



IT-Security in der Windbranche

Peter Sode | Operations & Maintenance
09. November 2022



IT-Security in der Windbranche

Agenda

01

Vorstellung der neuen JUWI
Wo stehen wir aktuell

02

Kommunikationsschema einer typischen WEA
Wer hat Zugriff auf eine WEA?
Was sind die typischen Kommunikationswege?

03

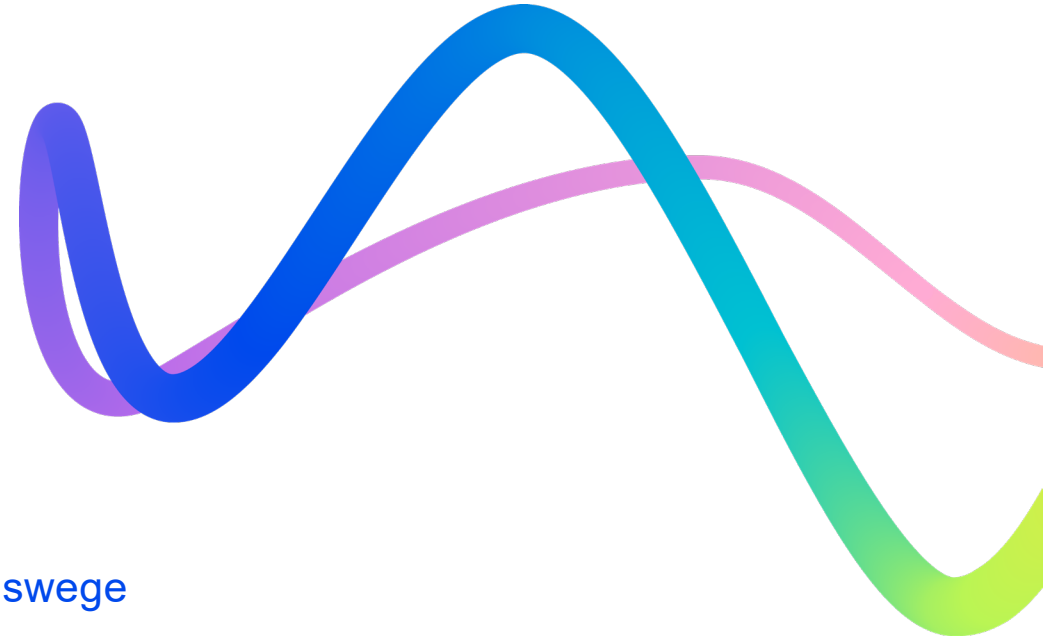
IT Sicherheit der Datenfernübertragung / Kommunikationswege
Schutz der Übertragungswege / Datenverbindungen
Beispiel zur PublicIP Problematik


04

Router Management für eine bessere IT-Sicherheit

05

Zukünftige Herausforderungen
Erhöhtes Datenaufkommen
BNK
Wechsel von IPv4 auf IPv6



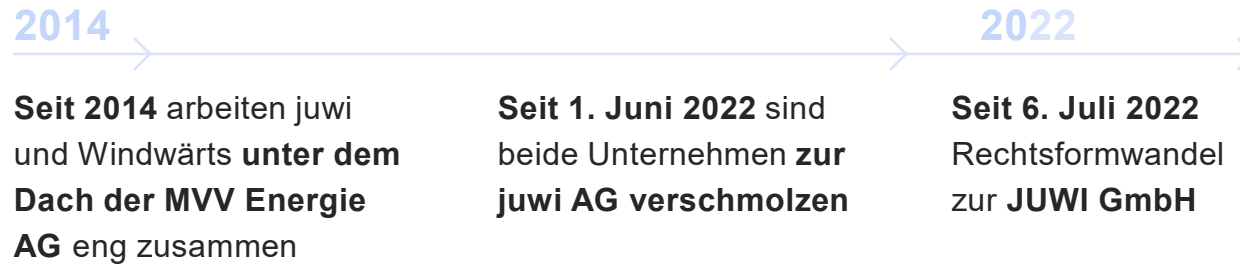


Unser Ziel: 100 Prozent erneuerbare
Energien. Packen wir's gemeinsam an!

Aus juwi und Windwärts wird JUWI

Mit langjähriger Erfahrung und Kompetenz – für noch mehr gute Energie

Beide Unternehmen zählen **seit mehr als 25 Jahren** zu den führenden Projektentwicklern und Betriebsführern in der Branche der erneuerbaren Energien



Gemeinsam ...

