HONEYWELL CONNECTED LIFE SAFETY SERVICES

CYBER SECURITY ÜBERSICHT

Version:1.0

Honeywell

INHALTS-VERZEICHNISS

ÜBER DIESES DOKUMENT

Dieses Dokument richtet sich in erster Linie an Honeywell Connected Life Safety Services (CLSS) Errichterfirmen, Systemintegratoren und Techniker, die daran interessiert sind, den von Honeywell verfolgten Ansatz zur Sicherung der CLSS-Lösung zu verstehen. Dieses Dokument enthält auch Details zur Sicherheitsarchitektur, zu Verfahren und Sicherheitskontrollen, die beschreiben, wie das CLSS-Gateway am Standort sicher konfiguriert werden kan

Haftungsausschluss:

EINFÜHRUNG IN CLSS

CLSS ist eine innovative All-in-One-Cloud-Plattform, die Systemintegratoren und Facility Manager in die Lage versetzt einen verbesserten Brandschutzservice zu bieten und gleichzeitig die Leistungseffizienz zu maximieren, die die bewährten Detektions- und Alarmsysteme von Honeywell bieten.

CLSS-GATEWAY

Der CLSS-Gateway dient als Schnittstelle zwischen der Brandmelderzentrale und der CLSS-Cloud-Plattform. Es bietet eine Möglichkeit, die Brandmelderzentrale vor Ort sicher mit der Cloud zu verbinden, und stellt durch einen einzigen Pfad vom Standort zur Cloud sicher, dass alle CLSS-Cloud-Dienste und -Anwendungen dieselbe geprüfte und überwachte Methode für den Zugriff auf das Netzwerk der Brandmelderzentrale vor Ort verwenden.

CLSS-WEB-APP (SITE MANAGER)

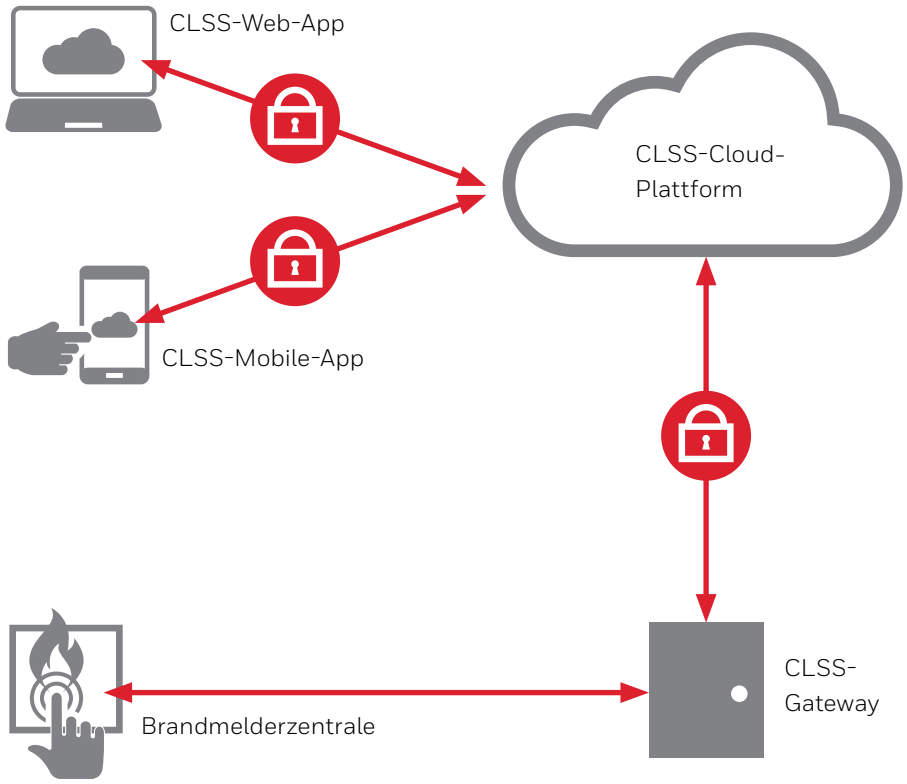
CLSS Site Manager ist eine Webanwendung, die von Errichterfirmen zur Durchführung von Administrativen- und Managementaktivitäten verwendet wird. Sie bietet eine konsolidierte Ansicht der Systeme ihrer Kunden. Sie ermöglicht den Errichtern die Integration von Gebäuden ihrer Kunden, ihrer Benutzer und Techniker sowie die Konfiguration von Zugriffsrechten für ihre Techniker.

