



Erkennung von Cyberangriffen

Die Erkennung von Cyberangriffen gewinnt im Zuge der zunehmenden Digitalisierung an Bedeutung. Datenbasierte Modelle ermöglichen die automatisierte Analyse großer Datenmengen, um Auffälligkeiten frühzeitig zu erkennen und Gegenmaßnahmen einzuleiten.

Cyberangriffe stellen eine zunehmende Bedrohung für Stromnetze dar, da die fortschreitende Digitalisierung und Vernetzung die Angriffsfläche deutlich vergrößern. Insbesondere die Integration von IT- und Kommunikationssystemen in den Netzbetrieb erhöht die Anfälligkeit gegenüber gezielten Angriffen (Humayun, 2024). Vor diesem Hintergrund gewinnt die frühzeitige Erkennung von Cyberangriffen zunehmend an Bedeutung, um die Sicherheit und Stabilität des Netzbetriebs zu gewährleisten.

Mit der fortschreitenden Entwicklung von KI-Methoden steigt zudem die Gefahr, dass auch Angriffe selbst zunehmend durch KI unterstützt werden. Klassische Sicherheitsmechanismen wie Firewalls oder Intrusion-Detection-Systeme (IDS) bleiben zwar essenziell, stoßen jedoch bei hochentwickelten und dynamischen Cyberangriffen teilweise an ihre Grenzen (Kim, 2022). Daher ist es naheliegend, dieselben Eigenschaften, die KI-basierte Angriffe besonders gefährlich machen (insbesondere Automatisierung, Skalierbarkeit und Anpassungsfähigkeit), gezielt zur Entwicklung

KI-basierter Modelle zur Erkennung von Cyberangriffen zu nutzen (Bundesamt für Sicherheit in der Informationstechnik, 2024).

In der Praxis äußern sich Angriffe grundsätzlich als Abweichungen vom Normalverhalten. Dabei ist jedoch zu beachten, dass solche Anomalien nicht zwangsläufig auf Cyberangriffe zurückzuführen sind, sondern auch durch technische Fehler oder Störungen verursacht werden können. Im Leitsystemumfeld ergänzen KI-basierte Modelle klassische Verfahren, indem sie Manipulationen, Dateninkonsistenzen und auffällige Muster in Mess- und Kommunikationsdaten frühzeitig erkennen, und erhöhen so die Sicherheit kritischer Infrastrukturen. Durch die kombinierte Analyse von Prozessdaten (z. B. Last-, Spannungs- und Schaltzustände) und Kommunikationsdaten lassen sich technische Störungen und gezielte Cyberangriffe (z. B. Datenmanipulation) besser unterscheiden, wodurch die Reaktionsfähigkeit steigt und der Netzbetrieb widerstandsfähiger wird (siehe Abbildung 1) (VDE Studie, 2025).

