Die Deutsche WindGuard

Anlagen- und Betreiberverantwortung aus der praktischen Perspektive des Technischen Betriebsführers unter Einbeziehung der KRITIS-Verordnung 2.0

Vorstellung

- Andre Reichert
- Leiter Technische Betriebsführung Deutsche WindGuard
- Diplom-Wirtschaftsingenieur

- Werdegang:

seit 2019	Deutsche WindGuard GmbH
	Leiter Technische Betriebsführung
bis 2019	ENERCON (WRD MS GmbH)
	F&E Projektmanagement, Kundenproblemprojekte (sog. HotSpots)
bis 2017	WindGuard Certification GmbH
	Weiterbetrieb von WEA, Qualitätswesen, Prozessverantwortung
bis 2014	Offizier der Bundeswehr (Luftwaffe)

Technische Betriebsführung

- TBF Deutsche WindGuard:
  - etwa 350 WEA
  - über 70+ Windparks
  - über 800 MW betreute Leistung
- Größe der WEA: 300kW bis 7.500 kW
- Erfahrung mit folgenden Anlagentypen:
  - Areva/Multibrid: M5000-116, M5000-135
  - Enercon: E40, E44, E48, E66, E70, E82, E 101, E 112, 115, E126, E126EP4
  - Fuhrländer: MD77
  - Gamesa: G80
  - GE: GE1.5s, GE1.5sl, GE2.5
  - Nordex: N60, N62, N90, N117, N131
  - PowerWind: PW90
  - Senvion/REpower: 3.2M, 3.3M, 3.4M, 5M, 6.2M152
  - Siemens/Bonus: AN-1.3, AN-2.0, AN-2.3, SWT-3.6, SWT-3.0
  - Vestas: V42, V66, V80, V90, V112; V126; V136

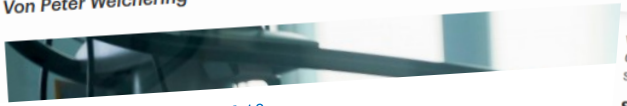
„Die aktuelle Sicherheitslage in Deutschland ist ungenügend und auf keinen Fall eine gute Basis für unsere digitale Zukunft."
- Prof. Norbert Pohlmann, IT-Professor
Quelle: Deutschlandfunk, 16.10.

Sicherheitsmesse Itsa

Experten warnen vor dem IT-Blackout

Die Corona-Pandemie hat der Digitalisierung in Deutschland einen kräftige[n] Schub verliehen – gleichzeitig haben Cyberangriffe deutlich zugenommen. Denn viele Bereiche sind nur unzulänglich abgesichert, etwa Homeoffice-Arbeitsplätze oder die IT-Sicherheit von Krankenhäusern. Das muss sich dringend ändern.

Von Peter Welchering



Quelle: Deutschlandfunk, 16.10.

Stadtwerke Wismar: Ermittlungen nach Cyberattacke laufen

Stand: 01.10.2021 17:22 Uhr

Cyberkriminelle haben am Dienstag die IT-Systeme der Stadtwerke in Wismar attackiert. Das wurde am Donnerstag bei der Sitzung der Bürgerschaft bekannt. IT-Sicherheitsexperten arbeiten an der Aufklärung.

Wie die Stadtwerke in Wismar jetzt mitteilten, ist der Versorger Anfang der Woche Ziel eines Cyberangriffes geworden. Schon am Dienstagmorgen hatten sich bisher Unbekannte in die IT-Systeme gehackt.

Spurensuche läuft, Stadtwerke im Notbetrieb

IT-Experten einer Berliner Firma prüfen nun, wie die Attacke ablief und wer dahinter steckt.

Quelle: ndr.de.

Notaufnahme geschlossen

Der Hackerangriff auf die Uniklinik Düsseldorf und die Folgen

Die Universitätsklinik Düsseldorf ist Opfer eines Hackerattacke geworden – wohl aus Versehen, aber mit enormen Folgen: Operationen waren nicht mehr möglich, die Notaufnahme musste schließen, möglicherweise kostete der Angriff sogar einen Menschen das Leben. Der Regelbetrieb ist noch immer gestört.