CLSS-MOBILE -APP

Die CLSS-Mobile-App wird von Technikern verwendet, um das Gateway während der Installation zu konfigurieren und um regelmäßige Wartungen von angeschlossenen und nicht angeschlossenen Geräten durchzuführen. Die App wird auch zur Erstellung von regelkonformen Berichten verwendet.

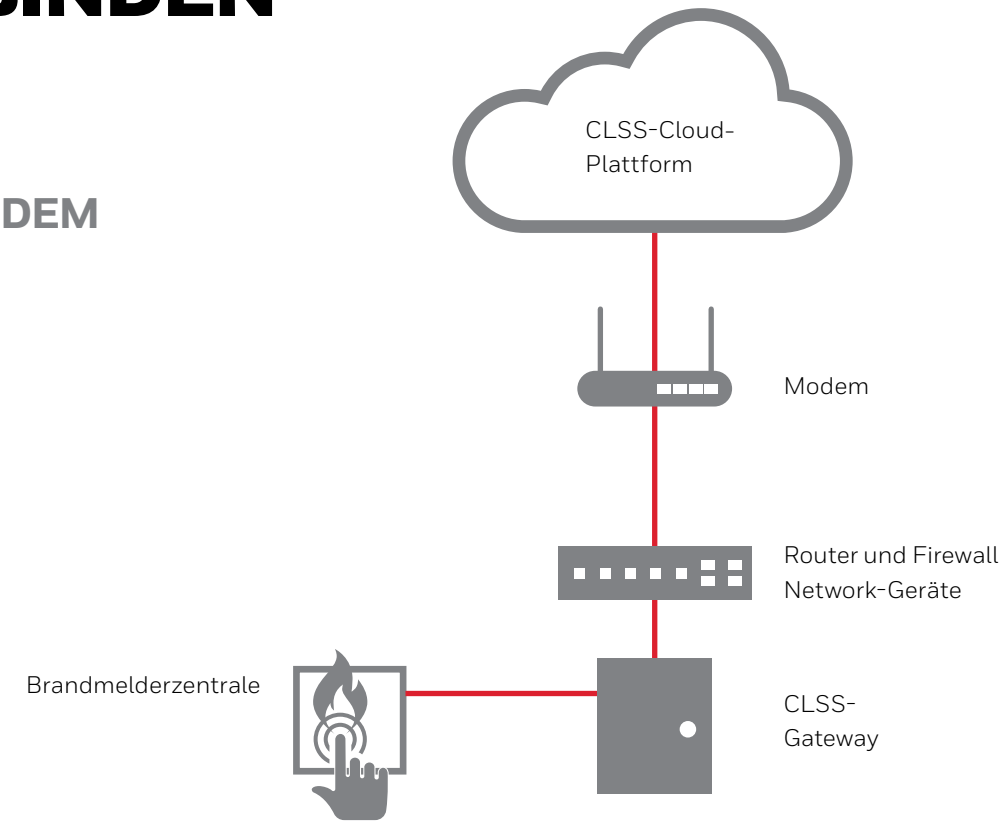
CLSS-CLOUD-PLATTFORM

Die CLSS-Cloud-Plattform enthält verschiedene Mikrodienste zur Unterstützung der Funktionalitäten von CLSS Gateway, mobiler App und Web-App. Sie ist sicher, skalierbar, standardisiert und basiert auf der Unternehmensmanagement-Plattform Honeywell Forge

