NOERR

Noerr Checkliste Cyberangriffe

Für den Fade eines Cyberangriff auf Ihre IT-Systeme/Ihre Daten ist eine rasche Reaktion essenziell. Dabei sind innerhalb sehr kurzer Zeit eine Fülle behördlicher Meldepflichten zu prüfen und umzusetzen, ebenso wie zahlreiche Schutzmaßnahmen, auch zur Daten- und Beweissicherung und späteren Verfolgung von Schadensersatzansprüchen.

Die folgende Checkliste gibt einen ersten Überblick über typische rechtlich notwendige und sinnvolle Maßnahmen im Fall eines Cyber-Angriffs. Sie ersetzt dabei keinen individuellen Notfallplan, der an die spezifischen Besonderheiten des jeweils betroffenen Unternehmens anzupassen ist und klare Zuständigkeiten und Verantwortlichkeiten regelt. Zudem sollte jedes Unternehmen präventiv ein Team bilden, das im Fall eines Cyber-Angriffs in der Lage ist, rasch zu reagieren und notwendige Maßnahmen umzusetzen („**Cyber Response Team**“). Der Notfallplan und die damit korrespondierende weitere Dokumentation sind schriftlich festzuhalten.

	Maßnahme	erledigt
Cyber Response Team	Informieren Sie, sofern vorhanden, Ihr Cyber Response Team, üblicherweise bestehend aus • Leiter der IT • Rechtsabteilung • Compliance • Datenschutzbeauftragter • Kommunikation/PR-Abteilung • _____	☐
Was ist passiert?	Sammeln Sie Informationen und Daten dazu, was genau vorgefallen ist. Handelt es sich insbesondere um einen • Hacking/Ausspähen von Daten (Advanced Persistent Threat) • Betrug (CEO-Fraud, Täuschungsversuch) • Informationsabfluss (Know-how/Daten) • Sabotage (physische Beschädigung) • Sabotage (Beeinträchtigung der Datenintegrität) • Schädlicher Code • Ransomware • Nicht autorisierte Verwendung von Ressourcen • (Distributed) Denial of Service („DDoS”) • _____ • Unbekannt	☐

	Maßnahme	erledigt
	Klären Sie, ob es sich um einen (vorsätzlichen) Angriff handelt oder um einen (zufälligen) Netzwerk-, Hardware- oder Softwarefehler.	☐
	Ist der IT-Sicherheitsvorfall abgeschlossen? • Falls ja, klären Sie, wie lange der IT-Sicherheitsvorfall angedauert hat. • Falls nein, klären Sie, wie lange der Vorfall bereits andauert.	☐
	Klären Sie, wie sich der Vorfall ereignet hat. Tragen Sie dabei alle notwendigen Informationen zusammen, auch wenn diese anfangs dürftig sind. Vergewissern Sie sich, dass alle Beteiligten einheitliche Informationen haben, sodass weder verschiedene Versionen des Vorfalls noch Gerüchte entstehen.	☐
	Klären Sie insbesondere folgende Punkte • Welche Systeme sind betroffen? • Welche Daten sind betroffen (z.B. Daten von Kunden oder Geschäftspartnern, personenbezogene Daten, Bankinformationen oder Kreditkartendaten, Gesundheitsdaten, Produktinformationen, Geschäftsgeheimnisse, usw.).	☐
	Sind negative Auswirkungen auf den Geschäftsbetrieb zu erwarten? Wenn ja, welche?	☐
Wer ist zu informieren?	Informieren Sie alle Mitglieder des Cyber Response Teams über Ihre Erkenntnisse.	☐
	Informieren Sie technische Berater, etwa ein Computer Emergency Response Team (CERT). • IT-Dienstleister _____ • Forensische Berater [ ] • _____ • Prüfen Sie die Information von Versicherern (insbesondere bei vorhandener Cyber-Versicherung)	☐
	Informieren Sie das Noerr Cyber Risk Team. **Ansprechpartner:** Ansprechpartner: Dr. Daniel Rücker T +49 89 28628457 M +49 171 9918893 Dr. Volker Rosengarten T +49 40 300397113 M +49 1515 1813393 Dr. Dan Schilbach T +49 211 49986175 M +49 151 26346930 Julian Monschke T +49 69 971477455 M +49 151 11712954	☐

	Maßnahme	erledigt
	Informieren Sie ggf. betroffene Mitarbeiter.	☐
Was ist zu tun?	Leiten Sie Notfallmaßnahmen unter Berücksichtigung interner Notfallrichtlinien und -pläne ein; insbesondere zur schnellstmöglichen Beendigung des Angriffs, zur Beweissicherung sowie zur Wiederherstellung von IT-Systemen/Daten.	☐
	Benachrichtigen Sie ggf. andere relevante Dritte z.B. den Hersteller oder Entwickler der betroffenen Systeme; diese können Ihnen unter Umständen auch bei technischen Notfallmaßnahmen helfen.	☐

INFOBOX KRITISCHE INFRASTRUKTUR („KRITIS“)

Wer ist betroffen?

