BUNDESVERBAND TECHNISCHER BRANDSCHUTZ e. V.

Der Branchenkompass des bvfa

BRANDSCHUTZKOMPAKT

Nr. 67 / März 2025

Brandschutz in Kritischen Infrastrukturen

Kritische Infrastrukturen stärken: Mehr Widerstandskraft für die Zukunft!

Cyber trifft Brandschutz: Die perfekte Kombination für maximale Sicherheit

Von der Windkraftanlage in die Steckdose: Offshore-Anlagen und Stromtrassen

Brandschutz wird kritisch

Kritische Infrastrukturen bilden das Rückgrat unserer modernen Gesellschaft. Krankenhäuser, Energieversorger, Kommunikationsnetze und Wasserwerke sind für das tägliche Leben und die wirtschaftliche Stabilität unverzichtbar. Ein Brand in solchen Einrichtungen gefährdet nicht nur Menschenleben, sondern führt auch zum Ausfall lebenswichtiger Funktionen. So kann ein Stromausfall in einem Krankenhaus oder ein Brand in einem Rechenzentrum lebensrettende Operationen gefährden oder die digitale Infrastruktur lahmlegen. Der Brandschutz in kritischen Infrastrukturen muss daher integraler Bestandteil unserer nationalen Sicherheitsstrategie sein.

Die Digitalisierung bringt zusätzliche Herausforderungen mit sich. Cyberangriffe können vernetzte Brandschutzsysteme per Fernzugriff manipulieren oder lahmlegen – eine Gefahr, die bislang oft unterschätzt wird. Cyberkriminelle und staatlich gesteuerte Hacker haben dabei nicht nur kritische Infrastrukturen im Visier, sondern auch kleine und mittlere Unternehmen. Daher ist eine enge Verzahnung von Brandschutz und IT-Sicherheit notwendig.

Mit dem KRITIS-Dachgesetz und der NIS2-Richtlinie mit klaren Vorgaben zu Risikoanalyse, Prävention und Resilienz wurden wichtige europäische Rahmenbedingungen geschaffen, die auch den Brandschutz betreffen. Es liegt nun an Ihnen, diese Vorgaben mit Leben zu füllen! Der bvfa und seine Mitgliedsunternehmen unterstützen Sie dabei mit Branchenkonzepten, Merkblättern und Positionspapieren – und mit diesem BrandschutzKompakt. Lesen Sie selbst!

Ihr

Raymund Hertelt
Leiter der Fachgruppe
Steuerungstechnik für Löschanlagen

Brand bei der französischen Cloud-Dienstleistungsfirma OVH Cloud in Straßburg, Frankreich.

Kritische Infrastrukturen stärken: Mehr Widerstandskraft für die Zukunft!

Schutz vor Bränden und anderen physischen Risiken und vor Cyberangriffen

Kritische Infrastrukturen sind lebenswichtig für das Funktionieren unserer Gesellschaft. Ihr Ausfall hätte unabsehbare Folgen. Zwei Richtlinien der Europäischen Union sollen deshalb sowohl die physische Sicherheit als auch den Schutz vor Cyberangriffen verstärken. Ein wichtiger Teil des Sicherheitskonzepts sind wirksame Brandschutzmaßnahmen, denn ein Feuer kann in kurzer Zeit ganze Liegenschaften zerstören und das Erbringen einer kritischen Dienstleistung für lange Zeit verhindern.

Kritische Infrastrukturen (kurz: KRITIS) wie die Energie- und Wasserversorgung, Krankenhäuser und IT-Netzwerke versorgen uns mit lebenswichtigen Gütern und Dienstleistungen. Bei Ausfall oder Beeinträchtigung von KRITIS-Einrichtungen kann es zu nachhaltigen Versorgungsengpässen und erheblichen Störungen der öffentlichen Sicherheit kommen. Abhängigkeiten zwischen KRITIS-Einrichtungen und anderen Branchen führen zu Ausfällen in nicht direkt betroffenen Unternehmen bis hin zu weitreichenden Dominoeffekten. So sind zum Beispiel bei einem großflächigen Stromausfall auch Tankstellen betroffen, da der Strom für die Pumpen fehlt. Das führt zu Störungen in der Logistik mit Auswirkung auf zahlreiche Lieferketten und damit zu weiteren Ausfällen. In sensiblen Bereichen können selbst kleine Störungen weitreichende Folgen haben. Im Jahr 2022 etwa legte das Durchtrennen zweier redundanter Glasfaserkabel den gesamten Zugverkehr in Norddeutschland lahm.

Europa reagiert

Die Bedrohungen für kritische Infrastrukturen sind zahlreich und reichen von Bränden, Unfällen und Naturkatastrophen bis hin zu Terrorangriffen, Cyberbedrohungen und Sabotage. Lieferkettenstörungen, medizinische Notlagen und vieles mehr können die Folge sein. Da diese Ereignisse nicht grundsätzlich vermeidbar sind, steht beim Schutz kritischer Infrastrukturen die Stärkung ihrer „Resilienz“ im Vordergrund. Darunter

Nach einem Großbrand fallen KRITIS-Einrichtungen für lange Zeit aus.

43 %
der Unternehmen

sind kurze Zeit nach einem größeren Brand insolvent, weitere 28 % nach drei Jahren.

IHK Trier

versteht man die Fähigkeit, Ereignissen zu widerstehen oder sich daran anzupassen und dabei die Funktionsfähigkeit zu behalten oder schnell wiederzuerlangen.