Ein Projekt der

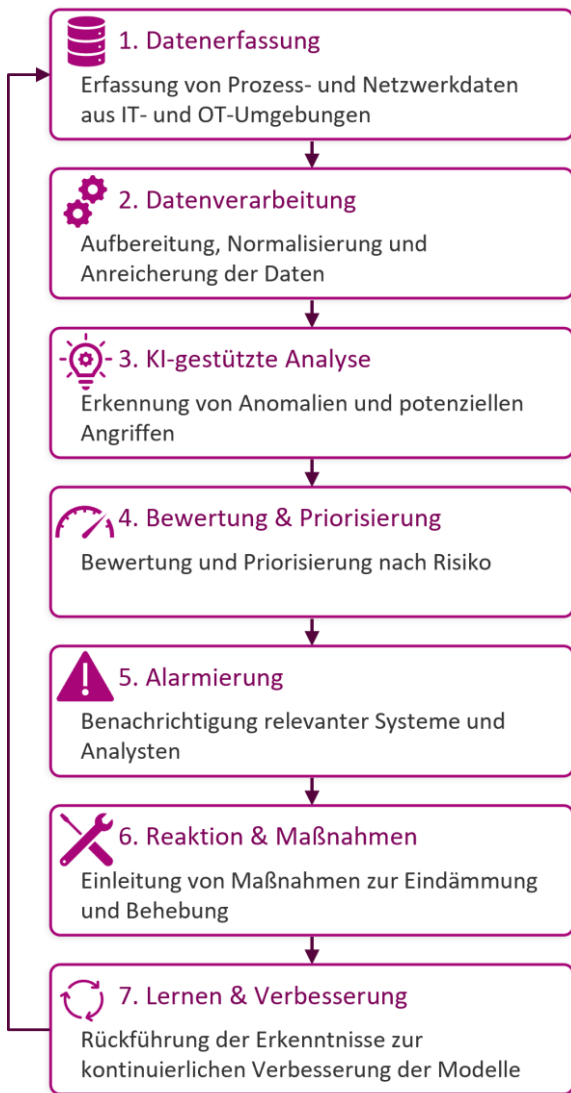


Abbildung 1: Prozesskette der KI-gestützten Anomalieerkennung in Stromnetzen

Bewertung der Umsetzbarkeit

Zur Bewertung der Umsetzbarkeit KI- und datenbasierter Methoden zur Erkennung von Cyberangriffen werden im Folgenden zunächst geeignete Modellansätze vorgestellt.

Darauf aufbauend erfolgt eine Einordnung hinsichtlich Implementierungsaufwand, Datenanforderungen und praktischer Integrationsaspekte.

Stand der Technik

Der Stand der Technik im Bereich der KI-basierten Angriffserkennung ist im IT-Sektor bereits weit fortgeschritten. Hier existieren zahlreiche marktreife Lösungen, die in der Praxis

eingesetzt werden und einen etablierten Bestandteil moderner IT-Sicherheitsarchitekturen darstellen.

Im Gegensatz dazu ist der Reifegrad im OT-Umfeld, insbesondere in SCADA-Systemen und der Energieinfrastruktur, deutlich geringer. Zwar gibt es erste spezialisierte Ansätze und Pilotlösungen (Kim, 2022; Kummerow, 2024; Mishra, 2025), jedoch ist die breite industrielle Verfügbarkeit und Standardisierung solcher Systeme noch begrenzt. Dies ist vor allem auf die höheren Anforderungen an Verfügbarkeit, Echtzeitfähigkeit und Systemsicherheit sowie die spezifischen Rahmenbedingungen kritischer Infrastrukturen zurückzuführen.

Für die Erkennung von Cyberangriffen kommen unterschiedliche Modellklassen zum Einsatz. Verfahren wie Isolation Forest erkennen statistische Anomalien und Ausreißer mit geringem Rechenaufwand und eignen sich insbesondere für einfache oder klar erkennbare Abweichungen. Autoencoder hingegen lernen komplexe und nichtlineare Muster des Normalverhaltens und können dadurch auch subtile oder koordinierte Manipulationen, beispielsweise an Sensordaten, über Abweichungen vom erlernten Verhalten identifizieren. Für zeitabhängige Daten werden häufig LSTM¹-Modelle genutzt, da sie zeitliche und sequenzielle Veränderungen in Mess- und Kommunikationsdaten erfassen können, beispielsweise schleichende Veränderungen oder wiederkehrende Angriffsmuster. Ergänzend werden Ensemble-Ansätze eingesetzt, um die Robustheit und Erkennungsgenauigkeit durch die Kombination mehrerer Modelle zu erhöhen. Zunehmend kommen auch Graph Neural Networks (GNN) zum Einsatz, da sie komplexe Beziehungen zwischen unterschiedlichen Datenstrukturen modellieren und dadurch koordinierte oder sich ausbreitende Angriffe im Netz besser erkennen können (Mitra, 2024).

