# Im Verbund

## Vermeidung von Cyberangriffen und Störungen bei virtuellen Kraftwerken

Kai-Oliver Detken

Der Energiesektor ist verstärkt Ziel von Cyberangriffen und aufgrund der mit der Digitalisierung einhergehenden Verbindung der Internet- und Strominfrastruktur anfälliger als das bisherige Energieversorgungssystem. Angreifern stehen nun sowohl die Angriffsvektoren aus herkömmlichen IT-Umgebungen als auch energieanlagenspezifische Angriffsmöglichkeiten zur Verfügung. Störungen und Angriffe müssen daher schnell und selbstständig identifiziert, Auswirkungen auf das System minimiert und die Fähigkeit entwickelt werden, möglichst schnell in den Normalzustand zurückzukehren. Diese Problematik wird im BMWI-Forschungsprojekt SecDER aufgegriffen, um ein Störfallinformationssystem (SIS) zu bauen, das dezentrale Energieanlagen und virtuelle Kraftwerke besser schützen soll. Eine wichtige Aufgabe, da auch das IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) ab Mai 2023 in den Startlöchern stehen wird.

Prof. Dr.-Ing. Kai-Oliver Detken ist Geschäftsführer der Decoit GmbH in Bremen


*Durch die Dezentralität von VK und der damit notwendigen Digitalisierung ist ein Energieversorger heute anfälliger für Cyberangriffe, als das noch bei geschlossenen Großkraftwerken der Fall war (Foto: Pete Linforth, pixabay)*

Durch die erhöhte Dezentralität der Energieerzeugung wird die Aggregation von Anlagen für die zukünftige Energieversorgung immer entscheidender. Virtuelle Kraftwerke (VK) gelten als zukünftige Kraftwerksstruktur, die konventionelle Großkraftwerke ablösen werden.

Ein VK bezeichnet hierbei die Bündelung vieler dezentraler Energieerzeuger, Speicher und Verbraucher zu einem technischen System. Die Daten jeder einzelnen Anlage werden dabei in kurzem zeitlichen Abstand ermittelt und von dem VK verarbeitet. Ein virtuelles Kraftwerk ist daher kein Kraftwerk im herkömmlichen Sinne, sondern besteht aus mehreren Erzeugungsanlagen, Lasten und Speichern, dessen Energie gebündelt ins Stromnetz eingespeist wird. Das VK soll daher aus einem Verbund von erneuerbaren und konventionellen Energien elektrische Leistung verlässlich zur Verfügung stellen (Bild 1).

Als Erzeuger können Wind- und Photovoltaikanlagen oder regelbare Anlagen wie Blockheizkraftwerke, Gas- und Dampfturbinen, Biogasanlagen oder flexible Verbraucher wie Industriebetriebe und Stromspeicher zum Einsatz kommen. Ziel ist es, erneuerbare Energien zuverlässiger und permanent zur Verfügung stellen zu können. Wie eine Steuerzentrale bündelt ein VK den Strom von vielen kleinen Erzeugern und speist ihn dort wieder ein, wo er neu vereinbart wurde. Das ist gar nicht so einfach, denn die zur Verfügung stehende Strommenge der angeschlossenen Erzeuger muss bekannt sein. Dafür wird ein Monitoring-System benötigt, das jeden einzelnen Erzeuger überwacht. Bei Solar- und Windkraftanlagen müssen dabei auch die Wetterdaten berücksichtigt werden, um

exakte Vorhersagen machen zu können. Zusätzlich muss der erzeugte Strom aber auch vermarktet werden, da dies seit dem Jahr 2014 für Betreiber von neuen erneuerbaren Energieanlagen ab 500 kW Leistung und ab 2016 für neue Anlagen ab 100 kW Leistung gilt. Da das VK für die angeschlossenen Erzeuger den Verkauf an der Strombörse übernimmt, muss die einzelne Anlage so gesteuert werden, dass der eingespeiste Strom der im Vorfeld vermarkteten Menge möglichst genau entspricht.