Die EU hat die Bedrohung kritischer Infrastrukturen auch vor dem Hintergrund zunehmender internationaler Krisen erkannt und zwei europaweit gültige Richtlinien verabschiedet. Die CER-Richtlinie (Critical Entities Resilience) verpflichtet die Mitgliedstaaten, kritische Einrichtungen zu identifizieren und deren physische Widerstandsfähigkeit zu stärken. Parallel dazu soll vor dem Hintergrund der stark ansteigenden Cyberbedrohungen die NIS2-Richtlinie ein hohes Cybersicherheitsniveau gewährleisten, um die Auswirkungen von Cyberangriffen und Störungen auf IT-Systeme und Netzwerke zu minimieren. In Deutschland werden die beiden EU-Richtlinien durch das KRITIS-Dachgesetz und das NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz umgesetzt. Mit ihrem Inkrafttreten wird im Jahr 2025 gerechnet. Dabei fallen die Betreiber kritischer Einrichtungen automatisch auch in den Geltungsbereich von NIS2.

Resilienz und physische Sicherheit

Das KRITIS-DachG soll die Resilienz und physische Sicherheit von kritischen Infrastrukturen stärken. Es geht von einem „All-Gefahren-Ansatz“ aus, d. h. KRITIS-Betreiber müssen sicherstellen, dass ihre Einrichtungen gegen alle möglichen Gefährdungen der physischen Sicherheit geschützt sind sowie Vorfälle verhindert, abgewehrt und in ihren Folgen begrenzt werden. Dazu müssen Betreiber eine Risikoanalyse vornehmen, die Risiken bewerten sowie Maßnahmen zur Risikominimierung erarbeiten und umsetzen. Alle Maßnahmen werden in einem Resilienzplan niedergelegt. Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) will dazu nationale und sektorenbezogene Risikoanalysen sowie in Abstimmung mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) einen Katalog von sektorenübergreifenden Mindestanforderungen zur Resilienz bereitstellen. Erhebliche Störungen müssen binnen 24 Stunden an eine gemeinsame Meldestelle von BSI und BBK gemeldet werden. Es wird empfohlen, auch Anlagen zu ertüchtigen, die nicht unter die Kriterien des KRITIS-DachG fallen. Zusätzliche Anforderungen könnten sich ergeben, wenn Unternehmen Teil der Lieferkette einer KRITIS-Einrichtung sind.

<< Die Betreiber kritischer Anlagen sind verpflichtet, verhältnismäßige technische, sicherheitsbezogene und organisatorische Maßnahmen zur Gewährleistung ihrer Resilienz zu treffen, ... um einen angemessenen physischen Schutz von Liegenschaften und kritischen Anlagen zu gewährleisten. >>

Gesetzentwurf
KRITIS-DachG, November 2024, §13

Risiken und Folgen durch Brände

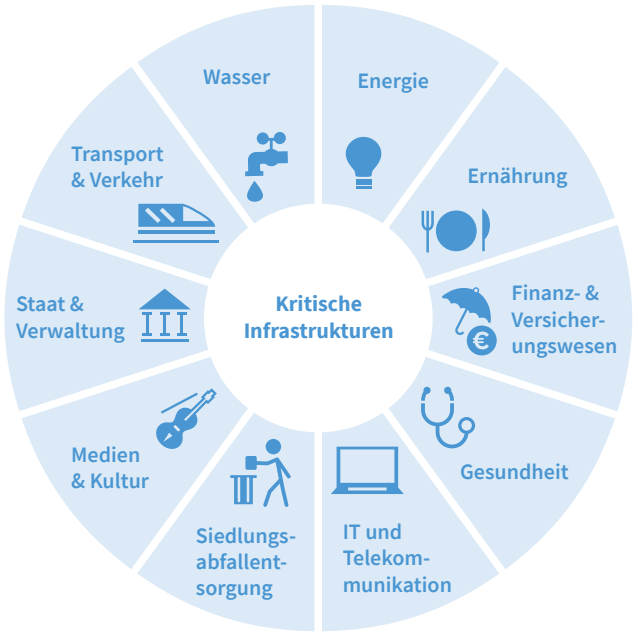
Brände können in kurzer Zeit ganze Liegenschaften zerstören. Viel schwerer als der eigentliche Sachschaden wiegen dabei langandauernder Betriebsstillstand, Kundenverlust durch Abwanderung und Imageschäden. Aus diesen Gründen stellen Brände auch für kritische Infrastrukturen ein erhebliches Risiko dar. Nach einem größeren Brandereignis ist die Bereitstellung der kritischen Dienstleistung für einen längeren Zeitraum nicht möglich. In sensiblen Bereichen können Brände durchaus globale Auswirkungen haben. Brände in einzelnen Produktionsstätten der Chiphersteller und Ausrüster Wuxi, Renesas und ASML führten zu Chipmangel und sofort zu weltweiten Störungen der Produktionsabläufe zahlreicher anderer Branchen. Brände entstehen nicht nur durch menschliches Versagen, Unfälle oder Sabotage, sondern zum Beispiel auch als Folge von Naturkatastrophen wie Erdbeben. Dadurch wird der ursprüngliche Schaden vervielfacht und die Wiederherstellung der kritischen Infrastruktur zusätzlich verzögert. →

Vorbeugender Brandschutz für KRITIS hat viele Aspekte

Die Bandbreite kritischer Infrastrukturen ist groß, sie reicht von Kraftwerken, Rechenzentren und Krankenhäusern über IT- und Stromnetze bis hin zu Banken und Versicherungen. Genauso vielfältig sind die Anforderungen an den Brandschutz; die Resilienz einer KRITIS-Einrichtung kann deshalb nur mit einem individuellen Brandschutzkonzept sichergestellt werden. Vorbeugender Brandschutz verringert Brandschäden und unterstützt die schnelle Wiederherstellung der kritischen Infrastruktur. Baulicher Brandschutz verhindert eine unkontrollierte Brandausbreitung, sorgt für sichere Flucht- und Rettungswege und für einen schnellen Löschangriff der Feuerwehr. Anlagentechnischer Brandschutz ist flexibel einsetzbar, auch bei Änderungen der Bedrohungslage.