1.200

Windenergieanlagen mit einer Leistung von 2.900 MW ans Netz gebracht

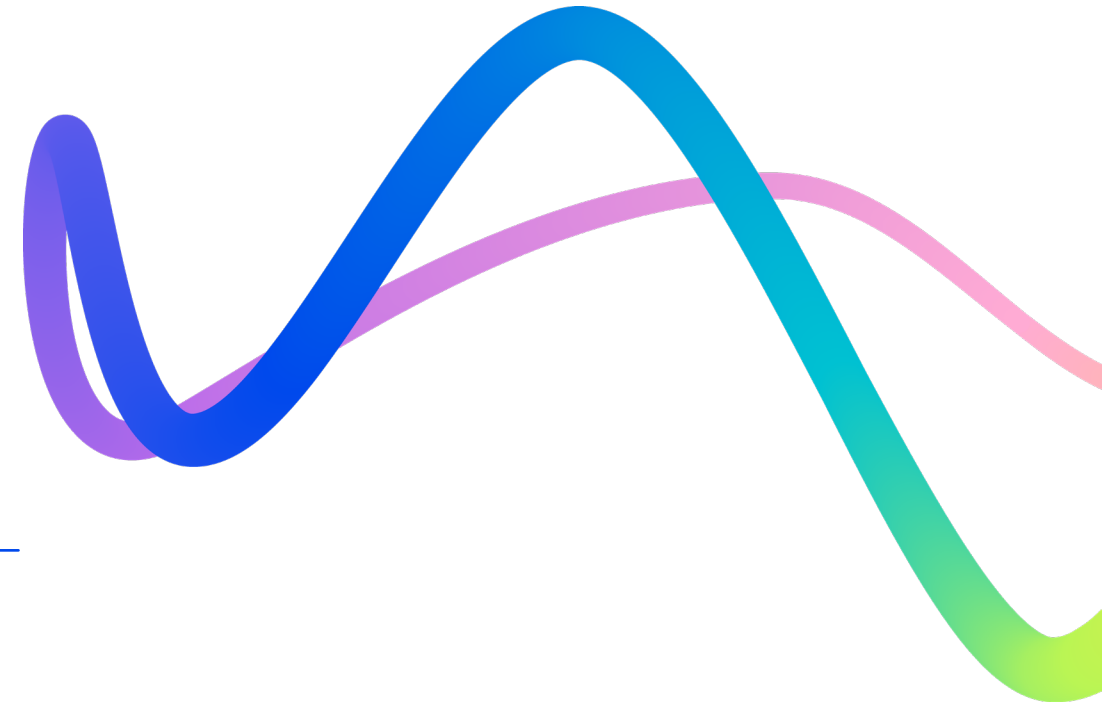
~3.500 MW

installierte PV-Leistung realisiert

~2.700 MW

Solar- und Windenergieleistung **in der Betriebsführung, deutschlandweit***

* Weltweit fast 5.000 MW Gesamtleistung



Wer sind wir?

Niederlassungen in Deutschland



Hauptsitz

Wörrstadt

LK Alzey-Worms, Rheinland-Pfalz



Standorte

Brandis (Sachsen)

Hannover (Niedersachsen)*



Regionalbüros

Bochum (Nordrhein-Westfalen)

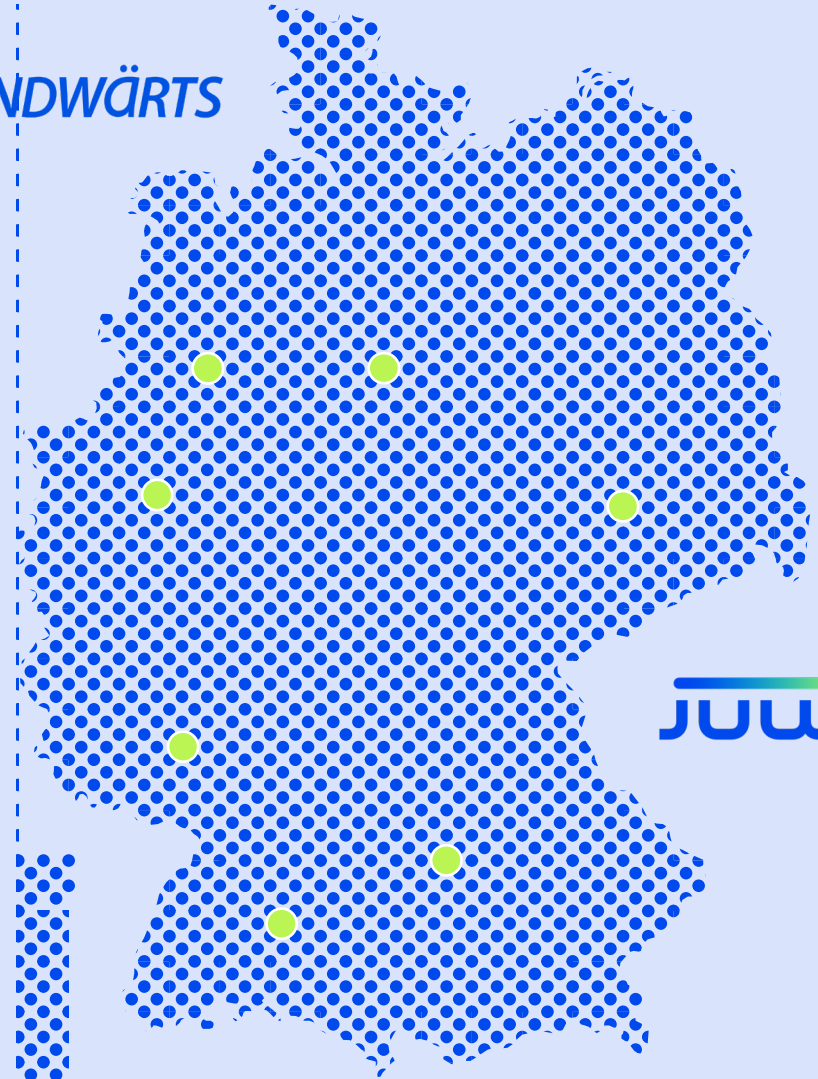
Dürrwangen (Bayern)

