this webinar is powered by

Kaco new energy

pv magazine webinars

18. März 2026

15:00 bis 16:00 Uhr

Cybersecurity in der Praxis: Wechselrichter-Design und das richtige Schutzkonzept für die Anlagen

Marian Willuhn

Senior Redakteur

pv magazine

Julian Reimer

Senior Technical Sales Engineer

Kaco new energy

Alexander Plonka

Product Lifecycle Manager

Kaco new energy

Cybersecurity in der Praxis:
Wechselrichter-Design und das richtige Schutzkonzept für die Anlagen
blueplanet 360 NX3

PV Magazin Webinar März 2026

KACO new energy.

Einführung: Hohe Bedrohungslage für PV-Großanlagen.

CYBERANGRIFF AUF POLENS KRITISCHE INFRASTRUKTUR

Bild- und Textquellen:
Poland Stops Cyberattacks on Energy Infrastrucutre – The Chancellery of the Prime Minister – Gov.pl // CERT Polska Details coordinated Cyber Attacks on 30+ Solar and Wind Farms

- Zwischen Weihnachten und Neujahr wurden gezielt 30+ Solar- und Windparks sowie ein Wärmekraftwerk in Polen angegriffen
- Zu dieser Zeit herrschen tiefe Temperaturen und Personal ist im Urlaub
- Es handelte sich um gezielte, gut vorbereitete Angriffe
- Polens Premieminister Donald Tusk sagte hierzu: „alles deutet darauf hin das diese Angriffe von Gruppen vorbereitet wurden, die direkt mit den russischen Diensten verbunden sind“

SYSTEME DER DEUTSCHEN BAHN GEHACKT

Bild- und Textquellen:
Anhaltende Probleme bei Deutscher Bahn - Cyberangriff ist Ursache | tagesschau.de

- Cyberangriffe legen Buchungssystem & Verbindungssuche der deutschen Bahn lahm
- Der DDoS-Angriff erfolgte in Wellen, die Attacke war ungewöhnlich groß

Hohe Bedrohungslage

Bedrohungslage bereits hoch – und weiter steigend

- Koordinierte Angriffe auf Solaranlagen von State-Level-Actors & State-Funded Hackergruppen
- Höhere Angriffsqualität:
  - Hoher Ressourceneinsatz: Zeit & Geld für die Vorbereitung und Durchführung von Angriffen
  - Ziele werden ausgespäht, komplexe Angriffe von Fachexperten vorbereitet & durchgeführt

→ Aktuell: Lediglich Spitze des Eisberges – mehr & bessere Angriffe werden kommen.

Riskien

Gesellschaft

- Strategische Verwundbarkeit in geopolitisch unruhigen Zeiten
- Gezielte Angriffe auf schwach geschützte Komponenten könnten Blackouts auslösen
- Zunehmende Digitalisierung & Fernzugriffe verstärken Verwundbarkeit

Hersteller

- Hersteller, Produkte und Lösungen aus dem Solarbereich können gezielt angegriffen werden
- Unsichere Komponenten können die Verfügbarkeit von Produkten & Lösungen reduzieren
- Reputationsschaden durch Cyber-Vorfälle

EPCs Investoren, Netz- & Anlagenbetreiber

- Ertragsausfälle, Vertragsstrafen (PPA) & nachteilige Finanzierungen/ Versicherbarkeit
- Strengere Cyber-Regulierungen: Risiko von Strafen bei Nichterfüllung + neue Anforderungen an Anlagenplanung
- Reputationsschaden durch Cyber-Vorfälle

→ Veränderte Bedrohungslage erfordert umfassende Maßnahmen.

Trends & Maßnahmen

Gesellschaft
- Verstärktes Bewusstsein für Cybersicherheit & daraus resultierenden Risiken
- Verstärkte regulatorische Anforderungen (CRA, KRITIS, …)

Hersteller
- Cybersicherheit muss integraler Bestandteil sämtlicher Unternehmensprozesse sein
- Produktentwicklung, Produktion, Sales, Service & mehr: Cybersicherheit ist bei KACO oberste Priorität

EPCs, Investoren, Netz- & Anlagenbetreiber
- Stärkeres Bewusstsein für Cybersicherheit inkl. Finanzierbarkeit & Versicherbarkeit
- Qualifizierung neuer Hersteller mit Fokus auf Cybersicherheit
- Fokus auf Cybersicherheit in Anlagenplanung & Betrieb