Besonders wirksam im Hinblick auf die notwendige Resilienz sind automatische Löschanlagen. Sie bekämpfen einen Brand aktiv bereits vor dem Eintreffen der Feuerwehr und verringern sowohl das Schadensausmaß als auch die Zeitspanne bis zur Wiederinbetriebnahme deutlich. Genauso wichtig sind auch organisatorische Brandschutzmaßnahmen. Dazu gehören neben Schulungen und Übungen auch festgelegte Abläufe im Alarm- bzw. Krisenfall und der richtige Umgang mit Feuerlöschern und Wandhydranten.

Bei der Bewertung bestehender Brandschutzmaßnahmen ist zu beachten, dass baurechtliche Brandschutzanforderungen im Wesentlichen auf den Schutz von Personen und der Umwelt abzielen. Das Weiterbestehen von Unternehmen nach einem Brand spielt in den Bauordnungen keine Rolle. Versicherungen haben daran naturgemäß ein größeres Interesse, allerdings sind Brandschutzauflagen der Sachversicherer individuelle Vereinbarungen ohne Gesetzescharakter. Deshalb ist bei der Risikoanalyse und beim Aufstellen des Resilienzplans zu prüfen, ob die bestehenden Brandschutzmaßnahmen den Anforderungen des KRITIS-DachG in Bezug auf Resilienz und Business Continuity Management genügen oder ob zusätzliche Maßnahmen erforderlich sind.



Die enorme Bandbreite kritischer Infrastrukturen erfordert ein individuelles Brandschutzkonzept für jede Einrichtung.

gut zu wissen

Welche Unternehmen sind vom KRITIS-DachG betroffen?

Nach dem KRITIS-DachG gelten Betriebsstätten bzw. Anlagen aus zehn im Gesetz festgelegten Sektoren als KRITIS, unter anderem wenn sie mehr als 500.000 Einwohner versorgen oder die Betreiber in mindestens sechs EU-Staaten tätig sind. Unternehmen haben selbstständig zu prüfen, ob ihre Anlagen unter die Definitionen des KRITIS-DachG fallen. Ist das der Fall, sind diese beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) zu registrieren.

Bei Nicht-Registrierung kann die zuständige Aufsichtsbehörde die Registrierung vornehmen.

Mehr Informationen:
www.openkritis.de

Sebastian Brose
VdS Schadenverhütung GmbH

Feuerfest und zukunftssicher: Brandschutz in KRITIS und NIS2-Verfügbarkeit und Resilienz sind zentrale Elemente im KRITIS-Dachgesetz und in der NIS2-Richtlinie.

<< Sicherheit ist kein einmaliger Zustand, sondern ein fortlaufender Prozess, der kontinuierliche Überprüfungen und allfällige Anpassungen erfordert. >>

Welche Rolle spielt der Brandschutz dabei?

Relevant sind vor allem zwei Aspekte: Einerseits ist Brandschutz essenziell, um die Verfügbarkeit eines Objekts zu sichern, indem Schäden verhindert oder so klein wie möglich gehalten werden. Eingebettet in ein umfassendes Business Continuity Management sorgt wirksamer Brandschutz dafür, dass das Produkt oder die Leistung weiterhin angeboten werden kann. Andererseits spielt die Cyber-Resilienz auch bei Schutzsystemen selbst eine immer größere Rolle. Sicherheitssysteme werden vermehrt ans Internet angeschlossen. Daraus ergeben sich viele Vorteile, wie die Fernauslesung von Daten, verbesserte Analysen, automatische Selbsttests oder Fernunterstützung im Betrieb – bis hin zur zielgerichteten Instandhaltung. Gleichzeitig entsteht aber ein neues Gefährdungspotenzial, das die Verfügbarkeit und Integrität dieser Systeme nicht beeinträchtigen darf. Sicherheitstechnik braucht nun also auch selbst einen erweiterten Schutz.

Was müssen betroffene Unternehmen jetzt tun?

Obwohl diese Gesetze erst noch verabschiedet werden, ist es sinnvoll, jetzt schon zu handeln, um den anstehenden Anforderungen zuvorzukommen. Zudem ist der mögliche Schaden durch Betriebsunterbrechungen häufig deutlich größer als der eigentliche Sachschaden. Daher sollten Produkte gegen neue Bedrohungsszenarien gehärtet sein, etwa nach der Richtlinie VdS 3836 zur Cyber-Sicherheit für Systeme und Komponenten der Brandschutz- und Sicherheitstechnik. Dienstleistungen im Sicherheitsbereich sollten nach den Standards der DIN EN 50710 erbracht werden, um höchste Qualität und Zuverlässigkeit zu gewährleisten. Grundsätzlich ist es wichtig, Sicherheit nicht als einen einmaligen Zustand zu betrachten, sondern als einen fortlaufenden Prozess. Nur durch kontinuierliche Überprüfung, Anpassung und Verbesserung können sich Unternehmen dauerhaft vor den sich ständig verändernden Bedrohungen schützen.

