CYBERSICHERHEIT: SCHUTZ IHRER ANLAGEN

Die Zahl und die Komplexität von Cyberangriffen auf die Branche der Erneuerbaren Energien nehmen ständig zu. Mit mehr als 40 Jahren Erfahrung in Entwicklung, Bau und Betrieb von Wind- und PV-Anlagen wissen wir, wie wichtig der Schutz Ihrer Anlagen ist, damit diese durchgehend zuverlässig, effizient und widerstandsfähig grüne Energie liefern können. Daher ist es unerlässlich, dass wir als Ihr Partner die Vertraulichkeit, Integrität und Verfügbarkeit der uns anvertrauten Daten und Systeme sicherstellen. Wir wissen, dass sich die Sicherheitsbedrohungen ständig ändern und man als Anlagenbetreiber immer wieder dem Risiko einer Eskalation ausgesetzt ist. Aus diesem Grund haben wir ein spezielles OT (Operational Technology)-Team gegründet, das mit Ihnen zusammenarbeitet, um die Widerstandsfähigkeit Ihrer Wind- und PV-Anlagen im Cyberspace zu bewerten und zu verbessern.

Für einen unserer Kunden konnten wir nach Identifizierung der Cybersicherheitsrisiken innerhalb von zwei Monaten eine effiziente und kostengünstige Lösung zum Schutz vor Angriffen implementieren. Diese Lösung wurde inzwischen auf weitere 425 MW an Anlagen ausgeweitet.

UNSERE LEISTUNGEN

Unser Ansatz steht im Einklang mit bewährten Verfahren zur Informationssicherheit, einschließlich des NIST Cyber Security Framework und ISO27001/2, die sowohl für Unternehmens-IT- als auch für OT-Umgebungen gelten. Diese werden jedes Jahr kontinuierlich durch Sicherheitstests bewertet.

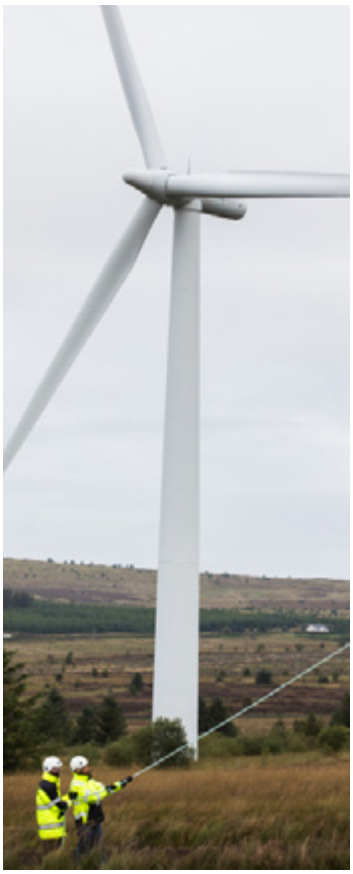
Unsere Maßnahmen zur Cybersicherheit umfassen vier Schlüsselbereiche:

IDENTIFIZIERUNG von Bedrohungen für Daten und Systeme durch Bewertung von Gefahreninformationen und Risikomanagement.

SCHUTZ vor identifizierten Bedrohungen durch die Umsetzung bewährter Sicherheitspraktiken, wie z.B. die Anwendung von Sicherheits-Patches und System-Updates, die Trennung der IT-Umgebung des Unternehmens von der operativen Technologie, den Einsatz von Web-, E-Mail- und Endpunkt-Sicherheitskontrollen und die proaktive Prüfung der Sensibilisierung von Mitarbeiter*innen für Phishing- und E-Mail-Angriffe.

AUFSPÜREN von Problemen mithilfe von Protokollen, Überwachungen, Scans und Penetrationstests.