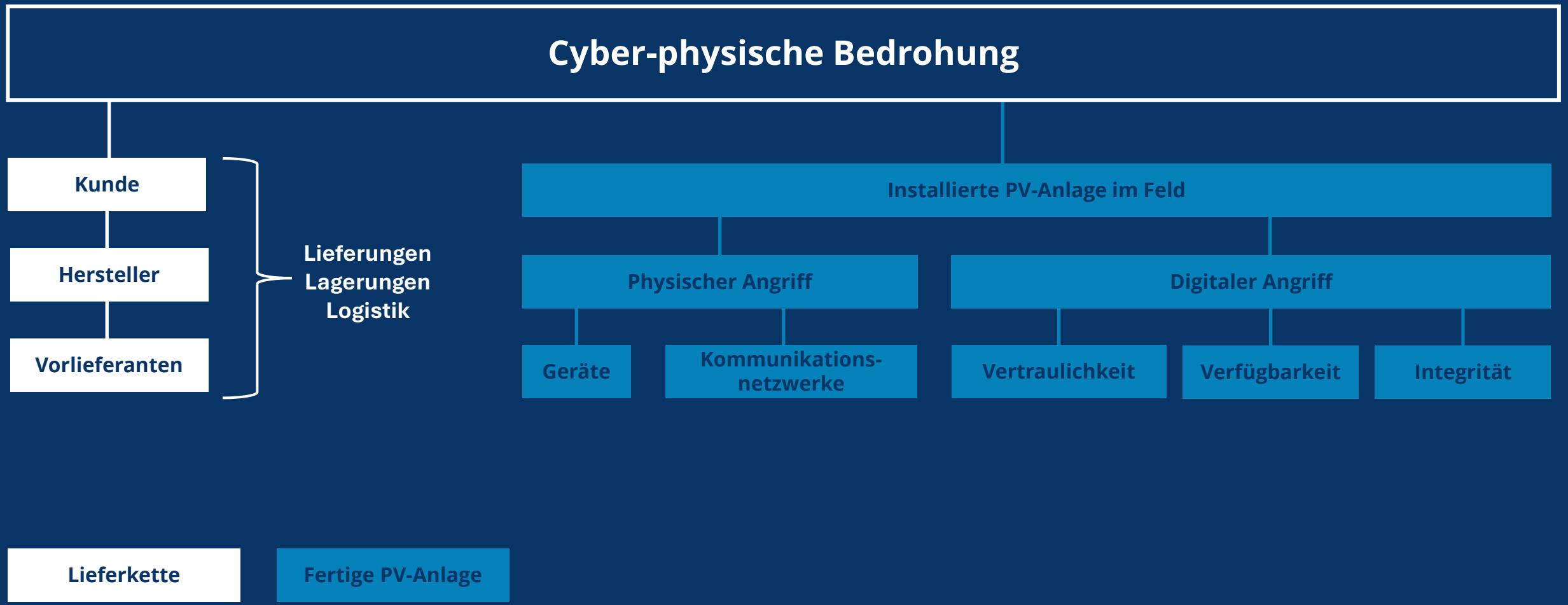
→ Hersteller, EPCs, Investoren, Netz- & Anlagenbetreiber gestalten gemeinsam eine sichere Energieversorgung. Wir können uns schützen.

KACO new energy.

Angriffszenarien Utility Solar.

