FACHINFORMATION

Cybersicherheit von Biogasanlagen

www.biogas-forum-bayern.de/bif69

Biogas Forum Bayern, Verfasser:

Christoph Reithmair
OmniCert Umweltgutachter GmbH

Marion Wiesheu
Fachverband Biogas e. V.

Foren des ALB Bayern e. V.

Der ALB Bayern e. V. ist ein offiziell anerkannter, gemeinnützig tätiger, eingetragener Verein mit Mitgliedern aus Landwirtschaft, Wissenschaft, Beratung und den landwirtschaftlichen Organisationen. Weiterhin sind die staatliche Verwaltung, Firmen sowie Dienstleistungsunternehmen aus Industrie, Handel, Gewerbe sowie dem Umweltbereich vertreten.

Der ALB unterstützt die Landwirtschaft mit Wissensvermittlung in den Themenbereichen Bauen in der Landwirtschaft, Bewässerung, Biogas und Landtechnik. Hierzu handelt sie als neutraler Mittler und Bindeglied zwischen landwirtschaftlicher Praxis, Forschung, Umwelt, staatlicher Verwaltung, Gewerbe und Industrie.

Für umfassende Informationen zur umweltschonenden und effizienten Anwendung in der Praxis werden zu den einzelnen Tätigkeitsbereichen Foren mit folgenden Aufgaben organisiert:

- Zusammenführen des aktuellen Wissensstandes,
- Reflektieren mit allen an der Thematik Beteiligten,
- Erarbeiten/Bekanntmachen konsensfähiger Lösungen

Foren des ALB Bayern e. V.:

- Bau Forum Bayern (BaF),
  Leitung: Jochen Simon, LfL-ILT
- Bewässerungsforum Bayern (BeF),
  Leitung Dr. Martin Müller
- Biogas Forum Bayern (BiF),
  Leitung: Dr. Martin Müller, ALB
- Landtechnik Forum Bayern (LaF),
  Leitung: Dr. Markus Demmel, LfL-ILT

Förderer

Bayerisches Staatsministerium für Ernährung, Landwirtschaft, Forsten und Tourismus

LfL Bayerische Landesanstalt für Landwirtschaft

Ämter für Ernährung, Landwirtschaft und Forsten

Impressum

Herausgeber	Arbeitsgemeinschaft Landtechnik und Landwirtschaftliches Bauwesen in Bayern e. V. (ALB), Vöttinger Straße 36, 85354 Freising
Telefon	08161 / 887-0078
Telefax	08161 / 887-3957
E-Mail	info@alb-bayern.de
Internet	www.alb-bayern.de
1. Auflage	2026
© ALB	Alle Rechte vorbehalten
Titelbild	Philipp Wagner, ALB (bearbeitet mit KI-Unterstützung - ChatGPT)

Inhaltsverzeichnis

Seite

1. Einleitung

Aufgrund der gestiegenen Anforderungen an die Flexibilität der Stromerzeugung, aber auch um die Betriebssicherheit zu erhöhen und die Arbeit zu erleichtern, werden Biogasanlagen zunehmend digitalisiert. Mithilfe moderner Steuerungssysteme können die Anlagen fernüberwacht werden, was rechtzeitiges Reagieren bei technischen Störfällen ermöglicht. Durch die automatische Datenübertragung können auch biologische Störungen, z. B. anhand verringerter Gasproduktionsraten und sinkender Methangehalte, rasch erkannt werden. Mittlerweile können auch Steuerungsparameter vom Betreiber über dessen Smartphone verändert werden. Häufig hat auch der BHKW-Hersteller einen Fernzugriff auf die Steuerung der Maschine, damit im Störfall fern gewartet oder zumindest die Störungsquelle identifiziert und eventuell erforderliche Ersatzteile bereitgestellt werden können. Ist eine Biogasanlage Teil eines großen „Speicherkraftwerks“, wird diese von extern so gesteuert, dass vornehmlich dann Strom erzeugt wird, wenn dieser lukrativ verkauft werden kann. Stromvermarkter haben in diesem Fall Zugriff auf die BHKW und können diese je nach Bedarf ein- oder ausschalten. Alle dafür erforderlichen digitalen Einrichtungen erleichtern den Anlagenbetrieb und steigern die Effizienz. Gleichzeitig bergen sie aber auch Risiken, denn alle mit dem Internet verbundenen Anlagenkomponenten sind potenzielle Eintrittspforten für Hacker oder Schadsoftware, die den Betrieb massiv beeinträchtigen können.