REAKTION auf Cyberattacken und **WIEDERHERSTELLUNG** der Systeme durch Eindämmungs- und Bereinigungsverfahren, um die Auswirkungen der Attacken zu begrenzen und die Widerstandsfähigkeit der Organisation gegenüber solcher Ereignisse zu maximieren.



Wir bieten verschiedene Leistungsstufen im Bereich der Cybersicherheit an, wie in der folgenden Tabelle dargestellt.

STUFE 1	STUFE 2	STUFE 3
• Cybersicherheitsscan der über das Internet zugänglichen EE-Anlagen um ausnutzbare Schwachstellen am Standort aufzudecken • Schwachstellenbericht mit empfohlenen Abhilfemaßnahmen • Unterstützung und Beratung durch Expert*innen zur Umsetzung der Empfehlungen, z. B. Implementierung zentraler Cyber-Funktionen wie RES-Fernzugriff mit Mehrfaktor-Authentifizierung • Nachfolgende monatliche externe Scans und Berichte zur Bewertung des laufenden Cyberzustands	• Cybersicherheitsscan der über das Internet und intern zugänglichen EE-Anlagen um ausnutzbare Schwachstellen am Standort aufzudecken • Schwachstellenbericht mit empfohlenen Abhilfemaßnahmen • Unterstützung durch Expert*innen bei der Planung und Umsetzung der empfohlenen Maßnahmen. Beispiele hierfür sind: » Implementierung zentraler Cyber-Funktionen wie RES-Fernzugriff mit Mehrfaktor-Authentifizierung » Entfernung oder Umstrukturierung von redundanten Geräten • Nachfolgende monatliche externe und interne Scans und Berichte zur Bewertung des laufenden Cyberzustands	• Ausführlicher Cybersicherheitsscan und Penetrationstest der über das Internet und intern zugänglichen EE-Anlagen um ausnutzbare Schwachstellen am Standort aufzudecken • Detaillierter Bericht über den Penetrationstest mit empfohlenen Abhilfemaßnahmen • Fachkundige Unterstützung und Beratung bei der Umsetzung der Empfehlungen. Beispiele hierfür sind: » Implementierung zentralisierter Cyber-Fähigkeiten wie RES-Fernzugriff unter Verwendung von Multi-Faktor-Authentifizierung » Entfernung oder Umstrukturierung von redundanten Geräten • Nachfolgende monatliche externe und interne Scans und Berichte zur Bewertung des laufenden Cyberzustands • Jährliche Penetrationstests

In Deutschland ist im Mai 2021 das IT-Sicherheitsgesetz 2.0 in Kraft getreten, das neue Herausforderungen für die Digitalisierung mit sich bringt. Zahlreiche Unternehmen, die bisher nicht unter die BSI-Kritis-Verordnung fielen, müssen nun neue und strengere Anforderungen erfüllen.

RES ist das weltweit größte unabhängige Unternehmen für erneuerbare Energien und ist in den Bereichen Onshore- und Offshore-Windkraft, Solarenergie, Energiespeicherung, grüner Wasserstoff, Übertragung und Verteilung tätig. Als Innovator der Branche hat RES seit über 40 Jahren mehr als 23 GW an Projekten im Bereich der erneuerbaren Energien auf der ganzen Welt realisiert und betreut weltweit ein Anlagenportfolio von 10 GW für einen großen Kundenstamm. RES kennt die besonderen Bedürfnisse von Unternehmenskunden und hat über 1,5 GW an Stromabnahmeverträgen (PPAs) für Unternehmen abgeschlossen, die den Zugang zu Energie zu den niedrigsten Kosten ermöglichen. RES beschäftigt über 2.500 engagierte Mitarbeiter*innen und ist in 11 Ländern aktiv.

res
power for good

KONTAKTIEREN SIE UNS FÜR WEITERE INFORMATIONEN

+49 (0) 7666 6189902 Supportservices.deutschland@res-group.com www.res-group.com
Reutener Str. 18, 79279 Vörstetten, Deutschland