Fraunhofer

IT-SA 2018 | DIE IT-SECURITY MESSE UND KONGRESS
9. - 11. OKTOBER 2018 | NÜRNBERG

# IT-SICHERHEIT MADE BY FRAUNHOFER

Software und Systeme sicher entwickeln

# SECURITY-RISIKOANALYSEN MITTELS MODULAR RISK ASSESSMENT (MoRA)

Die Komplexität vernetzter Systeme erfordert eine frühzeitige Security-Risikoanalyse. Erfolgt diese am Ende der Software- und Systementwicklung, bindet dies Ressourcen, die Fehlerbehandlung orientiert sich an Symptomen statt an Ursachen, und die Gefahr durch Cyberangriffe steigt.

Eine modular aufgebaute Risikobewertungsmethode führt zu einem sicheren Systementwurf und ist auch auf bestehende Systeme anwendbar. Zu diesem Zweck entwickelte das Fraunhofer AISEC die Methode Modular Risk Assessment (MoRA). Flankiert wird das methodische Vorgehen durch das Tool Security Analyst, das gemeinsam mit der itemis AG entwickelt wurde. Die Security von Software und Systemen lässt sich anhand eines Risikomodells einheitlich, vergleichbar und nachvollziehbar bewerten und Maßnahmen zur Minimierung des Risikos können erarbeitet bzw. implementiert werden. Zudem zeichnet sich MoRA durch Wiederholbarkeit und hohe Anpassungsfähigkeit an die jeweilige Anwendungsdomäne aus.

**Das Fraunhofer AISEC**

- berät bei der Auswahl von Methoden und Tooling zur Security-Risikoanalyse;
- unterstützt bei der Anpassung und Implementierung der Methode;
- begleitet bei der Anwendung des Tools Security Analyst;
- führt Security-Risikoanalysen durch.

**Kontakt**

Daniel Angermeier
Fraunhofer AISEC
Telefon +49 89 3229986-181
daniel.angermeier@aisec.fraunhofer.de
www.aisec.fraunhofer.de


**datensouveränität.einfach.machen**

# MYDATA CONTROL TECHNOLOGIES

Immer mehr Geschäftsmodelle erfordern den Austausch und die Verarbeitung von geschäftskritischen Daten. Dabei sieht der Gesetzgeber personenbezogene Daten als besonders schützenswert an. MYDATA Control Technologies bietet sowohl Geschäftspartnern als auch Bürgern mehr Transparenz und Selbstbestimmung bei der Nutzung ihrer Daten.

Viele existierende Technologien bieten für diese Herausforderungen keine praktikable Lösung. MYDATA Control Technologies (kurz: MYDATA) schließt diese Lücke: Der Nutzer kann seine individuellen Anforderungen hinsichtlich Datensouveränität festlegen, welche anschließend von unserer Technologie technisch umgesetzt werden.

Zur technischen Realisierung von Datensouveränität greift MYDATA in Datenflüsse ein und bietet umfassende Kontrollmöglichkeiten. Daten in Bewegung können feingranular maskiert und gefiltert werden, um sie beispielsweise zu anonymisieren. Der modulare und komponentenbasierte Aufbau von MYDATA erlaubt eine einfache Integration in bestehende Systeme.

**Vorteile**

- Einsatzbereite Technologie für die einheitliche Umsetzung von Datensouveränität
- Zentrale Services für die Verwaltung und Steuerung von Datenflüssen
- Flexibles Regelwerk zur Abbildung von Datensouveränitätsanforderungen
- Entwicklerunterstützung in Form eines Open-Source SDKs und Tutorials

**Kontakt**

Christian Jung
Fraunhofer IESE
Telefon +49 631 6800 2146
christian.jung@iese.fraunhofer.de
www.mydata-control.de

## INDUSTRIELLE IT-SICHERHEIT –

# IHRE PRODUKTION SICHER VERNETZT

Die fortschreitende Vernetzung in der Automatisierung unter dem Einfluss von Industrie 4.0 führt zu einem größeren Bedrohungsfeld für Produktionsanlagen. IT-Sicherheit in der industriellen Produktion muss dabei spezifische Randbedingungen berücksichtigen, die im Office-Bereich so nicht zu finden sind.