Osnabrück (Niedersachsen)*

Stuttgart (Baden-Württemberg)

*ehemals Windwärts

WINDWÄRTS



JUWI

Windenergie Deutschland

Wir wissen, woher der Wind weht



Linnich

- Kreis Düren
- Nordrhein-Westfalen
- 25,4 MW (8 Anlagen)



Kirchberg

- Rhein-Hunsrück-Kreis
- Rheinland-Pfalz
- 52,9 MW (23 Anlagen)



Thaden

- Kreis Rendsburg-Eckernförde
- Schleswig-Holstein
- 15 MW (4 Anlagen)

> **1.000** Anlagen an rund 80 Standorten

ca. 4,8 Mrd. kWh Jahresenergieertrag

ca. 2.700 MW Gesamtleistung

Windenergie international

Wir wissen, woher der Wind weht



Flatwater

- Nebraska
- USA
- 60 MW (40 Anlagen)



Garob

- Northern Cape
- Südafrika
- 144,9 MW (46 Anlagen)



Guanacaste

- Provinz Guanacaste
- Costa Rica
- 49,5 MW (55 Anlagen)

> **1.200** Anlagen an rund 200 Standorten

ca. 5,7 Mrd. kWh Jahresenergieertrag

ca. 2.800 MW Gesamtleistung

Wo stehen wir aktuell?