Digitale Angriffe auf Biogasanlagen sind keine theoretische Gefahr mehr, sondern Realität, wie zwei Vorfälle im Frühjahr 2025 in Niedersachsen gezeigt haben. In einem Fall verschafften sich Hacker Zugang über einen VNC-Port und veränderten wichtige Betriebsparameter, woraufhin einige Anlagenkomponenten beschädigt wurden und schließlich ersetzt werden mussten. Insgesamt entstand ein Schaden von rund 40.000 €. Im zweiten Fall wurde die Steuerung des BHKW manipuliert und nur aufgrund guter IT-Kenntnisse des Anlagenbetreibers konnten die Angreifer mittels einer Portsperre aus dem Netzwerk entfernt werden, bevor ein finanzieller Schaden entstand.

Anlagenbetreiber sind den digitalen Gefahren nicht hilflos ausgeliefert und sind sogar verpflichtet, sich vor Cyberangriffen zu schützen. Welche Anlagenkomponenten häufig das Ziel von Hackerangriffen darstellen und wie diese entsprechend geschützt werden können, ist Gegenstand dieser Fachinformation.

2. Digitale Risiken an Biogasanlagen

Davon auszugehen, eine Biogasanlage sei zu klein und unbedeutend, um Ziel eines Hackerangriffs zu werden, ist eine riskante Einstellung, denn bei einem Angriff wird automatisiert nach Schwachstellen gesucht, um dort Zugang zu erlangen und aktiv Schaden anzurichten. Dabei wird nicht nach Größe oder Bedeutung des Objekts unterschieden.

Die typischen Einfallstore an Biogasanlagen bilden Steuerungen, Sensoren, Fütterungscomputer, Messrechner, aber auch Smartphones (Vergleiche Abb. 1). Ebenso können Kommunikationsschnittstellen zu Energieversorgern oder Serviceunternehmen als Angriffsvektoren dienen. Entscheidend ist die Verbindung mit dem Internet, die einen Onlinezugriff ermöglicht. Ältere Anlagenkomponenten, die ursprünglich nicht für den Onlinebetrieb konzipiert wurden und deshalb häufig keine integrierten Sicherheitsfunktionen besitzen, sind besonders anfällig. Wichtig ist dabei zu wissen, dass bereits über eine einzige betroffene Komponente das gesamte Netzwerk manipuliert werden kann.

