Erneuerbare Energien in der MVV Gruppe

Sicher ist sicher:
Gewährleistung der IT-Sicherheit von Windenergie-Anlagen

Peter Sode – juwi Operations & Maintenance – Monitoring Systems – 10.11.2021

Sicher ist sicher: Gewährleistung der IT-Sicherheit von Windenergie-Anlagen

Agenda

Wo stehen wir aktuell?

Kommunikationsschema einer typischen WEA

- Wer hat Zugriff auf eine WEA?
- Was sind typische Kommunikationswege?

IT Sicherheit der Datenfernübertragung / Kommunikationswege

- Schutz der Übertragungswege / Datenverbindungen
- Beispiel zur PublicIP Problematik
- Zugriffe auf Hardware schützen

Router Management für eine bessere IT-Sicherheit

Zukünftige Herausforderungen

- Erhöhtes Datenaufkommen
- BNK
- Wechsel von IPv4 auf IPv6

Quelle: tornedo.de

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

Quelle: iStock

Kommunikationsschema einer typischen WEA

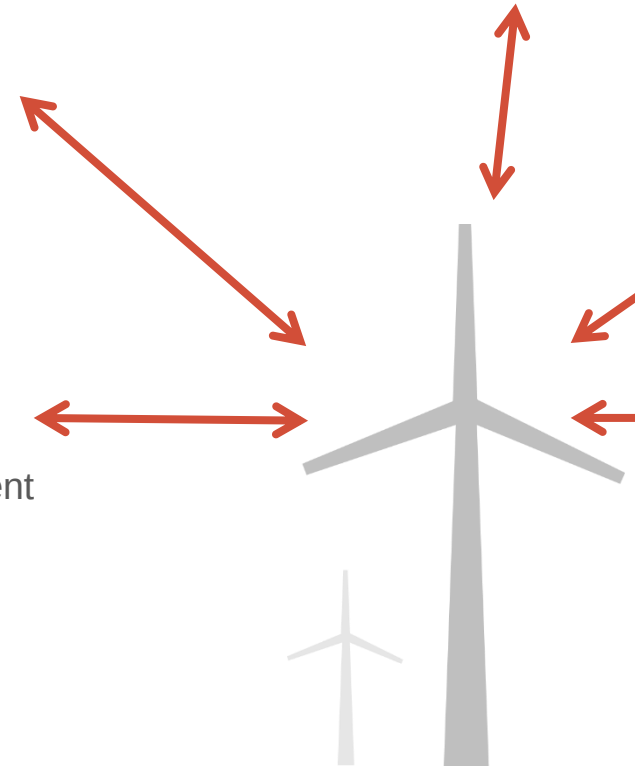
Wer hat Zugriff auf eine WEA?

Zugriff auf eine WEA haben typischerweise:

Hersteller
Zugriff auf SCADA System des Herstellers für z.B. Servicezwecke

Eigentümer
Zugriff auf z.B. Ertragsübersicht

Betriebsführer
Zugriff auf Router und evtl. dahinterliegende Hardware – Außerdem Datenaustausch für Überwachungsplattform