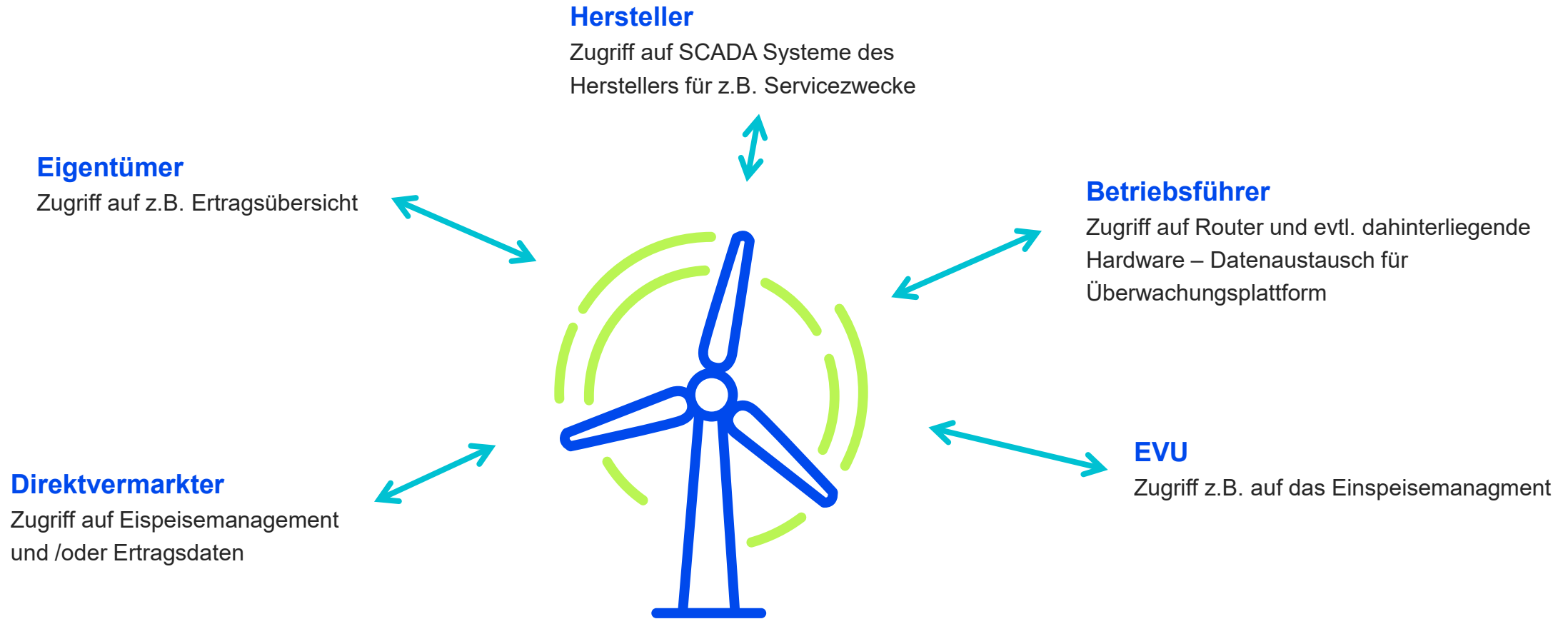
Ein kurzer Blick in die Gegenwart

- Die Sicherheit von Energieerzeugungs-Anlagen spielt eine immer größere Rolle. Durch die fortschreitende Digitalisierung sowie neue Kommunikationswege wird auch die Sicherheit der IT-Infrastruktur immer bedeutsamer.
- Energieerzeugungs-Anlagen sind immer häufiger Ziele für organisierte Angriffe von Hackern.
- Größte Schwachstelle sind die Mitarbeiter und veraltete Systeme
- Oftmals werden unsichere oder veraltete Kommunikations- bzw. Verschlüsselungsmethoden verwendet



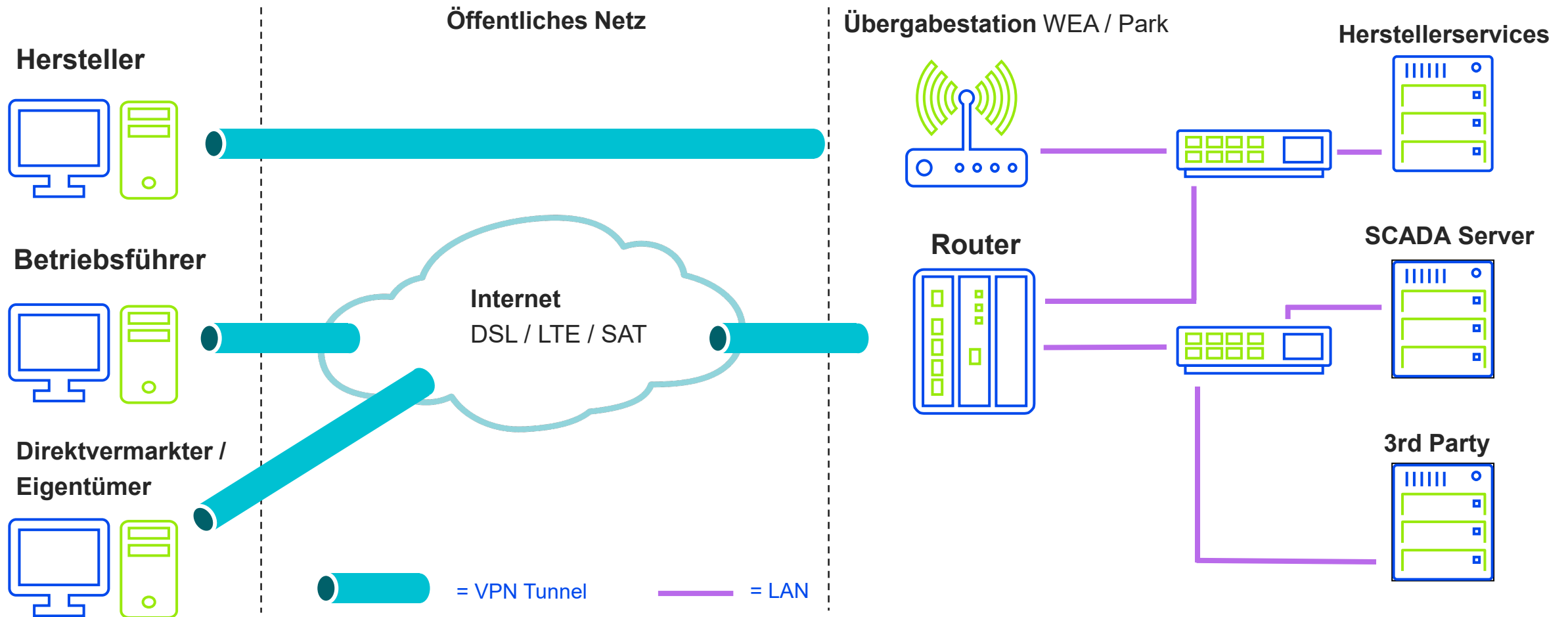
Kommunikationsschema einer typischen WEA

Wer hat Zugriff auf eine WEA?