KRITIS-Betreiber sind Unternehmen, die **kritische Leistungen in eigenen Anlagen** erbringen und dabei **500.000 Personen** oder mehr versorgen. Ob dies im konkreten Einzelfall zutrifft, ist anhand **detaillierter Schwellenwerte** zu ermitteln. Diese Schwellenwerte sind für jeden Sektor in der so genannten **BSI-Kritisverordnung** (BSI-KritisV) festgelegt. Der folgenden Übersicht können Sie entnehmen, ob Ihr Sektor grundsätzlich von den Vorschriften des Gesetzes über das Bundesamt in der Informationstechnik („**BSIG**“) betroffen sein kann.

Kategorie	Sektoren und kritische Dienstleistungen
Grundversorgung	**Energie** **Stromversorgung**: Erzeugung, Handel und Verteilung von Strom **Gasversorgung**: Förderung, Transport und Verteilung von Gas **Kraftstoff- und Heizölversorgung**: Förderung, Herstellung, Transport und Verteilung von Kraftstoff- und Heizöl **Fernwärmeversorgung**: Erzeugung und Verteilung von Fernwärme
	Wasser **Abwasserbeseitigung:** Siedlungsentwässerung, Abwasserbehandlung und Gewässereinleitung und die Steuerung und Überwachung von Abwasser **Trinkwasserversorgung:** Gewinnung, Aufbereitung, Verteilung und Steuerung und Überwachung von Trinkwasser
	Ernährung **Lebensmittelversorgung**: Herstellung, Behandlung und Handel von Lebensmitteln
	Gesundheit **Stationäre medizinische Versorgung**: Aufnahme, Diagnose, Therapie, Unterbringung/Pflege und Entlassung in Krankenhäusern **Versorgung mit lebenserhaltenden Medizinprodukten, die Verbrauchsgüter sind**: Herstellung und Abgabe von Medizinprodukten **Versorgung mit Arzneien und Blut/Plasma**: Herstellung, Vertrieb und Abgabe von verschreibungspflichtigen Arzneimitteln und Blut- und Plasmakonzentraten zur Anwendung im oder am menschlichen Körper **Laboratoriumsdiagnostik**: Transport und Analytik in Laboren
Versorgung	**Transport und Verkehr** **Luftverkehr**: Passagier- und Frachtabfertigung, Infrastruktur, Flugsicherung **Schienenverkehr**: Bahnhöfe, Netze, Verkehrssteuerung und Leitzentralen

	Binnen- und Seeschifffahrt: Bundeswasserstraßen, Verkehrssteuerung und Leitzentralen **Straßenverkehr**: Verkehrssteuerung und Leitzentralen
	Öffentlicher Personennahverkehr (ÖPNV): Netze, Verkehrssteuerung und Leitzentralen **Logistik**: Logistikzentren und Logistiksteuerung
	Entsorgung (derzeit noch nicht in die BSI-KritisV aufgenommen) *Entsorgung von Siedlungsabfällen: Sammlung, Beseitigung und Verwertung von Siedlungsabfällen*
Dienstleistungen	**IT und TK** **Sprach- und Datenübertragung:** Zugang, Übertragung, Vermittlung und Steuerung von Sprach- und Datennetzen **Datenspeicherung und -verarbeitung:** Housing, IT-Hosting und Vertrauensdienste
	Finanzen und Versicherungen **Bargeldversorgung:** Abhebungen, Einbringen in Zahlungsverkehr, Belastung Kundenkonto und Bargeldlogistik **Kartengestützter Zahlungsverkehr:** Autorisierung, Einbringen in Zahlungsverkehr, Belastung Kundenkonto und Gutschriften **Konventioneller Zahlungsverkehr:** Annahme, Einbringen in Zahlungsverkehr, Belastung Kundenkonto und Gutschriften von Überweisungen und Lastschriften **Wertpapier- und Derivatgeschäfte:** Verrechnung, Abwicklung und Verbuchung **Versicherungsdienstleistungen und Leistungen der Sozialversicherung sowie der Grundsicherung für Arbeitsuchende**: Inanspruchnahme

Was ist bei einem Cyberangriff zu tun?

KRITIS-Betreiber sind im Fall einer Störung oder eines Sicherheitsvorfalls insbesondere zu folgenden Maßnahmen verpflichtet:

Maßnahme	erledigt
Unverzügliche Meldung an das Bundesamt für Sicherheit in der Informationstechnik (BSI), wenn **Störungen** der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse zu einem Ausfall oder einer **erheblichen Beeinträchtigung der Funktionsfähigkeit** der von diesen betriebenen kritischen Infrastruktur **geführt haben** oder wenn **erhebliche Störungen** zu einer solchen **Beeinträchtigung führen können**. (§ 8b Abs. 4 S. 1 BSIG).	☐
Die Meldung muss **Angaben zur Störung** und ihren möglichen **internationalen Auswirkungen**, technischen Rahmenbedingungen, insbesondere der möglichen Ursache und der betroffenen Informationstechnik, der Art der betroffenen Einrichtung und der erbrachten kritischen Dienstleistung, sowie der Auswirkung der Störung auf diese Dienstleistung enthalten. Sollten noch nicht alle Informationen bekannt sein, sind diese **unverzüglich nachzureichen**.	☐

