IT-Sicherheit beim Betrieb von Biogasanlagen

Wer braucht das?

grüngas24 Kongress

Thomas Bleier

t@b-sec.net

☎ +43 664 3400559

Classification:	PUBLIC
Version:	01
Date:	6.12.2024
Status:	Final

B-SEC better secure

https://www.b-sec.net

Wie komme ich zu diesem Thema?

B-SEC better secure KG

- IT-Sicherheit in industriellen Umgebungen (OT / I4.0, etc.)
- **Assessment** – Prüfung von Sicherheitsmaßnahmen
- **Training** – Security Engineering, Security-Architektur, etc.
- **Beratung** – Design/Implementierung, Zertifizierung

Allgemein beeideter, gerichtlich zertifizierter Sachverständiger

- für IT-Sicherheit, Verschlüsselung, Datenschutz, Gebäudeautomation

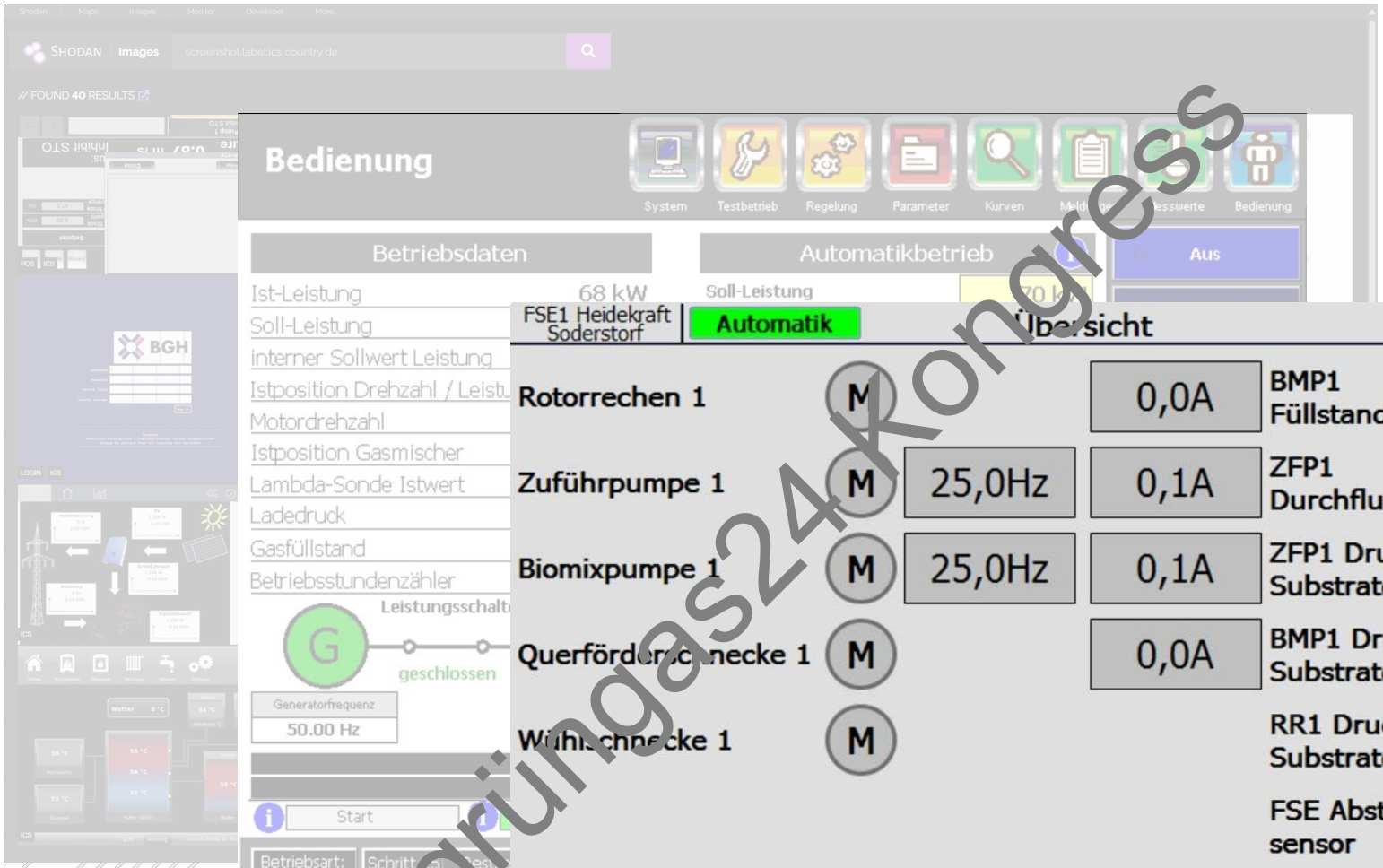
Bioenergie Bleier GmbH & Co KG

- Biogasanlage in Betrieb seit 2012 mit 250kW el. / AWN / Trocknung / PV

Strom Pool Manager

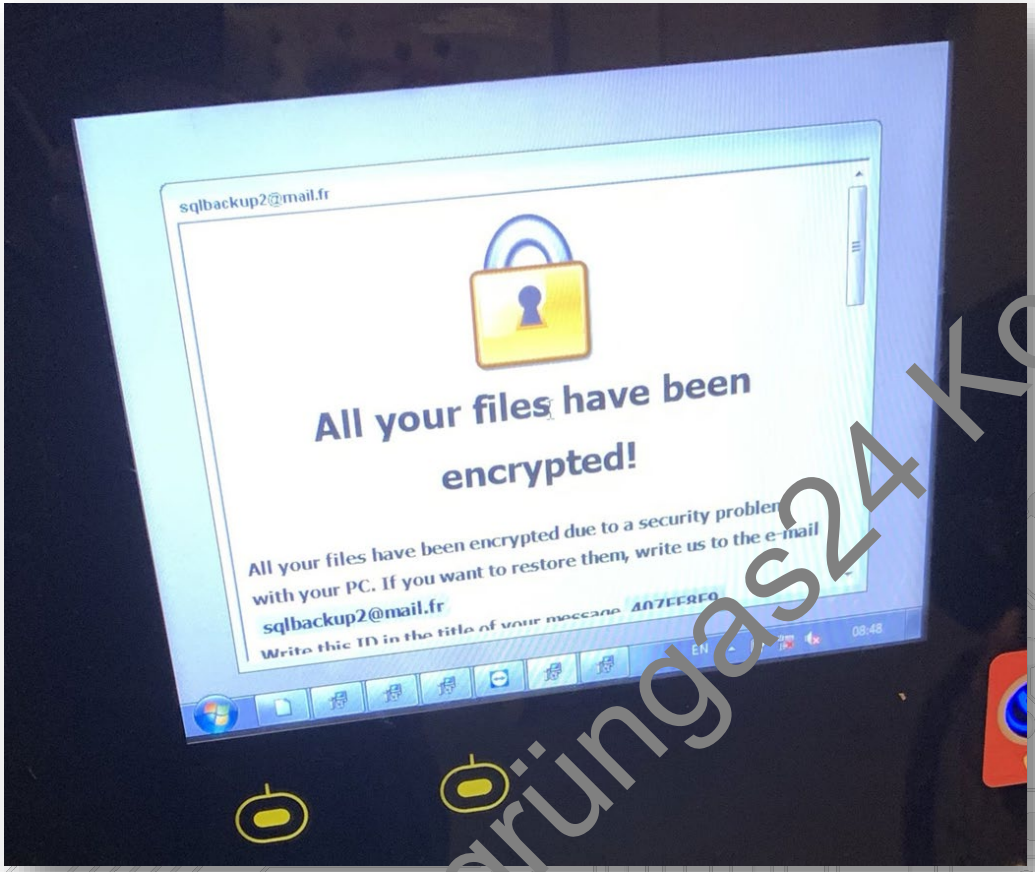
- Industrial IoT Plattform für Pooling von Biogas / PV Anlagen
- Vermarktung über Future / Day-Ahead / Regelenergiemärkte
- Anbindung von Anlagen, SPS, Stromhändler, Regelenergie, etc.
- Entwickelt Anfang 2022, seither Weiterentwicklung und Betrieb