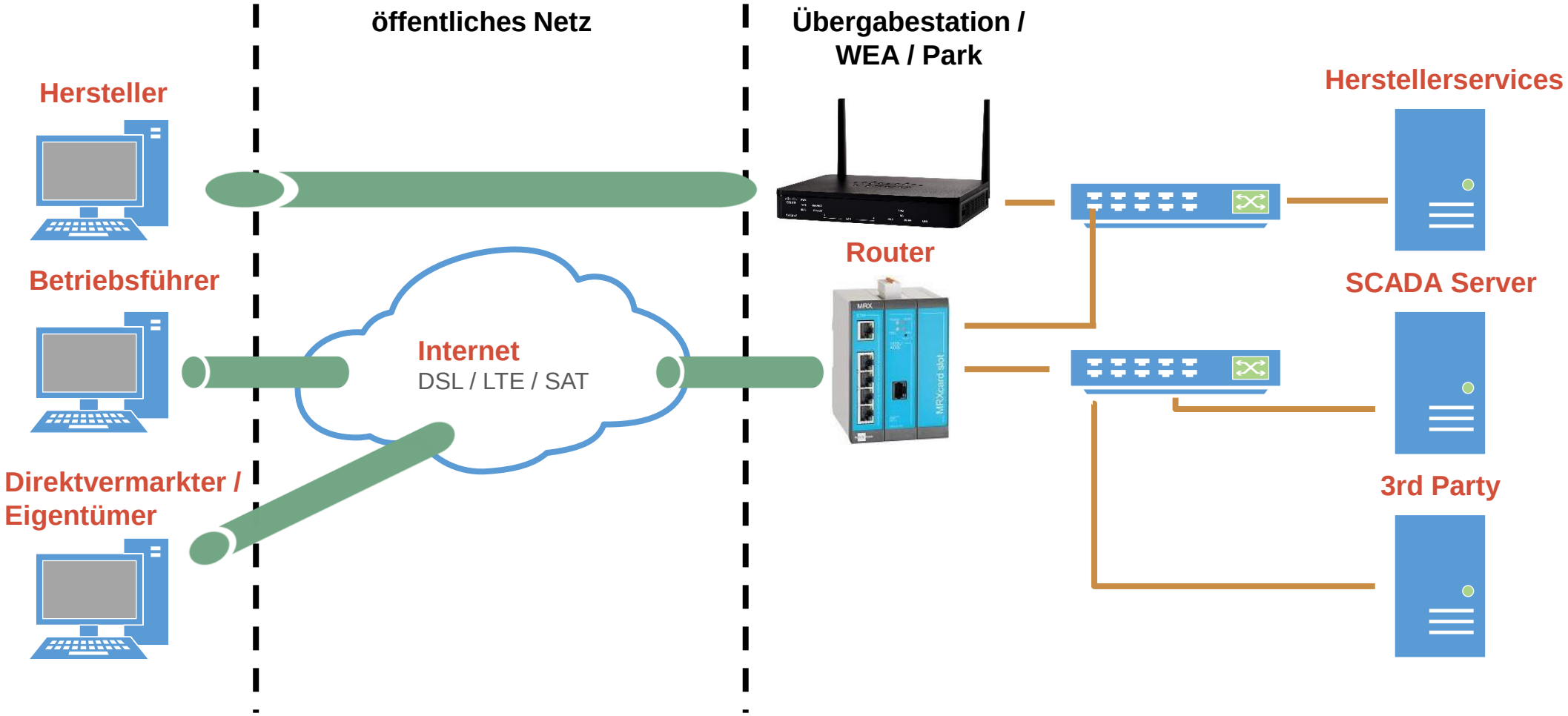


Direktvermarkter
Zugriff auf Einspeisemanagement und/oder Ertragsdaten

EVU
Zugriff auf z.B. das Einspeisemanagement

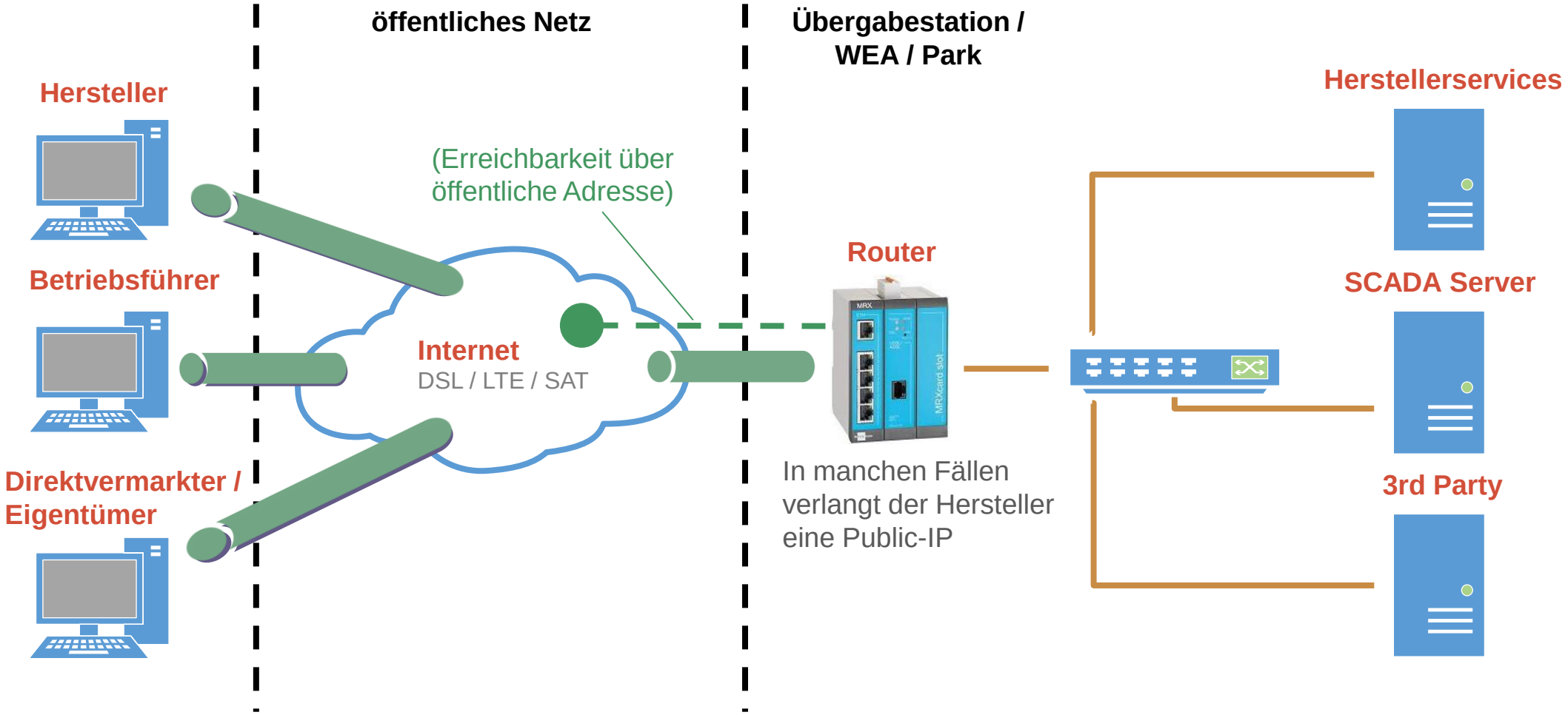
Kommunikationsschema einer typischen WEA