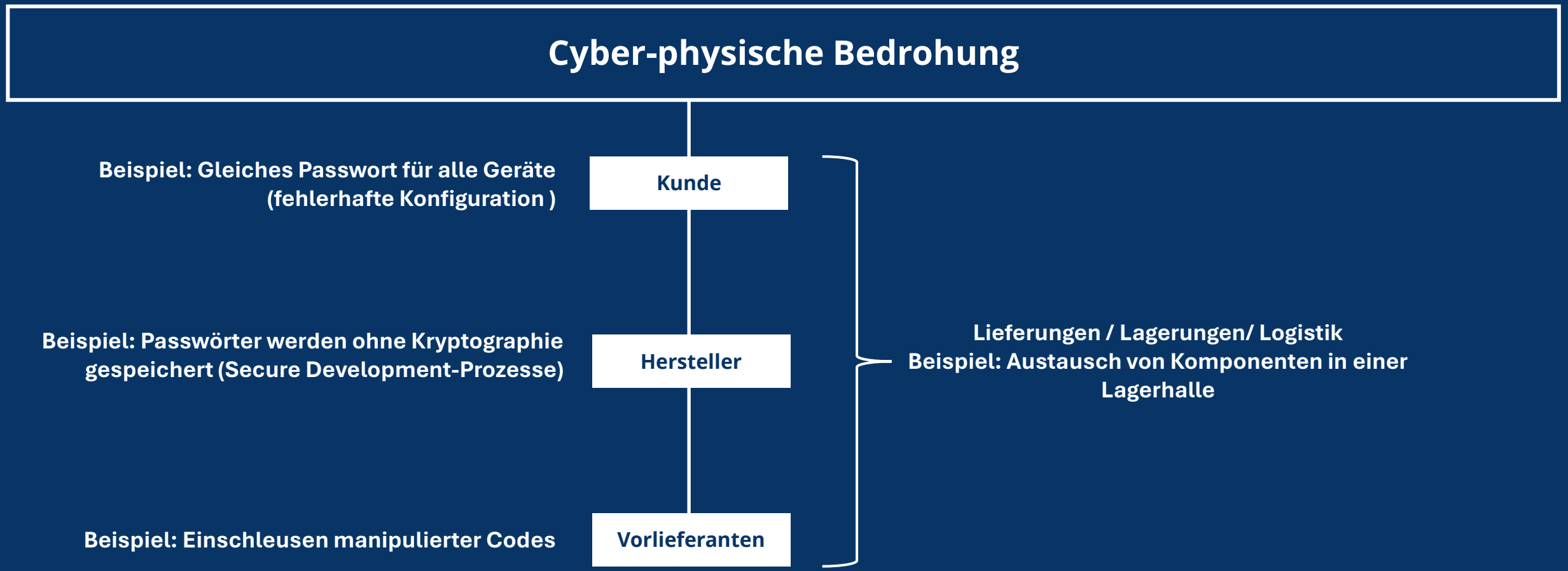
Bedrohungen in der Übersicht.

Lieferkette & Anlagen im Feld



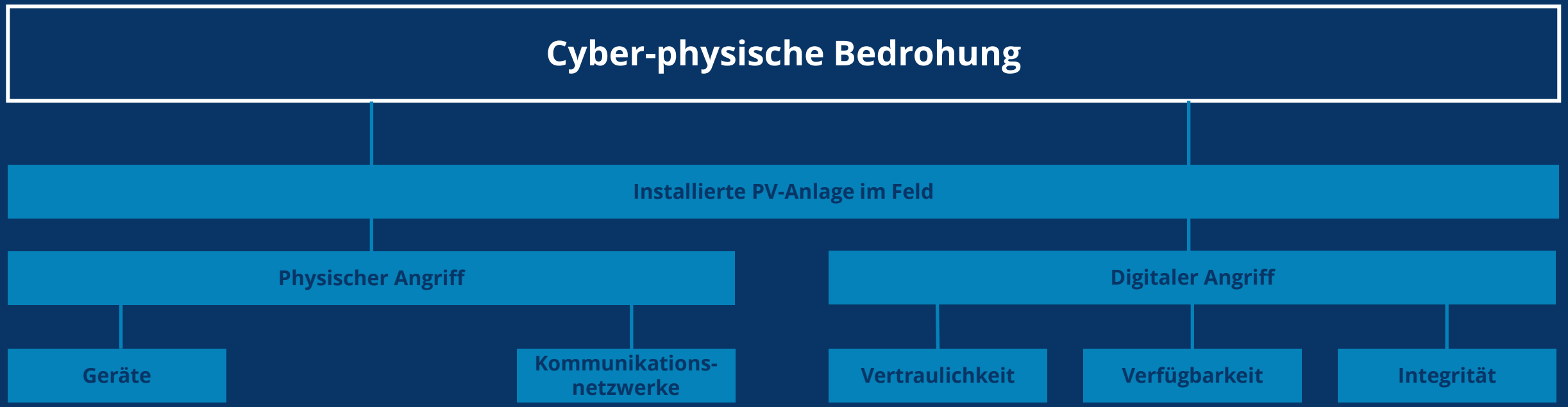
Bedrohungen in der Übersicht.