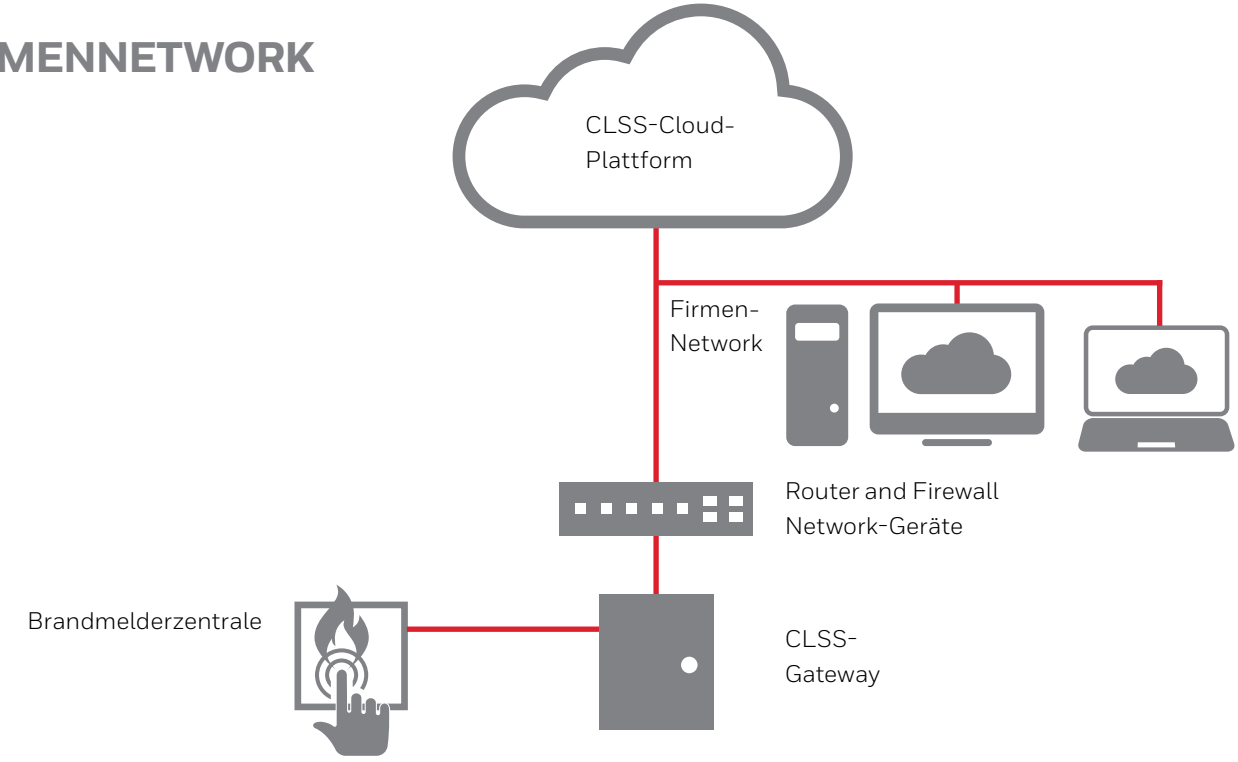


CLSS-GATEWAY MIT DER CLOUD VERBINDEN

ANSATZ 1
ÜBER MODEM



ANSATZ 2
ÜBER FIRMENNETWORK



WELCHE DATEN WERDEN VOM VOR-ORT-SYSTEM ZUR CLOUD ÜBERTRAGEN?

Zum Erreichen der CLSS-Mobile-App- und Web-App-Funktionalität (Inspection Manager und Site Manager) werden die folgenden Daten vom Vor-Ort-Gateway in die Cloud übertragen:

- Gerätedaten von der Brandmelderzentrale
- Ereignisse, Alarme und Störungen von der Brandmelderzentrale
- Vom Gateway generierte Ereignisse, Alarme und Störungen
- Gateway Audit-Protokolle mit Zeitstempel

Die Geräteübersicht enthält alle Geräte (z. B. Melder, Module, etc.) einschließlich der Brandmelderzentralen, die an das Netzwerk des Brandmeldesystems angeschlossen sind

SICHERUNG DER DATENÜBERTRAGUNG

Um die Oberfläche des Systems aus einer Sicherheitsperspektive zu verwalten, führt der CLSS Gateway Cloud Connector nur ausgehende Kommunikation aus und es wird keine eingehende Kommunikation akzeptiert. Die hergestellten ausgehenden Verbindungen sind auf HTTPS für die Initiierung der Kommunikation und dann AMQP über HTTPS für das Messaging mit TLS1.2 und höherer Verschlüsselung beschränkt. AMQP ist ein OASIS-Standard-Messaging-Protokoll, das für zuverlässiges und robustes Messaging entwickelt wurde und sich gut für Szenarien eignet, in denen die Bestätigung von Befehlen und die Datenübertragung erforderlich ist. Zwischen dem Gateway vor Ort und der CLSS-Cloud-Plattform wird eine zertifikatsbasierte Authentifizierung verwendet.