Was sind die typischen Kommunikationswege? (Getrennte Router)



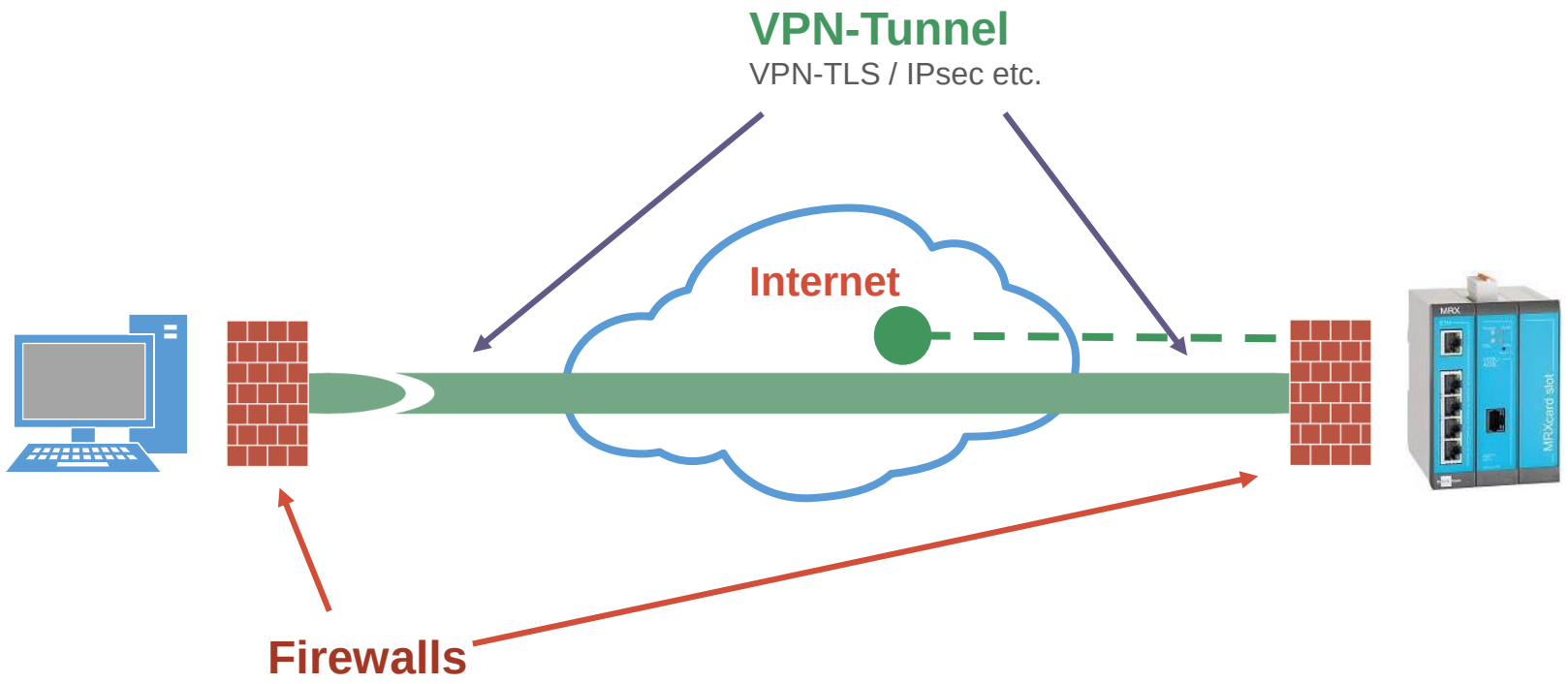
Kommunikationsschema einer typischen WEA

