Bundesamt für Verfassungsschutz

Sicherheitshinweis für die Wirtschaft | 01/2026 | 26. März 2026

Betreff | Energiesektor im Visier

Ausgangslage

Die regelbasierte internationale Ordnung ist tiefgreifenden Veränderungen ausgesetzt. Staatliche Akteure und deren Proxys wirken im Rahmen dieser „globalen Unordnung“ mit der vollen Bandbreite hybrider Instrumente auf Deutschland ein. Dazu zählen Spionage, Cyberspionage, Sabotage und Einflussnahme. Parallel verschärft sich auch die Bedrohung durch linksextremistische Akteure hierzulande, welche vermehrt und vor dem Hintergrund verschiedenster Begründungszusammenhänge Kritische Infrastrukturen (KRITIS) und andere Unternehmen angreifen. Energieinfrastrukturen stellen besonders hochwertige Ziele dar und unterliegen daher einer erhöhten Gefährdung.

Sachverhalte

Links-extremistisch motivierter Brandanschlag auf Berliner Strombrücke

Linksextremisten verursachen durch Sachbeschädigungen und Brandanschläge gegen KRITIS jedes Jahr Schäden in mehrstelliger Millionenhöhe. Zuletzt hat sich eine linksextremistische „Vulkangruppe“ zu dem folgenschweren Brandanschlag im Januar 2026 auf eine Kabelbrücke über den Teltowkanal in Berlin bekannt. Durch den Brand an mehreren Starkstromkabeln kam es in vier Stadtteilen zu einem großflächigen und mehrere Tage andauernden Stromausfall, der rund 45.000 Haushalte und etwa 2.200 Gewerbebetriebe betraf. Auch mehrere Krankenhäuser und Pflegeheime wurden in Mitleidenschaft gezogen. Außerdem kam es zu Beeinträchtigungen bei der Wärmeversorgung, der Festnetz- und Mobiltelefonie sowie im öffentlichen Personennahverkehr. Mit dem Angriff wollten die Täter gezielt Unternehmen in einem nahe gelegenen Technologiepark schädigen. Laut Taterklärung war ihnen bewusst, dass der großflächige Ausfall der Stromversorgung auch unbeteiligte Personen treffen würde.

Linksextremistische Kampagne „Switch off“

Anfang 2023 wurde mit „Switch off“ die inzwischen bedeutendste Kampagne des gewaltorientierten Linksextremismus initiiert. Die Kampagne lehnt jedes staatliche Handeln zur Lösung der Klimaerwärmung ab und fordert, die Verantwortlichen für „die Zerstörung der Natur“ sowie „die Infrastruktur des Kapitalismus“ anzugreifen. Auf der Website der Kampagne findet sich eine Auflistung verschiedener Energieversorger und Industrieunternehmen, die in besonderem Maße für die Klimaerwärmung verantwortlich seien. Die betroffenen Unternehmen werden hierdurch klar ersichtlich zu Zielen für Straftaten erklärt.

Koordinierte Cyberangriffe auf polnische Energieinfrastruktur

Im Dezember 2025 kam es zu mehreren abgestimmten Cyberangriffen auf Energieinfrastrukturen in Polen. Einer der Angriffe richtete sich gegen 30 Verteilerstationen bzw. Umspannwerke für erneuerbare Energien (Windkraftanlagen und Solarparks). Er führte zu einer Unterbrechung der Kommunikation zwischen den Umspannwerken und dem Netzbetreiber. Der Angreifer hatte umfangreich Zugang zu den Systemen und wäre grundsätzlich in der Lage gewesen, Störungen in den an die Umspannwerke angebundenen Clustern von Windkraftanlagen und Solarparks herbeizuführen. Ein anderer Teilangriff richtete sich gegen ein großes Blockheizkraftwerk mit dem Ziel, Daten im internen Netzwerk irreversibel zu zerstören. Die Angreifer hatten zuvor über längere Zeit sensible Daten gesammelt und sich dafür positioniert, Computer im internen Netzwerk mit einer destruktiven Schadsoftware zu infizieren. Der Angriff schlug fehl, da die lokal installierte Sicherheitssoftware anschlug und die maliziösen Aktivitäten blockierte. Bei der Schadsoftware handelte es sich um die gleiche, die bei dem Angriff auf die Umspannwerke verwendet wurde. Das polnische Cyber Emergency Response Team (CERT) sieht bei der Kampagne deutliche Überschneidungen mit Infrastrukturen der russischen Advanced-Persistent-Threat-(APT)-Gruppierung „Berserk Bear“. Der Akteur ist auch als „Energetic Bear“, „Dragonfly“ oder „Crouching Yeti" bekannt und seit mindestens 2004 aktiv. Seine Cyberangriffe zielen vorwiegend auf Unternehmen aus den KRITIS-Sektoren Energie, Wasser und Telekommunikation/ Informationstechnik ab.