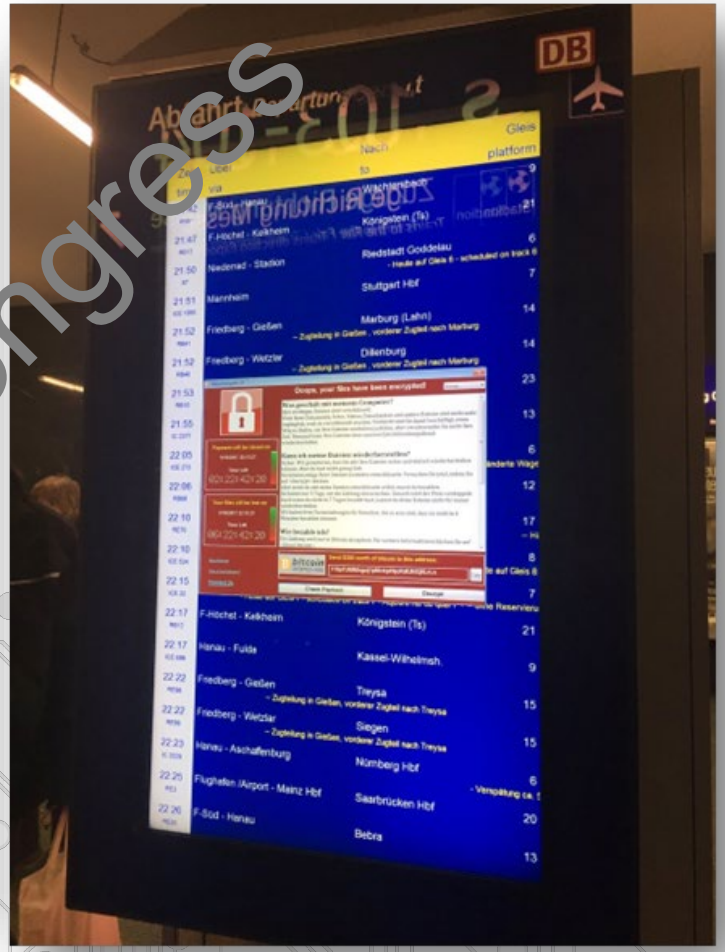
Warum man sich damit beschäftigen sollte?



images.shodan.io
screenshot.label:ics country:de

Cyberangriffe sind inzwischen allgegenwärtig





Wer sind die Angreifer?

„Script Kiddies“

Cyberkriminelle

Staatliche Angreifer

Deswegen reagiert inzwischen auch der Gesetzgeber

NIS (Netzwerk- und Informationssicherh.) **Richtlinie**	**Cyber Resilience Act (CRA)**
NIS 1 gilt seit 2018 für kritische Infrastrukturen	Sicherheit von Produkten mit digitalen Elementen
NIS 2 hätte bis 17. Okt. 2024 umgesetzt werden müssen	Beschlossen im Okt. 24, gilt ab 11. Dezember 2027
ca. 20 Sektoren u.a. Energie, Abfallwirtschaft, etc.	Hersteller/Händler müssen Konformität ihrer Produkte mit Stand der Technik sicherstellen
mittlere/große Unternehmen > 50 Pers. o. 10M Umsatz	Informationen über Sicherheitslücken, Dokumentation der Sicherheitsmechanismen, etc.
Verpflichtende IT-Sicherheitsmaßnahmen, Meldungen, etc.	