Welche Unterstützung können Unternehmen dabei erhalten?

VdS bietet Unternehmen eine umfassende Angebotspalette, mit der sie ihre Sicherheitsmaßnahmen optimal planen und umsetzen können. Unsere Abteilung Risikomanagement sowie die Portfolios von Security-Expertise und Geo-Expertise bieten unabhängige Beurteilungen verschiedener Gefahrenquellen sowie konkrete Handlungsempfehlungen zur Vorbeugung, insbesondere in Bezug auf Feuer- und Einbruch-/Diebstahlrisiken sowie Naturgefahren. Wir erarbeiten mit unseren Kunden Konzepte und Lösungen für deren ganzheitlichen Schutz. Die qualifizierten Experten von VdS agieren dabei auch als neutrale Sparringspartner für die Kunden. Sicherheitsmanagementsystemzertifizierungen wie VdS 3406 halten Sicherheit als Prozess konsequent auf dem aktuellen Stand. Sind diese Prozesse einmal etabliert, werden etwaige Gesetzesänderungen und neue Anforderungen automatisch erfasst.

Zur Umsetzung von NIS2 bietet das VdS-Bildungszentrum Onlineseminare an, wie etwa „NIS-2 umsetzen mit der VdS 10100“ oder „Give NIS(2) a KISS = Keep It Stupid Simple“. Mit dem Schutz kritischer Infrastrukturen beschäftigen sich der VdS-Lehrgang „Aufbau und Organisation einer kritischen Infrastruktur“ sowie die VdS-Onlinefachtagung „Sicherungsketten müssen KRITIS-fähig werden“ – weitere Veranstaltungen zum Thema sind bereits in Planung.

Die Cyberangriffe auf deutsche Unternehmen und Behörden haben massiv zugenommen.

Cyber trifft Brandschutz: Die perfekte Kombination für maximale Sicherheit

Cyberangriffe in Deutschland haben massiv zugenommen. Schätzungen gehen von 4.000 Angriffen pro Tag aus. Im Visier von Cyberkriminellen und staatlichen Akteuren stehen vor allem kritische Infrastrukturen, kleine und mittlere Unternehmen sowie IT-Dienstleister. Mit der NIS2-Richtlinie soll daher europaweit die Cybersicherheit in Unternehmen verbessert werden. Gefährdet sind auch (Brand-) Sicherheitsanlagen, da diese immer häufiger mit dem Internet verbunden sind.

Wie gefährlich Angriffe auf IT-Dienstleister sein können, zeigt das Beispiel Crowdstrike. Nach einem fehlerhaften Update stand weltweit bei tausenden Kunden auf Flughäfen, in Krankenhäusern, Supermärkten und Fernsehsendern plötzlich alles still. Mehr als 1.500 Kunden waren 2021 von einem Ransomware-Angriff auf Kaseya-Software betroffen. Aber nicht nur IT-Dienstleister werden angegriffen, auch KRITIS-Einrichtungen sowie kleine und mittelständische Unternehmen werden zunehmend zum Ziel.

Mehr Cybersicherheit durch NIS2

Die EU hat die Gefahren erkannt und mit der NIS2-Richtlinie ein Instrument geschaffen, das die Cybersicherheit europaweit stärken soll. Neben den KRITIS-Betreibern sind zahlreiche weitere „wichtige“ und „besonders wichtige“ Unternehmen betroffen, in Deutschland insgesamt rund 31.000. NIS2 gilt für Unternehmen bestimmter Branchen mit mehr als 50 Mitarbeitern oder einem Jahresumsatz oder einer Bilanzsumme von mehr als 10 Millionen Euro. Unternehmen müssen selbst prüfen, ob sie von NIS2 betroffen sind und sich gegebenenfalls beim BSI registrieren lassen. Die Sicherheitsanforderungen von NIS2 umfassen Maßnahmen zum Cyber-Risikomanagement, zur Meldung und Reaktion auf IT-Vorfälle, zur Schulung und Sensibilisierung sowie verschärfte Sanktionsmechanismen. Sie gelten für die gesamte IT-Infrastruktur eines Unternehmens.

Neue Risiken für Brandsicherheitsanlagen

Auch sicherheitstechnische Anlagen werden immer anfälliger für Cyberangriffe.

2,2 Mrd. €

jährlich kostet deutsche Unternehmen die Umsetzung von NIS2.

Quelle: NIS2-Gesetzesentwurf Oktober 2024

Waren sie früher in eigenen Netzwerken von der Außenwelt abgeschottet, sind sie zunehmend mit Gebäudemanagement- oder ERP-Systemen vernetzt, um die Bedienung zu zentralisieren, eine präventive Wartung zu ermöglichen oder Personalengpässe zu kompensieren. Der Fernzugriff auf diese Anlagen über allgemein zugängliche IT-Netze vereinfacht die Wartung und die Anlagenbetreiber erhalten unkomplizierte Unterstützung durch den Errichter, der nicht mehr zwingend vor Ort sein muss. Die dafür notwendigen IT-Technologien eröffnen aber auch neue Sicherheitsrisiken. Nicht auszudenken, wenn die durch einen Cyberangriff lahmgelegte Löschanlage im Brandfall versagt. Menschenleben wären in Gefahr, ein Totalausfall kritischer Infrastrukturen wahrscheinlich.