Datenbedarf, Datenverfügbarkeit & Datenqualität

Datenbedarf

Der Datenbedarf umfasst verschiedene Datenquellen aus dem IT- und OT-Umfeld. Dazu zählen insbesondere Netzwerkverkehrsdaten, System- und Kommunikationslogs, historische Angriffsmuster sowie Daten zum Normalbetrieb, die als Referenz für eine Baseline dienen. Für das Training und die Validierung der Modelle sind zusätzlich historische SCADA- und Prozessdaten sowie Kommunikationsdaten (z. B. Netzwerktraffic und SIEM-Logs) erforderlich. Je nach

¹ LSTM (Long Short-Term Memory) ist eine spezielle Form rekurrenter neuronaler Netze (RNN), um zeitliche Abhängigkeiten und langfristige Zusammenhänge in sequenziellen Daten, wie Zeitreihen, zu lernen und zu verarbeiten.

Modellansatz können außerdem gelabelte Anomalien, bekannte oder synthetisch erzeugte Angriffsszenarien genutzt werden, wobei insbesondere Anomalieerkennungsverfahren auch ohne explizit gelabelte Angriffsdaten auskommen. Im operativen Betrieb werden diese durch Live-Daten aus SCADA-Systemen, Kommunikationsprotokollen, Event-Logs und gegebenenfalls Gerätezustandsinformationen ergänzt.

Datenverfügbarkeit & Datenqualität

Die Datenverfügbarkeit stellt dabei eine zentrale Herausforderung dar. Für die Entwicklung robuster Modelle müssen Trainings- und Validierungsdaten ein breites Spektrum möglicher Angriffs- und Fehlerszenarien abdecken. Daher werden neben Betriebsdaten aus dem Normalbetrieb häufig auch synthetisch erzeugte Daten oder Simulationen genutzt.

Hinsichtlich der Datenqualität ist insbesondere auf Konsistenz, Vollständigkeit und zeitliche Synchronisation der unterschiedlichen Datenquellen zu achten. Unterschiedliche Systeme wie SCADA, Netzwerküberwachung und IT-Sicherheitsinfrastruktur erzeugen heterogene Datenformate, die vor der Nutzung aufbereitet und harmonisiert werden müssen. Zudem können Rauschen, Messfehler oder unvollständige Logs die Modellgüte beeinträchtigen, weshalb eine sorgfältige Datenvorverarbeitung und kontinuierliche Qualitätssicherung erforderlich ist.

Implementierungsaufwand & Ressourcenbedarf

Ein wesentlicher Treiber des Implementierungsaufwands ist die notwendige Kombination aus IT-Security- und OT-Domänenwissen, die nur durch gezielte Investitionen in qualifiziertes Personal und den Aufbau entsprechender Kompetenzen im Unternehmen abgedeckt werden kann.

Zudem stellt sich die grundsätzliche Make-or-Buy-Entscheidung². Aufgrund der hohen Komplexität des adversariellen Umfelds³ und der spezialisierten Anforderungen im OT-Bereich

ist für viele Verteilnetzbetreiber der Zukauf spezialisierter OT-Security-Lösungen gegenüber einer vollständigen Eigenentwicklung zu bevorzugen.

Auch die Wahl der Infrastruktur hat wesentlichen Einfluss auf den Aufwand. Aufgrund der Sensitivität von OT-Daten sowie der Anforderungen aus dem KRITIS⁴-Kontext ist der Einsatz von Cloud-Lösungen nur eingeschränkt möglich. In der Praxis kommen daher häufig On-Premise⁵ oder Private-Cloud-Architekturen zum Einsatz, die innerhalb der eigenen oder dedizierten Betreiberumgebung betrieben werden. Dies erfordert insbesondere den Aufbau und Betrieb eigener Rechenzentrums- bzw. Plattformkapazitäten, inklusive Maßnahmen zur IT-/OT-Trennung, Netzwerksegmentierung, Zugriffskontrolle sowie zum kontinuierlichen Patch- und Sicherheitsmanagement. Dadurch entstehen zusätzliche Anforderungen an Betrieb, Wartung, Monitoring und IT-Sicherheit der Systeme.