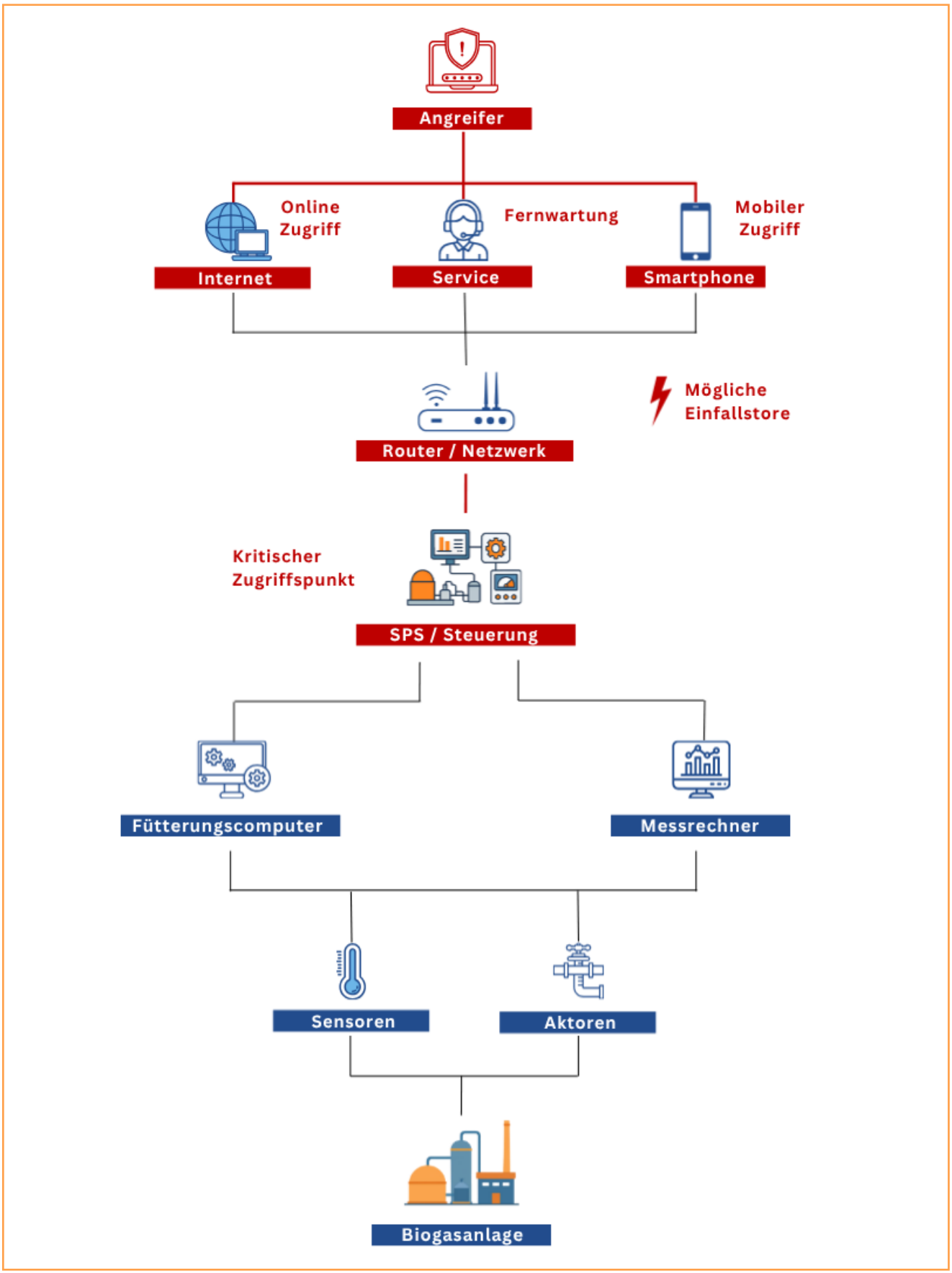

Abb. 1: Schematische Darstellung zu möglichen Einfallstoren (in rot dargestellt) für Cyber-Angriffe auf Biogasanlagen

3. Schadsoftware und typische Angriffswege

Schadsoftware, auch "Malware" genannt, sind Programme, die unerwünschte Aktionen auf Computern oder Steuerungssystemen ausführen. Dazu gehören Viren, Trojaner, Spionageprogramme oder sogenannte „Ransomware“, mit welcher systemrelevante Daten verschlüsselt werden, um anschließend für deren Entschlüsselung ein Lösegeld zu fordern. Schadprogramme gelangen häufig über infizierte E-Mail-Anhänge, USB-Sticks von externen Personen oder manipulierte Updates in die Systemumgebung von Biogasanlagen. Auch Fernwartungsverbindungen mit schwachen Passwörtern oder dauerhaft aktive Ports können Einfallstore sein.
Da es sich hierbei um ein äußerst dynamisches Problemfeld handelt, sollte man sich regelmäßig auf entsprechenden Web-Portalen über aktuelle Ereignisse und Entwicklungen rund um Sicherheitsrisiken und Cybersicherheit informieren.
Empfohlen sei hier insbesondere das diesbezügliche Informationsangebot vom Bundesamt für Sicherheit in der Informationstechnik (BSI) unter dem URL https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/cyber-sicherheitslage_node.html (frei zugänglich).
Darüber hinaus gibt es entsprechende privatwirtschaftliche Informationsdienste, z. B. von heise security (https://www.heise.de/security/Alerts; gegebenenfalls kostenpflichtig). Eine schematische Übersicht von IT-Gefährdungen für Biogasanlagen mit Unterscheidung der Folgen eines Cyberangriffs in Sabotage/Zerstörung bzw. Betriebsunterbrechung ist einsehbar unter https://biogas-itsec.umweltgutachter.de/gefaehrdungen.html.