Gesetzgeber und Regelsetzer haben deshalb zahlreiche Gesetze, Normen und Richtlinien auf den Weg gebracht. So gibt die DIN EN 50710 für den Brandschutz einen roten Faden für Aufgaben und Verantwortlichkeiten von der Vertragsgestaltung über die Risikoanalyse bis zum Abschluss eines Fernwartungseinsatzes vor. Für Systeme und Komponenten der Brandschutz- und Sicherheitstechnik beschreibt die VdS-Richtlinie 3.836 Anforderungen an die Cybersicherheit. Der bvfa fasst den aktuellen Stand der Technik und der Richtlinienarbeit für den Fernzugriff auf Brandmelde- und Löschanlagen in seinem Merkblatt „Fernzugriff auf automatische Löschanlagen“ zusammen.

Wachsam bleiben!

Cybersicherheit im Brandschutz erfordert immer mehr Aufmerksamkeit. Doch der Kampf zwischen Cyberkriminellen und Abwehrspezialisten wird ein ewiger Wettlauf bleiben. Es reicht nicht aus, nur die Technik auf dem neuesten Stand zu halten. Vielmehr müssen auch die Menschen immer wieder für Gefahren sensibilisiert und bei Veränderungen mitgenommen werden. Verantwortungsvoll eingesetzt, können Vernetzung und Fernzugriff sicherheitstechnische Anlagen effizienter und wartungsfreundlicher machen. ■

Die EU-Richtlinie NIS2 soll europaweit die Cybersicherheit erhöhen.

gut zu wissen

CYWARN – Automatisches Cyberlagebild

Bei der Bewältigung von Cyberangriffen und IT-Störungen ist die meist unübersichtliche Informationslage im Internet und in anderen Quellen eine große Herausforderung. Die Ziele des Projekts CYWARN sind die möglichst automatisierte Erfassung und Aufbereitung von Informationen aus öffentlichen und sozialen Datenquellen, die Erstellung eines akkuraten Cyberlagebildes sowie die Herausgabe von Handlungsempfehlungen und Warnmeldungen. Adressaten sind die „Computer Emergency Response Teams“ (CERT), die in Behörden und Unternehmen für die Erkennung und Bewältigung von Cyberangriffen verantwortlich sind. Dazu wurde ein Demonstrator (das sogenannte „Cyber Threat Observatory“) entwickelt, der mittelfristig auch direkt von den CERT eingesetzt werden soll.

Mehr Informationen:
www.sifo.de

Riffgat hatte als erster kommerzieller Windpark in der deutschen Nordsee eine Leistung von 108 MW. Heute sind dort 7.000 MW installiert.

Von der Windkraftanlage in die Steckdose: Offshore-Anlagen und Stromtrassen

Eine dezentrale Stromerzeugung macht unsere Energieversorgung robuster gegen Störungen und Angriffe. Die Übertragung großer Strommengen von den großen Offshore-Windparks im Norden in den stromhungrigen Süden wird jedoch zum Flaschenhals. Netzverknüpfungspunkte und Konverter müssen besonders geschützt werden, auch gegen Brände.

Die Resilienz unserer Stromversorgung wird durch die dezentrale Erzeugung deutlich erhöht. Statt in wenigen störanfälligen Großkraftwerken wird der Strom in vielen Windkraft- und Photovoltaikanlagen erzeugt. Der größte Teil des Stroms kommt jedoch aus den großen Offshore-Windparks in Nord- und Ostsee. Ihre Leistung soll von heute 7 GW auf 30 GW im Jahr 2030 und auf 75 GW im Jahr 2045 ausgebaut werden. Der Strom wird über leistungsfähige Trassen zu den Verbrauchern im Süden geleitet, zum Beispiel über die Windader West, die nach ihrer Fertigstellung über vier Trassen mit Gleichstromübertragung eine Gesamtleistung von 8 GW transportieren soll. Die Seekabel führen von den Windparks gebündelt als Erdkabel von der Küste zu ihren Netzverknüpfungspunkten in der Metropolregion Rhein-Ruhr.

Ausfall hätte fatale Folgen

Fällt die Verbindung aus, wären acht Millionen Menschen ohne Strom und zahlreiche Industrieanlagen müssten abgeschaltet werden. Hinzu kommen Dominoeffekte durch Frequenzschwankungen wie das Abschalten von Verbrauchern und Kraftwerken bis hin zur Abkopplung von Stromnetzen anderer europäischer Staaten. Der Anschlag auf die Nord-stream-Pipeline und jüngst die mutmaßliche Sabotage von zwei Telekommunikationsleitungen in der Ostsee zeigen, wie verwundbar solche Leitungen sind.

32 %

aller Brände entstehen durch Defekte in elektrischen Anlagen.

IFS-Brandursachenstatistik 2023

Das Herzstück schützen

Vorbeugender Brandschutz ist deshalb für die Anlagen der Windader West unerlässlich. Besonders kritisch sind die Netzverknüpfungspunkte und Konverterstationen an Land und auf See, denn hier wird der Strom aus Hunderten von Windkraftanlagen gebündelt. Der Vorteil: Konverter und Versorgungsplattformen können umfassend gegen Brandgefahren geschützt werden. Eine frühzeitige Branderkennung, kombiniert mit Systemen zur aktiven Brandvermeidung und verschiedenen Löschtechniken, bildet ein ganzheitliches Schutzkonzept und sichert so den Funktionserhalt der Einrichtung.