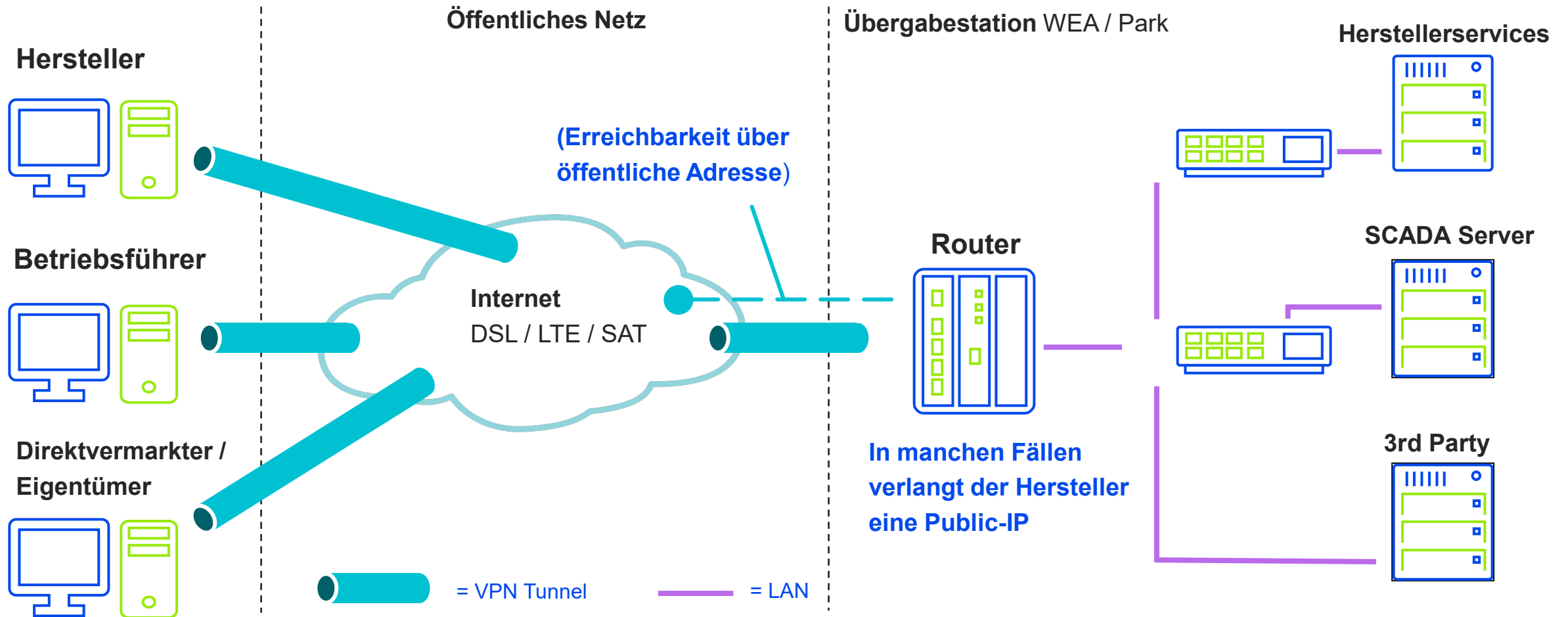
Kommunikationschema einer typischen WEA

Was sind die typischen Kommunikationswege? (Getrennte Router)