Bedrohungen in der Lieferkette & Beispiele



Bedrohungen in der Übersicht.

Bedrohungen im Feld & Beispiele



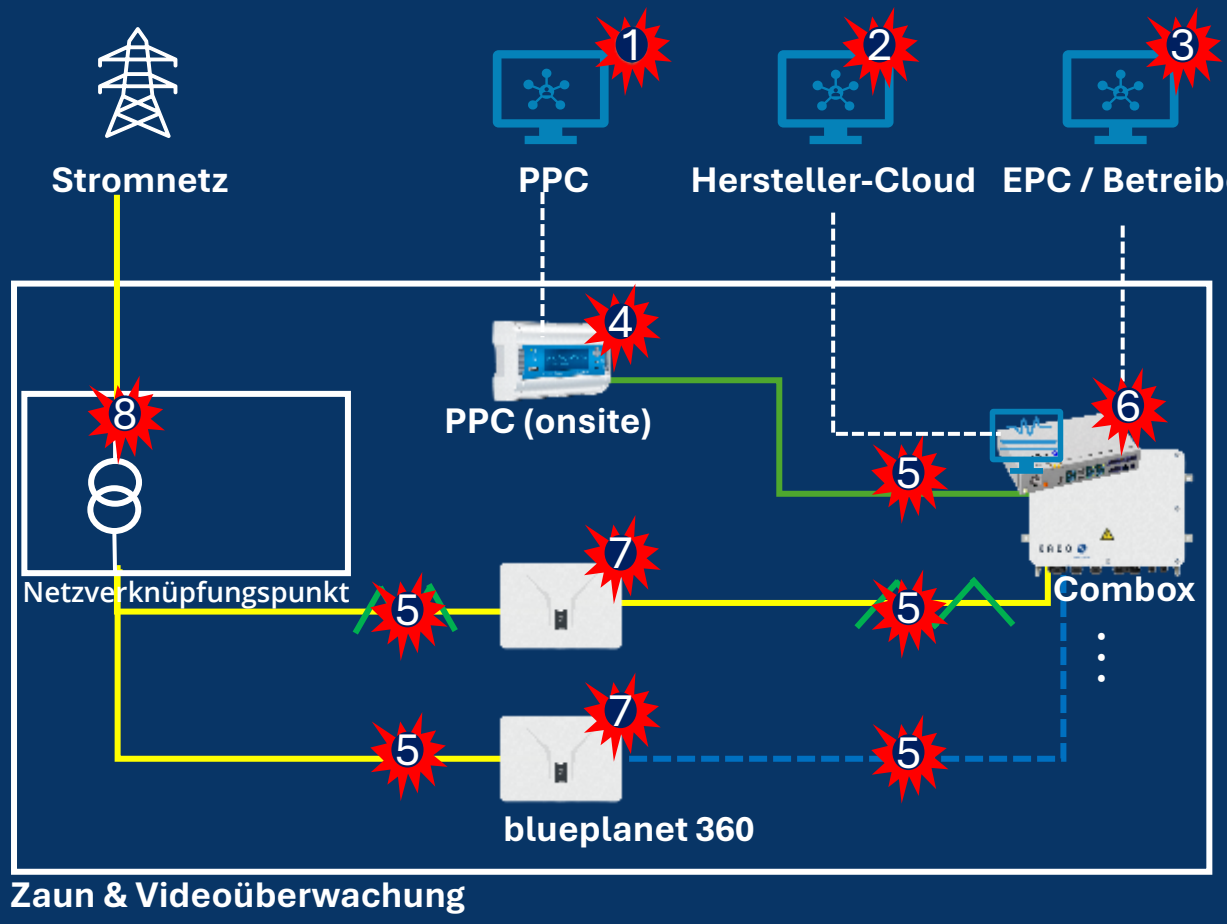
Beispiele:

- **Sabotage & Zerstörung von Anlagentechnik**
- **Upload von Schadsoftware via USB**
- **Anschluss eigener Geräte (Laptop, Debugger…)**
- **Diebstahl & Analyse von Produkten**

Beispiele:

- **Login mit gestohlenen VPN-Zugangsdaten (Phishing / Social Engineering)**
- **Ausspähen der Systemsoftware zur weiteren Angriffsplanung**
- **Software-Manipulation / Einspeisen von Schadsoftware**
- **Abhören & Einspeisen von Drahtlos-Signalen mit Antennen**

Angriffspunkte Utility Solarpark.