INFRASTRUKTURBEDARF FÜR DIE DATENÜBERTRAGUNG

Die Cloud-Verbindung vom CLSS-Gateway kann mit Standard-Sicherheits-Anwendungen realisiert werden. Das CLSS-Gateway verwendet nur ausgehende Kommunikation mit HTTPS/TLS-Verschlüsselung. Die detaillierten Anforderungen sind:

Eingehender (In) Port: Ein eingehender Port ist ein Port, über den ein anderer Computer eine Verbindung zum Gateway herstellt, um auf die Gateway-Funktionalität zuzugreifen; d.h. eine Anwendung auf dem Gateway lauscht aktiv auf diesem Port für Client-Verbindungen.

Ausgehender (Out) Port: Das Gateway verwendet ausgehende Ports für die Verbindung mit dem Internet/der CLSS-Cloud-Plattform, d. h. die Dienste in der Cloud lauschen auf diesen Ports und warten auf eine Verbindung des Gateways.

Standardmäßig werden alle ein- und ausgehenden Verbindungen blockiert und nur die in der folgenden Tabelle aufgeführten Ports zugelassen:

PORTNUMMER	TYPE	IN / OUT	ZWECK / NOTIZ
443	TCP	Aus	Https-Kommunikation zur CLSS-Cloud-Plattform
53	UDP	Aus	DNS-Client zu Server-Lookup
2020	TCP	Aus	Alarmübertragung

Im Folgenden finden Sie eine Liste der Endpunkte für die Kommunikation mit der CLSS-Cloud-Plattform:

REGION	ENDPUNKTE
Global	https://gaprodpkisystemauthenticationv2.sentience.honeywell.com/ https://gaprodregui.sentience.honeywell.com/ https://sentgaprod.blob.core.windows.net
Europe	https://t02aprodfileupload.sentience.honeywell.com/ https://sentt02aprodfu.blob.core.windows.net https://sentt02aprodv2.azure-devices.net/ https://t02aprodcloudapp.sentience.honeywel.com
US	https://t01aprodfileupload.sentience.honeywell.com/ https://sentt01aprodfu.blob.core.windows.net https://sentt01aprodv2.azure-devices.net/ https://t01aprodcloudapp.sentience.honeywell.com
Alarmübertragung US	https://honprodeast.rrmsalarm.com https://honprodwest.rrmsalarm.com

SICHERES BOOTEN UND SICHERES FIRMWARE-UPGRADE

Secure Boot ist der Prozess der Validierung der Firmware-Signatur vor dem Ausführen der Firmware. **Sicheres Firmware-Upgrade** ist der Prozess der Validierung neuer Firmware vor dem Ersetzen der aktuell laufenden Version. **Firmware-Signierung** ist ein Prozess zur Berechnung der digitalen Signatur der Firmware während des Firmware-Erstellung-Prozesses und stellt sicher, dass er nicht unbemerkt verändert werden kann.

Honeywell veröffentlicht in regelmäßigen Abständen Sicherheits-Hotfixes und Upgrade-Pakete für die Firmware des Gateways. Die freigegebenen Pakete sind verschlüsselt und von Honeywell digital signiert, um die Vertraulichkeit, Integrität und Authentizität des freigegebenen Pakets zu gewährleisten (d. h., das Paket stammt von Honeywell). Das Gateway verifiziert die Signatur während des sicheren Boot- und Firmware-Upgrade-Prozesses.

Sensible Details wie private Geräteschlüssel werden über Sicherheitschips gemäß den allgemein anerkannten Praktiken und Empfehlungen der Sicherheitsindustrie verwaltet.

CLSS-MOBILE-APP UND CLOUD-PLATTFORM

CLSS-MOBILE-APP

Kommunikation zwischen Mobilgerät und Cloud
Die gesamte Kommunikation aus dem Mobiltelefon zur CLSS-Cloud-Plattform erfolgt über HTTPS mit TLS 1.2 verschlüsseltem Tunnel.

Kommunikation zwischen Mobiltelefon und Gateway
Die Mobile App verwendet für die Konfiguration des CLSS-Gateways eine Secure BLE Link-Verbindung. Die BLE-Verbindung funktioniert nur, wenn sich der Benutzer in der Nähe des Gateways befindet. Die für die Kopplung mit dem CLSS-Gateway erforderlichen Sicherheitsschlüssel sind nur für autorisierte Techniker über die Cloud-Plattform zugänglich.