Von Vivien Leue

Quelle: Deutschlandfunk, 18.09.2020

CYBERSICHERHEIT

"ZUNEHMENDE VERNETZUNG MACHT VERSORGER ANGREIFBARER"

NEUE MÄRKTE 19.02.2021 - 17:02 MERKEN DRUCKEN

VON PHILIP AKOTO

Quelle:energate-messenger.de

BSI-Lagebericht 2021

Kritische Infrastruktur

Angreifer legen Krankenhäuser oder Verwaltungen lahm und gehen dabei immer professioneller vor. Die Bedrohung in Deutschland wächst, zeigt der Lagebericht des BSI.

Quelle: zeit.de

Die Antwort – Kritis-Verordnung 2.0

DEUTSCHE WINDGUARD

Neue Pflichten für Betreiber
Angriffserkennung

Neue Meldepflichten

Kritische Komponenten

Unmittelbare Registrierung

Mehr betroffene Unternehmen
KRITIS-Sektor Entsorgung

Unternehmen im besonderen öffentlichen Interesse

Niedrigere Schwellwerte

Mehr Anlagen

Mehr Befugnisse für das BSI
Zentrale Meldestelle

Tiefere Untersuchungen

Schutz der Bundesnetze (Kommunikation / IT)

Mehr Anlagen

Sanktionen und Verbraucherschutz
Höhere Sanktionen für Betreiber

Mehr mögliche Verstöße

Neue (freiwillige) Gütesiegel

Die Antwort – Kritis-Verordnung 2.0

DEUTSCHE WINDGUARD

Neue Pflichten für Betreiber
Angriffserkennung

Neue Meldepflichten

Kritische Komponenten

Unmittelbare Registrierung

Mehr betroffene Unternehmen
KRITIS-Sektor Entsorgung

Unternehmen im besonderen öffentlichen Interesse

Niedrigere Schwellwerte

Mehr Anlagen

Mehr Befugnisse für das BSI
Zentrale Meldestelle

Tiefere Untersuchungen

Schutz der Bundesnetze (Kommunikation / IT)

Mehr Anlagen

Sanktionen und Verbraucherschutz
Höhere Sanktionen für Betreiber

Mehr mögliche Verstöße

Neue (freiwillige) Gütesiegel

Mehr Anlagen / Neue Schwellwerte

- Grundsätzlich mehr Anlagen: +17 über alle Sektoren
  - aber -4 Anlagen im Sektor Strom
    - Erzeugungsanlage mit Wärmeauskopplung (i.S. §2 Nr. 14 KWKG)
    - Dezentrale Energieerzeugungsanlage (i. S. §3 Nr. 11 EnWG)
    - Speicheranlage (Speicherung elektrischer Energie)
    - Messstelle (i.S. §2 Nr. 11 MsbG)

- Niedrigere Schwellwerte: -6 über alle Sektoren

Mehr Anlagen / Neue Schwellwerte

Bereich Stromversorgung:

Anlage	Schwellenwert
Erzeugungsanlage	104 MW (vorher 420 MW)
Steuerung/Bündelung elektrischer Leistung	104 MW Netto-Leistung 0 MW Schwarzstart-Anlage 36 MW Primärregel
Übertragungsnetz/ Stromverteilernetz	3700 GWh/Jahr
Stromhandel	3700 GWh/Jahr (vorher 200 GWh)

Herleitung Schwellwert 104 MW:

Durchschnittsverbrauch / Person
→ 1815 kwh Strom
→ 500.000 Personen

Und nun?