Hacktivistische DDoS-Angriffe auf belgische Energieversorger

Die (pro-)russische Hacktivismus-Gruppierung „NoName057(16)“ hat im Dezember 2025 die Urheberschaft für eine Reihe von Distributed-Denial-of-Service-(DDoS)-Angriffen auf mehrere Energieversorgungsunternehmen in Belgien für sich reklamiert. Die Gruppe verwies zur Begründung auf die politische Haltung der belgischen Regierung gegenüber Russland und setzte damit ihr Muster von angeblichen Vergeltungsschlägen gegen KRITIS in Europa fort.

Debatten um ausländische Investoren und Zulieferer im KRITIS-Sektor Energie

In den vergangenen Monaten kam es vermehrt zu Debatten rund um den Einstieg ausländischer Investoren in bzw. die Auftragsvergabe an ausländische Zulieferer für die deutsche Energieinfrastruktur. So plant der US-amerikanische Finanzinvestor Warburg Pincus einen Mehrheitseinstieg beim Berliner Softwareunternehmen PSI, auf dessen Netzleitsysteme diverse deutsche Energieinfrastrukturbetreiber setzen. Der ebenfalls aus den USA stammende Mineralölkonzern Sunoco hat im Januar 2026 den deutschen Tanklagerbetreiber TanQuid übernommen, der unter anderem

Standorte der Luftwaffe mit Kerosin versorgt. Der Hamburger Asset Manager Luxcara wiederum hat erst kürzlich Pläne verworfen, Turbinen des chinesischen Herstellers Mingyang für zwei geplante Offshore-Windparks in der Nordsee zu beschaffen und sich stattdessen für eine europäische Alternative von Siemens Gamesa entschieden. Der italienische Ferngasnetzbetreiber Snam, dessen Muttergesellschaft zu mehr als einem Drittel dem chinesischen Netzbetreiber State Grid gehört, verzichtet auf einen eigentlich geplanten Einstieg beim deutschen Konkurrenten Open Grid Europe.

Bewertung

Andauernde linksextremistische Gefährdung

Die Intensität linksextremistisch motivierter Angriffe auf KRITIS hat zugenommen, was sich an den hohen Schadenssummen und den teils schwerwiegenden Auswirkungen auf die Bevölkerung erkennen lässt. Gewaltorientierte linksextremistische Akteure werden auch weiterhin Energieinfrastrukturen ins Visier nehmen. Sie zielen aber bei ihren Angriffen seltener direkt auf einen Ausfall von KRITIS ab. Vielmehr wollen sie ausgewählte Unternehmen schädigen, beispielsweise durch eine Unterbrechung der Stromversorgung. Kollateralschäden nehmen sie dabei billigend in Kauf. Angriffe auf Energieinfrastrukturen bieten gewalttätigen linksextremistischen Akteuren die Gelegenheit, drastische Bilder zu erzeugen und sich medial zu profilieren. Indem sie ihre Gewalttaten in einen gemeinsamen ideologischen Kontext setzen, wollen sie potenzielle Nachahmerinnen und Nachahmer gewinnen. Unternehmen stehen als tragende Säulen des „ausbeuterischen“ und „repressiven kapitalistischen Systems“ besonders im Fokus. Zurückliegende Angriffe haben gezeigt, dass linksextremistische Akteure über das notwendige Know-how verfügen, um klandestin erhebliche Schäden zu bewirken. Brandanschläge in verschiedenen Formen stellen das favorisierte Mittel der Tatbegehung dar. Anleitungen zur Herstellung unterschiedlichster Brandsätze sind auch digital zugänglich.

Abstrakt erhöhte Cybergefährdung insbesondere durch Russland

Es ist davon auszugehen, dass ausländische Nachrichtendienste und Cybergruppierungen deutsche KRITIS gezielt auskundschaften, um Einfallstore für Angriffe zu identifizieren und vorzubereiten. Ein Einsatz von Malware gegen Steuerungselemente in deutschen Energieinfrastrukturen könnte zu Beeinträchtigungen oder gar Ausfällen hierzulande führen und damit nicht nur unmittelbare Auswirkungen auf die betroffenen Unternehmen, sondern auch auf die Versorgung der Bevölkerung und der Wirtschaft haben. Das wiederum könnte das Vertrauen in die Funktionsfähigkeit der Daseinsfürsorge und des Staates insgesamt schädigen. Russland besitzt die Fähigkeiten und den Willen, entsprechende Aktivitäten gegen EU-Mitgliedsstaaten und NATO-Bündnispartner zu richten. 2025 waren vereinzelt niedrigschwellige Angriffsversuche von dort zu verzeichnen, darunter auch Aufklärungsaktivitäten von „Berserk Bear“. Aktuell liegen keine Erkenntnisse zu konkreten Kampagnen vor, die zu spürbaren Auswirkungen führen könnten. Im Falle einer weiteren Lageverschärfung im Umfeld des Angriffskriegs gegen die

Ukraine und des offensiven Agierens Russlands gegen die europäischen Demokratien ist jedoch mit einer erhöhten Gefährdung auch für deutsche KRITIS zu rechnen.