Daten, die über die CLSS-Mobile-App gespeichert und ausgetauscht werden
Für die Anwendungsfälle des Wartungsmanagements tauscht die mobile App Details mit der CLSS-Cloud-Plattform für die Gateway-Konfiguration aus. Die Daten werden nicht auf dem mobilen Gerät dauerhaft gespeichert. Sie dienen nur zur vorübergehenden Verwendung und die Details werden aus der App-Speicherdatenbank gelöscht, wenn die Daten mit der Cloud synchronisiert werden.

CLSS-CLOUD-PLATTFORM

Die cloudbasierte Bereitstellung wird gemäß Honeywells einheitlichem Konformitäts-Regelwerk verwaltet, das mit den wichtigsten IT-Sicherheits-Frameworks einschließlich NIST SP 800-171 und ISO 27001 abgestimmt wurden.

Datenkommunikation innerhalb der Cloud
Die gesamte interne Kommunikation zwischen verschiedenen Cloud-Diensten verwendet HTTPS für Integrität und Vertraulichkeit innerhalb der Cloud.

Sicherheitsmaßnahmen für die Cloud-Infrastruktur

- Starke Anmelde- und passwortbasierte Authentifizierung wird für mobile und Web-Apps verwendet.
- Durchsetzung rollenbasierter Berechtigungen zum Zugriff auf unterschiedliche Daten.
- Die Firewall in der Perimetersicherheit wird durch IPS/ IDS und Paketinspektion gewährleistet.
- WAF (Web Application Firewall) ist für CLSS-Anwendungen aktiviert.
- WAFs bieten Schutz vor Cyber-Attacken wie SQL-Injektionen, Cross-Site-Scripting, Malware-Uploads, Anwendungs-DDoS usw.
- Sensible Daten wie Sicherheits-Tokens und kryptografische Schlüssel werden über **Azure Key Vault** verwaltet. Azure Key Vault bietet FIPS 140-2 Level 2 validierte Hardware-Sicherheitsmodule (HSM) zum Speichern der sensiblen Daten.
- Die Sicherheit aller Server wird über virtuelle Netzwerke und virtuelle Server segmentiert
- Alle virtuellen Maschinen der CLSS-Cloud sind mit Anti-Malware geschützt.
- Standardprozess zur regelmäßigen Anwendung von Sicherheits-Patches mit Bestimmungen für risikobasierte Expedits.
- Auf Anwendungsebene wird eine starke Authentifizierung und Autorisierung verwendet, um den Zugriff auf Anwendungsdaten einzuschränken.
- Der Zugriff auf die Systemverwaltungsebene ist auf das autorisierte Betriebsteam von Honeywell Digital beschränkt. Regelmäßige Backups werden getroffen, um das System im Falle eines versehentlichen Verlusts wieder in den Normalzustand zu versetzen. Im Ruhezustand werden alle Daten mit SSE (Solid State Encryption) verschlüsselt.
- Die CLSS Cloud Platform nutzt Honeywell Forge und wird in der Microsoft Azure Cloud gehostet. Die Honeywell Forge-Plattform ist nach SOC2 Typ 1 auditiert. Microsoft Azure Cloud ist zertifiziert mit: SOC1 Typ2, SOC2 Typ2, ISO27001. Für eine vollständige Liste besuchen Sie bitte **hier**.

PERSÖNLICHE DATEN

Login und Passwörter und andere persönliche Daten werden im Active Directory in verschlüsselter Form verwaltet. Personenbezogene Daten werden gemäß der GDPR-Vorschriften und den Datenschutzstandards von Honeywell geschützt. Honeywell beschränkt die gesammelten und verarbeiteten personenbezogenen Daten auf das Minimum, das notwendig ist, um den rechtmäßigen Geschäftszweck zu erfüllen.

ANSATZ ZUR CYBERSICHERHEIT IN DER PRODUKTENTWICKLUNG

Jede Software sollte Best Practices (bewährte Praxis) für Cybersicherheit und Datenschutz enthalten, um das Auftreten von Cybersicherheits-problemen zu minimieren. Deshalb sind wir der Meinung, dass Sicherheit und Datenschutz bereits zu Beginn des Produktentwicklungsprozesses berücksichtigt werden sollten.

Die Produkte von Honeywell Building Technologies werden strengen Sicherheitsüberprüfungen und -tests unterzogen, bevor sie zur Freigabe freigegeben werden, unabhängig davon, wo sie hergestellt werden. Unsere Produkte werden anhand unserer Cyber-Standards bewertet und bedürfen der Genehmigung durch unseren Chief Technical Officer als Teil unseres Standardprozesses zur Einführung neuer Produkte.

