KUHSE
POWER SOLUTIONS

CYBER SECURITY IN KRITISCHEN INFRASTRUKTUREN

NETZERSATZANLAGEN
REGELKONFORM SCHÜTZEN

IST IHRE ANLAGE CYBER SECURE?

SIND SIE BETREIBER ODER ERRICHTER VON ANLAGEN DER KRITISCHEN INFRASTRUKTUR?

Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen und die Versorgungssicherheit, wie zum Beispiel große Krankenhäuser, Rechenzentren und unabhängige Stromversorger.

Gemäß BSI sind wirksame Cyber Security Maßnahmen nicht nur für kritische Infrastrukturen, sondern auch für Anlagen öffentlichen Interesses umzusetzen und zyklisch nachzuweisen. Aufgrund der stark zunehmenden Anzahl an Angriffen auf Unternehmen und Anlagen, die nicht unmittelbar zu diesen Kategorien gehören, wie z.B. kleinere Krankenhäuser, ist das Eigeninteresse auch dieser Unternehmen und Anlagenbetreiber an die Cyber Sicherheit Ihrer Anlagen deutlich gestiegen.

NOTWENDIGKEIT DER TECHNISCHEN & ORGANISATORISCHEN MAßNAHMEN

Netzersatzanlagen sind ein wesentlicher Bestandteil der zuverlässigen Energieversorgung und einem erhöhten Cyber-Angriffsrisiko ausgesetzt durch

- Cyber-Attacken auf Anlagen mit Fernzugriff bzw. Fernüberwachung
- Infektion mit Schadsoftware vor Ort und aus der Ferne
- lokalen Zugriff auf die Anlagen durch nicht- bzw. eingeschränkt-berechtigte Personen
- Angriffspunkte für Sabotagehandlungen

ENTSPRECHEN IHRE ANLAGEN DEN AKTUELLEN CYBER SECURITY NORMEN?

EU CYBER SECURITY ACT:

Aufbau einer sicheren, Cyber Security - konformen Umgebung (Hersteller, Integratoren und Betreiber) für Produkte und Systeme der Industrie 4.0

IEC 62443:

internationale Normenreihe für Cyber Security von industriellen Steuerungssystemen, Regelwerk und Leitfaden für eine verbindliche Sicherheit in Industriedatennetzen (OT) - Umgebungen

IT-SICHERHEITSGESETZ 2.0:

Gesetz zur Erhöhung der Sicherheit von Unternehmensdatennetzen (IT)-Systemen zum Schutz der Bundesverwaltung, kritischer Infrastrukturen und Unternehmen öffentlichen Interesses

WIR MACHEN IHRE NETZERSATZANLAGEN CYBER SECURE!

Als Spezialist für Netzersatzanlagen in kritischen Infrastrukturen bieten wir Ihnen **Cyber Security Kits** für Neuanlagen sowie einen **Cyber Security Check** für Ihre bestehenden Netzersatzanlagen und Systeme an.

Wir analysieren Schwachstellen und ermitteln Optimierungspotenziale, um Ihre Applikationen gegen Cyber Angriffe zu schützen und eine maximale Verfügbarkeit zu sichern.

Gern unterstützen wir Sie beratend bei der Zertifizierung ihrer Organisation und Prozesse gemäß den Richtlinien der Cyber Security Norm IEC 62443-2-4.

KUHSE CYBER SECURITY PRODUKTE

KUHSE CYBER SECURITY PREMIUM KIT

für Netzersatzanlagen mit **erhöhten** Cyber Security Anforderungen

TECHNISCHE MAßNAHMEN

- Netzwerk-Architektur und erhöhte Netzwerk-Sicherheit mittels entsprechender Netzwerkgeräte
- Cloud-basiertes zentrales Management von Benutzer-Konten, Zugriffs- und Nutzungsrechten
- Benutzerauthentifizierung mittels Zwei-Faktor-Authentifizierung
- Minimierung der Zugangs- und Zugriffsmöglichkeiten und somit der potentiellen Angriffsstellen
- Härtung der Systeme (Hardware, Software, Dienste, Cloud)
- Loggen von Anmelde-, Angriffsversuchen und Verstößen
- Datensicherung / -wiederherstellung, Notfallplan

SERVICE MAßNAHMEN

- Prozesshandbuch für Betrieb und Wartung sowie den Umgang mit Cyberangriffen
- Schulung des kundenseitigen Bedien- und Servicepersonals
- Wiederholungsprüfungen zur Sicherstellung der Wirksamkeit der technischen Maßnahmen und umgesetzten Prozesse
- Aktualisierung der Netzwerk- und Sicherheitsgeräte, relevanter Anlagenkomponenten sowie der eingesetzten Sicherheitstools (Patching, Anti-Malware, Application Whitelisting, digitale Zertifikate)

KUHSE CYBER SECURITY BASIS KIT

für Netzersatzanlagen mit **elementaren** Cyber Security Anforderungen

TECHNISCHE MAßNAHMEN

- Netzwerk-Architektur und Basis-Netzwerk-Sicherheit mittels entsprechender Netzwerkgeräte
- Cloud-basiertes zentrales Management von Benutzer-Gruppenkonten, Zugriffs- und Nutzungsrechten
- Benutzerauthentifizierung mittels Zwei-Faktor-Authentifizierung
- Begrenzung der Zugangs- und Zugriffsmöglichkeiten und somit der potentiellen Angriffsstellen
- Härtung des Kuhse Gateways und der Cloud-Umgebung
- Loggen von Anmeldungen und Anmeldeversuchen
- System-Datensicherung nach Auslieferung und Inbetriebnahme

SERVICE MAßNAHMEN

- Prozesshandbuch für Betrieb und Wartung
- Regelmäßige Aktualisierung der Sicherheitsmechanismen in der Cloud-Umgebung

KUHSE CYBER SECURITY LEISTUNGEN

SYSTEME (CYBER SECURE BASIEREND AUF IEC 62443)

- Steuerungen / Schaltanlagen für Prime Power Anlagen
- Steuerungen / Schaltanlagen für Netzersatzanlagen (NEA)
- Steuerungen / Schaltanlagen für Hybrid Power Anlagen

SERVICE

- Gesicherte Inbetriebsetzung und Wartung des Systems
- Schulung des Bedien- und Wartungspersonals
- Überprüfung der Wirksamkeit und Aktualität der Cyber Security Maßnahmen
- Durchführung von Sicherheitsupdates
- Remote Support bei Cyber-Attacken

CONSULTING

- Schulung Cyber Security Normen
- Evaluierung notwendiger technischer Maßnahmen und Prozesse
- Festlegung geeigneter technischer Maßnahmen und Prozesse
- Prozesshandbuch für Integration, Betrieb, Wartung, Backup/Restore, Notfallwiederherstellung des Systems und für den Umgang mit Cyber-Attacken

WARUM SIE SICH FÜR KUHSE ENTSCHEIDEN

- langjährige Erfahrung mit Steuerungssystemen für Netzersatzanlagen zur dezentralen Energieerzeugung
- umfangreiches Know-How über komplexe Steuerungsprozesse im Gesamtanlagenzusammenhang
- Unterstützung von Anlagenbetreibern und Integratoren in allen Phasen des Anlagen-Lebenszyklus
- alle Leistungen - von der Beratung bis zur Inbetriebnahme und Wartung - aus einer Hand

KONTAKT

Kuhse Power Solutions GmbH
Norbert Reichert
Ohepark 2
21224 Rosengarten
Tel. +49 4171 798-176
n.reichert@kuhse.de
www.kuhse-energy.com