Angriffspunkte

1. PPC (Hersteller, Grid Operatoren, Direktvermarkter, VPN)
2. Hersteller-Cloud (bei KACO: Nicht vorhanden, kein Risiko)
3. EPC / Betreiber (Unternehmen & Anlagenzugriffe, VPN)
4. PPC (onsite)
5. Datenverbindungen
6. Hersteller-Datenlogger (onsite, bei KACO: AI Manager)
7. Wechselrichter (bei KACO: blueplanet 360)
8. Netzverknüpfungspunkt

LAN / LWL
K-Bus
RS485
Mobile network
AC-Verkabelung
AI Manager Webinterface
Angriffspunkte
Remote-Zugriffe

Angriffs- & Schutzziele

Vertraulichkeit, Integrität, Verfügbarkeit

Beeinträchtigung	Begriffsbedeutung	Beispiel Angrifsszenario Utility Solar
Verfügbarkeit	Rechtzeitige und zuverlässig Verfügbarkeit von Geräten, Systemen & Daten	Großflächiger Blackout (Worst-Case)
Integrität	Korrekte, unveränderte und vertrauenswürdige Daten	Veränderung an Firmware // Manipulation von Leistung & Blindleistung
Vertraulichkeit	Informationszugriff nur für nur berechtigten Personen & Systeme	Auslesen von Monitoring-Daten & Servicepaketen

→ Schutz ist zentrale Aufgabe aller Beteiligten (Hersteller, EPCs, Betreiber, Netzbetreiber,...)

KACO new energy.

Systematische Cybersecurity: Organisation, Prozesse & Prüfungen.

Cybersecurity bei KACO

Konsequente Cybersecurity – in Lieferkette, Organisation, Produkten & Lösungen

Aktivitäten bei KACO

- ISO 27001 Zertifizierung
- Penetrationstests
- Cybersecurity ist integraler Bestandteil des Produktlebenszyklus
- Siemens-Guidelines zu Secure Design und Coding
- Bedrohungs- und Risikoanalysen & Maßnahmendefinition (englisch: „TRA“)
- Lieferkette: Qualifizierung & Auditierung Vorlieferanten, Cybersecurity-Vertäge
- Einhaltung Siemens Baseline Cybersecurity Requirements
- Vulnerability Handling für Fremdsoftware
- Bereitstellen von Security Updates
- Siemens Product-CERT
- Mehr

Systematische Cybersecurity

Organisation, Prozesse & Prüfungen – Beispiel Prüfung Vorlieferanten

Prüfung von Vorlieferanten

- Auditierung von Vorlieferanten, inkl. Prüfung von Prozessen hinsichtlich Cybersecurity
- Hardware- und Software-Reviews
- Analyse von BOM / S-BOM / SW-Architektur
- Cybersecurity-Verträge
- Certifications (ISO 27001)

→ **Cybersecurity fängt bei den Grundprinzipien der Organisation & Lieferkette an. Es handelt sich um ein mehrstufiges, ganzheitliches Konzept.**

KACO new energy.

blueplanet 360 NX3
Architektur & Grundprinzipien.

AMAZING FACTS.

Sicher. Effizient. Kraftvoll.

- ✓ Hohe Leistung: Bis zu 363 kW
- ✓ Cybersecurity der Spitzenklasse
- ✓ Sehr spätes Derating
- ✓ Next Generation IGBTs

Technische Highlights.

Kraftvoll
Bis zu 363 kW bei 100 % U_{nom}
326,7 kW bei 90 % U_{nom} gemäß VDE 4110

Cybersicher
Vollständige Datenhoheit, zertifizierte Sicherheit, laufende Penetrationstest, reduzierte Angriffsfläche und zahlreiche weitere Schutzfeatures

Einzigartig
Hochleistungs-Utility Wechselrichter eines Deutschen Herstellers

Verbessertes Derating
Volle Leistung bei bis zu 40° C Umgebungstemperatur

Effizient
98,9 % Wirkungsgrad
Mehr Ertrag für Ihr Projekt

KACO new energy.