Eingriffstiefe der Anwendung in Prozesse

Die Eingriffstiefe der KI-Anwendung in bestehende Sicherheitsprozesse ist vom gewählten Integrations- und Automatisierungsgrad abhängig. Grundsätzlich erfolgt die Einbindung in die bestehende IT- und OT-Systemlandschaft über Kommunikationsnetzwerke, Monitoring- und Log-Systeme sowie zentrale Sicherheitsplattformen wie SIEM⁶ und Security Operations Center (SOC).

- **Passives Monitoring (Shadowing):** In der ersten Stufe analysiert die KI den Netzwerkverkehr ausschließlich passiv und ohne Eingriff in den Betrieb. Es werden lediglich Alarme generiert, während die Entscheidung über Gegenmaßnahmen beim Sicherheitsteam verbleibt. Diese Stufe ist ohne Auswirkungen auf den laufenden Betrieb sofort umsetzbar und stellt den empfohlenen Einstieg dar.
- **Teilautomatisierung:** In einer weiterführenden Stufe können bereits teilweise automatisierte Reaktionen erfolgen, bei denen vordefinierte Sicherheitsmaßnahmen durch das System selbstständig ausgelöst werden.

² Make-or-Buy-Entscheidungen sind grundlegende strategische Entscheidungen darüber, ob eine Leistung oder ein Produkt selbst im Unternehmen entwickelt („Make“) oder von externen Anbietern bezogen („Buy“) wird.

³ Ein adversarielles Umfeld bezeichnet eine Umgebung, in der Systeme gezielt durch Angreifer bedroht werden, die Schwachstellen ausnutzen, Daten manipulieren oder den Betrieb stören wollen.

⁴ KRITIS (Kritische Infrastrukturen) bezeichnet Einrichtungen und Systeme von hoher Bedeutung für das staatliche Gemeinwesen, deren Ausfall oder Beeinträchtigung erhebliche Auswirkungen auf Versorgungssicherheit, öffentliche Sicherheit oder wirtschaftliche Stabilität hätte. (Bundesamt für Verfassungsschutz, 2026)

⁵ On-Premise bedeutet, dass IT-Systeme, Software und Daten lokal im eigenen Unternehmen betrieben werden.

⁶ SIEM (Security Information and Event Management) bezeichnet Systeme zur zentralen Erfassung, Korrelation und Analyse sicherheitsrelevanter Ereignis- und Protokolldaten aus IT- und OT-Umgebungen zur Erkennung und Bewertung von Cyberbedrohungen.

Dadurch wird die Zeit zwischen Erkennung und Reaktion deutlich reduziert, allerdings steigt gleichzeitig die Eingriffstiefe in die operativen Prozesse.

Robustheit & Fehlertoleranz

Die Robustheit ist im adversariellen Kontext von besonderer Bedeutung, da gezielte Angriffe aktiv darauf ausgelegt sind, Erkennungsmodelle zu umgehen oder zu täuschen. Ein robustes Modell bleibt stabil gegenüber Variationen im normalen Verhalten und reagiert nicht übermäßig auf zufällige Abweichungen. Dadurch werden False Positives⁷ reduziert, während gleichzeitig echte Anomalien zuverlässig erkannt werden (Mitra, 2024). Dies ist entscheidend, um frühzeitig auf potenzielle Angriffe hinweisen zu können und die allgemeine Sicherheitslage zu verbessern. Eine hohe False-Positive-Rate überlagert dabei relevante Sicherheitsereignisse und erschwert deren zeitnahe Erkennung und Priorisierung.

Ergänzend sind klassische Intrusion-Detection-Systeme (IDS) als Fallback-Mechanismus zwingend erforderlich, um bekannte Angriffsmuster zuverlässig abzusichern und eine zusätzliche Sicherheitsebene bereitzustellen. Insgesamt ergibt sich damit die Notwendigkeit hybrider Architekturen, die sowohl lernbasierte als auch regelbasierte Verfahren kombinieren, um eine hohe Robustheit im operativen Betrieb zu gewährleisten.