- Wenige neue Verpflichtungen für den Betreiber durch KritisV 2.0
  - Angriffserkennung
  - Neue Meldepflichten
  - Kritische Komponenten
  - Unmittelbare Registrierung

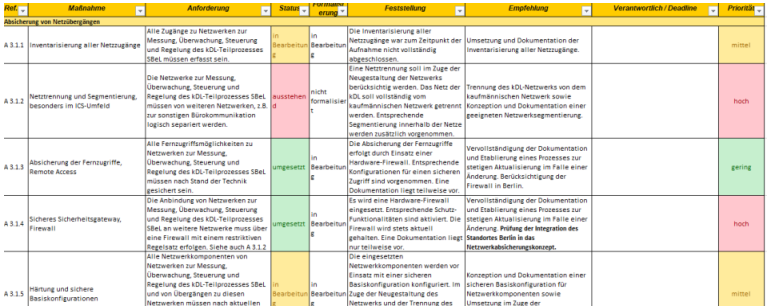
- Umsetzung des Branchenstandards nach §8a Abs. 2 BSIG
  → „Anlagen oder Systeme zur Steuerung / Bündelung elektrischer Leistung (B3S Aggregatoren)" des BDEW
  → Starten einer GAP Analyse der Kerndienstleistung (KDL)
  - Ziel: Schließen von operativen Lücken (GAP)

➔ Unmittelbare Registrierung (https://mip.bsi.bund.de/registerstart)

Und nun? Maßnahmenplan gem. B3S

1. Informationssicherheitsmanagement-system (ISMS)
2. Risikoanalysemethoden
3. Continuity und Notfall-Management
4. Asset Management
5. Bauliche / physische Sicherheit
6. Personelle und organisatorische Sicherheit
7. Branchenspezifische Technik
8. Vorfallserkennung und –bearbeitung
9. Überprüfung im laufenden Betrieb
10. Externe Informationsversorgung und Unterstützung
11. Lieferanten, Dienstleister und Dritte
12. Technische Informationssicherheit

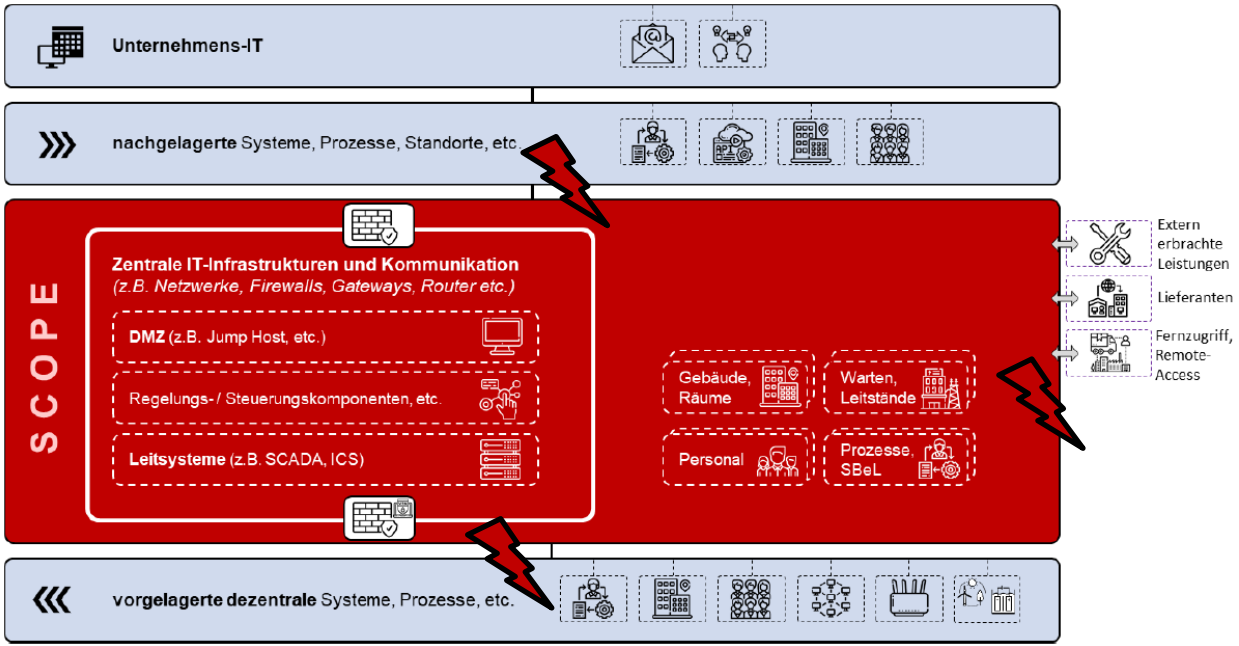
➔ Jeweiliger Verweis auf ISO/IEC 27001 und 27019