IT-Sicherheit = Betriebssicherheit

Welcher Betrieb kann heute ohne IT arbeiten? Daher:

Top 5 IT Security Themenbereiche

…die jeder Betrieb beachten sollte

- Organisation & Zuständigkeiten
- Netzwerksicherheit & Segmentierung
- Zugänge & Berechtigungen
- Notfall- & Backupkonzept
- Systemsicherheit & Updates

Organisation & Zuständigkeiten

- Asset Management - Welche Geräte haben wir?
  - Alle IT/OT Systeme – Server, Netzwerk, Firewall, Router, SPS, HMI, Drucker, Scanner, Telefon, Webcam, etc.
- Wer verwaltet welche Geräte?
  - Konfiguration, Updates, Backup, etc.
- Priorisierung – welche Geräte sind wofür wichtig?
  - Investierte Aufwände, Ausfallzeiten, Wiederherstellung, etc.
- Personal/Ressourcen
  - Was machen wir selbst? (→ Aus- und Weiterbildung, Awareness)
  - Wofür brauchen wir Dienstleister? (→ Vereinbarungen)
- Regelmäßige Überprüfung und Verbesserung

Netzwerksicherheit & Segmentierung

- Reduktion Erreichbarkeit = Reduktion Angriffsfläche
- Trennung in unterschiedliche Netzwerke/Zonen
  - Die SPS gehört nicht in das Büro-LAN
- Erreichbarkeit
  - Keine kritschen Systeme direkt aus dem Internet
  - Nur unbedingt notwendige Funktionen aus anderen LANs
- Filterung
  - Nur notwendige Kommunikation erlauben
  - Komfort vs. Sicherheit?
- Sichere Datenübertragung
  - Verschlüsselte Verbindungen, VPN für Fernzugriffe, etc.

Zugänge & Berechtigungen

- Authentifizierung
  - Sichere Passwörter verwenden
  - Nicht mehrfach dasselbe Passwort verwenden!!!
  - Bei kritischen Zugängen 2-Faktor-Authentifizierung
- Berechtigungen
  - Nur minimal notwendige Berechtigungen
  - Trennung von Accounts nach Rolle (Admin vs. User)
  - Entzug von Berechtigungen wenn nicht mehr benötigt
- Überwachung der Zugänge & Login-Vorgänge
  - Erkennung von Missbrauch