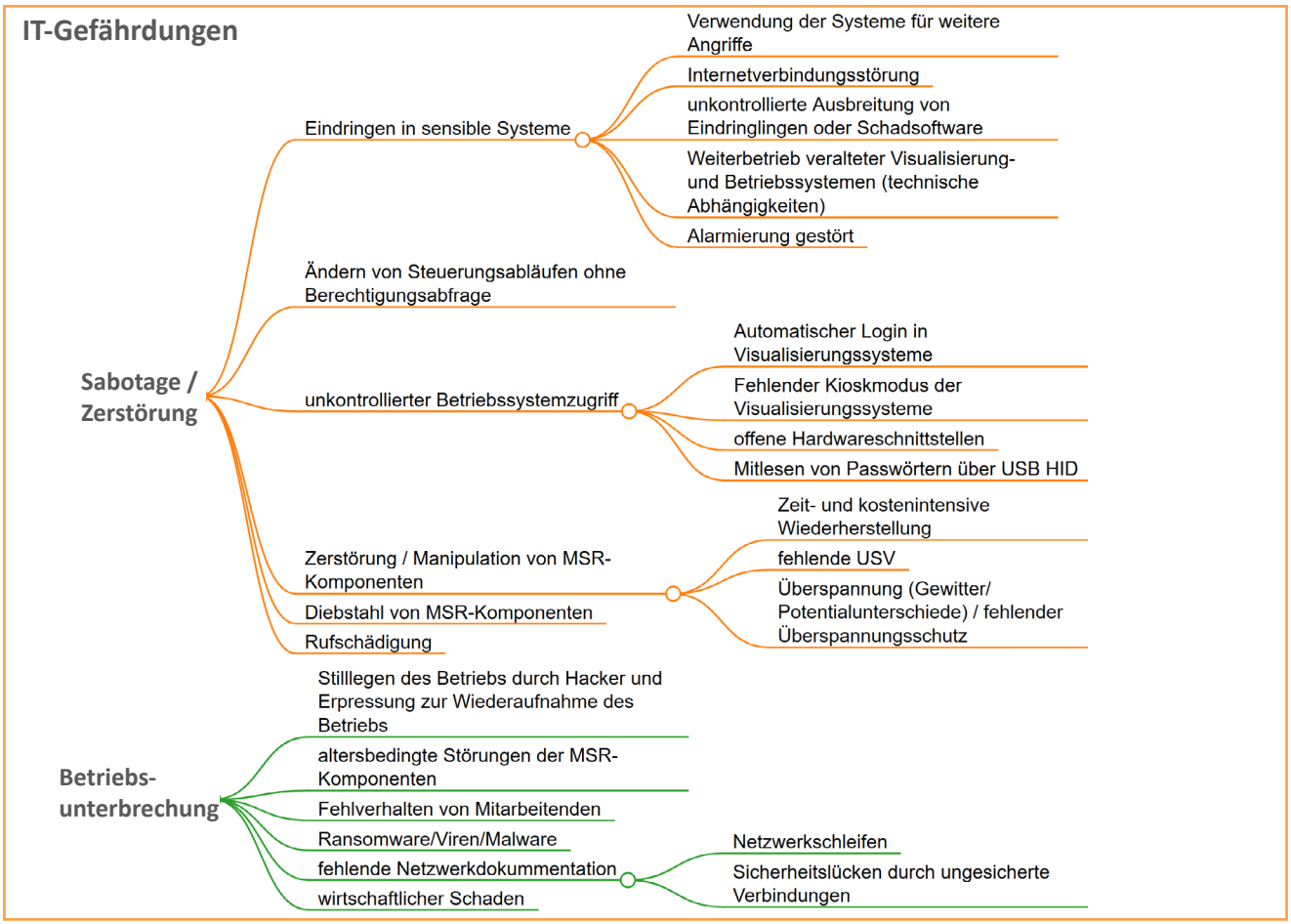

Abb. 2: Schematische Übersicht von IT-Gefährdungen für Biogasanlagen (Quelle: https://biogas-itsec.umweltgutachter.de/gefaehrdungen.html)