Ref.	Maßnahme	Anforderung	Status	Formalisierung	Feststellung	Empfehlung	Verantwortlich / Deadline	Priorität
Absicherung von Netzübergängen								
A 3.1.1	Inventarisierung aller Netzzugänge	Alle Zugänge zu Netzwerken zur Messung, Überwachung, Steuerung und Regelung des kDL-Teilprozesses SBeL müssen erfasst sein.	in Bearbeitung	in Bearbeitung	Die Inventarisierung aller Netzzugänge war zum Zeitpunkt der Aufnahme nicht vollständig abgeschlossen.	Umsetzung und Dokumentation der Inventarisierung aller Netzzugänge.		mittel
A 3.1.2	Netztrennung und Segmentierung, besonders im ICS-Umfeld	Die Netzwerke zur Messung, Überwachung, Steuerung und Regelung des kDL-Teilprozesses SBeL müssen von weiteren Netzwerken, z.B. zur sonstigen Bürokommunikation logisch separiert werden.	ausstehend	nicht formalisiert	Eine Netztrennung soll im Zuge der Neugestaltung der Netzwerks berücksichtig werden. Das Netz der kDL soll vollständig vom kaufmännischen Netzwerk getrennt werden. Entsprechende Segmentierung innerhalb der Netze werden zusätzlich vorgenommen.	Trennung des kDL-Netzwerks von dem kaufmännischen Netzwerk sowie Konzeption und Dokumentation einer geeigneten Netzwerksegmentierung.		hoch
A 3.1.3	Absicherung der Fernzugriffe, Remote Access	Alle Fernzugriffsmöglichkeiten zu Netzwerken zur Messung, Überwachung, Steuerung und Regelung des kDL-Teilprozesses SBeL müssen nach Stand der Technik gesichert sein.	umgesetzt	in Bearbeitung	Die Absicherung der Fernzugriffe erfolgt durch Einsatz einer Hardware-Firewall. Entsprechende Konfigurationen für einen sicheren Zugriff sind vorgenommen. Eine Dokumentation liegt teilweise vor.	Vervollständigung der Dokumentation und Etablierung eines Prozesses zur stetigen Aktualisierung im Falle einer Änderung. Berücksichtigung der Firewall in Berlin.		gering
A 3.1.4	Sicheres Sicherheitsgateway, Firewall	Die Anbindung von Netzwerken zur Messung, Überwachung, Steuerung und Regelung des kDL-Teilprozesses SBeL an weitere Netzwerke muss über eine Firewall mit einem restriktiven Regelsatz erfolgen. Siehe auch A 3.1.2	umgesetzt	in Bearbeitung	Es wird eine Hardware-Firewall eingesetzt. Entsprechende Schutz-Funktionalitäten sind aktiviert. Die Firewall wird stets aktuell gehalten. Eine Dokumentation liegt nur teilweise vor.	Vervollständigung der Dokumentation und Etablierung eines Prozesses zur stetigen Aktualisierung im Falle einer Änderung. **Prüfung der Integration des Standortes Berlin in das Netzwerkabsicherungskonzept.**		hoch
A 3.1.5	Härtung und sichere Basiskonfigurationen	Alle Netzwerkkomponenten von Netzwerken zur Messung, Überwachung, Steuerung und Regelung des kDL-Teilprozesses SBeL und von Übergängen zu diesen Netzwerken müssen nach aktuellen	in Bearbeitung	in Bearbeitung	Die eingesetzten Netzwerkkomponenten werden vor Einsatz mit einer sicheren Basiskonfiguration konfiguriert. Im Zuge der Neugestaltung des Netzwerks und der Trennung des	Konzeption und Dokumentation einer sicheren Basiskonfiguration für Netzwerkkomponenten sowie Umsetzung im Zuge der		mittel

