3. Innovationstag, 1. Juli 2022

Sichere IT für Industrie 4.0 und Produktion

Einblick in die Normen, insbesondere die neue IEC 62443
Vortrag von Sebastian Fritsch
Wichtigste Normen: ISO/IEC 27001, IT-Grundschutz, IEC 62443, ISO/IEC 15408, ETSI EN 303 645
Warum: Normen vereinfachen den Prozess deutlich. Bilateraler Abstimmungsbedarf nicht so notwendig
Prinzipp IEC 62443: ua definierte Rollen, Anwendbarkeit in brown- und greenfield
Ziel ist Security Concept. Dazu gehört auch Risiko-Analyse
Systeme erhalten unterschiedliche Zonen
Unterere Teil der Norm: Wie sicherer ich eine Zone ab.
Cloud ist nicht in der Norm enthalten - Schade
7 Fundamentale Requirements, 8 Praktiken, 47 Detail-Anforderungen

Wrum ein Security Development Lifecycle SDL:
Security by Design, Reaktionsfähigkeit, Update-Fähigkeit, ...

OWASP SAMM - alternativer SDL-Standard www.owaspsamm.org

Tipps: Stufenweise einführen und SDL-Gedanke in Unternehmenskultur reinbringen, keine radikale Einführung, vorhandene Werkzeuge weiter nutzen

Start KI Checker Neckar-Alb plus
Stefan Engelhard, IHK Reutlingen
"PLUS" Startet heute am 1.7.2022 und ist gefördert bis zum 31.12.2024
ohne PLUS war es erfolgreich. 50 KI-Checks von Unternehmen. IM PLUS ist die EInbindung Proof of Concept Projekte

Begrüßung
- Dr. Tobias Adamczyk, IHK Reutlingen
- Götz Martinek, sodge IT GmbH

Teilnehmerabfrage/Vorstellungsrunde
- WLAN als Einfallsstor
- SW Entwickler im Bereich Security. Stellenprofil
- Schnittstelle zwischen Entwicklung und IT.
- Interesse an der Norm IEC 62443
- Risiko für Unternehmen die SW lastige Produkte herstellen minimieren

Zielscheibe Unternehmen - was gibt es in der SW-Entwicklung zu beachten?
Götz Martinek
Kein Mensch kennt die IEC 62443, obgleich 10 Jahre alt.
10 Jahre alt ist auch sodgeit mit 19 Mitarbeitern
Security muss in den Entwicklungsprozess mit rein, möglichst weit vorn (Shift Left Ansatz).
- 8 Punkte wie in die SW eine Security Problem bekommt
- Pen-Testing ist oft am Schluss einer Entwicklung oder Release-Wechsel, sollte aber regelmäßig stattfinden, ggf auch automatisierbar
- Release-Frequenz sollte hoch sein. Warum nicht täglich. Wird im Zuge der Norm eh relevant.
- Durch Normen redet man weniger aneinander vorbei.

Diskssion
- Wenn Lieferanten nicht die Sicherheit liefern, sollte man eine Roadmap "in 5 Jahren" aufstellen
- Sicherheitsgesetz: Für Bereiche kann Sicherheit gefordert werden, aber nocht nichts im IoT
- Erste BSI Gütesiegel sind seit ein paar Wochen möglich. BSI macht dazu Plausi Prüfung
- Ein Security-Verantwortlicher ist otwenig, obgleich er es sehr schwer haben wird. Zur Not aiuch einen externen.
- Ein erster Schritt wäre, wenn man vom Liefererantен das Siegel für die IEC 62443
- Aus dem Automotive-Bereich kommen entsprechende Anfragen mit so 50-Punkten. Andere Branchen machen quasi nichts.
- Schwachstellung Fernwartung. Jeder macht sein eigenes Ding
- Im IT ist Security gut bewusst, im OT-Sektor, der Produktionsmaschinen, ist dies nicht der Fall.