Erforderliche vorbereitende Maßnahmen

Dem Cyberangriff vorgelagert stellt das Gesetz weitergehende Anforderungen an den KRITIS-Betreiber. Dazu gehören insbesondere geeignete und verhältnismäßige **technische und organisatorische Maßnahmen**, um Risiken für die Sicherheit der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind, , (§ 8a Abs. 1 BSIG). Diese sollen den Stand der Technik einhalten, das dem bestehenden Risiko angemessen ist (§ 8a Abs. 1 S. 2 und 3 BSIG). Dazu gehören:

Maßnahme	erledigt
Management-System für Informationssicherheit (ISMS), um KRITIS-Risiken zu mindern.	☐
Business Continuity Management (BCM) und IT-Notfallmanagement/Desaster Recovery Planzur Reduktion der Ausfallrisiken und IT-Notfälle	☐
Technologische Maßnahmen nach dem **Stand der Technik**, die die Infrastruktur schützen.	☐
Angriffserkennung zur Ermöglichung angemessener Reaktionen. Das BSIG fordert seit 2023 explizit Systeme und Prozesse zur Angriffserkennung (z.B. SIEM oder SOC).	☐
Zweijährige Nachweisprüfung, die der KRITIS-Betreiber selbst vorbereiten und organisieren muss (§ 8a Abs. 3 BSIG)	☐

INFOBOX DIGITALE DIENSTE
Wer ist betroffen?

Sektorunabhängig sind alle Anbieter digitaler Dienste von den Vorschriften des BSIG betroffen. Erfasst werden Dienstleistungen der Informationsgesellschaft gemäß Art. 1 Abs. 1 lit. b) der Richtlinie (EU) 2015/1535. Das umfasst damit jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf des Empfängers erbrachte Dienstleistung. Zusätzlich muss der Dienst wie aus der folgenden Tabelle ersichtlich qualifiziert sein.

Sektor	Ausnahmen
Online-Marktplätze Dienste, die es Verbrauchern oder Unternehmern ermöglichen, Kaufverträge oder Dienstleistungsverträge mit Unternehmern entweder auf der Website dieser Dienste oder auf der Website eines Unternehmers, die von diesen Diensten bereitgestellte Rechendienste verwendet, abzuschließen.	**Ausnahmen**: (gemäß § 8d Abs. 4 S. 1 BSI-G i.V.m. KMU-Definitionsempfehlung) **Kleinstunternehmen** (< 10 Beschäftigte und Jahresumsatz <= EUR 2 Mio.) und **kleine Unternehmen** (< 50 Beschäftigte und Jahresumsatz <= EUR 10 Mio.)
Online-Suchmaschine Dienste, die es Nutzern ermöglichen, Suchen grundsätzlich auf allen Websites oder auf Websites in einer bestimmten Sprache anhand einer Abfrage zu einem beliebigen Thema in Form eines Stichworts, einer Wortgruppe oder einer anderen Eingabe vorzunehmen, die daraufhin Links anzeigen, über die der Abfrage entsprechende Inhalte abgerufen werden können.	
Cloud-Computing-Dienste Dienste, die den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglichen. „Rechenressourcen“ umfassen verschiedene Arten der Ressourcen, wie Netze, Server oder sonstige Infrastruktur, Speicher und Anwendungen	

Was ist bei einem Cyberangriff zu tun?

Anbieter digitaler Dienste sind im Fall einer Störung oder eines Sicherheitsvorfalls insbesondere zu folgenden Maßnahmen verpflichtet:

Maßnahme	erledigt
Anbieter digitaler Dienste müssen dem BSI **jeden Sicherheitsvorfall mit erheblichen Auswirkungen** auf ihre Dienstleistung **unverzüglich** melden. Die **Erheblichkeit richtet sich insbesondere nach** der Anzahl der betroffenen Nutzer, der Dauer des Vorfalls, dem betroffenen geographischen Gebiet, dem Ausmaß der Unterbrechung der Bereitstellung des Dienstes und der Beeinträchtigung von wirtschaftlichen und gesellschaftlichen Tätigkeiten. Die Europäische Kommission (Artikel 4 der Durchführungsverordnung der EU-Kommission 2018/151 vom 30. Januar 2018) hat für die Bewertung von Sicherheitsvorfällen auszugsweise folgende Kriterien festgelegt: • Der von einem Anbieter digitaler Dienste bereitgestellte Dienst war mehr als 5.000.000 Nutzer- stunden lang nicht verfügbar, wobei sich der Begriff Nutzerstunde auf die Zahl der Nutzer in der Union bezieht, die während einer Dauer von sechzig Minuten betroffen waren. • Der Sicherheitsvorfall hat zu einem Verlust der Integrität, Authentizität oder Vertraulichkeit gespeicherter oder übermittelter oder verarbeiteter Daten oder der entsprechenden Dienste, die über ein Netz- und Informationssystem des Anbieters digitaler Dienste angeboten werden beziehungsweise zugänglich sind, geführt, von dem mehr als 100.000 Nutzer in der Union betroffen sind. • Durch den Sicherheitsvorfall ist eine öffentliche Gefahr oder ein Risiko für die öffentliche Sicherheit entstanden oder es sind Menschen ums Leben gekommen. • Der Sicherheitsvorfall hat für mindestens einen Nutzer in der Union zu einem Sachschaden in Höhe von mehr als 1.000.000 EUR geführt.	☐
Der **Inhalt** der Meldung entspricht dem der Meldung kritischer Infrastrukturen (s.o.)	☐
Die **Meldepflicht entfällt, wenn** der Anbieter keinen Zugang zu den Informationen hat, um die Erheblichkeit des Vorfalls zu prüfen.	☐
Hersteller und Entwickler von Programmen können bei einem Angriff auf das von ihnen angebotene Produkt ebenfalls einem Cyber-Angriff ausgesetzt sein. Diese können unter Umständen **fachgerechter auf den Angriff reagieren** und Ihnen weitere Informationen über den Vorfall mitteilen. So können möglicherweise weitere **Schäden am System und beim Datenabfluss verhindert** werden.	☐

INFOBOX SPEZIALGESETZLICHE INFORMATIONSPFLICHTEN

Wer ist betroffen?

Unternehmen können auch spezialgesetzlichen Informationspflichten unterliegen. Die betroffenen Unternehmen werden im folgenden dargestellt:

Sektor	erledigt
Unternehmen im besonderen öffentlichen Interesse Unternehmen im besonderen öffentlichen Interesse sind solche im Sinne des § 2 Abs. 14 BISG und werden in drei Kategorien unterteilt. **UBI1** sind Hersteller und Entwickler von Gütern im Sinne von § 60 AWV, also Unternehmen, die im Bereich Waffen, Munition und Rüstungsmaterial oder im Bereich von Produkten mit IT-Sicherheitsfunktionen zur Verarbeitung staatlicher Verschlusssachen oder für die IT-Sicherheitsfunktion wesentlicher Komponenten solcher Produkte tätigt sind. **UBI2** sind nach ihrer inländischen Wertschöpfung größten Unternehmen Deutschlands sowie wesentliche Zulieferer für diese Unternehmen. Hier wäre eine konkretisierende Rechtsverordnung notwendig, um dies genauer zu bestimmen. Diese wurde jedoch nicht erlassen. Aller Voraussicht nach wird sie das auch nicht, da das Umsetzungsgesetz zur NIS2-Verordnung die hinfällig werden lässt. **UBI3** sind Betreiber eines Betriebsbereichs der oberen Klasse im Sinne der Störfall-Verordnung in der jeweils geltenden Fassung oder Betreiber, die nach § 1 Abs. 2 der Störfall Verordnung diesen gleichgestellt sind.	☐
Betreiber oder Anbieter öffentlicher Telekommunikationsnetze und Erbringer öffentlich zugänglicher Telekommunikationsdienste Ein Telekommunikationsnetz ist ein Telekommunikationsnetz, das ganz oder überwiegend der Erbringung öffentlich zugänglicher Telekommunikationsdienste dient, die die Übertragung von Informationen zwischen Netzabschlusspunkten ermöglichen. Telekommunikationsdienste sind gewöhnlich gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen, etwa Internetzugangsdienste oder interpersonelle Telekommunikationsdienste.	☐
Betreiber von Energieversorgungsnetzen Ein Energieversorgungsnetz dient dem Transport und der Verteilung des Stroms von Kraftwerken zu Verbrauchern. Die rein physikalisch technische Anbindung von Anschlussnehmer an die Energieversorgung wird also durch Betreiber von Energieversorgungsnetzen gewährleistet. Ihre zentralen Aufgaben sind der diskriminierungsfreie Betrieb, die Wartung, bedarfsgerechte Optimierung, Verstärkung und der wirtschaftlich zumutbare Ausbau von sicheren, zuverlässigen und leistungsfähigen Energieversorgungsnetzen.	☐