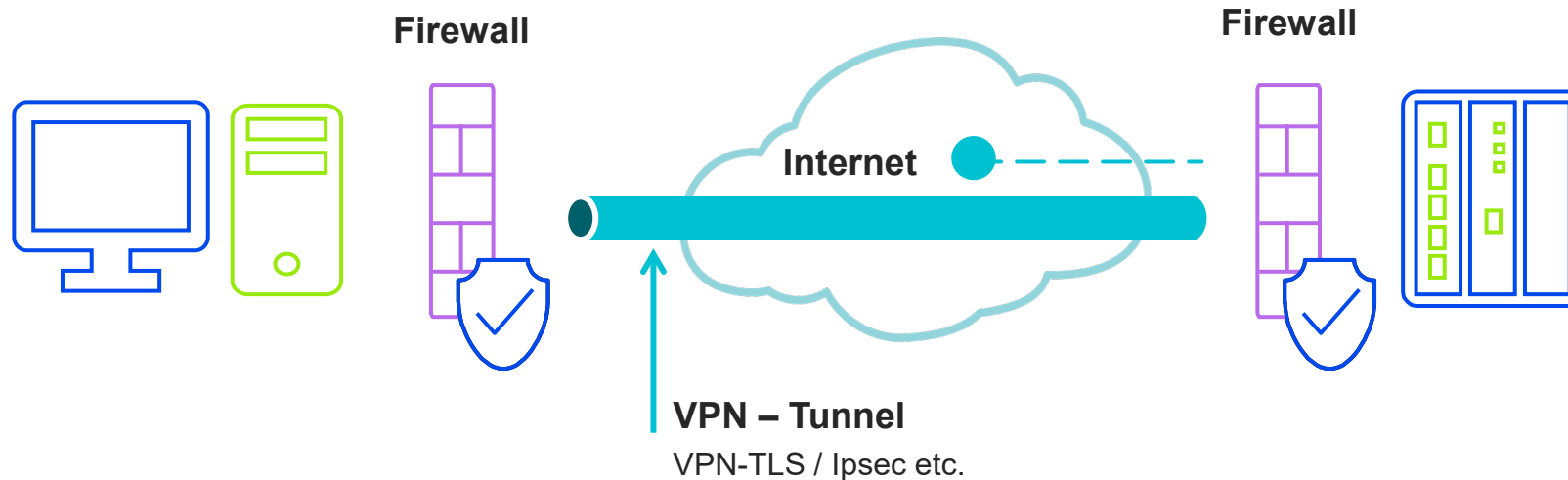
Kommunikationschema einer typischen WEA

Was sind die typischen Kommunikationswege? (Getrennte Router)



IT-Sicherheit der Datenfernübertragung / Kommunikationswege

Schutz der Übertragungswege / Datenverbindungen



Public-IP

Einige Hersteller verlangen eine Public-IP für den Zugriff auf den Windpark. Zwar werden die Datenverbindungen durch die VPN-Tunnel geschützt, dennoch ist eine öffentliche IP-Adresse im Internet leicht zu finden und ermöglicht es Angreifern, evtl. Schaden anzurichten. Öffentliche IP-Adressen sollten daher in Zukunft möglichst vermieden werden.

IT-Sicherheit der Datenfernübertragung / Kommunikationswege

Beispiel zur Public-IP Problematik

- PublicIPs haben den Nachteil, dass diese frei aus dem Internet heraus gefunden werden können
- Die Absicherung der Systeme mit einem Passwort etc. ist in den meisten Fällen gegeben
- Die Daten laufen in der Regel über einen VPN-Tunnel, die Weboberflächen für z.B. Serviceeinsätze sind aber sehr oft für jeden erreichbar



Auch wenn eine zusätzliche Absicherung erfolgt, ist dies eine potenzielle Schwachstelle, welche man leicht unterbinden kann. Wenn ein Angreifer erstmal auf einem System ist, oder eine Netzwerkkomponente gefunden hat, ist für ihn der erste Schritt getan!

Weitere mögliche Schutzmaßnahmen:

- Nur bestimmte Dienste zulassen und andere benutzte Ports sperren
- Standardbenutzer und Standardpasswort ändern

IT-Sicherheit in der Datenfernübertragung / Kommunikationswege

Beispiel zur Public-IP Problematik

The screenshot shows the EasyOperation S2350-28TP-EI-AC web interface. A 'Modify User' dialog box is open, allowing the user to change the 'admin' user's password and level. The dialog box includes fields for 'User name', 'Old password', 'New password', 'Confirm password', and 'Level'. The 'Level' is currently set to 'Administrator'. The background interface shows a 'Monitor' section with a 'Panel' view of network slots, a 'System Description' section with details like Product ID, Device name, Uptime, Serial number, MAC, Software, Running patch, and Web platform version, and a 'Log' section showing recent login attempts.

Modify User Dialog:

- * User name: admin (1~64characters)
Can not be / : * ? " < > | ' % , @ can not in the first place.
- * Old password: (8~128characters)
- * New password: (8~128characters)
In order to enhance password security, including at least 2 of the following characters: the uppercase letters, lowercase letters, numbers, special symbols (for example #, !, \$, %).
Can not be blank and the single quotes.
- * Confirm password: (8~128characters)
- * Level: Administrator
Monitor-level user: only the ping tracer operation right.
Management-level user: all operation rights.