Und nun? Maßnahmenplan gem. B3S

1. Informationssicherheitsmanagementsystem (ISMS) für die Kerndienstleistung - gem. ISO/IEC 27001 „Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Anforderungen“



Und nun? Maßnahmenplan gem. B3S

2. Risikoanalysemethoden
   - → Risikoreduktion oder Risikovermeidung in Bezug auf die 21 benannten Bedrohungskategorien und Schwachstellen bzw. Gefährdungen.
   - → B3S zählt hier die branchenspezifische Relevanz auf

Hacking und Manipulation

Unbefugter Zugriff

Terroristische Akte

Schadprogramme

Naturgefahren

Manipulation, Diebstahl, …

Social Engineering

Identitätsmissbrauch

Missbrauch (Innentäter)

Unbefugter Zugriff

Gezielte Störung

Abhängigkeit von Dienstleistern und Herstellern

Und nun? Maßnahmenplan gem. B3S

3. Continuity und Notfall-Management
   → Betreiber muss kDL auch bei IT-Störungen und Angriffen - soweit möglich – aufrecht erhalten

4. Asset Management
   → Identifizierung, Klassifizierung und Inventarisierung informationstechnischer Prozesse, Systeme und Komponenten sowie deren Verantwortliche

5. Bauliche / physische Sicherheit
   → Zutritt und Zugriff auf sensible Bereiche für Unbefugte verhindern

6. Personelle und organisatorische Sicherheit
   → Sabotageschutz im Unternehmen (innere Sicherheit)

Und nun? Maßnahmenplan gem. B3S

7. Branchenspezifische Technik
   → Sicherheitsniveau muss dem Stand der Technik entsprechen

8. Vorfallserkennung und -bearbeitung
   → IT-Vorfälle, Störungen und Angriffe zeitnah (kontinuierlich) detektieren, behandeln (Nach KristisV 2.0) nun auch explizit gefordert

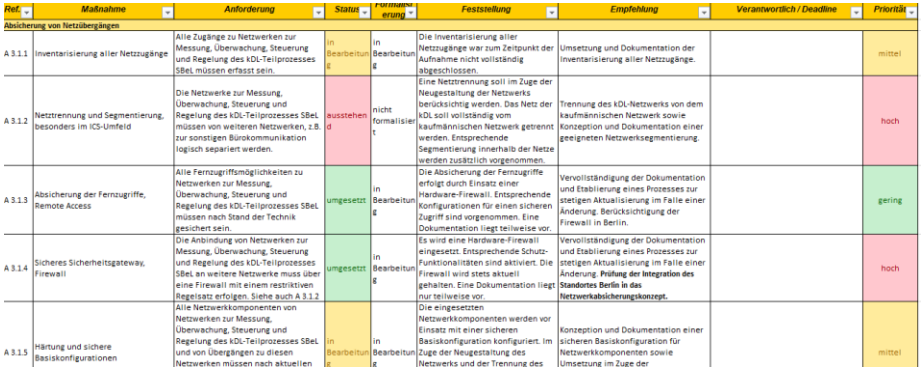
9. Überprüfung im laufenden Betrieb
   → Effektivität der ergriffenen Maßnahmen regelmäßig durch Betreiber zu überprüfen

10. Externe Informationsversorgung und Unterstützung
    → Beschaffung und Bearbeitung von externen und internen sicherheitsrelevanten Informationen (z.B. BSI IT-Tageslagebericht)

Und nun? Maßnahmenplan gem. B3S

11. Lieferanten, Dienstleister, Dritte
    → Sicherheitsanforderungen durch Lieferanten, Dienstleister und Dritte gewährleisten