Sektor	erledigt
Atomrechtliche Genehmigungsinhaber (wie etwa Kernkraftwerksbetreiber) Inhaber von Genehmigungen nach §§ 6, 7 oder 9 AtomG, also insbesondere Anlagen, die der Aufbewahrung von Kernbrennstoffe außerhalb der staatlichen Verwahrung dienen oder Anlagen, die zur Erzeugung, Verarbeitung, Spaltung oder zur Aufarbeitung bestrahlter Kernbrennstoffe errichtet oder betrieben werden oder deren Betrieb wesentlich geändert werden soll.	☐
Kreditinstitute Kreditinstitute sind Dienstleister, deren Kerngeschäft darin besteht, gewerbsmäßig Bankgeschäfte und Finanzdienstleistungen in einem Umfang zu betreiben, der kaufmännisch und als Geschäftsbetrieb organisiert sein muss. .	☐
Zahlungsdienstleister Zahlungsdienste dienen der Abwicklung des Zahlungsverkehrs, indem sie als zwischen Kunden, Unternehmen und Banken zwischengeschalteter Dienstleister die reibungslose Abwicklung von Transaktionen gewährleisten. Ihre zentralen Aufgaben sind die technische Durchführung von Zahlungen, Gewährleistung der Sicherheit, Einhaltung von datenschutzrechtlichen Anforderungen und das Zurverfügungstellen von unterschiedlichen Zahlungsmethoden.	☐
Betreiber, Luftfahrtunternehmen und Stellen Betreiber, Luftfahrtunternehmen und Stellen im Sinne von DVO (EU) 2019/1583: Betreiber sind private oder öffentliche Unternehmen, die als Betreiber von Flughäfen auftreten und die komplette Flughafeninfrastruktur den Luftfahrtunternehmen und der Flugsicherung zur Verfügung stellen. Luftfahrtunternehmen sind meist Betreiber von Luftfahrzeugen; darüber hinaus aber auch Flugschulen, Rettungsdienste, Luftwerbedienstleister oder Händler von Flugtickets. Mit den Stellen sind diejenigen gemeint, die im nationalen Programm für die Sicherheit der Zivilluftfahrt genannt sind.	☐

Was ist bei einem Cyberangriff zu tun?

Sektor	erledigt
Unternehmen im besonderen öffentlichen Interesse **UBI1** müssen gemäß § 8f Abs. 7 BSIG **unverzüglich** dem **Bundesamt für Sicherheit in der Informationstechnik** (BSI) melden: **Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse**, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Erbringung der Wertschöpfung geführt haben oder zu diesen Folgen führen können. Die Meldung muss Angaben zur Störung, zu den technischen Rahmenbedingungen, insbesondere zu der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik und der Art der betroffenen Einrichtung oder Anlage enthalten. Für **UBI3** gilt gemäß § 8f Abs. 8 BSIG seit dem 01.11.2021 dasselbe.	☐

Sektor	erledigt
Betreiber und Anbieter öffentlicher Telekommunikationsnetze und Erbringer öffentlich zugänglicher Telekommunikationsdienste **Betreiber und Anbieter öffentlicher Telekommunikationsnetze und Erbringer öffentlich zugänglicher Telekommunikationsdienste** müssen gemäß § 168 TKG bei Sicherheitsvorfällen mit beträchtlichen Auswirkungen auf den Betrieb der Netze oder die Erbringung der Dienste unverzüglich darüber die **Bundesnetzagentur** und das BSI informieren. Weiterhin müssen Erbringer öffentlich zugänglicher Telekommunikationsdienste eine **Verletzung des Schutzes personenbezogener Daten** unverzüglich der **Bundesnetzagentur** und dem **Bundesdatenschutzbeauftragten** anzeigen, § 169 TKG. Bei einer schwerwiegenden Beeinträchtigung ihrer Rechte oder schutzwürdigen Interessen muss zusätzlich die **betroffene Person** entsprechend § 169 Abs. 1 Satz 2 TKG benachrichtigt werden. Außerdem muss in allen Fällen ein Verzeichnis der Verletzungen des Schutzes personenbezogener Daten geführt werden, § 169 Abs. 3 TKG. Gehen die Störungen von einem Nutzer aus, ist dieser darüber zu benachrichtigen.	☐
Betreiber von Energieversorgungsnetzen **Betreiber von Energieversorgungsnetzen** müssen gemäß § 11 Abs. 1c EnWG **unverzüglich** dem **Bundesamt für Sicherheit in der Informationstechnik** melden: **Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse**, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung des Energieversorgungsnetzes geführt haben oder führen können. Die Meldung muss Angaben zur Störung, zu den technischen Rahmenbedingungen, insbesondere zu der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik und der Art der betroffenen Einrichtung oder Anlage enthalten.	☐
Genehmigungsinhaber (wie etwa Kernkraftwerksbetreiber) **Kernkraftwerksbetreiber** haben gemäß § 44b AtomG **Beeinträchtigungen ihrer informationstechnischen Systeme**, Komponenten oder Prozesse, die zu einer Gefährdung oder Störung der nuklearen Sicherheit der betroffenen kerntechnischen Anlage oder Tätigkeit führen können oder bereits geführt haben, unverzüglich an das **Bundesamt für Sicherheit in der Informationstechnik** zu melden. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, und der betroffenen Informationstechnik enthalten. Weiterhin müssen Kernkraftwerksbetreiber gemäß § 6 Abs. 1 AtSMV **Unfälle, Störfälle oder sonstige für die kerntechnische Sicherheit bedeutsame Ereignisse** den atomrechtlichen Aufsichtsbehörden melden.	☐
Kreditinstitute **Kreditinstitute** müssen gemäß § 24 Abs. 1 Nr. 19 KWG der **Bundesanstalt für Finanzdienstleistungsaufsicht** und der **Deutschen Bundesbank unverzüglich** die **Absicht einer wesentlichen Auslagerung und deren Vollzug** sowie **wesentliche Änderungen und schwerwiegende Vorfälle** im Rahmen von bestehenden wesentlichen Auslagerungen, die einen wesentlichen Einfluss auf die Geschäftstätigkeit des Instituts haben können, anzeigen.	☐

