

# KOMPETENZZENTRUM CyberProtect

EIN QUICK-CHECK DES KOMPETENZZENTRUMS CyberProtect



Quelle: Phönix Design

## IT-SICHERHEITSANALYSE CARE-O-BOT® ARCHITEKTUR

### KONTAKT



#### Fraunhofer IOSB

Erik Krempel

erik.krempel@iosb.fraunhofer.de

#### FZI Forschungszentrum Informatik

Niklas Goerke

goerke@fzi.de



### IN ZUSAMMENARBEIT MIT



Mojin Robotics GmbH

Florian Weißhardt

info@mojin-robotics.de

### Ausgangssituation und Problem

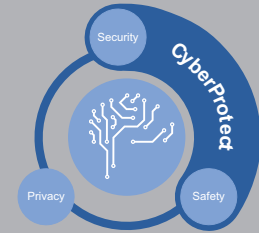
Die Firma Mojin Robotics GmbH bietet mit dem Care-O-bot® eine Roboterplattform für den flexiblen Einsatz in beispielsweise Haushalt, Hotel oder Healthcare an. Der Roboter wird auf die individuellen Anforderungen des Kunden angepasst und übernimmt verschiedene Aufgaben wie Lotsenfunktion, Verkaufsassistenten oder Concierge-Service. Um diese Aufgaben übernehmen zu können, benötigt er ein umfangreiches Backend für Zugriff auf verschiedene Dienste wie Navigation, Produktdatenbank oder Dialogsysteme. Die dafür gebaute Architektur vernetzt die internen Systeme des Roboters mit dem Netz von Mojin Robotics, den Systemen des Kunden und dem Internet. Die benötigte Komplexität der Architektur und Verteilung der einzelnen Komponenten bergen das Risiko, dass nicht erkannte Schwachstellen sich auf das gesamte System auswirken können. Deshalb soll eine

umfassende Analyse der IT-Sicherheit der Architektur vorgenommen werden.

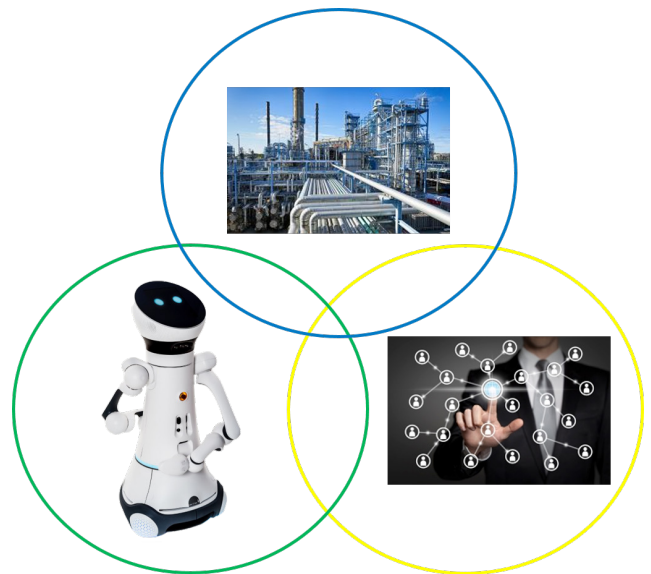
### Lösungsansatz

Zur Analyse der IT-Sicherheit der Architektur wurde ein Workshop zwischen Mojin Robotics und den Experten des Projekts CyberProtect durchgeführt. In diesem wurden zuerst die aktuelle Architektur und die umgesetzten IT-Sicherheitsmaßnahmen besprochen. Danach begann die eigentliche Analyse. Die Architektur wurde dazu in verschiedene Zonen eingeteilt und für jede Zone untersucht, welcher Angreifer hier realistisch betrachtet werden muss. Beispielsweise ist es für die Zone des Roboters wichtig zu betrachten, welche Angriffe durch einen direkten physischen Zugriff am Roboter möglich sind. Solche Angriffe müssen für Dienste, die in einem geschützten Rechenzentrum laufen, nicht beachtet werden. Im nächsten Schritt wurde untersucht, welche Verbindungen es zwischen den Zonen gibt und ob Angreifer

# IT-SICHERHEITSANALYSE CARE-O-BOT® ARCHITEKTUR



EIN QUICK-CHECK DES KOMPETENZZENTRUMS CyberProtect



Quelle: Phönix Design

sich zwischen den Zonen bewegen können und wie dies ggf. verhindert werden kann.