Die Steuerung von Produktionsanlagen stellt Echtzeitanforderungen, die Veränderungen in den Systemen schwierig bis unmöglich machen. So kann die Funktionsfähigkeit beispielweise durch Software-Patches in den Systemen, die Installation von Überwachungssoftware oder durch Antivirusprogramme beeinträchtigt werden. Auch der vergleichsweise lange Nutzungszeitraum von Hard- und Software in der Produktion unterscheidet sich erheblich von anderen IT-Einsatzgebieten. Für Produktionsumgebungen müssen daher neue Strategien und Verfahrensweisen gefunden werden, um IT-Sicherheit in der Praxis umzusetzen, und das nicht nur in neuen Systemen, sondern vor allem in Altanlagen.

**Leistungsangebot**

- Konzeption, Implementierung und Integration sicherer Automatisierungssysteme
- Sicherheitskonzepte für den Einsatz von OPC UA
- Security-Tests von Automatisierungskomponenten mit IsuTest
- Seminare und Schulungen im Lernlabor Cybersicherheit

**Kontakt**

Dr.-Ing. Christian Haas
Fraunhofer IOSB
Telefon +49 721 6091-605
christian.haas@iosb.fraunhofer.de
www.iosb.fraunhofer.de


## Appicaptor

# APP SECURITY-TESTS

Welche Apps dürfen Mitarbeiter auf Tablets und Smartphones der Firma installieren? Wer die eigenen Angestellten wahllos Apps nutzen lässt, gefährdet die Sicherheit des Unternehmens. Mit dem Test-Framework »Appicaptor« des Fraunhofer SIT, können Unternehmen automatisiert testen, ob Apps den eigenen IT-Sicherheitsvorschriften entsprechen.

Viele App-Entwickler besitzen keine ausreichenden IT-Sicherheitskenntnisse, was zu unbeabsichtigten Sicherheitslücken führt. Aus Effizienzgründen werden Teile eines Software-Codes wiederverwertet. Dadurch pflanzen sich die Fehler eines Entwicklers mitunter in anderen Apps fort. Angreifer können solche Schwachstellen gezielt ausnutzen, um Passwörter zu stehlen oder Betriebsgeheimnisse auszuspähen. »Appicaptor« erstellt für Unternehmen zu jeder App einen Bericht zur Sicherheitsqualität, der an die eigenen Sicherheitsanforderungen angepasst werden kann. Bei erkannten Sicherheitslücken erzeugt das System Warnhinweise und prüft, ob die Sicherheitsanforderungen verletzt werden.

**Vorteile**

- Durchführung von App-Tests mit zyklischer Aktualisierung
- Einsatzempfehlung sicherer Apps nach kundenspezifischen Funktionalitäts- und Sicherheitsanforderungen
- Erstellung von Negativ- und Positivlisten

**Kontakt**

Dr. Jens Heider
Fraunhofer SIT
Telefon +49 6151 869-233
appicaptor@sit.fraunhofer.de
www.appicaptor.de

SeDaFa

# SELBSTDATENSCHUTZ IM VERNETZTEN FAHRZEUG

Das Internet hat längst Einzug in die Automobilindustrie gehalten. Vernetzte Fahrzeuge senden Daten an Fahrzeughersteller, Werkstätten oder Versicherungen. Diese Masse an anfallenden Daten ermöglicht einerseits viele neue Anwendungen und Geschäftsmodelle. Andererseits birgt dies neue Risiken und verursacht große Datenschutzprobleme.