Da sich ein beginnender Cyber-Angriff zunächst durch kleinere Auffälligkeiten bemerkbar machen kann, die gerne übersehen werden, sollte man für folgende typische Warnzeichen besonders sensibel sein:

- Steuerungs- oder Leitsystemen reagieren ungewöhnlich langsam.
- Das System wird unerwartet neu gestartet oder Programme stürzen wiederholt ab.
- Visualisierungs- und Monitoring-Anwendungen zeigen fehlerhafte oder widersprüchliche Werte.
- Dateien oder Protokolle lassen sich nicht mehr öffnen oder sind verändert.
- Unbekannte Programme oder Prozesse laufen im Hintergrund.
- Es treten ungewöhnlicher Netzwerkverkehr oder Verbindungsversuche zu externen Servern auf.
- Systemeinstellungen erscheinen ohne erkennbaren Grund verändert.
- Anmeldeversuche schlagen fehl oder Benutzerkonten sind gesperrt.

Gleichzeitig ist moderne Schadsoftware häufig gezielt darauf ausgelegt, möglichst unentdeckt zu bleiben. Ein Angriff kann daher auch ohne offensichtliche Auffälligkeiten erfolgen und über längere Zeit unbemerkt bleiben.

Bei einem erfolgten Cyber-Angriff ist besonnenes Handeln entscheidend. Beispielsweise kann vorschnelles Neustarten der Systeme oder das Löschen von Dateien die Situation verschlimmern. Besser ist es, alle mit dem Internet verbundenen Komponenten sofort zu trennen und IT-Fachleute hinzuzuziehen. Da diese zur effektiven Schadensabwehr möglichst detaillierte Informationen benötigen, sollten alle Vorkommnisse sorgfältig dokumentiert werden.

Der Betreiber hat für mögliche Vorfälle mit Gefährdung der IT-Sicherheit einen Notfallplan zur Aufrechterhaltung des Geschäftsbetriebs zu erstellen (einschließlich Dokumentation!) und die Mitarbeitenden entsprechend zu unterweisen.

Zusätzlich ist es sinnvoll, einen Aushang mit entsprechenden Informationen für den Notfall anzufertigen, z. B. mit Hilfe der Vorlage des BSI für eine IT-Notfallkarte (siehe Abb. 3).

Eine Meldung bei der Polizei ist notwendig, insbesondere bei strafbaren Handlungen oder bei Erpressungsversuchen. In besonderen Fällen, etwa wenn sicherheitsrelevante Systeme betroffen sind, ist eine Meldung bei der zuständigen Landesbehörde für Sicherheit in der Informationstechnik verpflichtend.

Um weiteren Schaden zu vermeiden, sind gegebenenfalls Angestellte mit IT-Anschluss unverzüglich über den Angriff zu informieren. Außerdem sind die Vorkommnisse zeitnah der Versicherung zu melden, sollte der Versicherungsbaustein Cybersicherheit mitversichert sein. Eine Versicherung gegen Cyberangriffe muss, wie z. B. auch eine Versicherung gegen Diebstahl/Vandalismus, in der Regel separat abgeschlossen werden.

Abb. 3: IT-Notfallkarte "Verhalten bei IT-Notfällen" des BSI

4. Prävention und Schutzmaßnahmen

Ein erhebliches, auf Biogasanlagen häufig anzutreffendes Sicherheitsrisiko stellen IT-Komponenten mit veralteten Betriebssystemen wie beispielsweise Windows 7 dar: da diese keine Sicherheitsupdates mehr erhalten, können bekannte Schwachstellen dauerhaft ausgenutzt werden. Daher sollte grundsätzlich der Umstieg auf aktuell unterstützte Systeme angestrebt werden, auch wenn dies mit Kosten und technischem Aufwand verbunden ist.