Durch die Dezentralität von VK und der damit notwendigen Digitalisierung ist ein Energieversorger heute anfälliger für Cyberangriffe, als das noch bei geschlossenen Großkraftwerken der Fall war. Zusätzlich werden digitale Infrastrukturen zunehmend komplexer und anfälliger für Cyberangriffe und technische Störungen, die zur Beeinträchtigung des Betriebs bis hin zu einem teilweisen oder kompletten Ausfall der Stromversorgung führen können. Hierbei setzt ein sicherer und fahrplantreuer Betrieb eines VK auch die frühzeitige Erkennung und Planbarkeit technischer Stillstände voraus. Störungen und Angriffe müssen schnell und selbstständig identifiziert, Auswirkungen auf das System minimiert und die Fähigkeit entwickelt werden, möglichst schnell in den Normalzustand zurückzukehren.

## Das SecDER-Projekt

In dem dreijährigen BMWI-Forschungsprojekt „Störfallinformationssystem für virtuelle Kraftwerke“ (SecDER), das im April 2021 gestartet wurde, werden speziell angepasste Verfahren zur Erkennung und Vermeidung von Cyberangriffen auf die betrachteten Systeme entwickelt und diese in Kombination mit Ansätzen zur Erkennung von technischen Störungen in ein Gesamtsystem integriert (Projektwebseite siehe Bild 2). Auch ist es von besonderer Bedeutung, dass das zu entwickelnde System aufgrund der verteilten Struktur von virtuellen Kraftwerken und Energieanlagen die Möglichkeit bietet, verteilte und mehrstufige Cyberangriffe zu erkennen und so ein ganzheitliches Lagebild der IT-Sicherheit für die betrachteten Systeme bereitzustellen. Dies soll ein Störfallinformationssystem (SIS) ermöglichen, das nicht nur auf Anomalien achten, sondern auch Verfügbarkeiten mit monitoren soll.

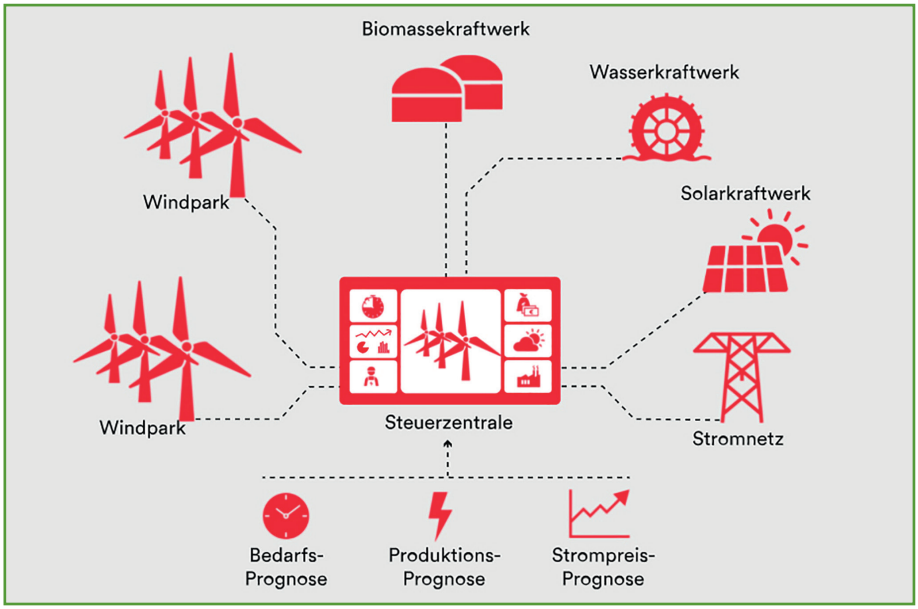


*Bild 1: Topologie virtueller Kraftwerke: Sie bestehen aus mehreren Erzeugungsanlagen, Lasten und Speichern, deren Energie gebündelt ins Stromnetz eingespeist wird (Quelle: BMWI, Statkraft Markets GmbH)*

Hinzu kommt die Pflicht für die Energieversorger und Betreiber, das im letzten Jahr verabschiedete IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) bis zum Mai 2023 umsetzen zu müssen. Darin heißt es ausdrücklich, dass die Verpflichtung der Betreiber kritischer Infrastrukturen (Kritis) darin besteht, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind. Dies umfasst auch den Einsatz von Systemen zur Angriffserkennung.