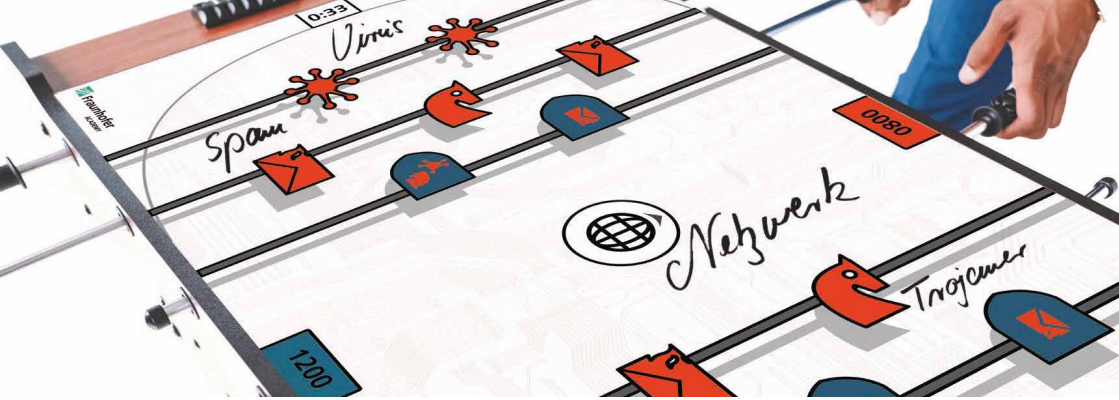
Im Projekt SeDaFa wurden Lösungen zum Selbstdatenschutz von Autofahrern entwickelt, die Fahrzeughersteller, Infrastrukturanbieter und Entwickler für Auto-Apps nutzen können, um ihre Geschäftsmodelle datenschutzfreundlich zu gestalten. Dabei werden Fahrzeugnutzer transparent und übersichtlich darüber informiert, welche Daten gesendet und für welche Zwecke genutzt werden können – auf dieser Basis sollen sie selbst entscheiden, welche Daten sie preisgeben möchten bzw. ob diese vor dem Senden z.B. anonymisiert oder pseudonymisiert werden sollen. Der Datenfluss soll also nicht komplett unterbunden werden, sondern es soll ein datenschutzwahrender Zugriff auf Fahrzeugdaten gewährleistet werden.

**Leistungsangebot**

- Beratung
- Entwicklung von Datenschutzkonzepten
- Umsetzung von Demonstratoren und Prototypen
- Erstellung von Privacy Impact Assessments

**Kontakt**

Prof. Dr. Christoph Krauß
Fraunhofer SIT
Telefon +49 6151 869-116
christoph.krauss@sit.fraunhofer.de
www.sedafa-projekt.de




**Lernlabor Cybersicherheit**

# SICHERHEITSLÜCKEN SCHLIESSEN – MIT WEITERBILDUNG ZU IT-SECURITY

Cyberangriffe auf Unternehmen steigen immer weiter an, gleichzeitig fehlen aber Fachkräfte in der IT-Sicherheit. Im Lernlabor Cybersicherheit können sich Manager und Spezialisten gezielt weiterbilden – und am Cyberkicker ihre Skills beweisen.

Im Weiterbildungsprogramm Lernlabor Cybersicherheit schulen Fraunhofer und Fachhochschulen praxisnah zu den aktuellsten Themen der IT-Sicherheit. Mitarbeiter aus Unternehmen können so ihre Kompetenzen aktualisieren und weiter spezialisieren.

Besonderes Merkmal ist die Anwendungsorientierung: In den Lernlaboren stehen sowohl die technische Infrastruktur als auch die Fachexperten bereit, um Bedrohungsszenarien nachzustellen und Lösungskonzepte zu entwickeln.

Aktionen wie das Infotainment-Spiel Cyberkicker machen auf IT-Sicherheit aufmerksam und lassen die Spieler unter anderem den Blickwinkel des Hackers kennen lernen.

**Qualitätsmerkmale im Lernlabor Cybersicherheit**

- Simulationen und Anwendungsfälle in hochwertigen Laboren erproben
- Aktuellstes und unabhängiges Forschungswissen praxisnah erleben
- Flexibel kombinierbare Bausteine, die auf den jeweiligen Bedarf der Zielgruppen und des Unternehmens zugeschnitten sind

**Kontakt**

Martin Priester
Fraunhofer Academy
Telefon +49 89 1205-1555
cybersicherheit@fraunhofer.de
www.cybersicherheit.fraunhofer.de