Erklärbarkeit & Nachvollziehbarkeit

Die Erklärbarkeit und Nachvollziehbarkeit sind sowohl operativ als auch regulatorisch zwingend erforderlich. Aus forensischer Sicht muss nach einem Sicherheitsvorfall der vollständige Angriffspfad rekonstruierbar sein, um eine fundierte Analyse für Behörden, Versicherungen und die interne Aufarbeitung zu ermöglichen. KI-Systeme müssen hierfür lückenlose Audit-Trails⁸ bereitstellen, die alle relevanten Entscheidungen und Datenflüsse nachvollziehbar dokumentieren.

Darüber hinaus bestehen konkrete regulatorische Anforderungen, insbesondere aus der NIS2-Richtlinie⁹ sowie den BSI-Vorgaben, die verbindliche Incident-Response-Prozesse¹⁰, Meldepflichten und eine lückenlose Nachvollzieh-

barkeit von Sicherheitsvorfällen vorschreiben. Dazu gehören insbesondere dokumentierte Abläufe zur Erkennung, Bewertung, Meldung und Behandlung sowie revisionssichere Protokollierung (Audit Trails). Ohne nachvollziehbare und erklärbare KI-Entscheidungen kann diese geforderte Transparenz in der Vorfallsbearbeitung nur eingeschränkt erfüllt werden.

Auch rechtlich ist die Nachvollziehbarkeit entscheidend, da im Falle einer Meldepflicht gegenüber dem BSI gemäß §8b BSIG sowie gegenüber betroffenen Kunden eine präzise und begründbare Beschreibung des Sicherheitsvorfalls erforderlich ist.

Organisatorische & regulatorische Rahmenbedingungen

Die regulatorischen Anforderungen sind durch verschiedene europäische und nationale Vorgaben klar geprägt und gewinnen im Zuge der zunehmenden Digitalisierung weiter an Bedeutung. Mit der NIS2-Richtlinie, die seit Oktober 2024 in nationales Recht zu überführen ist, werden Energieversorger ausdrücklich als „wesentliche Einrichtungen“ eingestuft. Daraus ergibt sich die Pflicht, geeignete technische und organisatorische Maßnahmen zur Angriffserkennung umzusetzen, wobei KI-basierte Systeme einen skalierbaren Ansatz zur Erfüllung dieser Anforderungen darstellen können.

Ergänzend verschärft das KRITIS-Dachgesetz (KRITIS-DachG) ab 2025 die Anforderungen an die Resilienz und die Fähigkeit zur frühzeitigen Erkennung von Angriffen in kritischen Infrastrukturen (Deutscher Bundestag, 2025). Technische Standards wie der BSI IT-Grundschutz sowie die IEC 62443 bilden dabei zentrale Referenzrahmen für die Absicherung von OT-Systemen und konkretisieren die erwarteten Sicherheitsniveaus.

Darüber hinaus besteht gemäß §8b BSIG eine Meldepflicht für erhebliche IT-Sicherheitsvorfälle gegenüber dem BSI, wodurch Systeme zur Angriffserkennung eine zentrale Rolle bei der frühzeitigen Identifikation und Dokumentation von Vorfällen einnehmen. Auf europäischer Ebene ist zudem der EU AI Act relevant, unter dem KI-basierte Sicherheitssysteme in kritischen Infrastrukturen voraussichtlich als

⁷ Falsch-positive Klassifikationen, bei denen normale Aktivitäten irrtümlich als sicherheitsrelevante Anomalien oder Angriffe eingestuft werden.

⁸ Ein Audit Trail ist eine nachvollziehbare, manipulationssichere Protokollierung aller sicherheitsrelevanten System- und Benutzeraktionen zur späteren Prüfung und Nachvollziehbarkeit.

⁹ NIS2 (Network and Information Security Directive 2) ist eine EU-Richtlinie zur Stärkung der Cybersicherheit, die erweiterte Anforderungen an Risikomanagement, Meldepflichten, Incident Response und Sicherheitsmaßnahmen für Betreiber kritischer Einrichtungen festlegt.

¹⁰ Incident Response bezeichnet den strukturierten Prozess zur Erkennung, Analyse, Eindämmung, Behebung und Nachbereitung von Sicherheitsvorfällen in IT- und OT-Systemen.