Was sind die typischen Kommunikationswege? (Gemeinsamer 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 der Regel gegeben
- Die Daten laufen in der Regel über einen VPN-Tunnel, die Weboberflächen für z.B. Serviceeinsätze sind aber sehr oft für jeden erreichbar

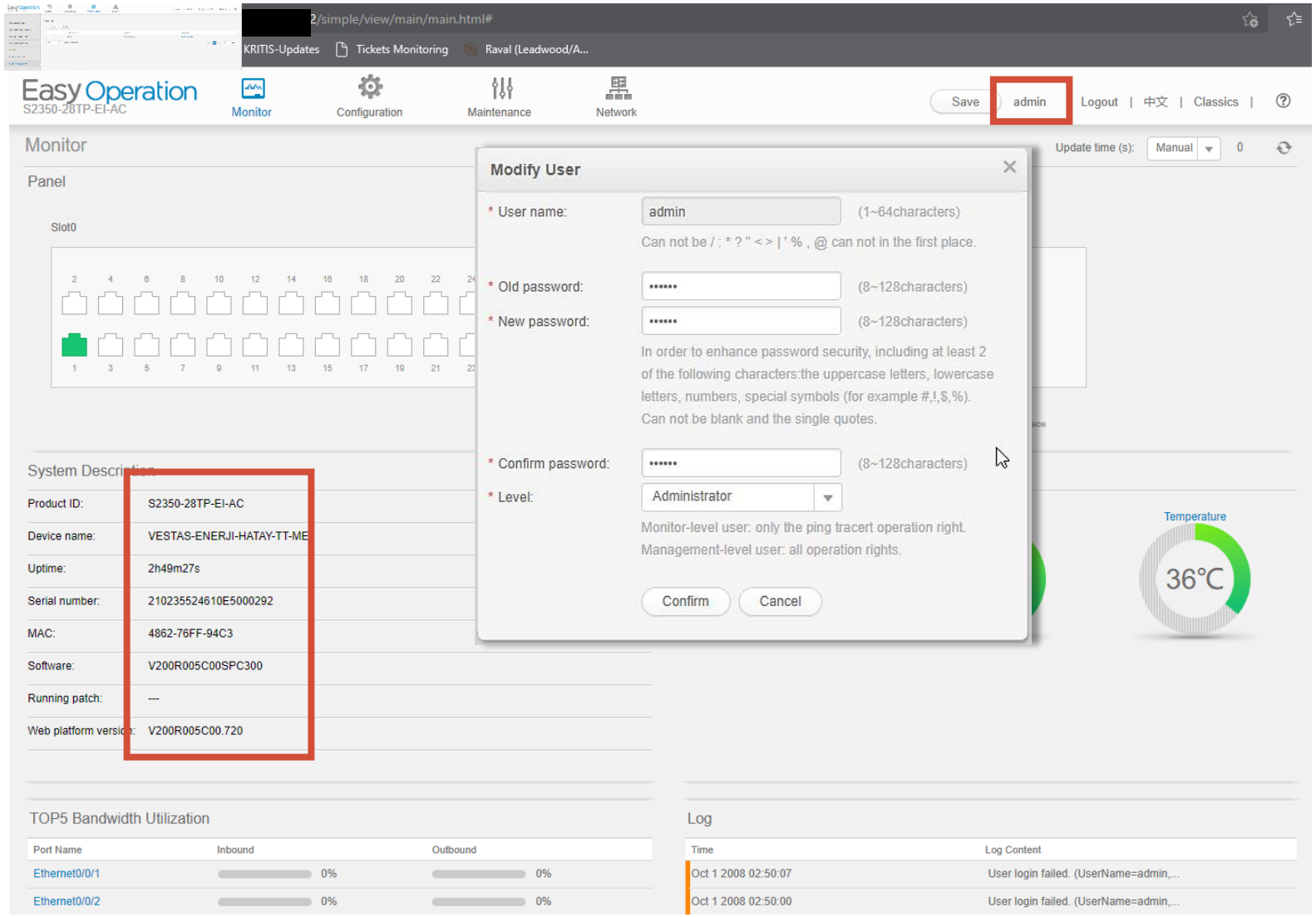
Weitere mögliche Schutzmaßnahmen:

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

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

IT-Sicherheit der Datenfernübertragung / Kommunikationswege

Beispiel zur Public-IP Problematik



IT-Sicherheit der Datenfernübertragung / Kommunikationswege

Zugriffe auf Hardware schützen

Standardbenutzer nach Einrichtung löschen!

Regelmäßige Änderung der Passwörter

Möglichst wenige Benutzer hinterlegen

Hardware im Schrank durch z.B. Schlüssel schützen

Personifizierte Benutzer

Zugang zur WEA absichern

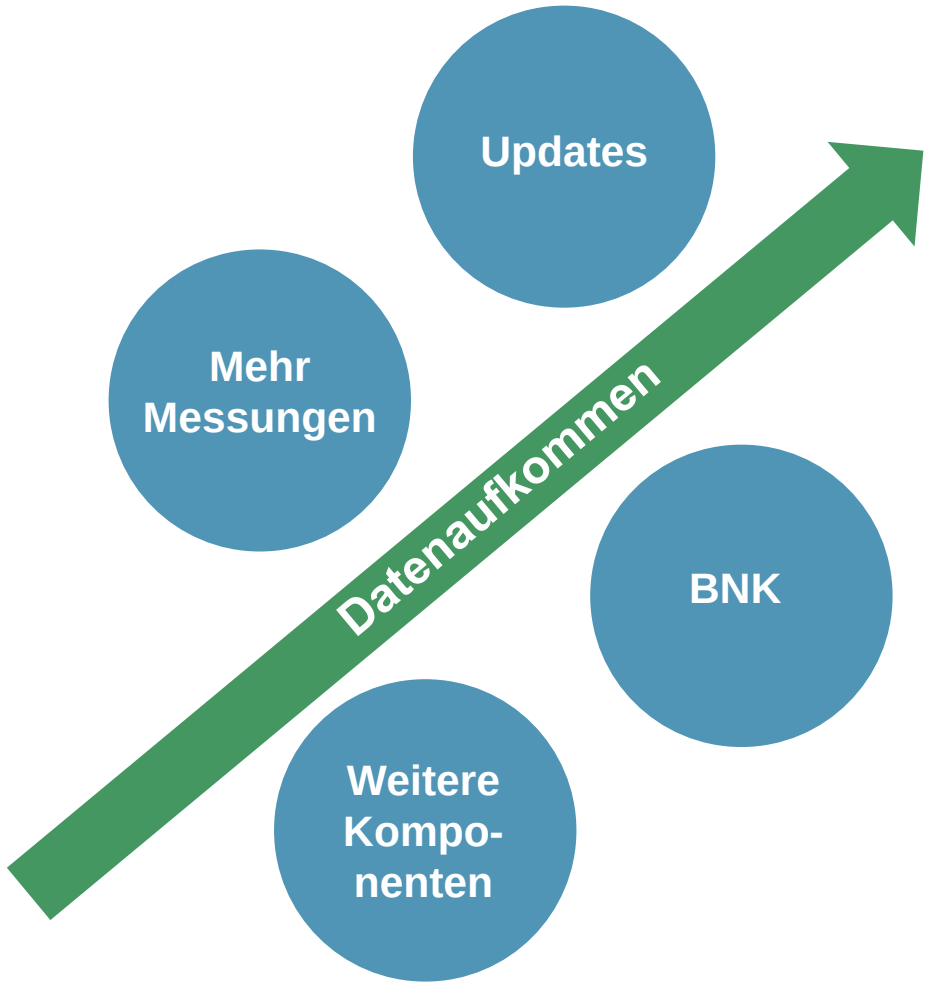
Routermanagement für eine bessere IT-Sicherheit

- 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

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 (Bedarfsgesteuerte Nachtkennzeichnung)