## Nutzen

Im Rahmen der Analyse konnten bis dahin unentdeckte Schwachstellen identifiziert werden. Für diese wurden gemeinsam Maßnahmen entwickelt, die für die kritischen Schwachstellen auch bereits umgesetzt sind. Zusätzlich zur Untersuchung auf konkrete technische Schwachstellen wurde vor allem über die Architektur und dort konzeptionelle Stärken und Schwächen sowie kritische Stellen identifiziert, auf die besonderes Augenmerk gelegt werden sollte. Durch die Zusammenarbeit zwischen den Mitarbeitern der Mojin Robotics GmbH und den Fachexperten konnte auch ein Wissenstransfer erfolgen. Dies vereinfacht es für die Mitarbeiter der Mojin Robotics GmbH, bei der Weiterentwicklung des Produkts besonderes Augenmerk auf die kritischen Abschnitte der Architektur zu legen und methodischer

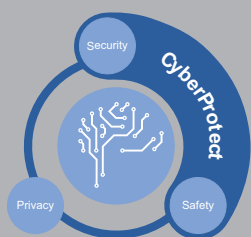
die Anforderungen an die IT-Sicherheit der einzelnen Komponenten zu prüfen und ggf. auch selbst potentielle Schwachstellen zu erkennen. Dies ist insbesondere relevant, da das Produkt auch in absehbarer Zeit noch flexibel weiterentwickelt wird und somit auch mit größeren Änderungen an der Architektur zu rechnen ist.

## Projektergebnisse

Die Firma Mojin Robotics GmbH hat im Rahmen des Projekts eine umfangreiche Analyse der IT-Sicherheit ihrer Architektur erhalten. Der Großteil der Analyse erfolgte in einem mehrstündigen Workshop gemeinsam mit Mitarbeitern von Mojin Robotics, sodass auch ein Wissenstransfer stattfand. Dieser vereinfacht es Mojin Robotics bei der Weiterentwicklung ihrer Produkte, potentielle Schwachstellen frühzeitig selbst zu erkennen.

Auch der Analysebericht kann bei späteren Anpassungen oder regelmäßigen Prüfungen

als Vorlage für einen Abgleich genutzt werden. Änderungen zur im Bericht beschriebenen Situation sollten dann einer erneuten Untersuchung der IT-Sicherheit unterzogen werden. Die definierten Maßnahmen zur Reduktion der Risiken sind ein weiteres wichtiges Ergebnis des Projekts. Hier werden konkrete Änderungen zur Verbesserung der IT-Sicherheit vorgestellt. Weiter wurden für einige zukünftig anstehende Entwicklungen bereits Best Practices aufbereitet.



# KOMPETENZZENTRUM CyberProtect

EIN QUICK-CHECK DES KOMPETENZZENTRUMS CyberProtect



Forschungszentrum Informatik FZI



**Fraunhofer**  
IOSB

Fraunhofer-Institut für Optronik,  
Systemtechnik und Bildauswertung



**Fraunhofer**  
IPA

Fraunhofer-Institut für Produktions-  
technik und Automatisierung

Gefördert durch:



**Baden-Württemberg**

MINISTERIUM FÜR WIRTSCHAFT, ARBEIT UND WOHNUNGSBAU

Ministerium für Wirtschaft, Arbeit und  
Wohnungsbau

Ansprechpartner

**Dr.-Ing. Arne Rönnau**

Telefon 0721 9654-228

roennau@fzi.de

**Dr.-Ing. Erik Krempel**

Telefon 0721 6091-292

erik.krempel@iosb.fraunhofer.de

**Dipl.-Wi.-Ing. Ramez Awad**

Telefon 0711 970-1844

ramez.awad@ipa.fraunhofer.de

## ÜBER DAS KOMPETENZZENTRUM CyberProtect

Das durch das Ministerium für Wirtschaft, Arbeit und Wohnungsbau Baden-Württemberg geförderte Projekt CyberProtect verfolgt im Sinne der Stärkung von Firmen in Baden-Württemberg das Ziel der besseren Absicherung von komplexen Softwaresystemen. Dabei werden alle drei Bereiche von Sicherheit (Security, Safety und Privacy) betrachtet, der Fokus liegt hierbei auf dem Teilgebiet der Security. Im Rahmen des Projektes werden hierfür Methoden entwickelt, um das Verhalten bzw. die Entscheidungen von komplexen Softwaresystemen z.B. von KI-Systemen sichtbar zu machen und somit Aussagen über den Sicherheitszustand der Systeme zu ermöglichen. Über ein weitreichendes Angebot wie Quick-Checks, Schulungen und Open Lab Days werden Firmen in das Projekt einbezogen, um ihnen die Möglichkeit zu bieten, ihre komplexe Software auf Sicherheit untersuchen und ggf. verbessern zu lassen.

### Bereit für Ihre Anwendung

Quick-Checks sind ein kostenloses, individuelles Angebot hinsichtlich Sicherheit in der Produktion für Firmen aus Baden-Württemberg. In diesen Quick-Checks werden mit ausgewählten Unternehmen die Themen Safety, Security und Privacy bearbeitet. Die Ergebnisse aller Quick-Checks werden als Steckbriefe im Webauftritt des Kompetenzzentrums CyberProtect ([www.cyberprotect-bw.de](http://www.cyberprotect-bw.de)) veröffentlicht.