Weiterhin hacktivistische Angriffe

DDoS-Angriffe wie die von „NoName057(16)“ verursachen in der Regel nur kurze Unterbrechungen und damit vergleichsweise geringe Schäden. Als eine der führenden Unterstützernationen der Ukraine steht Deutschland allerdings besonders im Fokus (pro-)russischer Hacktivismus-Gruppierungen. Abhängig vom weiteren Kriegsverlauf muss weiterhin mit entsprechenden Angriffen gegen Energieinfrastrukturen hierzulande gerechnet werden. Diese sollen nicht nur Prozesse stören, sondern in erster Linie in den Informationsraum hineinwirken und vor allem Unsicherheit schüren und Angst verbreiten.

Risiko ausländischer Einflussnahme

Andere Staaten erzeugen gezielt einseitige wirtschaftliche und technologische Abhängigkeiten, um in Zeiten geopolitischer Umbrüche und in politischen Konfliktsituationen Druck ausüben zu können. Insbesondere China und Russland haben sich in der jüngeren Vergangenheit durch entsprechende Einflussnahmeversuche hervorgetan. Der Instrumentenkasten reicht von strategischen Investments bis hin zur Beherrschung von Technologien und Lieferketten. Gerade bei Übernahmen besteht darüber hinaus die Gefahr, dass Betriebs- und Geschäftsgeheimnisse ungewollt abfließen. Der Einstieg eines ausländischen Investors in ein einzelnes KRITIS-Unternehmen mag auf den ersten Blick unproblematisch erscheinen. Eine Häufung derartiger Investments kann mittel- bis langfristig allerdings nicht nur die Wettbewerbsfähigkeit schmälern, sondern auch die öffentliche Sicherheit und Ordnung gefährden sowie die strategischen Handlungsoptionen der deutschen Außen- und Sicherheitspolitik schmälern.

Handlungsempfehlungen

Maßnahmen für Sicherheitsverantwortliche:

- Etablieren Sie ein ganzheitliches Risikomanagement, das physische Sicherheit, Informations- und Cybersicherheit sowie organisatorische Maßnahmen integriert und regelmäßig anhand der aktuellen Bedrohungslage insbesondere für KRITIS-Sektoren wie Energie, Wasser sowie Informationstechnik und Telekommunikation überprüft wird.
- Richten Sie das materielle Schutzniveau von Anlagen und Netzkomponenten an deren kritischer Versorgungsfunktion aus (z. B. Umspannwerke, Leitstellen, Schaltanlagen). Berücksichtigen Sie dabei die möglichen Folgewirkungen für Versorgungssicherheit und öffentliche Sicherheit im Sinne der KRITIS-Definition.
- Sensibilisieren und schulen Sie Ihre für Anwerbungsversuche besonders gefährdeten Mitarbeitenden regelmäßig mit Blick auf aktuelle Gefahren durch ausländische Nachrichtendienste und – aufgrund ihrer aggressiven Vorgehensweisen – insbesondere durch die Nachrichtendienste Russlands.