Hochrisiko-Anwendungen eingestuft werden, was zusätzliche Anforderungen u. a. an Transparenz und Robustheit mit sich bringt.

Kosten-Nutzen-Analyse

Der Einsatz KI-gestützter Verfahren zur Angriffserkennung leistet einen hohen Beitrag zur betrieblichen Effizienz. Durch die frühzeitige Erkennung von Cyberangriffen und technischen Störungen können Ausfallzeiten reduziert und Schäden begrenzt werden. Gleichzeitig ermöglicht die verbesserte Unterscheidung zwischen Störungen und gezielten Angriffen eine gezieltere und effizientere Reaktion. Projekte aus der Praxis zeigen dabei bereits sehr hohe Erkennungsraten bei gleichzeitig geringen Fehlalarmraten (Kummerow, 2024). Die kontinuierliche, automatisierte Überwachung entlastet zudem das Leitstellenpersonal. Insgesamt führt dies auch zu einer Reduzierung potenzieller Folgekosten sowie zu einer erhöhten Netzstabilität durch eine zusätzliche Schutzebene über klassische Sicherheitsmechanismen hinaus.

Das Potenzial für Wissensgewinn ist gegeben, da Modelle kontinuierlich aus neuen Angriffsmustern und Anomalien lernen und sich entsprechend weiterentwickeln. Wiederkehrende Auffälligkeiten ermöglichen zudem die Identifikation systematischer Schwachstellen im Netz, wodurch strukturelle Probleme gezielt adressiert werden können. Die gewonnenen Erkenntnisse fließen direkt in Sicherheitsprozesse ein, etwa in die Weiterentwicklung von SOC-Strategien¹¹ und Schutzmaßnahmen. Gleichzeitig verbessert die Kombination von Prozess- und Kommunikationsdaten das Gesamtverständnis des Systems und erhöht die Qualität der Datenbasis. Insgesamt ermöglicht dies eine kontinuierliche Optimierung der Modelle sowie eine Anpassung an neue Betriebszustände und Angriffsszenarien.

Einmalige Investitionskosten

Die einmaligen Investitionskosten (CAPEX) für die Implementierung werden von einigen zentralen Kostenblöcken besonders geprägt, wie aus Abbildung 2 hervorgeht. Hervorzuheben sind die Investitionen in OT-Monitoring-Hardware, wie Sensoren oder TAPs (Test Access Point) für die passive Netzwerküberwachung, da diese flächendeckend und strategisch im Netz platziert werden müssen (Stouffer, et al., 2023; National Institute of Standards and

Technology, 2024). Ebenfalls kostenintensiv sind Anforderungen im Bereich Sicherheit und KI-Compliance, insbesondere durch regulatorische Vorgaben, die zusätzliche Maßnahmen und Dokumentation erforderlich machen (Deutscher Bundestag, 2025; Europäisches Parlaments und Rat, 2022; National Institute of Standards and Technology, 2024).

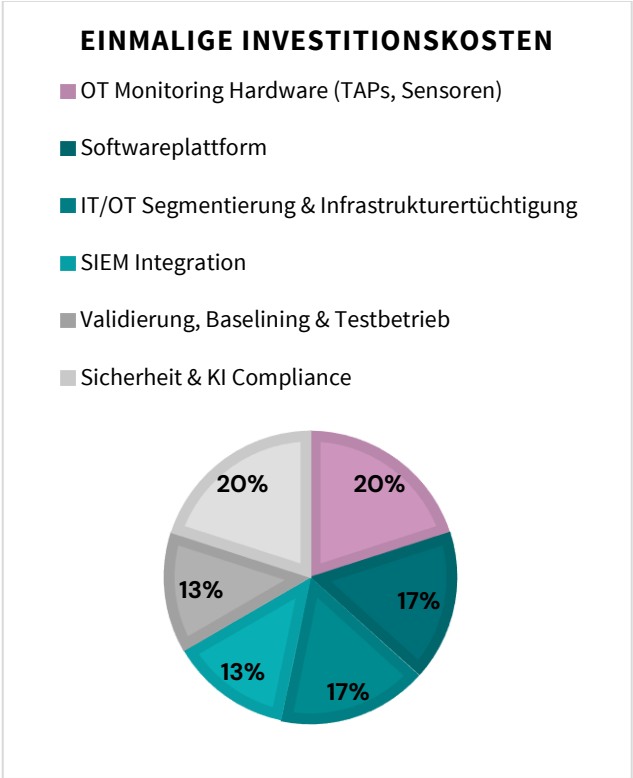


Abbildung 2: Einmalige Investitionskosten. Anteile sind indikativ.