Technische Security Features.

Cybersecurity der Spitzenklasse.

- ✓ **Deutschlands Antwort auf Cybersecurity der Spitzenklasse in Utility-Scale-Solar:** Der blueplanet 360 NX3 ist der erste Utility-Wechselrichter eines deutschen Anbieters und setzt neue Maßstäbe für Cybersecurity. Er leistet einen Beitrag zu Resilienz und Unabhängigkeit der europäischen Energieversorgung.
- ✓ **SIEMENS AG und KACO new energy entwickeln das ganzheitliche Cybersecurity-Konzept** des blueplanet 360 konstant weiter – Für den Schutz Ihrer Anlage.
- ✓ **Datenhoheit:** Der blueplanet 360 NX3 ist an keine externe Herstellercloud angebunden und sicher vor fremden Zugriffen.
- ✓ **Zertifizierte Sicherheit:** ISO 27001 Zertifizierung für standardisierte, sichere und klare Prozesse innerhalb von KACO new energy.
- ✓ **Systematische Bedrohungs- und Risikoanalysen** zur Bewertung von Bedrohungen und zur gezielten Definition von Gegenmaßnahmen.

Cybersecurity der Spitzenklasse.

- ✓ **Kontinuierliche Penetrationstests:** Abgestimmt mit KACO new energy führen „Friendly-Hacker“ regelmäßig Cyber-Angriffe auf den blueplanet 360 NX3 durch, um das Sicherheitskonzept stets auf dem aktuellsten Stand zu halten.

- ✓ **Proaktiver Informationsfluss:** Die SIEMENS AG ProductCERT ist ihr Partner für transparente Kommunikation und informiert im Bedarfsfall proaktiv. Zudem können Hinweise zu Cybersecurity-Themen gerne an ProductCERT gemeldet werden unter CERT Services - Siemens Global.

- ✓ **Reduzierte Angriffsfläche:** Drahtlose Datenkommunikation über WIFI oder Mobilfunk wurden bewusst ausgelassen, um potenziellen Hackern keine Chance zu geben.

- ✓ **Zahlreiche und gut dokumentierte Features stellen den zuverlässigen Betrieb ihres PV-Parks sicher:** Signierte Firmware, IP-Whitelists, verschlüsselte Modbus TLS Kommunikation oder deaktivierbare USB-Schnittstellen schützen vor Manipulationen und Angriffen.

- ✓ **Umfassende Dokumentation:** In unseren Anleitungen finden Sie ausführliche Informationen zu unseren herausragenden Security-Features. Einfach. Schnell. Unkompliziert.

Maßnahmen KACO.

Umfassende Cybersecurity – in allen Bereichen

Maßnahme KACO

Cyber-physische Bedrohung

Kunde

Security-Dokumentation

Hersteller

Prozesse / Organisation

Vorlieferanten

Auditierung, Verträge, ...

Lieferungen / Lagerungen/ Logistik
Beispiel: Austausch von Komponenten in einer Lagerhalle

Auditierung, Verträge, ...

Maßnahmen KACO.

Umfassende Cybersecurity – in allen Bereichen

Maßnahme KACO

Cyber-physische Bedrohung

Installierte PV-Anlage im Feld

Physischer Angriff

Digitaler Angriff

Geräte

Kommunikations-netzwerke

Vertraulichkeit

Verfügbarkeit

Integrität

Security-Dokumentation (Zäune & Videoüberwachung), ...

Modbus/TLS, IP Whitelist
Reduzierte Angriffsfläche: Deaktivierbare USB-Schnittstelle, kein WIFI & Mobilfunk, verschlossene Ports, ...

Secure-Development
Pentests
Keine Hersteller-Cloud
Backup-Feature
Telemetry-Logging
...

KACO new energy.

Transparenz und Incident Handling.

Systematische Cybersecurity.