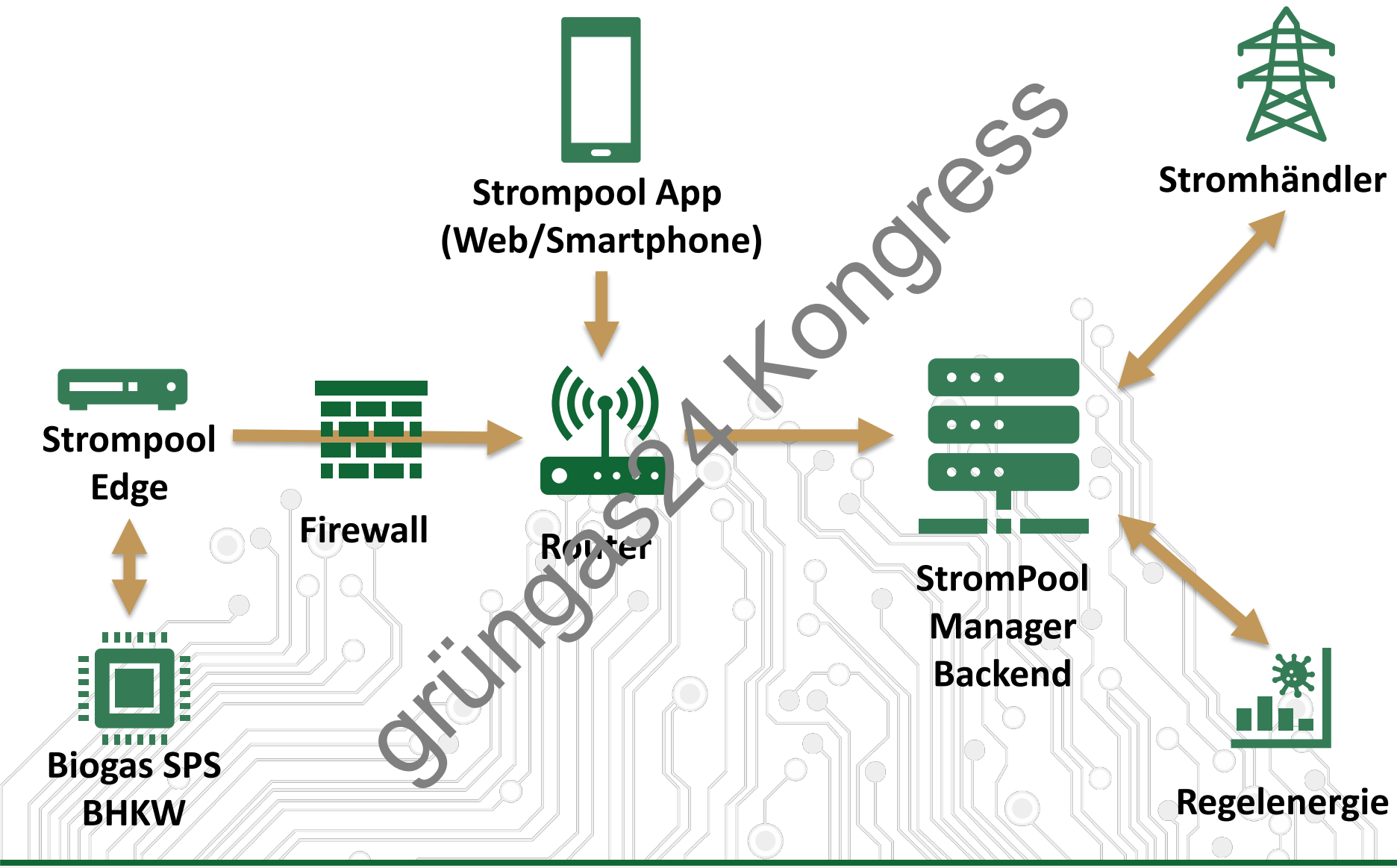
Backup- & Notfallkonzept

- Datensicherung – „3-2-1 Backup Regel“
  - 3 unabhängige Kopien auf 2 Medientypen, 1 davon offline
  - Welche Daten? Office-IT – aber auch Automatisierung!
  - Abhängigkeiten von Dienstleistern beachten
- Notfallplanung/Notfallhandbuch
  - Kontaktdaten,
  - Abläufe/Prozeduren zur Wiederherstellung, etc.
  - Konfigurationsdaten, Passwörter, etc.
- Notfallübungung/tests?
  - Prioritäten – was ist am wichtigsten?
  - Funktioniert die Wiederherstellung im Ernstfall wie geplant?

Systemsicherheit & Updates

- Sichere Konfiguration von Systemen
  - Sicherheitseinstellungen / „Härtung“ von Systemen
  - Installierte Software – wer darf Software installieren?
  - Schadsoftware-Schutz (EP/EDR/„Antivirus“) wo notwendig/sinnvoll
- Verwendungszweck / Risiko
  - Mehrfachnutzung – techn. möglich, aber Komfort vs. Risiko
  - Auf der Steuerung/HMI hat ein Web-Browser nichts verloren…
- Einspielen von Sicherheitsupdates
  - Je nach System, Bedrohung und Risiko
  - Auf der SPS muss man nicht jedes Monat ein Update einspielen…
  - Auf dem Internet-PC schon

Beispiel – Biogas-Anlage mit Strom Pool Manager



Damit ist alles erledigt?

Nein ☺ – aber dem Abdecken dieser wichtigsten Bereiche ist ein guter Anfang gemacht:

- Organisation & Zuständigkeiten
- Netzwerksicherheit & Segmentierung
- Zugänge & Berechtigungen
- Notfall- & Backupkonzept
- Systemsicherheit & Updates

Kontakt

Thomas Bleier

Dipl.-Ing. MSc CISSP-ISSAP,ISSMP,ISSEP CISA CISM CSSLP GICSP GPEN

t@b-sec.net ☎ +43 664 3400559

B-SEC better secure

https://www.b-sec.net