Von: **Max Weidele** max.weidele@sichere-industrie.de
Betreff: Aufzeichnung zum Webinar "Corona-Downtime nutzen – 5 Chancen für Ihre OT-Security
Datum: 30. April 2020 um 08:11
An: Events - sichere-industrie.de events@sichere-industrie.de

Sehr geehrte Webinar-Teilnehmer,

herzlichen Dank für Ihre zahlreiche Teilnahme am Webinar
„**Corona-Downtime nutzen – 5 Chancen für Ihre OT-Security**".

Für Sie und alle Ferngebliebenen finden Sie hier einmal unsere Aufzeichnung des Webinars:
https://vimeo.com/413042353/6a94d26e65

Zusätzlich finden Sie etwas weiter unten unsere Antworten zu Fragen, die während des Webinars unbeantwortet blieben.
Sollten Sie darüber hinaus noch Fragen an die Referenten haben, können Sie diese gerne direkt an contact.cybersecurity@airbus.com schicken.

Für Hinweise zu weiteren On- und Offline-Veranstaltungen oder auch Gesprächsrunden,
können Sie sich hier zu meinem sichere-industrie.de Stammtisch anmelden!
https://www.sichere-industrie.de/industrial-und-iiot-security-stammtisch/

Viele Grüße und vielleicht ja sogar bis zum nächsten Mal
Max Weidele

***** Webinar-Teilnehmer Fragen *****

Wer bewertet, welche Systeme relevant genug sind, um gepatcht zu werden?
Wie bei allen Security-Maßnahmen, sollte auch die Frage „Was soll gepatcht werden?" anhand
von Kritikalität und Risikofaktor beantwortet werden. Hierfür sind im Prinzip zwei Rollen verantwortlich.

Die technische Fachabteilung (z.B. die Produktion) muss bewerten, wie kritisch die Prozesse sind,
welche durch das jeweilige System unterstützt werden. Darüber hinaus muss aber auch die IT-Sicherheit
bzw. das Risikomanagement das Risiko für das System bestimmen.

Wenn das jeweilige System im Fokus der Angriffsvektoren steht und eine Störung weitreichende Konsequenzen
für den Betriebsablauf nach sich zieht, sollte gepatcht werden.

Bietet sich die aktuelle Zeit auch für Lieferanten an, um über digitale Services wie Remote-Zugriffe zu reden?
Ja, definitiv. Höchstwahrscheinlich ist auf Seiten der Betreiber sowohl die Akzeptanz als auch die
Kompromissbereitschaft für moderne Services gestiegen.

Kompromissbereitschaft für moderne Services gestiegen.

Was empfehlen Sie Herstellern von digitalen Services (IoT, Predictive Maintenance, Condition Monitoring, etc.),
um die Anforderungen der OT Security zu erfüllen?

Allen voran, ist es wichtig bei der Entwicklung von Services rechtzeitig Kundenfeedback einzuholen, insbesondere durch die IT-Abteilung des Kunden. In diesem Rahmen sollten dann auch die Security-Anforderungen erfragt werden. Darüber hinaus sollten sich die Hersteller an gängige Security-Best-Practices halten (z.B. Beachtung der Grundsätze sicherer Softwarenentwicklung, Code-Reviews durchführen, Qualitätssicherung, etc.).

--

Max Weidele
Referent & Initiator

sichere-industrie.de steht für ehrliche und praxisnahe Informationen zu industrieller Sicherheit, abseits der Marketing-Buzzwords.

Erhalten Sie ausgewählte Inhalte und Erfahrungsberichte aus Industrial Security Projekten direkt per Mail in Ihr Postfach. Werden Sie kostenlos Mitglied in unserem Stammtisch: https://www.sichere-industrie.de/industrial-und-iiot-security-stammtisch/

--- Rechtliche Informationen ---
sichere-industrie.de ist ein Projekt der bluecept GmbH.

bluecept GmbH - Simplified Industrial Security
Poststrasse 33, 20354 Hamburg
e: info@bluecept.com
t: +49 40 3688132 - 0 **f:** +49 40 3688132 - 99

Amtsgericht Hamburg HRB 148338, USt-IDNr: DE314136875
Geschäftsführung: Maximillian Weidele