Ist ein Austausch solcher Komponenten kurzfristig nicht möglich, sind kompensierende Maßnahmen zwingend erforderlich! Dazu gehört insbesondere eine konsequente Abschottung der betroffenen Systeme vom Internet sowie von anderen Netzwerken (Netzwerk-Segmentierung). Zusätzlich kann der Betrieb in einer virtualisierten Umgebung (z. B. als virtuelle Maschine) dazu beitragen, die Ausfallsicherheit zu erhöhen und die Wiederherstellung im Schadensfall zu vereinfachen. Regelmäßige Backups der Betriebsparameter der Anlage auf externen Datenträgern (offline) ermöglichen die schnelle Wiederaufnahme des Anlagenbetriebs nach einem Angriff.

Die meisten Cyber-Risiken lassen sich mit vergleichsweise geringem Aufwand deutlich reduzieren: Firewalls, aktuelle Antivirensoftware und regelmäßige Updates / Sicherheitspatches Systemupdates bilden die Grundlage für jegliches Schutzkonzept. Werden aber schwache Passwörter verwendet oder sind überhaupt keine Zugangsbeschränkungen eingerichtet, bleiben diese Maßnahmen wirkungslos. Das Gleiche gilt für segmentierte Netzwerke, die verhindern, dass Schadsoftware von einem Büro-PC auf die Steuerung übergreift.

Neben den technischen Aspekten spielt die Organisation eine zentrale Rolle. Klare Zuständigkeiten, Dokumentation von Systemen und Zugangsdaten, Schulungen der Mitarbeitenden und die Sensibilisierung aller Beteiligten sind entscheidend (siehe dazu Tabelle 1). Wer weiß, welche Gefahren bestehen und wie man reagiert, kann viele Probleme bereits im Vorfeld verhindern. Unterstützung bieten Beratungsangebote von Herstellern, IT-Dienstleistern oder regionalen Energieagenturen. In vielen Fällen lohnt es sich, einen Sicherheitscheck speziell für Biogasanlagen durchführen zu lassen, um Schwachstellen zu identifizieren und konkrete Handlungsempfehlungen zu erhalten.

Eine schematische Übersicht von technischen und organisatorischen Maßnahmen zur IT-Sicherheit ist unter https://biogas-itsec.umweltgutachter.de/massnahmen.html verfügbar. Zusätzlich kann der Abschluss einer Cyberversicherung sinnvoll sein. Für den Leistungsanspruch müssen dann ohnehin umfangreiche Schutzmaßnahmen getroffen werden.