Schnell absenken und halten

Das Prinzip dieses Konzepts für Umspannwerke und Konverter zeigt das Beispiel Riffgat, dem ersten kommerziellen Windpark in der deutschen Nordsee. Herzstück des Brandschutzsystems ist ein Ansaugrauchmeldesystem, das kontinuierlich Proben aus der Umgebungsluft auf Rauchpartikel analysiert. Wird ein Brand detektiert, reduziert eine Stickstoff-Gaslöschanlage den Sauerstoffgehalt im Raum und erstickt das Feuer. Nach der Schnellabsenkung durch die Gaslöschanlage hält eine Brandvermeidungsanlage den Sauerstoffgehalt so lange auf niedrigem Niveau, bis ein erneuter Schwelbrand oder eine Rückzündung ausgeschlossen werden kann. Da die Anlage den dafür benötigten Stickstoff vor Ort aus der Umgebungsluft gewinnt, kann der niedrige Sauerstoffgehalt im Schutzbereich beliebig lange – im Bedarfsfall auch tagelang – aufrechterhalten werden.

Sprinkler und Schaumlöschanlagen als Sonderlösungen

Einige Bereiche, wie die Traforäume und die Netzersatzanlagen mit den Dieselmotoren, sind mit Sprinkleranlagen ausgestattet. In Außenbereichen wie auf dem Hubschrauberlandeplatz kommen Schaumlöschanlagen zum Einsatz. Der Anteil beider Systeme wurde bewusst gering gehalten. Anfallendes Löschwasser bzw. Löschschaum darf aus Umweltschutzgründen nicht in Gewässer oder ins Erdreich gelangen, sondern muss aufgefangen und entsorgt werden.

Investitionen schützen

Brennt eine Windenergieanlage mit einer Nabenhöhe von 200 Metern, ist ein Löschangriff der Feuerwehr ausgeschlossen und die Anlage wird zerstört. Der Verlust einer einzelnen Windenergieanlage hat zwar kaum Einfluss auf die Funktionsfähigkeit der gesamten kritischen Infrastruktur, bedeutet aber für Betreiber und Versicherungen Schäden in Millionenhöhe. Aus diesem Grund werden auch in Windenergieanlagen Rauchansaugsysteme und Gaslöschanlagen eingesetzt. Zum Schutz brandkritischer mechanischer Komponenten wie Getriebe, Lager und Bremsen kommt die gezielte Wasserfeinsprühlöschung zum Einsatz. ■

<< Wir werden unglaubliche Mengen erneuerbarer Energie brauchen. Und dazu werden wir die Offshore-Windkraftwerke massiv ausbauen müssen. >>

Dan Jörgensen

Dänemarks Energieminister auf der Nordsee-Konferenz in Esbjerg 2022

gut zu wissen

Universell einsetzbar

Gaslöschanlagen löschen Brände in elektrischen Anlagen und Rechenzentren zuverlässig und rückstandsfrei.

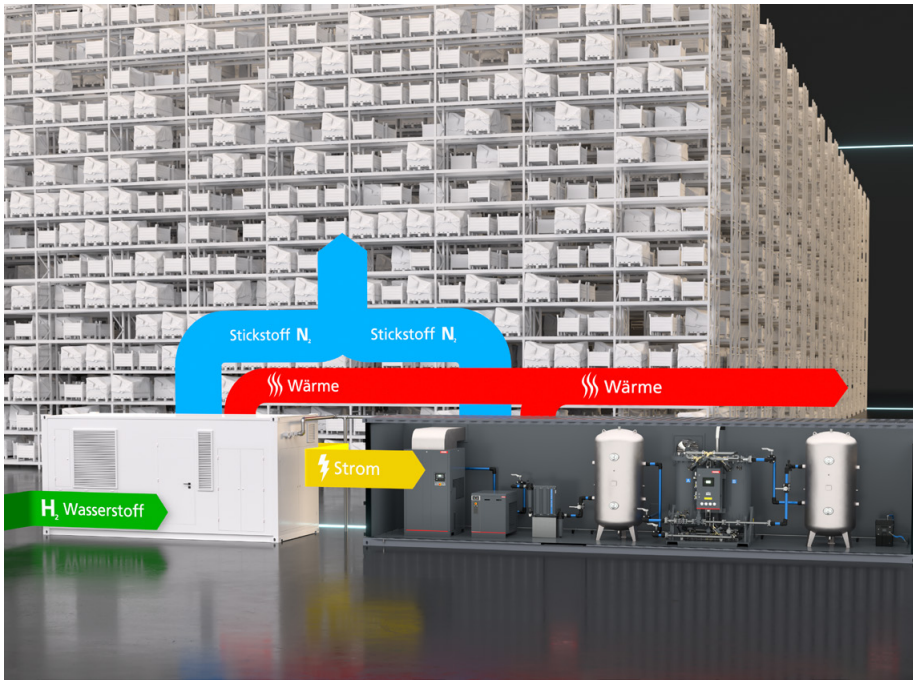
Die Brandschutzkonzepte von Riffgat und Windader West gelten auch für viele andere kritische Infrastrukturen. Nahezu alle KRITIS-Einrichtungen verfügen über elektrische Betriebsräume und eine umfangreiche IT-Infrastruktur. Für den Brandschutz können dort Gaslöschanlagen mit elektrisch nicht leitfähigen Löschgasen sowie Brandvermeidungssysteme mit Sauerstoffreduzierung eingesetzt werden. Kabel- und Rohrabschottungen verhindern die Brandausbreitung über die meist kilometerlangen Leitungsnetze. Sprinkleranlagen sind weit verbreitet und sorgen unter anderem in Krankenhäusern, Industrieanlagen und großen Hochregallagern für Sicherheit und eine schnelle Wiederinbetriebnahme im Schadensfall. In modernen Behälterkompaktlagern und in den für unsere Lebensmittelversorgung wichtigen Tiefkühllagern werden häufig Brandvermeidungssysteme eingesetzt. Bei Anlagen mit hohen Brandlasten wie Transformatoren, Recyclingbetrieben oder Lackieranlagen kommen Sprühwasserlöschanlagen oder Wassernebelanlagen zum Einsatz. Jüngster Spross in der Familie der Löschanlagen sind automatische Mini-Feuerlöscher, die Entstehungsbrände in Schaltschränken oder auf Leiterplatten elektronischer Geräte mit einem Löschgas direkt an der Entstehungsstelle bekämpfen.

