# KOMPETENZZENTRUM CyberProtect

EIN QUICK-CHECK DES KOMPETENZZENTRUMS CyberProtect

# SICHERHEITSANALYSE


KONTAKT

Fraunhofer IOSB

**Fraunhofer IOSB**
Anne Borcherding
anne.borcherding@iosb.fraunhofer.de

Christian Haas
christian.haas@iosb.fraunhofer.de

**IN ZUSAMMENARBEIT MIT**

SICK
Sensor Intelligence.

SICK AG
info@sick.de

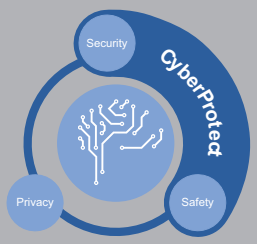

## Ausgangssituation und Problem

Der thermische Durchflussmesser FTMg der SICK AG mit seinen vielfältigen Industrie-4.0-Schnittstellen wie ein Webserver, MQTT und OPC-UA wurde in diesem Quick-Check analysiert. In der Zukunft werden immer mehr industrielle Automatisierungs- und Steuerungskomponenten hochgradig vernetzt sein und hauptsächlich auf Ethernet-Technologien basieren. Viele der angebotenen Zusatzfunktionen wie beispielsweise ein Webserver, der die Konfiguration der Komponente erleichtert, bieten mögliche Einfallstore für einen Angreifer. Bei der frühzeitigen Erkennung von Schwachstellen können verschiedene moderne Verwundbarkeitsscanner hilfreich sein. Im Rahmen dieses Quick-Checks sollen verschiedene Verwundbarkeitsscanner verwendet werden, um eine konkrete, industrielle Komponente auf Schwachstellen zu untersuchen. Der Fokus soll hier auf der Webanwendung liegen. So können zum einen Schwachstellen in der Komponente aufgedeckt werden und zum anderen kann die Performanz der verschiedenen Verwundbarkeitsscanner an realen Komponenten weiter untersucht werden. Die automatisierten Untersuchungen werden durch eine manuelle Untersuchung ergänzt, um mögliche weitere Schwachstellen aufzudecken.

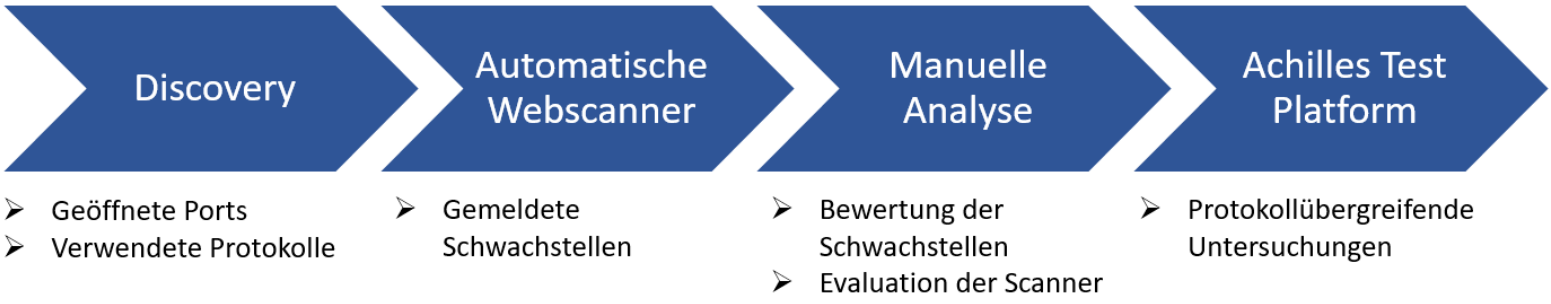
## Lösungsansatz

Zunächst wird in einer Discovery-Phase ein sogenannter Portscanner eingesetzt, um geöffnete Ports des zu untersuchenden Geräts aufzudecken. Im Anschluss werden sechs verschiedene Web-Verwundbarkeitsscanner eingesetzt, um die Webanwendung automatisiert auf Schwachstellen zu überprüfen. Die gemeldeten Ergebnisse der Web-Verwundbarkeitsscanner werden anschließend manuell überprüft und durch weitere manuelle Analysen ergänzt. Zusätzlich zu den spezialisierten Untersuchungen

# SICHERHEITSANALYSE




**EIN QUICK-CHECK DES KOMPETENZZENTRUMS CyberProtect**



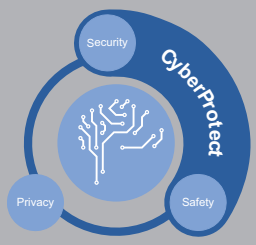

der Webanwendung wird die Komponente protokollübergreifend durch eine Untersuchung durch die Achilles Test Platform auf Schwachstellen überprüft. Die Ergebnisse der Untersuchungen werden in einem Abschlussbericht zusammengefasst.

**Nutzen**

Analog zu den zwei Zielen des Quick-Checks kann auch der Nutzen in zwei Bereiche eingeteilt werden. Zunächst hilft die Untersuchung der Komponente dabei, einen Überblick über den aktuellen Sicherheitsstand der Komponente zu erhalten. Die Ergebnisse des Quick-Checks können dafür verwendet werden, die Komponente weiterzuentwickeln und die Sicherheit weiter zu verbessern. Außerdem konnten durch die Anwendung der verschiedenen Web-Verwundbarkeitsscanner vertiefende Ergebnisse bezüglich deren Performanz erreicht werden. Diese Ergebnisse und die dabei gesammelten Erfahrungen werden in das IT-Sicherheitslabor am Fraunhofer IOSB einfließen. So werden die Ergebnisse dieses Quick-Checks auch in weiteren Untersuchungen und Analysen verwendet und können diese effizienter und effektiver machen.

**Projektergebnisse**

Die Evaluation der Web-Verwundbarkeitsscanner konnte bisherige Erfahrungen bestätigen. Zum einen konnte sie zeigen, dass Web-Verwundbarkeitsscanner teilweise Falsch-Positive erzeugen, wenn eine Webanwendung Inhalt anzeigt, der ständig aktualisiert wird. Wie auch bereits in anderen Untersuchungen, konnten die verwendeten kommerziellen Verwundbarkeitsscanner kein signifikant besseres Ergebnis liefern als quelloffene Verwundbarkeitsscanner.
Entgegen bisherigen Erfahrungen zeigte sich allerdings auch, dass in dem Fall der untersuchten Komponente bereits drei der sechs verwendeten Web-Verwundbarkeitsscanner alle Meldungen abdeckten. In anderen Untersuchungen, die im Rahmen des IT-Sicherheitslabors durchgeführt wurden, konnte jeder Web-Verwundbarkeitsscanner eine einzigartige Meldung vorweisen, die von keinem anderen Web-Verwundbarkeitsscanner gemeldet wurde. Diese Ergebnisse werden in den weiteren Ausbau des IT-Sicherheitslabors einfließen.




# KOMPETENZZENTRUM CyberProtect

EIN QUICK-CHECK DES KOMPETENZZENTRUMS CyberProtect

FZI Forschungszentrum Informatik

Fraunhofer IOSB

Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung

Fraunhofer IPA

Fraunhofer-Institut für Produktionstechnik 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) veröffentlicht.