

Das Prüflabor für Industrial Security deckt Sicherheitslücken auf

Key Facts

- Sicherheitslücken in Industriesteuerungen werden zunehmend ausgenutzt, um die Systeme anzugreifen
- Das Labor für Industrial Security des Instituts für Arbeitsschutz der DGUV (IFA) führt Unfalluntersuchungen für Unfallversicherungsträger durch
- Produktprüfungen nach den neuen, erweiterten DGUV Test-Prüfgrundsätzen für Industrial Security haben für Hersteller einen großen Mehrwert

Autor

➔ Jonas Stein

Gefährliche Angriffe auf Industriesteuerungen nehmen zu und stellen die Unfallversicherungsträger und ihre Mitgliedsunternehmen vor neue Herausforderungen. Das Prüflabor für Industrial Security am Institut für Arbeitsschutz der DGUV (IFA) prüft daher Produkte auf Sicherheitslücken, unterstützt in der Prävention und begleitet Unfalluntersuchungen durch IT-Forensik.

Das neue Labor für Industrial Security im IFA ist in der Lage, Aufträge aus drei wesentlichen Bereichen des Arbeitsschutzes auszuführen:

- Prävention
- Prüfung und Zertifizierung
- Unfalluntersuchung

Präventionsarbeit

Im Rahmen von Abschlussarbeiten und Forschungsprojekten werden prototypische Sicherheitslücken im Industrieumfeld untersucht und dazu passende Lösungen ausgearbeitet. So beschäftigte sich ein Forschungsprojekt damit, wie die Datenübertragung zwischen zwei fehlersicheren Industriesteuerungen über ein fremdes Netzwerk geschützt werden kann. Eine besonders vielversprechende Lösung, die auch auf sehr rechenschwachen Systemen herstellerübergreifend funktioniert und zudem leicht zu validieren ist, wurde bereits realisiert und Belastungstests unterzogen.

Es existieren unterschiedliche Softwaretools, die den Menschen dabei unterstützen können, Fehler im Quelltext aufzuspüren, bevor diese zu Sicherheitslücken oder

Gefahr bringenden Ausfällen führen. Diese Tools an einem Satz typischer Programmierfehler zu testen und die Leistungsfähigkeit zu analysieren, war Gegenstand eines weiteren Forschungsprojektes.

Die Ergebnisse fließen in die Ausbildung der Aufsichtspersonen der Unfallversicherungsträger ein: Sie helfen Aufsichtspersonen dabei, einzuschätzen, ob zur Klärung eines Unfallhergangs auch ein Angriff auf eine Steuerung in Betracht gezogen werden muss. Ferner dienen die Ergebnisse dazu, in den Mitgliedsunternehmen das Bewusstsein für die Gefahr durch Angriffe auf Steuerungen zu schärfen und entsprechende Schriftwerke zu empfehlen. Eine Zusammenstellung aller wesentlichen Verordnungen und Schriften dazu findet sich auf ➔ <https://cert.dguv.de/> zum Download.

Anhand von Modellen mit echten Industriekomponenten können typische Designfehler, die zu kritischen Sicherheitsproblemen führen, erklärt werden. Dabei ist es wichtig, dass zu jedem Problem auch gleich eine praxistaugliche Lösung angeboten wird. Die Lösungen werden herstellerneutral in Vorträgen auf Arbeitsschutz-

tagungen, in Seminaren und Workshops sowie schrittweise auch online auf der Webseite des IFA präsentiert.

Eine Präventionsmaßnahme, die jeder Betrieb sofort umsetzen kann, ist das Einrichten eines Notfallkontaktes nach dem neuen internationalen Standard RFC 9116. Wie das in wenigen Minuten durch eine einfache Textdatei funktioniert und warum das so wichtig ist, wird auf der bereits genannten Webseite erklärt. Auch die DGUV hat diesen Standard umgesetzt und kann nun Mitteilungen von Behörden sowie von Sicherheitsforscherinnen und -forschern ohne Umwege erhalten. Die neuen EU-Verordnungen zu Security fordern auch von Herstellern das Bereitstellen eines Kontaktes.^[1]

Prüfung und Zertifizierung im Bereich Industrial Security

Das Prüflabor Industrial Security kann alle Teilprüfungen der DGUV Test-Prüfgrundsätze GS-IFA-M24 für Industrial Security durchführen. Hersteller von Maschinen und Anlagen sowie von Komponenten der funktionalen Sicherheit können ihre Produkte kostenpflichtig prüfen und zertifizieren lassen. Dazu war umfangreiche