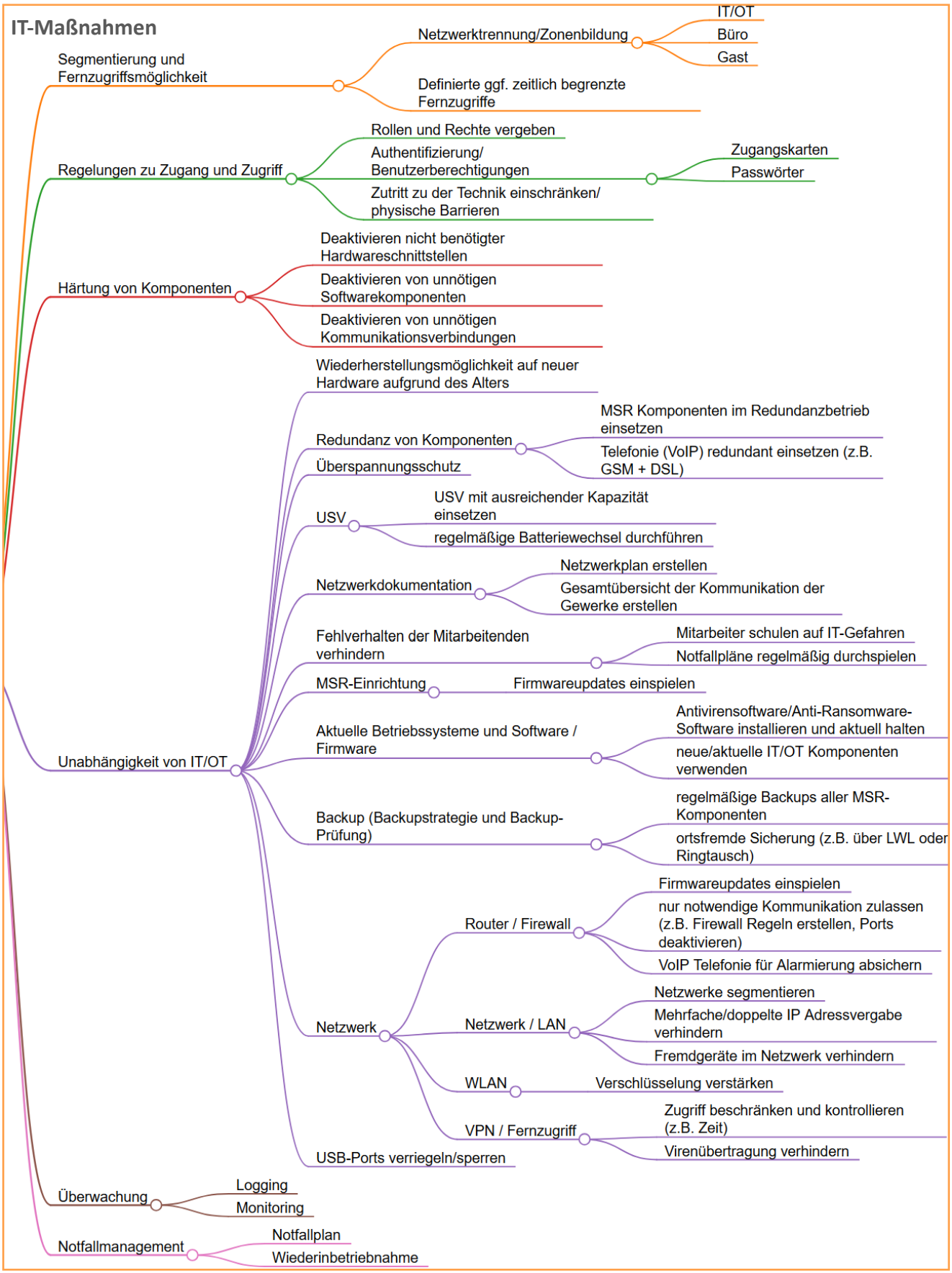

Abb. 4: Schematische Übersicht von technischen und organisatorischen Maßnahmen zur IT-Sicherheit (Quelle: https://biogas-itsec.umweltgutachter.de/massnahmen.html)

Tab. 1: Beispiele für organisatorische Schutzmaßnahmen gegen Cyber-Risiken

Kategorie	Maßnahmen inkl. Praxisbeispiel	Ziel / Nutzen
Zugriffs-management	Benutzerrechte und Rollen → Nur der Anlagenbetreiber darf Zugriff auf das Verstellen der Grenzwerte in der Steuerung haben	Minimierung unautorisierter Zugriffe
	Passwort- & Authentifizierungsrichtlinien → Verwendung von Zwei-Faktor-Authentifizierung und sicheren Passwörtern	Schutz vor Identitätsdiebstahl
Qualifikation und Schulung	Fachkundige, für die IT verantwortliche Person → Unterstützung durch einen Dienstleister	Sensibilisierung und Reduzierung menschlicher Fehler
	Mitarbeiterschulungen → Mind. einmal jährlich, zusätzlich anlassbezogen	Sensibilisierung und Reduzierung menschlicher Fehler
IT-/OT*-Sicher-heitsprozesse	Sicherheitsrichtlinien für die IT/OT → Festlegen, wer für die Durchführung regelmäßiger Soft-wareupdates verantwortlich ist	Beseitigung von Sicherheitslücken
Netzwerk-management	Segmentierung von Netzwerken → Trennung der Netzwerke für die Anlagensteuerung und die Verwaltung	Verhinderung von lateralem Zugriff
	Regelungen für Fernzugriffe → Dokumentiert und nur zeitweise aktiviert → Über VPN mit Zwei-Faktor-Authentifizierung	Sicherer Fernzugriff
Monitoring & Audit	Protokollierung und Monitoring → Logfile-Analyse der Biogasanlagensteuerung	Früherkennung von Auffälligkeiten
	Regelmäßige Sicherheitsüberprüfungen → Externe Penetrationstests	Schwachstellen erkennen
Kontinuitäts-management	Backup- und Wiederherstellungsprozesse → Regelmäßig Backups durchführen	Daten- und Systemverfügbarkeit sichern
	Notfall- und Krisenübungen → Übung eines Hackerangriffs mit den Mitarbeitenden: Was ist zu tun?	Praxisnahe Vorbereitung auf Ausfälle