Mehr Informationen:
www.bvfa.de

Brandschutz und Klimaschutz verbinden

Brandvermeidungssysteme mit Sauerstoffreduzierung sind ein wichtiger Bestandteil des Brandschutzkonzepts in kritischen Infrastrukturen. Durch das Einleiten von Stickstoff wird die Sauerstoffkonzentration im Schutzbereich so weit reduziert, dass ein Brand in der „brandsicheren“ Atmosphäre gar nicht erst entstehen kann. Ein innovatives Konzept verbindet nun Brandschutz und Klimaschutz. Der benötigte Stickstoff wird aus der sauberen, stickstoffreichen und sauerstoffarmen Abluft einer Brennstoffzelle gewonnen und muss nicht aufwendig aus der Umgebungsluft aufbereitet werden.

Darüber hinaus kann der in der Brennstoffzelle erzeugte Strom den konventionellen Strombezug deutlich reduzieren oder alternativ zur Notstromversorgung genutzt werden. Das gleichzeitig erzeugte Warmwasser kann in das Heizsystem integriert, in Produktionsprozesse eingebunden oder über ein optionales Ad-/Absorber-System in Kälte umgewandelt werden.



Klimafreundliche Stickstoffgewinnung aus einer Brennstoffzelle.

Besonderer Brandschutz für besonders Schutzbedürftige

Krankenhäuser, Pflegeeinrichtungen und Altenheime sind wichtige Bestandteile unseres Gesundheitssystems. Diese Einrichtungen zeichnen sich durch einen hohen Anteil an Patienten mit eingeschränkter Mobilität aus. Im Brandfall bindet eine Evakuierungszeit von durchschnittlich drei Minuten pro Patient das Pflegepersonal massiv. Hinzu kommt, dass teure medizinische Einrichtungen bei einem Brand durch korrosive und toxische Brandgase meist irreparabel geschädigt werden. Optimalen Schutz bieten Sprinkleranlagen, die einen Brand frühzeitig und aktiv bekämpfen.

Mehr Informationen:
www.sprinkler-protected.de

Automatisch auslösende Löschmittelzylinder löschen Entstehungsbrände direkt vor Ort.

Geräteintegrierter Brandschutz schützt kritische Infrastruktur

Nahezu alle kritischen Infrastrukturen verfügen über umfangreiche elektrische Schaltschränke und Maschinen – von elektronischen Komponenten bis hin zu Mittelspannungsverteilungen mit mehreren Tausend Volt. Gleichzeitig sind elektrische Anlagen eine der häufigsten Brandursachen. Brände in elektrischen und elektronischen Einrichtungen sollten daher möglichst frühzeitig erkannt und bekämpft werden, um Betriebsunterbrechungen zu verkürzen oder sogar zu verhindern.

Mit innovativem Brandschutz ist dies vollautomatisch möglich. Feuerlöschende Thermosicherungen basieren auf der bewährten Sprinklerglas-Technologie und werden zum Beispiel direkt in Netzteile integriert. Bei einem Brand im Gerät tritt das ungiftige und nichtleitende Löschgas aus der Glasampulle aus. Eine Wiederentzündung wird durch Unterbrechung der Stromzufuhr verhindert. Für größere Geräte, wie zum Beispiel Schaltschränke, eignen sich automatisch auslösende Mini-Feuerlöscher, die im Brandfall durch das Zerbersten eines Glaselements aktiviert werden und das Löschmittel freisetzen. Beiden Methoden ist gemeinsam, dass ein Entstehungsbrand direkt vor Ort gelöscht und eine Brandausbreitung verhindert wird.

Nürnberg, 25. Juni 2025

Brandschutzdirekt 2025 – Wissen kompakt auf den Punkt gebracht!

Auch in diesem Jahr lädt der bvfa – Bundesverband Technischer Brandschutz e.V. – zum bewährten Kompakt-Seminar Brandschutzdirekt Löschtechnik ein. Im Rahmen der FeuerTrutz 2025 findet das Fachseminar am 25. Juni 2025 in Nürnberg statt und bietet topaktuelle Einblicke in neueste Entwicklungen des anlagentechnischen Brandschutzes. Moderiert wird die Veranstaltung in bewährter Weise von Jörg Wilms-Vahrenhorst.

