ALLTEC®
... und alles hat System.

> Industrial Control System Security

Wir kümmern uns auch um die Sicherheit Ihrer technologischen Anlagen

AllTec ist Solution Partner von Siemens im Programm-Modul „Industrial Strength Networks“

Solution Partner
Automation Drives
SIEMENS

AllTec Automatisierungs- und Kommunikationstechnik GmbH

Gewerbegebiet Eula-West Nr. 11
04552 Borna
Tel.: +49 3433 246-0
Fax: +49 3433 246-333
info@alltec-borna.de

www.alltec-borna.de

> Industrial Security

In der Ver- und Entsorgungswirtschaft, wie auch in Industrieunternehmen sind SCADA und Industriesteuerungssysteme (Betriebstechnologienetzwerke) meist verantwortlich für unternehmenskritische Prozesse.

Mit der Digitalisierung wachsen IT und OT (Operational Technology) zusammen. Die bisher getrennten Datennetzwerke für Geschäftsanwendungen und Produktion werden immer mehr miteinander verbunden. Unternehmen implementieren immer mehr IoT-Geräte und Automatisierungstechnologien mit dem Ziel der Effizienzsteigerung. Diese Veränderungen sorgen für eine neue Art der Infrastrukturbelastung, deren negative Folgen mögliche Störungen sind.

Unkontrollierte und ungeplante Ausfälle der Betriebstechnologie (OT) beeinträchtigen jedoch nicht nur die Produktivität, sie können auch für Mitarbeiter, Kunden oder das Unternehmen selbst eine Gefahr darstellen.

Digitalisierung und Industrie 4.0 funktionieren nur mit zuverlässigen und zukunftssicheren industriellen Kommunikationsnetzwerken. Unternehmen benötigen heute für stabile Prozesse Industrial Security.

AllTec liefert Ihnen mit der Bewertung Ihrer Anlagen einen umfassenden Überblick über den Security-Ist-Zustand Ihrer Automatisierungssysteme. Damit kennen Sie den Handlungsbedarf und können gemeinsam mit uns die richtigen Maßnahmen ergreifen.

> AllTec hilft Ihnen:

- Defizite zu erkennen
- Risiken zu minimieren
- Maßnahmen umzusetzen

Grundlegende Maßnahmen zur IT Security

Organisatorische

- Regelmäßige Backups – Konzept überprüfen
- Umgang mit USB-Sticks & Co. regeln
- Passwort – Umgang und Umsetzung regeln
- Inventarisierung IT-Infrastruktur
- IT-Sicherheits-Check oder Penetrationstest durch externe Fachfirmen durchführen

Technische

- Prozessnetzwerke segmentieren und trennen
- Firewalls einbauen und warten
- Fernwartungszugänge absichern und regeln
- Veraltete Betriebssysteme absichern bzw. auf aktualisierte Version umstellen
- Schutz gegen unbefugten Zutritt verbessern

Top 10 Bedrohungen*

1. Social Engineering und Phishing
2. Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
3. Infektion mit Schadsoftware über Internet und Intranet
4. Einbruch über Fernwartungszugänge
5. Menschliches Fehlverhalten und Sabotage
6. Internet-verbundene Steuerungskomponenten
7. Technisches Fehlverhalten und höhere Gewalt
8. Kompromittierung von Extranet und Cloud-Komponenten
9. (D)DoS Angriffe
10. Kompromittierung von Smartphones im Produktionsumfeld

* laut der Veröffentlichung BSI-CS 005 | Version 1.20 vom 01.08.2016 des Bundesamtes für Sicherheit in der Informationstechnik