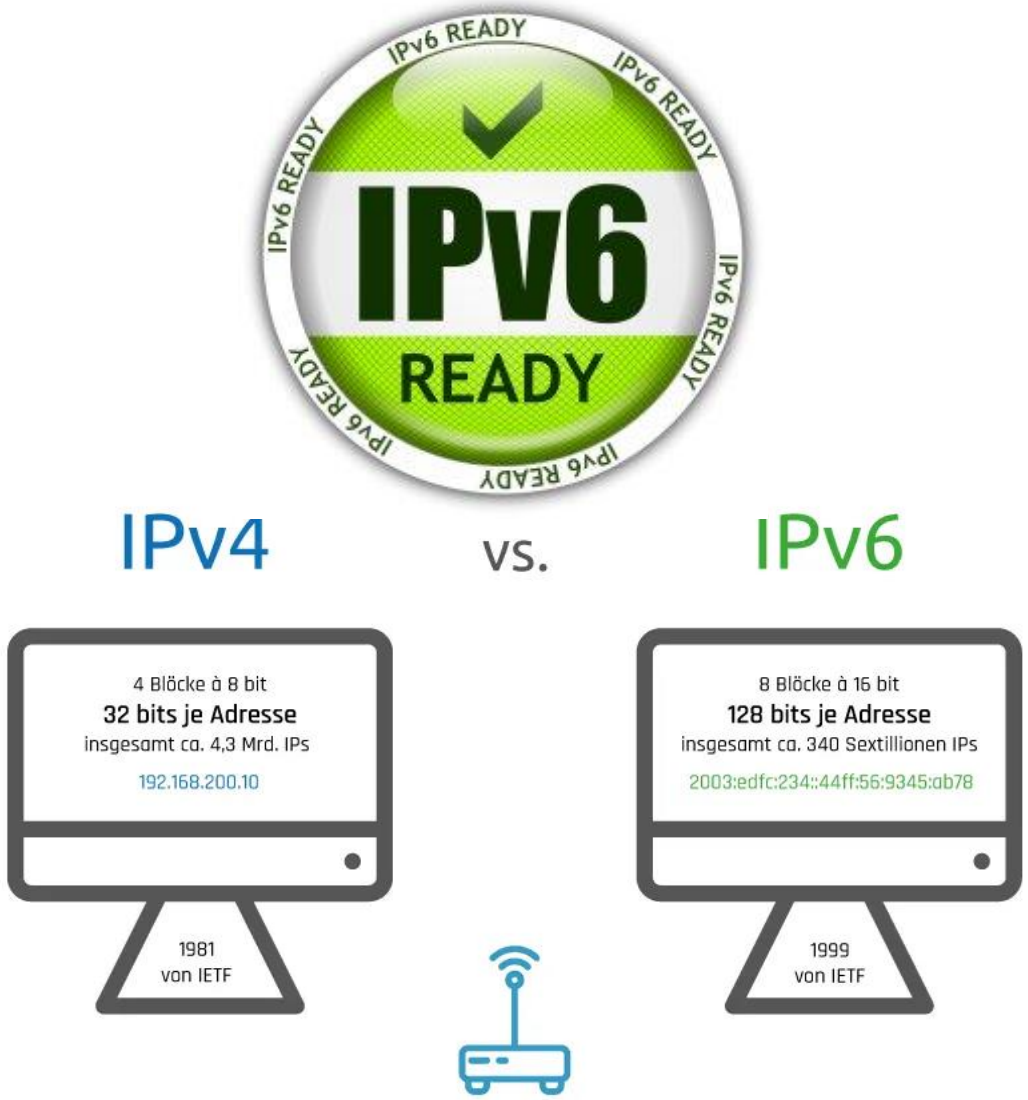
- Die BNK wird ab dem 01.01.2023 Pflicht
- Durch die BNK kommen weitere Komponenten zur Anlage hinzu.
- Auch die neuen Komponenten müssen abgesichert werden und durch Fremdzugriffe geschützt werden
- Die BNK benötigt eine weitere Schnittstelle des Routers -> Weiterer Angriffspunkt bzw. Schwachstelle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

Quelle: Dark-Sky

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



Vielen Dank für Ihre Aufmerksamkeit!

Bei Fragen oder Anregungen melden Sie sich gerne telefonisch oder schreiben mir eine E-Mail:

Peter Sode
juwi Operations & Maintenance GmbH
Teamleader Monitoring Systems & stv. ISB

Telefon: +49 6732 9657 5126
Mobil: +49 162 230 96 67

E-Mail: peter.sode@juwi.de