12. Technische Informationssicherheit
    → Anhang „Maßnahmen Technische Informationssicherheit“ umsetzen



Ref.	Maßnahme	Anforderung	Status	Formalisierung	Feststellung	Empfehlung	Verantwortlich / Deadline	Priorität
Absicherung von Netzübergängen								
A 3.1.1	Inventarisierung aller Netzzugänge	Alle Zugänge zu Netzwerken zur Messung, Überwachung, Steuerung und Regelung des kDL-Teilprozesses SBeL müssen erfasst sein.	in Bearbeitung	in Bearbeitung	Die Inventarisierung aller Netzzugänge war zum Zeitpunkt der Aufnahme nicht vollständig abgeschlossen.	Umsetzung und Dokumentation der Inventarisierung aller Netzzugänge.		mittel
A 3.1.2	Netztrennung und Segmentierung, besonders im ICS-Umfeld	Die Netzwerke zur Messung, Überwachung, Steuerung und Regelung des kDL-Teilprozesses SBeL müssen von weiteren Netzwerken, z.B. zur sonstigen Bürokommunikation logisch separiert werden.	ausstehend	nicht formalisiert	Eine Netztrennung soll im Zuge der Neugestaltung der Netzwerks berücksichtig werden. Das Netz der kDL soll vollständig vom kaufmännischen Netzwerk getrennt werden. Entsprechende Segmentierung innerhalb der Netze werden zusätzlich vorgenommen.	Trennung des kDL-Netzwerks von dem kaufmännischen Netzwerk sowie Konzeption und Dokumentation einer geeigneten Netzwerksegmentierung.		hoch
A 3.1.3	Absicherung der Fernzugriffe, Remote Access	Alle Fernzugriffsmöglichkeiten zu Netzwerken zur Messung, Überwachung, Steuerung und Regelung des kDL-Teilprozesses SBeL müssen nach Stand der Technik gesichert sein.	umgesetzt	in Bearbeitung	Die Absicherung der Fernzugriffe erfolgt durch Einsatz einer Hardware-Firewall. Entsprechende Konfigurationen für einen sicheren Zugriff sind vorgenommen. Eine Dokumentation liegt teilweise vor.	Vervollständigung der Dokumentation und Etablierung eines Prozesses zur stetigen Aktualisierung im Falle einer Änderung. Berücksichtigung der Firewall in Berlin.		gering
A 3.1.4	Sicheres Sicherheitsgateway, Firewall	Die Anbindung von Netzwerken zur Messung, Überwachung, Steuerung und Regelung des kDL-Teilprozesses SBeL an weitere Netzwerke muss über eine Firewall mit einem restriktiven Regelsatz erfolgen. Siehe auch A 3.1.2	umgesetzt	in Bearbeitung	Es wird eine Hardware-Firewall eingesetzt. Entsprechende Schutz-Funktionalitäten sind aktiviert. Die Firewall wird stets aktuell gehalten. Eine Dokumentation liegt nur teilweise vor.	Vervollständigung der Dokumentation und Etablierung eines Prozesses zur stetigen Aktualisierung im Falle einer Änderung. **Prüfung der Integration des Standortes Berlin in das Netzwerkabsicherungskonzept.**		hoch
A 3.1.5	Härtung und sichere Basiskonfigurationen	Alle Netzwerkkomponenten von Netzwerken zur Messung, Überwachung, Steuerung und Regelung des kDL-Teilprozesses SBeL und von Übergängen zu diesen Netzwerken müssen nach aktuellen	in Bearbeitung	in Bearbeitung	Die eingesetzten Netzwerkkomponenten werden vor Einsatz mit einer sicheren Basiskonfiguration konfiguriert. Im Zuge der Neugestaltung des Netzwerks und der Trennung des	Konzeption und Dokumentation einer sicheren Basiskonfiguration für Netzwerkkomponenten sowie Umsetzung im Zuge der		mittel

DEUTSCHE
WINDGUARD

Beste Grüße vom WindGuard-Team

Head of Technical Management
Andre Reichert
+49 (0)4451 9515-198

andre.reichert@windguard.de