*IT (Information Technology - Daten und Computer)
OT (Operational Technology - Betriebstechnik wie Maschinen, Anlagen , Sensoren oder Steuerungen)

5. Rechtliche Vorgaben zur IT-Sicherheit

Da der/die Betreiber(in) sicherstellen muss, dass von seiner Biogasanlage keine Gefahr für Personen oder die Umwelt ausgeht, ist er auch rechtlich dazu verpflichtet, die Anlage gegen Cyberangriffe zu schützen. Dazu wurde im April 2023 die TRBS 1115-1 als Technische Regel Betriebssicherheit – Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen (MSR) veröffentlicht, welche den Stand der Technik für überwachungsbedürftige Anlagen definiert. Da jede Biogasanlage die Vorgaben der BetrSichV einzuhalten hat, müssen alle Biogasanlagen - unabhängig von ihrer Größe oder ihrem Genehmigungsstatus- diese Anforderungen berücksichtigen. Die TRBS 1115-1 fordert auch ein Schutzkonzept zur IT-Sicherheit, welches zukünftig in alle wiederkehrenden Prüfungen gemäß §§ 15 und 16 BetrSichV (jährlich, dreijährig und sechsjährig) einzuschließen ist. Der Fachverband Biogas bietet auf seinen Webseiten die Arbeitshilfe „A033-01 Beispiel für ein Schutzkonzept der IT-Sicherheit für eine Biogasanlage“ an (PDF-Version frei verfügbar, Version für MS Word nur für Mitglieder).

Biogasanlagen, welche der Störfallverordnung unterliegen, müssen zusätzliche Anforderungen an die Cybersicherheit erfüllen. Noch höhere Anforderungen an die Cybersicherheit werden an „wichtige“ und „besonders wichtige“ Einrichtungen sowie „kritische Anlagen“ gemäß dem BISG (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen) gestellt. Die entsprechenden Schwellenwerte werden allerdings in der Regel nur von großen Abfallvergärungsanlagen (genehmigte Behandlungskapazität an Bioabfall von mehr als 33.500 Mg/Jahr) und Biogasanlagen im Verbund von Betreibergemeinschaften erreicht.

6. Fazit

Eine wachsende Anzahl der in Deutschland betriebenen Biogasanlagen ist stark digitalisiert. Während die Digitalisierung für die Zwecke der Direktvermarktung obligatorisch ist, erleichtert sie die Betriebsführung von Biogasanlagen deutlich und kann sich positiv auf deren Effizienz auswirken. Gleichzeitig steigen mit wachsender Digitalisierung die Anforderungen an die Sicherheit der digitalen Systeme, denn Cyberangriffe stellen auch für Biogasanlagen eine reale Gefährdung dar. Deshalb ist ein wirksames IT-Schutzkonzept mit geeigneten Maßnahmen notwendig und im Übrigen auch vorgeschrieben. Dieses schließt insbesondere ein, dass alle IT-Komponenten stets auf dem aktuellen Stand gehalten werden, das Personal sensibilisiert ist und die Abläufe im Falle eins Cyberangriffs gut organisiert sind. Auf diese Weise können längere Betriebsunterbrechungen oder gar Schäden an Anlagenkomponenten in aller Regel verhindert werden.

Zitiervorlage: Reithmair, Ch. und Wiesheu, M. (2026): Cybersicherheit von Biogasanlagen. In: Biogas Forum Bayern, 1. Auflage - 05/2026, Hrsg. ALB Bayern e. V., www.biogas-forum-bayern.de/bif69, Stand [Abrufdatum]

Arbeitsgemeinschaft Landtechnik und
Landwirtschaftliches Bauwesen (ALB)
in Bayern e. V.
Vöttinger Straße 36, 85354 Freising

Telefon	08161 / 887-0078
Telefax	08161 / 887-3957
E-Mail	info@alb-bayern.de
Internet	www.alb-bayern.de