Ein weiterer relevanter Kostenblock ist die Softwareplattform. Während kommerzielle Lösungen direkte Lizenzkosten verursachen, führen Open-Source-Ansätze häufig zu erhöhtem Integrations- und Betriebsaufwand. Ergänzend entstehen Aufwände für die IT/OT-Segmentierung und Infrastrukturertüchtigung, die in vielen Fällen Voraussetzung für den sicheren Betrieb solcher Systeme sind (Stouffer, et al., 2023). Auch Kosten für SIEM-Integration, Validierung und Testbetrieb sowie Schulung und Change-Management sind relevant (National Institute of Standards and Technology, 2024), fallen jedoch im Vergleich zu den genannten Haupttreibern meist moderater aus. Insgesamt hängt die Höhe der Investitionen stark vom Ausgangszustand der bestehenden Infrastruktur und dem angestrebten Integrationsgrad ab.

¹¹ Ansätze und organisatorische Maßnahmen in einem Security Operations Center (SOC), die festlegen, wie Sicherheitsereignisse überwacht, analysiert und behandelt werden, um Cyberangriffe frühzeitig zu erkennen und effektiv darauf zu reagieren.

Jährliche Kosten

Die laufenden Betriebskosten (OPEX) werden durch mehrere kontinuierliche Kostenblöcke geprägt. Ein wesentlicher Anteil entfällt auf die Bereitstellung von Rechenressourcen für die Inferenz im Dauerbetrieb, typischerweise über On-Premise-Server. Ergänzend entstehen Kosten für Rechenkapazitäten zum Retraining der Modelle, wobei der Bedarf stark vom eingesetzten Modell abhängt.

Ein weiterer relevanter Kostenblock ist die Datenhaltung, insbesondere für Log- und Netzwerkdaten, die häufig in manipulationssicheren und revisionskonformen Speichersystemen abgelegt werden müssen. In diesem Zusammenhang fallen auch erhöhte Kosten für Backup- und Archivierungslösungen an, etwa für Cold Storage und Audit-Logs im KRITIS-Kontext.

Zusätzlich entstehen laufende Aufwände für den Betrieb eines Monitoring-Stacks, der die Systemverfügbarkeit sicherstellt, Alarme bewertet und die Pflege von Signaturen unterstützt. Auch Plattformkosten, beispielsweise für Lizenzen, Softwareupdates und Threat-Intelligence-Dienste¹², stellen einen kontinuierlichen Kostenfaktor dar.

Besonders hervorzuheben sind zudem die Kosten für Compliance und Audit, die durch regulatorische Anforderungen entstehen und unter anderem Nachweispflichten, Penetrationstests sowie Schulungen umfassen. Insgesamt ergeben sich daraus laufende Kosten, die vor allem durch Monitoring, Compliance und Plattformbetrieb geprägt sind, während reine Rechen- und Speicherkosten vergleichsweise moderat bleiben.

Fazit

Insgesamt zeigen die betrachteten KI-Ansätze ein hohes Potenzial für die Erkennung von Cyberangriffen in Stromnetzen. Sie ermöglichen eine frühzeitige Identifikation von Angriffen, verbessern die Transparenz des Netzbetriebs und unterstützen eine effizientere Reaktion auf sicherheitsrelevante Ereignisse. Insbesondere vor dem Hintergrund der hohen potenziellen Schäden durch erfolgreiche Cyberangriffe können KI-gestützte Verfahren zur Anomalieerkennung einen wichtigen Beitrag zur Stärkung der Cybersicherheit in kritischen Infrastrukturen leisten.

