Innovationsworkshop CERT@VDE

„..für Betreiber von Automatisierungstechnik“

10:00 - 10:15 Uhr: Begrüßung, Vorstellung und Motivation der Teilnehmer

10:15 - 11:00 Uhr: Vorstellung CERT@VDE (Andreas Harner, Christian Link, CERT@VDE)

- Status CERT@VDE
- Zielgruppen, Scope, Netzwerk, Prozesse

11:00 - 12:30 Uhr: Offener Austausch und Diskussion (alle)

- Wie gehen Betreiber heute mit von Herstellern und CERTs veröffentlichten Advisories um?
- Was fehlt Betreibern bei den Advisories um eine Bewertung der tatsächlichen Kritikalität für ihr Unternehmen vorzunehmen?
- Was passiert bei einem Vorfall:
  - Welche Prozesse braucht man dabei?
  - Wie sollte das Zusammenspiel zwischen Betreiber und Hersteller aussehen?
  - Wie kann CERT@VDE dabei unterstützen?
- Anforderungen aus dem Betreiberumfeld (e.g. BDEW Whitepaper)
- Status: Bedrohungs-, Risiko- und Gefährdungsanalyse bei Betreibern?
- weitere Themen

12:30 - 13:30 Uhr: Mittagspause und Networking

13:30 - 16:30 Uhr: Fortsetzung: Offener Austausch und Diskussion (alle)

16:30 Uhr: Resümee & Abschluss

CERT@VDE:

Die erste IT-Sicherheitsplattform in Deutschland für Unternehmen der Industrie im Bereich der Automatisierung.

Während die meisten Großunternehmen über eigene spezialisierte Sicherheits- und Notfallteams (Computer Emergency Response Team - CERT) als zentrale Koordinierungsstelle verfügen, fehlt es kleineren Unternehmen meist an notwendigen Ressourcen und Routine im Umgang mit Schwachstellen und gemeldeten Vorfällen.

Wer ist überhaupt ein „Betreiber“?

Ein Betreiber von Automatisierungstechnik ist ein Anwender, der Komponenten/Zulieferungen eines Maschinen-, Anlagenbauers, Integrators oder eines Herstellers einsetzt. Ein Betreiber hat ein besonderes Interesse, verschiedene Informationen bzgl. der Sicherheit der betriebenen Anlagen zu erhalten, dazu gehören:

- **Meldungen über Vorfälle** im Zusammenhang mit den betriebenen Anlagen, um auf dieser Basis Schäden zu minimieren, vorhandene Schwachstellen zu identifizieren und entsprechend schnell zu beseitigen

- **Meldungen über konkrete Schwachstellen** in den eingesetzten Anlagen bzw. in verwendeten Komponenten eines Herstellers, um diese entsprechend schließen zu können

- **Meldungen über typische Angriffe bzw. die Merkmale** anhand derer Angriffe erkannt werden können.

- **Kontaktinformationen seitens der Hersteller, Maschinen- und Anlagenbauer bzw. Integratoren** für sicherheitsrelevante Aspekte der eingesetzten Anlagen und Systeme.

Motivation für den Betreiberworkshop:

Betreiber verfügen über die beste Informationslage bzgl. konkreter Vorfälle in ihren betriebenen Anlagen.

Um die Hintergründe der Angriffe oder Aufschlüsse über die dabei eingesetzten Methoden und Verfahren in Erfahrung zu bringen, müssen bestimmte technische Details preisgegeben werden um gemeinsam an einer Lösung arbeiten zu können. **Damit eine solche Kollaboration funktioniert, braucht man CERT@VDE als vertrauenswürdige Plattform.**

Betreiber sollten daher Interesse an Meldungen über Vorfälle mit Hinweisen auf weitere Betroffene haben, so dass diese selbst Maßnahmen ergreifen können bzw. damit diese Vorgehensweisen der Angreifer und Erkenntnisse über die Angreifer erkennen. Ohne dass Informationen über konkrete Vorfälle weitergegeben werden, besteht jedoch keine Möglichkeit, selbst Informationen in Erfahrung zu bringen, die eben nicht bekannt sind – aber für die Aufklärung benötigt werden.

Datum: **16. Oktober 2018,**

Zeitraum: **10:00-16:30 Uhr**

Ort: **VDE, Frankfurt am Main**

Stresemannallee 15

Da die Teilnehmerzahl beschränkt ist,

bitten wir Sie um Anmeldung bei

andreas.harner@vde.com

bis zum 11. Oktober 2018!

VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V.
Andreas Harner
Abteilungsleiter CERT@VDE
Stresemannallee 15
60596 Frankfurt am Main
Tel. +49 69 6308 – 392