- Schulen Sie Ihre Mitarbeitenden regelmäßig mit Blick auf aktuelle Gefahren im Cyberraum, insbesondere zu Angriffen auf Leit- und Fernwirktechnik (OT), auf Schnittstellen zwischen OT und IT sowie auf Betriebsführungs- und Leitsysteme. Vermitteln Sie zudem, welche öffentlich zugänglichen Informationen (z. B. Netzpläne, Schaltbilder, Standortdaten) potentiell für Angriffe auf Energieinfrastrukturen missbraucht werden können.
- Informieren Sie im Rahmen der Prävention gezielt über Szenarien physischer Sabotagehandlungen gegen Energieanlagen sowie darüber, dass diese mit Cyberangriffen abgestimmt sein können. Berücksichtigen Sie dabei vorrangig Prozesse und Anlagen, deren Ausfall weitreichende und langanhaltende Versorgungsunterbrechungen verursachen kann.
- Etablieren Sie klare Melde-, Alarmierungs- und Eskalationswege und kommunizieren Sie diese verbindlich an die Beschäftigten. Unterstützen Sie Ihr Personal dabei, Melde- und Berichtspflichten einzuhalten und üben Sie die Abläufe regelmäßig, damit alle Beteiligten im Ernstfall sicher und routiniert handeln können.
- Überprüfen Sie bestehende und geplante Veröffentlichungen (z. B. Netzausbaukarten, Lagepläne, Referenzprojekte) kritisch im Hinblick auf deren Nutzen für potenzielle Angreifer. Hinterfragen Sie insbesondere Veröffentlichungen, die über das gesetzlich erforderliche Maß hinausgehen, unterlassen Sie diese im Zweifel und nutzen Sie gesetzliche Ausnahmeregelungen von Transparenzpflichten. Geben Sie sensible Inhalte restriktiv nur an einen auf das notwendige Minimum beschränkten Personenkreis heraus („Need-to-know“-Prinzip), sofern keine Veröffentlichungspflichten entgegenstehen.
- Schaffen Sie für sensible Informationen geeignete, abgesicherte Übermittlungswege – zum Beispiel Zwei-Faktor-Authentifizierung (2FA) und verschlüsselte E-Mail-Kommunikation.
- Führen Sie in geeigneten Abständen Penetrationstests durch, um ein Feedback zum Umsetzungsstand der IT-Sicherheit aus Angreifer-Sicht zu erhalten. Sorgen Sie dafür, dass interne Server-, Leitstellen- und Fernwirkdienste grundsätzlich nicht ohne Weiteres aus dem Internet erreichbar sind. Es bietet sich an, einen Zugriff lediglich aus dem Unternehmensnetzwerk oder über Virtual Private Network (VPN) zuzulassen.
- Prüfen Sie, inwieweit eine konsequente Netzsegmentierung und – wo sinnvoll – eine Verschleierung eigener IP-Adressbereiche durch Reseller dazu beitragen kann, Aufklärungsaktivitäten und automatisierte Angriffe auf kritische Systeme zu erschweren.

Maßnahmen für Personalverantwortliche:

- Wägen Sie bei Stellenausschreibungen kritisch ab, welche Informationen zwingend veröffentlicht werden müssen, um qualifiziertes Personal anzusprechen. Beschreiben Sie hierbei möglichst generische Anforderungen. Verzichten Sie nach Möglichkeit auf Details zu konkreter Netzarchitektur, eingesetzter Leit- und Schutztechnik und spezifischen Systemkonfigurationen.
- Stellen Sie in Ihrer Social-Media-Policy sicher, dass Beschäftigte Zurückhaltung bei Bezügen zu KRITIS- und insbesondere Energieinfrastrukturen üben. Falls keine solche Policy existiert, prüfen Sie eine Einführung.

Maßnahmen für Beschäftigte:

- Treten Sie in sozialen Netzwerken und Karriereplattformen möglichst datensparsam auf und vermeiden Sie Angaben zu konkreten Standorten, Anlagen, Schaltaufgaben oder sicherheitsrelevanten Projekten in KRITIS-Sektoren oder der Energieversorgung Ihres Unternehmens. Seien Sie sich bewusst, dass solche Informationen in Verbindung mit anderen frei verfügbaren Daten zur Planung von Angriffen genutzt werden können.
- Nutzen Sie für dienstliche Kommunikation möglichst nur die vorgesehenen, abgesicherten Kommunikationskanäle und verzichten Sie auf private Messenger-Dienste oder ungesicherte Cloud-Dienste für betriebskritische Informationen in der Energieversorgung.
- Achten Sie auf Anzeichen physischer Sabotage, etwa Beschädigungen an Umzäunungen, Manipulationen an Masten, Kabeltrassen oder Schaltanlagen, Drohnenüberflüge oder sonstige Ausspähversuche. Melden Sie entsprechende Beobachtungen – auch wenn diese zunächst banal erscheinen – konsequent über die dafür vorgesehenen Meldewege.
- Seien Sie sich bewusst, dass Sie durch Ihre Funktion besonders exponiert sein und deshalb in den Fokus ausländischer Nachrichtendienste geraten können. Öffentliche Meinungsäußerungen, gerade in sozialen Medien, können gegen Sie instrumentalisiert werden, um nachrichtendienstliche Ausforschungs- und Sabotageinteressen durchzusetzen. Dies kann auch ohne Ihr Wissen und von Ihnen unbemerkt geschehen.

So erreichen Sie uns

Für Informationen zu Bedrohungen für Ihre Branche durch Spionage und Sabotage, Terrorismus oder gewaltbereiten Extremismus sowie für konkrete Sicherheitsanfragen oder Verdachtsfälle kontaktieren Sie den Bereich Wirtschaftsschutz:

wirtschaftsschutz@bfv.bund.de
+49 30 18792-3322

Natürlich steht Ihnen auch die Landesbehörde für Verfassungsschutz in Ihrem Bundesland als Ansprechpartner zur Verfügung. Sollte Ihnen der Kontakt nicht bekannt sein, vermitteln wir Ihnen diesen gerne.

Ihre Angaben werden in jedem Fall vertraulich behandelt.

PRÄVENTION
WIRTSCHAFTSSCHUTZ