Die Umsetzung ist jedoch mit hohem technischem, organisatorischem und regulatorischem Aufwand verbunden. Insbesondere die Verfügbarkeit geeigneter Daten, die Integration in bestehende Systeme sowie die Nachvollziehbarkeit und Absicherung der Modelle stellen relevante Anforderungen an Implementierung und Betrieb.

Die Anwendung ist daher als eher aufwändig und langfristig ausgerichtet einzuordnen. Dem hohen initialen und laufenden Aufwand steht jedoch ein potenziell hoher Nutzen gegenüber, insbesondere durch die frühzeitige Erkennung von Angriffen und die Reduzierung möglicher negativer Auswirkungen.

Referenzen

Bundesamt für Sicherheit in der Informationstechnik. (2024). *Einfluss von KI auf die Cyberbedrohungslandschaft (Version 1.0)*.

Bundesamt für Verfassungsschutz. (06.08.2026). *Glossar: Kritische Infrastrukturen (KRITIS)*. Von <https://www.verfassungsschutz.de/SharedDocs/glossareintraege/DE/K/kritische-infrastrukturen-kritis.html> abgerufen

Deutscher Bundestag. (2025). *Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-Dachgesetz – KRITIS-DachG)*. Von <https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/KM4/KRITIS-Dachgesetz.html> abgerufen

Europäisches Parlament und Rat. (2022). *Richtlinie (EU) 2022/2555*.

Humayun, M. (2024). *Securing the Internet of Things in Artificial Intelligence Era: A Comprehensive Survey*. doi:10.1109/ACCESS.2024.3365634

Kim, Y. (2022). *Smart grid security: Attacks and defence techniques*. doi:10.1049/stg2.12090

Kummerow, A. (2024). *PROTECT – Sicherer Netzbetrieb durch Einsatz selbstlernender KI-Firewalls in Energieversorgungsunternehmen*

¹² Threat-Intelligence-Dienste stellen aktuelle Informationen über bekannte Bedrohungen, Angriffsvektoren, Schadsoftware und Angriffsmuster bereit, um Cyberangriffe frühzeitig zu erkennen und Sicherheitsmaßnahmen gezielt anzupassen.

– *Gesamtabschlussbericht*. Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB. Von <https://publica.fraunhofer.de/entities/publication/1759c8a2-db4c-4d57-b843-b31f73670d83> abgerufen

Mishra, S. K. (2025). *Multi-Layered Cybersecurity for Smart Power Grids Using AI and Machine Learning for Real-Time Threat Detection and Prevention*.
doi:10.1109/GIEST66547.2025.11387477

Mitra, S. (2024). *Use of Graph Neural Networks in Aiding Defensive Cyber Operations*.
doi:10.48550/arXiv.2401.05680

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. doi:10.6028/NIST.CSWP.29

Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., . . . Thompson, M. (2023). *NIST SP 800-82r3: Guide to Operational Technology (OT) Security*.
doi:10.6028/NIST.SP.800-82r3

VDE Studie. (2025). *Künstliche Intelligenz in der Netzleittechnik*. Offenbach am Main: VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V.



Bundesministerium
für Wirtschaft
und Energie

Die Veröffentlichung dieser Publikation erfolgt im Auftrag des Bundesministeriums für Wirtschaft und Energie. Die Deutsche Energie-Agentur GmbH (dena) unterstützt die Bundesregierung in verschiedenen Projekten zur Umsetzung der energie- und klimapolitischen Ziele im Rahmen der Energiewende.

KONTAKT
Dr. Jakob Schieder-Hestermann
Themengebietsleiter Stromnetze

Tel.: +49 30 66 777-159
E-Mail:
Jakob.Schieder-Hestermann@dena.de

Deutsche Energie-Agentur GmbH (dena)
Chausseestraße 128 a
10115 Berlin

<https://www.dena.de/> Stand: 10/2026

Alle Rechte sind vorbehalten. Die Nutzung steht unter dem Zustimmungsvorbehalt der dena.