Honeywell folgt dem BSIMM-Framework (Building Security In Maturity Model) und gewährleistet Standards und Anforderungen für den sicheren Entwicklungslebenszyklus von Produkten.

Die CLSS-Plattform integriert Sicherheitsüberlegungen in alle Aspekte der Entwicklung, der Bereitstellung und des Risikomanagements. Das System wurde unter Verwendung des Secure Software Development Lifecycle (SSDLC) von Honeywell entwickelt, der Sicherheitsüberlegungen in folgende Bereiche integriert - alle Phasen von den Anforderungen bis zum Testen der Bereitstellung und des laufenden Betriebs. Die Systementwicklung umfasst alle Aspekte von der Ableitung der Anforderungen aus den Standards ANSI/ISA 62443 und Best Practices, der sicheren Architektur und dem Design über die architektonische Risikoanalyse, die Bedrohungsmodellierung, sichere Codierungsrichtlinien sowie die statische und dynamische Codeanalyse bis hin zu Sicherheitstests mit manuellen und automatisierten Ansätzen.

Die gesamte CLSS-Plattform wird von Honeywell entwickelt und der Quellcode wird gemäß den Honeywell-Richtlinien zur Quellcodeverwaltung verwaltet. Es werden Code-Reviews durchgeführt, um Sicherheitslücken im Quellcode zu erkennen.

Die im Produkt verwendeten Open-Source-Bibliotheken haben eine Sicherheitsüberprüfung durchlaufen,

gemäß der Honeywell-Standardpraxis.

Statische Code-Analyse und Binär-Scan-Tools sind in die CI/CD-Pipeline (Continuous Integration/ Continuous Delivery) integriert und

ausgeführt, wenn jeder Build erzeugt wird. Die Sicherheitsrisiken werden aufgezeichnet in

JIRA-Tools mit CVSS-Scoring und Behebung nach vereinbarten Plänen zu einem vorgegebenen Zeitplan auf Basis des Schweregrads.

Penetrationstests und Ereignisse zur Testauslösung

Penetrationstests werden vor jeder größeren Veröffentlichung und vor der Bereitstellung einer neuen Version von Cloud-Diensten in der Produktionsumgebung durchgeführt. Das Team führt Penetrationstests von Anwendungen durch, basierend auf identifizierte Schwachstellen und diese werden nach der Behebung erneut getestet, um die Korrekturen zu überprüfen. Befunde werden protokolliert und zur Schließung verfolgt.

Die Produktanwendungen werden gemäß dem aktuellen OWASP-Testleitfaden und die zugrunde liegende Produktinfrastruktur gemäß den Richtlinien von NIST 800-115 bewertet.

HONEYWELL SUPPORT UND DEVOPS PROZESS

Das gesamte System wird von einem 24/7-Supportteam verwaltet, das sowohl die Infrastruktur als auch die Anwendungen überwacht. Es gibt detaillierte interne Richtlinien, die regeln, wie wir Sicherheits- und Datenschutzvorfälle erkennen, untersuchen und darauf reagieren.

Honeywell verwendet verschiedene Anwendungsdiagnosetools für verschiedene Teile des Systems, um den Systemzustand zu überwachen. Wir verfolgen den Systemzustand und jede Abweichung löst automatisch eine Warnung aus (z. B. CPU-Auslastung, Speichernutzung, Festplatten-IO-Vorgänge).

WIE SIE EINE SICHERHEITSLÜCKE MELDEN

Honeywell verfügt über ein Product Security Incident Response Team (PSIRT) zur Überwachung und Vorfälle zu managen und das Risiko der Kunden im Zusammenhang mit Sicherheitslücken zu minimieren, indem wir rechtzeitig Informationen, Anleitungen und Abhilfemaßnahmen für Schwachstellen in unseren Produkten bereitstellen.

Klicken Sie **hier**, um mehr über den Honeywell PSIRT-Prozess zu erfahren. Um eine potenzielle Sicherheitslücke bei einem Honeywell-Produkt zu melden, folgen Sie bitte den Anweisungen **hier**.

Novar GmbH a Honeywell Company
Forumstraße 30
D-41468 Neuss
www.esser-systems.com

Honeywell Life Safety Austria GmbH
Technologiestrasse 5,
AT-1120 Wien
www.hls-austria.com

HW-WP-CLSSCyberSec | DE | 03/2021

THE
FUTURE
IS
WHAT
WE
MAKE IT

Honeywell