System Description:

- Product ID: S2350-28TP-EI-AC
- Device name: VESTAS-ENERJI-HATAY-TT-ME
- Uptime: 2h49m27s
- Serial number: 210235524610E5000292
- MAC: 4862-76FF-94C3
- Software: V200R005C00SPC300
- Running patch: ---
- Web platform version: V200R005C00.720

TOP5 Bandwidth Utilization:

Port Name	Inbound	Outbound
Ethernet0/0/1	0%	0%
Ethernet0/0/2	0%	0%

Log:

Time	Log Content
Oct 1 2008 02:50:07	User login failed. (UserName=admin,...)
Oct 1 2008 02:50:00	User login failed. (UserName=admin,...)

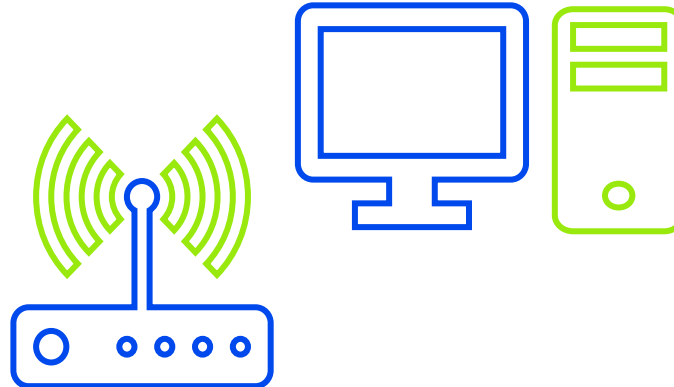
IT-Sicherheit in der Datenfernübertragung / Kommunikationswege

Zugriff auf Hardware schützen

**Standardbenutzer nach
Einrichtung löschen!**

**Möglichst wenige
Benutzer hinterlegen**

**Personalisierte
Benutzer**



**Regelmäßige Änderung
der Passwörter**

**Hardware im Schrank durch
z.B. Schlüssel schützen**

**Zugang zur WEA
absichern**

Routermanagement für eine bessere IT-Sicherheit

- Zugriff auf den Router nur für Personen aus dem entsprechenden Fachbereich (Fachkenntnisse)
- Prozess für eine kontinuierliche Überwachung der Benutzer sowie Passwörter (Ausscheiden eines Kollegen, Wechsel der Abteilung)
- Dokumentation des Routers incl. Backupdateien sicher aufbewahren, z.B. auf einem SharePoint / gesichertes Netzlaufwerk
- Prozess zur regelmäßigen Überprüfung auf Sicherheitsupdates oder wichtige Firmwareupdates
- Nicht verwendete Ports des Routers sperren – nur ein Port zur Konfiguration ermöglichen
- Whitelist anstatt Blacklist: Firewall blockt alles, bis auf freigegebene Verbindungen



JUWI ist nach ISO27001 zertifiziert

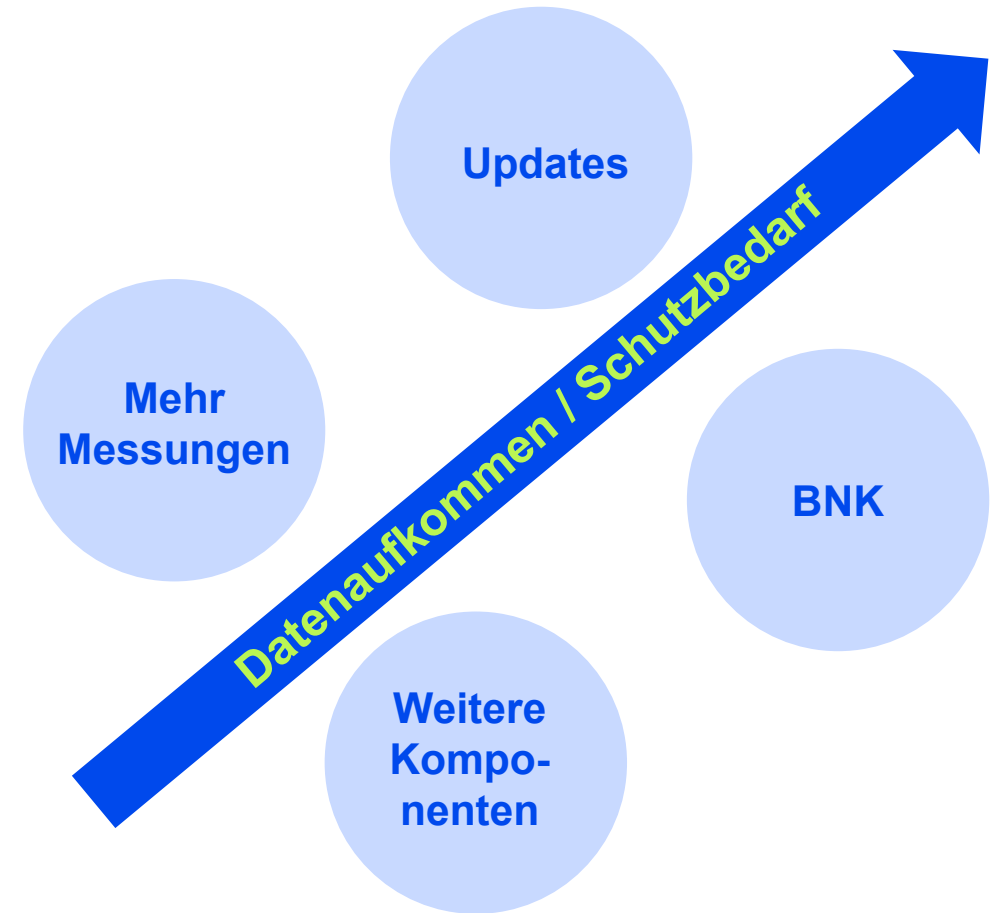
- Als Betreiber kritischer Infrastruktur ist JUWI verpflichtet, ein ISMS zu führen
- Dieses ISMS ist vom TÜV geprüft und im letzten Audit Ende 2021 erfolgreich rezertifiziert worden
- Das Managementsystem wird fortlaufend und kontinuierlich verbessert
 - Durch regelmäßige Audits wird die Wirksamkeit des ISMS geprüft