Sektor	erledigt
Zahlungsdienstleister **Zahlungsdienstleister** haben gemäß § 54 Abs. 1 ZAG der **Bundesanstalt für Finanzdienstleistungsaufsicht unverzüglich** über einen **schwerwiegenden Betriebs- oder Sicherheitsvorfall** zu melden, sodass diese wiederum der Europäischen Bankenaufsichtsbehörde und der Europäischen Zentralbank sowie der in ihrer sachlichen Zuständigkeiten betroffene inländische Behörden unverzüglich nach Eingang der Meldung unterrichtet.	☐
Gematik GmbH (zuvor Gesellschaft für Telematikanwendungen der Gesundheitskarte) und Anbieter von Komponenten und Diensten sowie Anbieter von Anwendungen **Anbieter von Komponenten und Diensten sowie Anbieter von Anwendungen** haben gemäß § 329 Abs. 2 SGB V **unverzüglich Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit** der Komponenten und Dienste an die Gematik GmbH zu melden, sofern die Störungen **erheblich** sind, also zum Ausfall oder zur Beeinträchtigung der Sicherheit oder Funktionsfähigkeit der Telematikinfrastruktur oder wesentlicher Teile führen können und bereits geführt haben. Soweit von Komponenten und Diensten eine **Gefahr für die Funktionsfähigkeit oder Sicherheit der Telematikinfrastruktur** ausgeht, ist die **Gematik GmbH** gemäß § 329 Abs. 1 SGB V verpflichtet, **unverzüglich** das **Bundesamt für Sicherheit in der Informationstechnik** über die Gefahr und die zur Abwendung der Gefahr getroffenen Maßnahmen zu informieren. Ferner muss die **Gematik GmbH** gemäß § 329 Abs. 4, 5 SGB V die ihr **von den Anbietern gemeldeten Störungen** sowie **darüber hinausgehende bedeutende Störungen**, die zu beträchtlichen Auswirkungen auf die Sicherheit oder Funktionsfähigkeit der Telematikinfrastruktur führen können oder bereits geführt haben, **unverzüglich** an das **Bundesamt für Sicherheit in der Informationstechnik** sowie an das **Bundesministerium der Gesundheit** melden.	☐
Betreiber, Luftfahrtunternehmen und Stellen **Betreiber, Luftfahrtunternehmen und Stellen** sind nach der DVO (EU) 2019/1583 verpflichtet, dem **Bundesamt für Sicherheit in der Informationstechnik unverzüglich erhebliche IT-Störungen** zu melden. Eine erhebliche IT-Stötung liegt insbesondere dann vor, wenn eine Nicht-Reaktion weiterführende negative Auswirkungen auf die Informationssicherheit sowie auf die Sicherheit des zivilen Luftverkehrs hat; zusätzliche Aufwände und Mittel zur Beseitigung der Störung eingesetzt werden müssen, die über die Aufwände und Mittel des Regelbetriebs oder bereits geplanter Arbeiten hinausgehen; die Beseitigung durch speziell vorgehaltene Incident-Responder oder Störfallteams durchgeführt werden muss; wichtige IT-Systeme oder Komponenten zur Vermeidung weiterer Auswirkungen abgeschaltet oder isoliert werden müssen; für den Bewältigungszeitraum Betriebsprozesse geändert werden müssen; sie einen hohen finanziellen Schaden verursacht oder der Verdacht besteht, dass das Unternehmen Ziel eines neuartigen, außergewöhnlichen, zielgerichteten oder aus technischer Sicht bemerkenswerten Angriffs oder Angriffsversuchs ist, zum Beispiel ein sogenannter Advanced Persisentent Threat (APT).	☐

INFOBOX PFLICHTEN BEI VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN

Wer ist betroffen?

Jedes Unternehmen hat Zugang zu personenbezogenen Daten und ist somit von den im folgenden dargestellten Maßnahmen betroffen.

Was ist bei einem Cyberangriff zu tun?

Sind von einem Cyberangriff auch personenbezogene Daten betroffen, sind nach der Datenschutz-Grundverordnung insbesondere folgende Maßnahmen zu treffen:

Maßnahme	erledigt
Klären Sie, ob von dem Angriff **personenbezogene Daten** betroffen sind (z.B. von Kunden, Mitarbeitern, Dienstleitern, Lieferanten oder sonstigen Dritten).	☐
Bei einer Verletzung des Schutzes personenbezogener Daten, also aller Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen, muss der datenschutzrechtlich Verantwortliche regelmäßig unverzüglich (möglichst binnen 72 Stunden) die zuständige **Aufsichtsbehörde informieren** (Art. 33 DS-GVO). Dies gilt nur dann nicht, wenn die Verletzung zu keinem Risiko (oder nach Auffassung des European Data Protection Boards nur zu einem geringen Risiko) für die Rechte und Freiheiten natürlicher Personen führt. Eine solche Meldung muss mindestens Folgendes enthalten: • eine Beschreibung der Art der Verletzung des Datenschutzes, wenn möglich mit Kategorien, Anzahl der ungefähr betroffenen Personen, sowie der betroffenen Kategorie und Anzahl der betroffenen personenbezogenen Datensätze • Name und Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen • eine Beschreibung der wahrscheinlichen Folgen der Datenschutzverletzung • eine Beschreibung der ergriffenen und vorgeschlagenen Maßnahmen zur Behebung der Verletzung und ggf. Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen	☐
Besteht durch die mit dem Cyberangriff einhergehende Datenschutzverletzung ein hohes Risiko für die Rechte der betroffenen Personen, hat der Verantwortliche grundsätzlich auch diese Personen zu benachrichtigen (Art. 34 DS-GVO). Diesen Personen ist insbesondere in klarer und einfacher Sprache Informationen über die wahrscheinlichen Folgen und die ergriffenen und etwaige durch die Betroffenen zu ergreifenden Maßnahmen mitzuteilen. Unter bestimmten engen Voraussetzungen kann eine solche Benachrichtigungspflicht entfallen und/oder durch eine öffentliche Bekanntmachung oder ähnliche Maßnahmen ersetzt werden.	☐
Wenn personenbezogene Daten betroffen sind und Ihr Unternehmen Auftragsverarbeiter ist, informieren Sie unverzüglich den datenschutzrechtlich Verantwortlichen (Art. 33 Abs. 2 DS-GVO).	☐

Maßnahme	erledigt
Unabhängig von etwaigen Melde- und Benachrichtigungspflichten ist der datenschutzrechtlich Verantwortliche verpflichtet, die Verletzung des Schutzes personenbezogener Daten zu dokumentieren, einschließlich aller damit in Zusammenhang stehenden Fakten, deren Auswirkungen sowie der ergriffenen Abhilfemaßnahmen (Art. 33 Abs. 5 DS-GVO). Diese Dokumentation muss es der Aufsichtsbehörde erlauben, zu beurteilen, ob/inwieweit der Verantwortliche die Anforderungen der Meldepflicht nach Art. 33 DS-GVO korrekt umgesetzt hat.	☐

Erforderliche vorbereitende Maßnahmen

Die Unternehmensleitung hat den Datenschutz im Unternehmen so zu organisieren, dass auch die ordnungsgemäße Erfüllung von datenschutzrechtlichen Melde-, Benachrichtigungs- und Dokumentationspflichten sichergestellt ist.

Eine ordnungsgemäße Datenschutzorganisation erfordert die klare Benennung interner Zuständigkeiten und konkreter Aufgaben, typischerweise in einer Leitlinie zum Datenschutz sowie in internen Richtlinien zur Umsetzung verschiedener datenschutzrechtlicher Anforderungen. Diese schließt auch eine Richtlinie zum Umgang mit Datenschutzverletzungen mit ein. Die Schaffung der erforderlichen Richtlinien und unternehmensinternen Dokumentation ist auch unter dem Aspekt der datenschutzrechtlichen Rechenschaftspflicht (Art. 5 Abs. 2 DS-GVO) erforderlich, wonach Unternehmen durch geeignete Dokumentation nachweisen müssen, dass und wie sie ihre datenschutzrechtlichen Pflichten erfüllen.

Maßnahme	erledigt
Datenschutz-Management System, insbesondere Schaffen einer ordnungsgemäßen unternehmensinternen Datenschutzorganisation, um die Einhaltung der DS-GVO sicherzustellen, sowohl präventiv zur Verhinderung von Verletzungen des Schutzes personenbezogener Daten als auch reaktiv zum Umgang mit etwaigen dennoch eingetretenen Datenschutzverletzungen.	☐
Interne Richtlinie zum Umgang mit Datenschutzverletzungen, insbesondere mit Blick auf Melde-, Benachrichtigungs- und Dokumentationspflichten und die damit einhergehenden Risikobeurteilungen.	☐
Werkzeuge und Checklisten zur systematischen Ermittlung und Dokumentation datenschutzrechtlicher Risiken.	☐
Musterdokument zur ordnungsgemäßen Dokumentation eines Datenschutzvorfalls unter allen datenschutzrechtlich erforderlichen Aspekten.	☐

INFOBOX STRAFVERFOLGUNGSBEHÖRDE

Wer ist betroffen?

Jedes Unternehmen muss sich die Frage stellen, ob Strafverfolgungsbehörden eingeschaltet werden sollen.