*Cyberattacken auf Kraftwerke müssen absorbiert werden und das System daraus gestärkt hervorgehen*

Im Anschluss an die Erkennung von Störungen ist die resiliente Behandlung von besonderer Bedeutung. Resilient sind virtuelle Kraftwerke nur dann, wenn technische sowie menschgemachte Störungen (z.B. Cyberattacken) absorbiert werden und das System gestärkt daraus hervorgeht. Hierzu müssen VK im sog. Resilience-Cycle mit den Phasen Vorbereiten, Verhindern, Beschützen, Reagieren und Wiederherstellen betrieben werden. In Summe tragen alle fünf Phasen dazu bei, mögliche Schäden vor, während und nach einem Störfall zu minimieren und die Funktionalität schnellstmöglich wiederherzustellen. Inwiefern der Resilience-Cycle und die aktuellen IKT-Konzepte bez. resilienter Software auf die Energiedomäne übertragbar sind, soll im Rahmen des Projektes ebenfalls untersucht werden.

Die konkreten Ziele des SecDER-Projektes sind:

- die Erhöhung von Angriffs- und Ausfallsicherheit durch KI-basierte, vorausschauende Erkennung von Cyberangriffen sowie technischen Störungen;
- Entwicklung von robusten Verfahren, die eine Erkennung der Cyberangriffe und technischen Störungen in kürzest möglicher Zeit bis hin zu Echtzeit ermöglichen;
- Entwicklung von Methoden zur Aggregation aller Ereignisse zu einem gesamtheitlichen Lagebild der IT-Sicherheit;
- Erhöhung der Verfügbarkeit, Integrität und Vertraulichkeit durch resiliente Abwehr von Cyberangriffen und technischen Störungen.

## Angriffs- und Ausfallerkennung

Durch immer zielgerichtetere und professionellere Cyberangriffe auf die IKT-Infrastruktur von Unternehmen ist ein alleiniger Schutz durch Firewall-Lösungen nicht mehr ausreichend. Zu modernen Sicherheitskonzepten gehören daher immer häufiger IDS-/IPS-Systeme (IDS – Intrusion Detection System, IPS – Intrusion Prevention System) zum vorausschauenden Schutz, indem kontinuierlich der Netzverkehr und Serverlogs auf Angriffe untersucht werden. Diese Systeme werden in der Regel an das zu überwachende System angepasst und haben dadurch die Möglichkeit, feingranularer zu erkennen, ob ein Cyberangriff stattfindet. Zum Einsatz können dafür verschiedene Angriffserkennungssysteme kommen, wie Snort, Zeek (Bro), Samhain, Prelude oder OSSEC. Aufgrund zu vieler Alarmfalschmeldungen (False Positives) und dem notwendigen Know-how bei der Auswertung, werden IDS-/IPS-Systeme allerdings immer mehr von SIEM-Systemen (Security Information and Event Management) abgelöst. Diese aggregieren die Logdateien verschiedener Systeme und ermöglichen deren Echtzeit- und Offlineanalyse. SIEM-Lösungen erkennen im Idealfall auch unbekannte Sicherheitsbedrohungen und erleichtern die Umsetzung von Compliance-Vorgaben. Bekannte Lösungen sind Logrhythm, Logpoint, OSSIM (AlienVault) oder Splunk.

Die signaturbasierte Erkennung von Angriffen, wie sie in den meisten kommerziellen Systemen im Einsatz ist, hat allerdings den Nachteil, dass nur bekannte Angriffe erkannt werden können. Systeme zur Anomalieerkennung sollen diesen Nachteil ausräumen und außergewöhnliches Verhalten auf Basis von Normalverhaltensmodellen automatisch entdecken. Abweichungen vom Normalverhalten von Nutzern oder von Maschinen stellen dann Hinweise auf mögliche Angriffe dar. So können auch neuartige Angriffe erkannt werden. Der Nachteil ist jedoch die potenziell hohe Anzahl an Falschmeldungen.

