dass es sich bei der Wiederholung eines falschen Codes um einen betrügerischen Versuch handelt, wird aus Sicherheitsgründen sowohl auf der APP als auch auf dem Portal die Meldung FALSCHER CODE angezeigt und bei jeder nachfolgende Eingabe wird die Sperrzeit des Systems um weitere 9 Minuten verlängert. In der lokalen Steuertafel wird in der „Historie“ „Code blockiert“ aufgezeichnet.