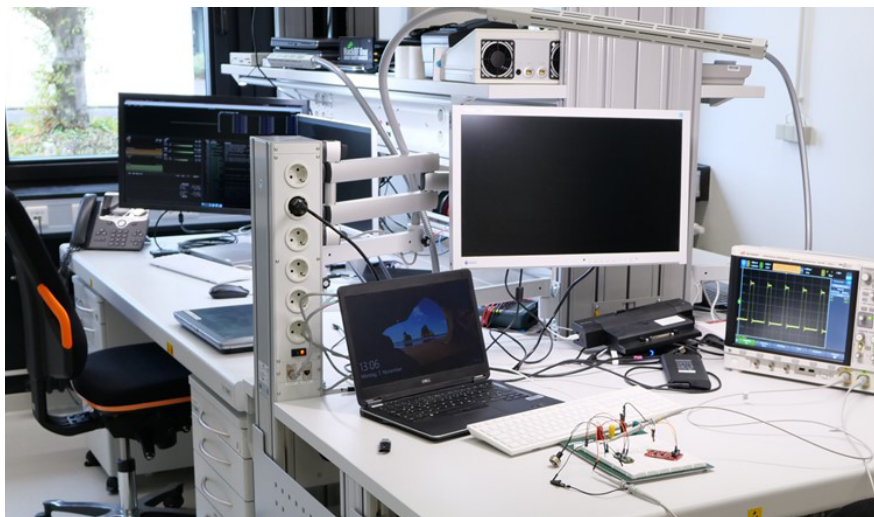
Pionierarbeit notwendig, denn im Vergleich zur Safety sind die Prüfung und Zertifizierung der Security noch sehr neu.

Unfalluntersuchungen

Kommt es doch einmal zu einem Unfall, untersucht das Labor für Industrial Security im Auftrag der Unfallversicherungsträger die Arbeitsmittel und Steuerungen mit IT-Forensik. Dazu kann es nicht nur Aufzeichnungen des Netzwerkverkehrs auswerten und Logfiles analysieren (siehe Abbildung 1). Bei Bedarf werden sogar einzelne Speicherchips ausgelesen (siehe Abbildung 2). Im Auftrag der Unfallversicherungsträger führt das Labor auch Penetrationstests und individuelle Untersuchungen an Arbeitsmitteln und Steuerungen durch.

Die Unfallversicherungsträger können somit umfangreiche Dienstleistungen abrufen und sind für die neuen Herausforderungen bestens vorbereitet. Die versicherten Mitgliedsunternehmen können

ihre durch den oben beschriebenen Notfallkontakt mit geringem Aufwand einen wichtigen Beitrag leisten.



Quelle: Stein/IFA

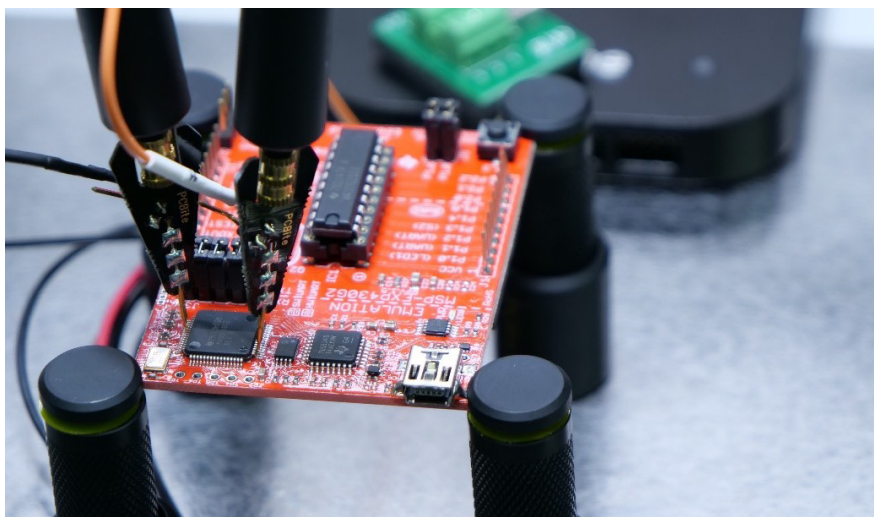
Abbildung 1: Die Spezialisten und Spezialistinnen im Prüflabor für Industrial Security setzen wirkungsvolle Werkzeuge zur IT-Forensik ein und können damit den Unfallhergang belastbar rekonstruieren.



DGUV Test-Prüfzeichen „industrial security tested“:



Produkte, die nach den DGUV Test-Prüfgrundsätzen für die Prüfung und Zertifizierung von Security-Aspekten in der funktionalen Sicherheit von industriellen Automatisierungssystemen GS-IFA-M24 geprüft und zertifiziert wurden, dürfen mit dem DGUV Test-Prüfzeichen „industrial security tested“ gekennzeichnet werden.



Quelle: Stein/IFA

Abbildung 2: Zur Rekonstruktion eines Unfallhergangs kann es mitunter erforderlich sein, dass der Speicher auf direktem Weg aus dem Chip ausgelesen werden muss, wie in diesem Foto beispielhaft nachgestellt wurde.

Fußnote

[1] Vorschlag für eine Verordnung des Europäischen Parlamentes und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020: <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52022PC0454> (abgerufen am 22.09.2023).