Bei einem Cyberangriff werden in der Regel auch strafrechtliche Normen verletzt, deren Verfolgung von der Staatsanwaltschaft betrieben wird. Mögliche Straftatbestände sind insbesondere

- § 202a StGB: Ausspähen von Daten
- § 202b StGB: Abfangen von Daten

- § 202c StGB: Vorbereiten des Ausspähens und Abfangens von Daten
- § 202d StGB: Datenhehlerei
- § 263a StGB: Computerbetrug
- § 269 StGB: Fälschung beweiserheblicher Daten
- § 303a StGB: Datenveränderung
- § 303b StGB: Computersabotage

Darüber hinaus stehen die Unternehmen oftmals sehr hohen Lösegeldforderungen gegenüber. Kommen die Unternehmen den Lösegeldzahlungen nach, ist zu berücksichtigen, dass durch die Zahlung ggf. kriminelle Vereinigungen unterstützt werden. Zu prüfen ist, ob sich das Unternehmen, etwa nach §§ 129, 129b StGB, strafbar macht oder gegen das Sanktions- und Außenhandelsrecht verstößt.

Was ist bei einem Cyberangriff zu tun?

In den meisten Bundesländern bestehen inzwischen Schwerpunktstaatsanwaltschaften und Sondereinheiten bei den Landeskriminalämtern, die mit nötigem Sachverstand und Behutsamkeit bei den Ermittlungen vorgehen und insbesondere Beweise sichern können.

Maßnahme	erledigt
Prüfen Sie in Abstimmung mit den Rechtsanwälten, ob Strafverfolgungsbehörden eingeschaltet werden sollen.	☐
Prüfen Sie oder Ihre Rechtsanwälte, ob straf- oder sanktionsrechtliche Risiken durch die Zahlung von Lösegeldern bestehen könnten.	☐
Dokumentieren Sie die vorgenannten Prüfungen und Entscheidungen.	☐

INFOBOX AD-HOC-PUBLIZITÄT

Wer ist betroffen?

Für Emittenten, die am geregelten Markt zugelassen sind, bestehen gemäß Art. 17 Abs. 1 MAR Ad-hoc-Publizitätspflichten und Pflichten zur Weiterleitung an das Unternehmensregister, wenn der Cyberangriff so beschaffen ist, dass er sich auf den Preis des Finanzinstruments auswirkt.

Was ist bei einem Cyberangriff zu tun?

Maßnahme	erledigt
Prüfen Sie in Abstimmung mit den Rechtsanwälten, ob Strafverfolgungsbehörden eingeschaltet werden sollen.	☐

INFOBOX CYBER-VERSICHERUNG

Wer ist betroffen?

Cyber-Versicherungen sollen Unternehmen gegen **finanzielle und operative Risiken** eines Cyberangriffs schützen. Diese gleichen mitunter nicht nur die finanziellen Schäden des Vorfalls (Haftpflichtschäden und Eigenschäden) aus, sondern können Ihnen auch IT-Dienstleister zur Seite stellen, um Ihre Daten zu sichern und Ihr System schnell wieder in Betrieb zu bringen. Es besteht auch die Option, interne von Ihren eigenen Mitarbeitern verursachte Gefahren abzusichern. Vor Abschluss der Cyber-Versicherung sollten deshalb geprüft werden, welche Risiken durch die Versicherung abgedeckt sind und welchen Schutz Sie schon durch Ihre bereits bestehenden Versicherungen erhalten.

Beachten Sie außerdem, dass viele Cyber-Versicherungen Mindestsicherheitsanforderungen an Ihr IT-System stellen, die Sie erfüllen müssen.

Besteht Versicherungsschutz, so muss an versicherungsvertragsrechtliche Obliegenheiten gedacht werden, allen voran die Pflicht zur Meldung des Versicherungsfalles, da ansonsten der Versicherungsschutz verloren gehen kann. Hieran ist auch zu denken, wenn keine ausdrückliche Cyber-Versicherung besteht, da das Schadenszenario ggf. auch über andere Versicherungen abgedeckt sein kann.

Was ist bei einem Cyberangriff zu tun?

Maßnahme	erledigt
Prüfen Sie, ob möglicherweise Versicherungsschutz besteht (Cyber-Versicherung, Betriebsausfall, Haftpflichtversicherung) und benachrichtigen Sie Ihren Versicherer. Sofern Versicherungsschutz z. B. über eine Cyberversicherung besteht, prüfen Sie ob weitergehende Obliegenheiten (z.B. vertragliche Zustimmungsvorbehalte vor Beauftragung externer Berater, Mitwirkungsobliegenheiten) bestehen.	☐

ABSCHLUSS DES ANGRIFFS

Situation	Maßnahme	erledigt
Ende des Angriffs	Prüfen Sie, ob/inwieweit der Cyber-Angriff öffentlich bekannt wurde. Wenn ja, oder die Möglichkeit eines Bekanntwerdens besteht, erarbeiten Sie ein Kommunikationskonzept.	☐
	Prüfen Sie gemeinsam mit den externen Anwälten die Möglichkeit einer Anspruchsverfolgung und sichern Sie mit Unterstützung des IT-Forensikers bzw. der Strafverfolgungsbehörden hierfür notwendige Beweise.	☐
	Ziehen Sie Rückschlüsse aus dem Vorfall und nehmen Sie dokumentiert notwendige Verbesserungen an Ihrer IT vor.	☐