Prozesse & Prüfungen

ProductCERT als zentrale Anlaufstelle für

- Schwachstellenmeldungen
- Sicherheitswarnungen
- Koordinierte Reaktionen

Strukturierter Incident-Response-Prozess

- Bewertung der Kritikalität
- Klare Handlungsempfehlungen
- Zeitnahe Kommunikation

Vorteil für Betreiber

- Verlässlicher Ansprechpartner
- Nachweisbare Professionalität gegenüber Stakeholdern
- Patchmanagement

KACO new energy.

Zusammenfassung.

KACO ist Ihr sicherer Ansprechpartner

Konsequente Cybersecurity – in Lieferkette, Organisation, Produkten & Lösungen

Hohe Bedrohungslage – weiter steigend

- Sehr hohe und weiter steigende Bedrohungslage: State-Fundet Actors agieren mit Expertenwissen, Zeit & Geld
- Sichere Auswahl von Komponenten entscheidend für die Sicherheit unserer Energieversorgung

Cybersecurity

- Beginnt bei Organisation & Lieferkette
- Ist elementarer Bestandteil aller Unternehmensprozesse
- Stellt einen Wettbewerbsvorteil dar (Lieferantenqualifizierung, Finanzierung, Versicherung, Vertrauen)
- Kontinuierlicher Prozess: 100% Sicherheit gibt es nicht

KACO new energy setzt auf

- Organisatorische Maßnahmen intern und in der Lieferkette
- Umfassende Maßnahmen (Risikoanalysen, Penetration-Tests, Base-Line-Cyber-Sicherheitskriterien, mehr)
- Professionelles Incident-Handling

KACO new energy.

Q&A.

KACO new energy.

DANKE FÜR IHRE AUFMERKSAMKEIT.

KACO new energy GmbH

A Siemens Company

Werner-von-Siemens-Allee 1
D-74172 Neckarsulm

Kaco-newenergy.com

this webinar is powered by
Kaco new energy

pv magazine webinars

18. März 2026
15:00 bis 16:00 Uhr

Cybersecurity in der Praxis: Wechselrichter-Design und das richtige Schutzkonzept für die Anlagen | Fragen und Antworten

Marian Willuhn
Senior Redakteur
pv magazine

Julian Reimer
Senior Technical Sales Engineer
Kaco new energy

Alexander Plonka
Product Lifecycle Manager
Kaco new energy

pv magazine webinars

Lesen Sie weiter:

10% Rabatt
auf Ihr Abo
mit Code
Webinars10

Neue Ausgabe

Schwerpunkt Batteriespeicherzubau & -vermarktung

Netzanschlüsse: Zusagen und Realität, Marktübersicht Gewerbe- und Großbatteriespeicher, Algotrader-übersicht, Vertragsgestaltung bei der Beschaffung

Gewerbeanlagen werden flexibel

Börsenhandel mit Gewerbespeichern, vom Energieaudit zum Photovoltaik- und Batterieprojekt, Anwendungsfälle für den wirtschaftlichen Einsatz von Gewerbespeichern, Vermarktung vor und hinter dem Zähler

Online-News unter www.pv-magazine.de

Beliebt bei Lesern

EEG-Entwurf geleakt – komplette Streichung der Förderung privater Photovoltaik-Anlagen vorgesehen

Bundesverband Solarwirtschaft warnt vor Kahlschlag.

Battery Business & Development Forum 2026

*Registrieren Sie sich für das **Battery Business und Development Forum** vom 31. März bis 1. April 2026 in Frankfurt und seien Sie Teil der Diskussionen um **Strategien und Trends** in den schnell wachsenden europäischen Märkten für **netzgekoppelte Batteriespeichersysteme**.*

Nächste Veranstaltungen...

pv magazine webinars

Dienstag, 21. April 2026
14:00 - 15:00 Uhr

Redispatch-Entschädigungen: Was Anlagenbetreiber nach den Änderungen durch die EnWG-Novelle wissen und beachten müssen

Zum Nachsehen

Webinar vom 5. März 2026

Technologiesprung bei Topcon – Solarerträge steigern mit Jinko Tiger Neo 3.0 Modulen

Ständig neue Webinare zu interessanten Themen!

Weitere Webinare unter www.pv-magazine.de/webinare

Auch auf Englisch unter: www.pv-magazine.com/webinars

this webinar is powered by

Kaco new energy

pv magazine webinars

Marian Willuhn

Senior Redakteur

pv magazine

Vielen Dank und auf Wiedersehen!