Da die Verfügbarkeit von Energieanlagen die oberste Priorität darstellt, existieren in der Betriebsführung von solchen

Anlagen verschiedene Ansätze zur Erkennung sich anbahnender Ausfälle durch technische Störungen und der Bewertung des Betriebsverhaltens. Hierbei unterscheidet man zwischen physikalischen, statistischen und physikalisch-statistischen Modellen. Physikalische Modelle setzen die genaue Kenntnis der Systeme und der einzelnen Messgrößen voraus, während statistische Modelle entsprechende Zusammenhänge aus Trainingsdaten herleiten. In verschiedenen Ausprägungen befinden sich solche Systeme sowohl in der Windenergie als auch in der Photovoltaik in der Entwicklung oder der Einführung. Als zusätzliche Indikatoren für die Betriebssicherheit werden im praktischen Einsatz Betriebskennzahlen (Key Performance Indicator – KPI) herangezogen. Zusätzlich sind Kennzahlen in der Entwicklung,

*Erneuerbare Energien müssen zukünftig zuverlässiger und vor allem permanent zur Verfügung stehen*

die zur Quantifizierung von technischen Anomalien dienen werden.

Methoden der künstlichen Intelligenz (KI) werden heute immer mehr in Bereichen zur Entscheidungsfindung und -Unterstützung eingesetzt, in denen falsche Entscheidungen zu potenziell sicherheitskritischen Zuständen führen können. So werden Verfahren des maschinellen Lernens (ML) z.B. zur Steuerung von Fahrzeugen und Drohnen, aber auch zur Spracherkennung verwendet. Forscher von Google zeigten in der Vergangenheit bereits, wie einfach sich neuronale Netze durch leichte, aber unmerkliche Veränderungen des Eingabebildes täuschen lassen. Beispielsweise wurde ein Stoppschild durch Aufkleben von schwarzen Stickern leicht verändert, so dass der Verkehrsschild-Klassifikator ein Tempo-45-Schild erkannte. Leider sind neuronale Netze sehr anfällig gegen diese „Adversarial Attacks", was eine Anwendung in sicherheitskritischen Bereichen nach wie vor schwierig macht.


*Bild 2: Im SecDER-Projekt werden Verfahren zur Erkennung und Vermeidung von Cyberangriffen entwickelt und diese mit Ansätzen zur Erkennung von technischen Störungen in ein Gesamtsystem integriert (Quelle: secder project)*

Im SecDER-Projekt werden daher speziell angepasste Verfahren zur Erkennung und Vermeidung von Cyberangriffen auf die betrachteten Systeme entwickelt und diese in Kombination mit Ansätzen zur Erkennung von technischen Störungen in ein sog. Störfallinformationssystem (SIS) integriert. Auch ist es von besonderer Bedeutung, dass das zu entwickelnde System aufgrund der verteilten Struktur von virtuellen Kraftwerken und Energieanlagen die Möglichkeit bietet, verteilte und mehrstufige Cyberangriffe zu erkennen und so ein ganzheitliches Lagebild der IT-Sicherheit für die betrachteten Systeme bereitzustellen.

## Fazit

Cyberresiliente Systeme zeichnen sich dadurch aus, dass sie auch beim Auftreten unerwünschter Ereignisse und unter widrigen Umständen (z.B. Cyberangriffe, Bugs, technische Störungen) stets ihren Dienst leisten. Bekannte Prinzipien zur sicheren Verteilung von IT-Diensten in unabhängige Komponenten stammen bisher aus den Bereichen Cloud-Computing, Microservices sowie verteilter Systeme und verbessern neben der Resilienz auch die Verfügbarkeit und Flexibilität. Durch einen von entsprechenden Prinzipien geleiteten Systementwurf werden Störungen schnell, effektiv und ganzheitlich abgefangen. Weiterhin gehört zur Resilienz eines Systems auch die Fähigkeit, Angriffe und Ausfälle vorherzusagen und zu erkennen, um entsprechende Maßnahmen zur Abwehr und Vermeidung einzuleiten. Die Notfallwiederherstellung (Disaster Recovery) im Fall eines erfolgreichen Angriffs stellt aber eine neue Herausforderung dar.

Einige virtuelle Kraftwerke sind bereits in Betrieb, z.B. Next Pool von der Next Kraftwerk GmbH oder das VK der Firma Statkraft. Beide zusammen greifen auf fast 10.000 MW Leistung zu, was einer Leistung von zehn Kernkraftwerken ungefähr entspricht. Eine Untersuchung und die Entwicklung entsprechender cyberresilienter Systeme im virtuellen Kraftwerk ist daher dringend notwendig und wird durch das SecDER-Projekt nun umgesetzt.

*www.decoit.de*