Zukünftige Herausforderungen

Erhöhtes Datenaufkommen

- Durch die fortschreitende Digitalisierung und neuer moderner Techniken nimmt das Datenaufkommen einer Windenergieanlage rasant zu.
- Dies stellt in erster Linie keinen Aspekt der IT-Sicherheit dar, dennoch ist es eine Herausforderung, welche es zu meistern gilt.
- LTE-Tarife sind für sehr hohe Datenaufkommen immer noch sehr teuer. Ein Umbau auf Alternativen (DSL) ist empfehlenswert
- Durch Umbauarbeiten und weitere, neue Komponenten können weitere IT-Sicherheitsrisiken entstehen.



Zukünftige Herausforderungen

BNK (Bedarfsgerechte Nachtkennzeichnung)

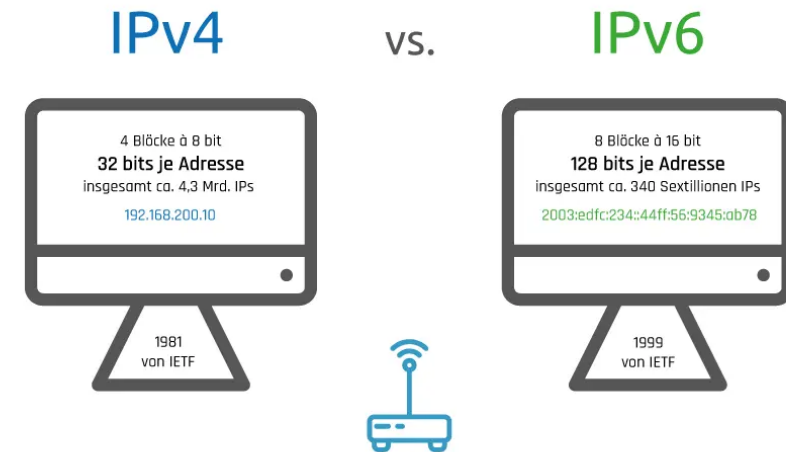
- Die BNK wird ab dem 01.01.2023 Pflicht
- Durch die BNK kommen weitere Komponenten zur Anlage hinzu.
- Auch die neuen Komponenten müssen abgesichert werden und durch Fremdzugriffe geschützt werden
- Die BNK benötigt eine weitere Schnittstelle des Routers -> Weiterer Angriffspunkt bzw. Schwachstelle
- Es ist sicher zu stellen, dass alle Komponenten und Verbindungen die IT-Sicherheit gewährleisten können.



Zukünftige Herausforderungen

Wechsel von IPv4 auf IPv6

- Am 25.11.2019 wurde in Europa der letzte Block IPv4 Adressen vergeben.
- IPv4 Public-IPs, welche viele WEA-Hersteller noch verlangen, werden bald nicht mehr verfügbar sein.
 - Telekom und Vodafone bieten diese schon gar nicht mehr an
- Unternehmen müssen sich langfristig auf den Umstieg auf IPv6 vorbereiten, dies läuft allerdings sehr schleppend
 - Umbauaufwand / Komponentenaustausch / Schulungen der Mitarbeiter
- Wenn auf IPv6 umgerüstet wird, so wird dies auch neue Herausforderungen in der IT-Sicherheit mit sich bringen
 - Neue Spezifikationen / Vorgaben





Peter Sode

Head of Data Management & Security
Operations & Maintenance

Telefon: +49 6732 9657 5126

E-Mail: peter.sode@juwi.de