Aktuelle Entwicklungen in der Löschtechnik

Löschtechnik entwickelt sich stetig weiter – neue Materialien, veränderte Rahmenbedingungen und innovative Technologien stellen die Branche vor immer neue Herausforderungen. Im Seminar beleuchten führende Fachleute aktuelle Entwicklungen:

- Wie beeinflusst Brandschutz die CO_2-Bilanz von Gebäuden?
- Welche Neuerungen gibt es bei PFAS-freien Schaumlöschmitteln?
- Welche neuen Regelungen bringt die DIN EN 12845 Teil 2 mit sich?

Erleben Sie ein kompaktes Seminar voller praxisnaher Einblicke und aktueller Erkenntnisse.

Praxisnahes Wissen für Fachleute

Das bvfa Kompakt-Seminar richtet sich an Planer, Betreiber, Industrieunternehmen, Versicherer und Errichterfirmen. Die Vorträge bieten eine ausgewogene Mischung aus Theorie und Praxis. Besonders spannend sind die praxisnahen Vorträge zu:

- Druckentlastung bei Löschanlagen und drehzahlgesteuerte Pumpen
- Einsatzmöglichkeiten und Anwendungsgrenzen von Aerosollöschanlagen
- Der Einfluss von Sprinklerschutz auf die Versicherungswirtschaft

Das Seminar ist die perfekte Plattform, um sich mit anderen Fachleuten auszutauschen und wertvolle Kontakte zu knüpfen.

Besuchen Sie uns auch an unserem Stand!

Neben unserem Kompakt-Seminar sind wir auch mit einem Stand auf der FeuerTrutz 2025 vertreten. Nutzen Sie die Gelegenheit, um sich über unsere neuesten Merkblätter, Positionspapiere und Fachpublikationen zu informieren. Natürlich steht Ihnen unser Team auch für persönliche Gespräche zur Verfügung. Tauschen Sie sich mit unseren Expertinnen und Experten aus, stellen Sie Fragen oder diskutieren Sie mit uns über die neuesten Entwicklungen im Brandschutz. Besuchen Sie uns an Stand 4-402!

Jetzt anmelden!

www.feuertrutz.de/brandschutzdirekt

Wir schützen die Zukunft

Der bvfa und KRITIS

Die Brandschutzkonzepte für kritische Infrastrukturen und Unternehmen mit IT-Infrastrukturen sind so individuell wie die KRITIS-Einrichtungen und Betriebe selbst. Die Mitgliedsunternehmen des bvfa unterstützen Kunden und Interessenten bei der Realisierung eines individuellen Brandschutzes unter Berücksichtigung der Anforderungen des KRITIS-DachG und der NIS2-Richtlinie – von der Ist-Analyse auf der Grundlage von bewährten Branchenkonzepten über wirtschaftliche Neuanlagenkonzepte bis hin zu Sanierung, Austausch und Funktions-Upgrades. Die Fachgruppen des bvfa stellen darüber hinaus eine Vielzahl von Merkblättern und Positionspapieren kostenlos zur Verfügung.

Auch wenn wir an einigen Stellen aus Lesbarkeitsgründen nur eine Form eines Wortes verwenden, meinen wir damit ausdrücklich jeden Menschen – gleich welchen Geschlechts.

BrandschutzSpezial Feuerlöschanlagen

Feuerlöschanlagen sind ein wichtiger Baustein zur Erhöhung der Resilienz in kritischen Infrastrukturen. Das kostenlose BrandschutzSpezial Feuerlöschanlagen beschreibt auf 68 Seiten detailliert den Nutzen, die Technik und die Anwendungsgebiete der verschiedenen Löschanlagentypen und unterschiedlichen Löschgase, auch für zahlreiche KRITIS-Sektoren.

Merkblatt Remote Service

Das Merkblatt fasst den aktuellen Stand der Technik und der Richtlinienarbeit für Fernzugriffe zusammen. Es unterstützt Betreiber, Planer und Errichter solcher Anlagen auch bei der Erfüllung der europäischen NIS2-Richtlinie.

Positionspapier
Einsatz von Kohlendioxid in stationären Löschanlagen

Positionspapier
Auslegung, Dimensionierung und Prüfung von Hochdruckrohrleitungen für Gaslöschanlagen

Positionspapier
Einsatz von Aerosol-Löschanlagen im Brandschutz

Weitere Publikationen zum kostenlosen Download: www.bvfa.de

IMPRESSUM

Herausgeber: bvfa – Bundesverband Technischer Brandschutz e.V. (www.bvfa.de), Geschäftsstelle Würzburg
Redaktion: Angela Krause, Koellikerstr. 13, D-97070 Würzburg, Tel. +49 (0) 931 35292-25, Fax +49 (0) 931 35292-29, info@bvfa.de, www.bvfa.de
Gestaltung: heller & greller GmbH, Axel Treffkorn, info@hellerundgreller.de. Konzept und Text: rhs – technik kommunizieren Dr. Henning Salié

Bilder: S. 1 imagebrokermicrostock/Depositphotos.com; S.2 bvfa, ifeelstock/Depositphotos.com; S. 3 PantherMediaSeller/Depositphotos.com; S. 5 VdS Schadenverhütung GmbH, hansenn/Depositphotos.com; S. 6 solarseven+ TTstudio/Depositphotos.com; S. 7 Dobby_01/Depositphotos.com; S. 8 Offshore-Windpark Riffgat GmbH & Co. KG; S. 9 Siemens AG; S. 10 Minimax GmbH, JOB GmbH; S. 11 bvfa; S. 12 bvfa.