

Cyberresilience-Framework. In IT-Krisen schneller agieren. (Kurz: RESI)

Anlagen zu den
Handreichungen:
Merkblätter und Checklisten

Inhaltsverzeichnis

Checkliste Lagerfassung	3
Checkliste Krisenkommunikation	5
Notfall-Kontaktliste: Wichtige Ansprechpartner im Krisenfall.....	7
Merkblätter Behördliche Meldepflichten	11
Merkblatt Meldepflichten Allgemein.....	11
Übersicht	11
Welche Meldepflichten können bestehen?.....	12
Leitfragen für die Evaluierung können dabei sein:	12
Meldung an die Polizei?	13
Freiwillige Meldungen.....	13
Merkblatt Meldepflicht nach DSGVO nach einem erfolgreichen Ransomware-Angriff für KRITIS-Betreiber	15
Übersicht	15
Für wen besteht eine Meldepflicht?.....	15
Wann besteht eine Meldepflicht?	15
Welche Fristen bestehen?	16
Rechtsgrundlagen.....	16
FAQ:.....	16
Übersicht Anschriften Landesdatenschutzbeauftragte	18
Merkblatt Meldepflicht an das BSI nach einem erfolgreichen Ransomware-Angriff nach BSIG (Stand: Nach Bundestagsversion des NIS2UmseCG, Drucksache 20/13184).....	22
Übersicht	22
Für wen besteht eine Meldepflicht?.....	22
Wann besteht eine Meldepflicht?	23
Welche Fristen bestehen?	23
Rechtsgrundlagen.....	23
FAQ:.....	24
Merkblatt Meldepflicht an das BSI nach einem erfolgreichen Ransomware-Angriff nach Landesgesetzen	25
Übersicht	25
Freiwillige Meldung an das CERT.....	25
Rechtsgrundlagen.....	25
Übersicht:	26
Notfall-Kontaktliste: Zentrale Ansprechstellen Cybercrime (ZAC) der Polizeien in den Ländern .	28

Checkliste Lageerfassung

Anhand der Checkliste können die wichtigsten Fragen zur Lageerfassung nachvollzogen und abgearbeitet werden. Sie dient als „roter Faden“ in der Akutphase der Krise und sollten regelmäßig aktualisiert/ergänzt werden.

Leitfragen	Erledigt (abhaken)
DER ANGRIFF	
Was konkret ist vorgefallen? Was ist es für ein Angriff?	
Wann wurde der Angriff bemerkt?	
Seit wann läuft der Angriff?	
Sind Menschen in Gefahr? (z.B. durch Einschränkung technischer Funktionen, Nichtfunktionieren von Rettungsleitstellen)? Funktionieren Notrufnummern? Sind Rettungsdienste einsatzfähig?	
AUSWIRKUNGEN (nach INNEN)	
Ist der Krisenstab organisiert und arbeitsfähig? Ist er mit allen relevanten Personen besetzt?	
In welchem Ausmaß ist die Arbeitsfähigkeit der Mitarbeitenden eingeschränkt?	
Müssen alle Mitarbeitenden vor Ort sein? Welche Mitarbeitenden werden grade besonders benötigt? Welche können andere Aufgaben übernehmen?	
Ist die Arbeitszeiterfassung der Mitarbeitenden möglich? Werden Regelungen zur Arbeitszeiterfassung, Urlaub, Überstunden, Kurzarbeit benötigt?	
Bis wann ist die Arbeitsfähigkeit eingeschränkt?	
AUSWIRKUNGEN (nach AUßEN)	
Welche Systeme bzw. Daten sind derzeit nicht verfügbar? (Server, Telefonie, Mailverkehr, Webseite, etc.)?	
Welche Fachverfahren und angeschlossene Dienstleistungen sind dadurch nur eingeschränkt oder gar nicht verfügbar?	
Welche weiteren Auswirkungen haben der Angriff und seine Folgen auf die Bürger?	
Wie lange sind die Dienste voraussichtlich nicht verfügbar?	
Gibt es Workarounds für betroffene Dienstleistungen?	
Stehen Anspruchsgruppen unmittelbar unter Druck oder entwickeln Zugzwang (Ermittlungen/Untersuchungen/Prüfungen durch Behörden, Stellungnahmen durch Politiker, Verbände, NGOs)?	
Sind Backups verschlüsselt oder nutzbar?	
DATENSCHUTZ	
Sind Daten abgeflossen? Wenn ja, welche Art von Daten?	
Liegt eine meldepflichtige Datenschutzverletzung vor?	
Liegt eine Datenschutzverletzung vor, bei der auch betroffene Personen benachrichtigt werden müssen?	
Was können potenziell betroffene Personen tun, um sich jetzt vor den Auswirkungen des Angriffs zu schützen?	

MAßNAHMEN UND ZEITPLAN	
Was konkret wird aktuell sowie kurzfristig unternommen, um den Angriff abzuwehren und seine Folgen einzudämmen?	
Mit welchen Einrichtungen/Behörden und externen Experten wird zusammengearbeitet, um den Angriff abzuwehren und seine Folgen einzudämmen?	
Wenn Dienste erst nach und nach wiederhergestellt werden: Wie und durch wen werden diese priorisiert?	
Wie ist der antizipierte Zeitrahmen?	

Checkliste Krisenkommunikation

Anhand der Checkliste können die wichtigsten Schritte der Krisenkommunikation nachvollzogen und abgearbeitet werden. Sie dient als „roter Faden“ in der Akutphase der Krise und kann entweder fortlaufend geführt/aktualisiert oder als Vorlage für jede Krisenstabssitzung genutzt werden.¹

Aufgabe	Zuständigkeit	Datum/Uhrzeit	Erledigt
SOFORT			
Issue/Krise melden	Erkennende/r		
Krisenstab einberufen & besetzen	Geschäftsführung		
Lage erfassen	Krisenstab		
Anzeige bei Polizei/LKA, Meldung an LDI und ggf. BSI	Krisenstab		
Relevante Zielgruppen definieren	Kommunikation		
Kommunikationsstrategie und -plan abstimmen: Botschaften, Inhalte, Zielgruppen, Kanäle	Kommunikation		
Medienmonitoring aufsetzen/erweitern	Kommunikation		
Erst-Information an Mitarbeiter erstellen/versenden	Kommunikation		
FAQ intern/Sprechzettel erstellen/versenden	Kommunikation		
Erst-Information an Bürger erstellen/publizieren	Kommunikation		
Erst-Information an Medien erstellen/versenden	Kommunikation		
FAQ extern erstellen/ggf. publizieren			
Ggf. Erst-Information an weitere Partner erstellen/ versenden	Kommunikation		
IM VERLAUF			
Ggf. Zielgruppen anpassen/ausweiten			
Medienmonitoring auswerten, Lageänderung feststellen, ggf. Kommunikationsplan und -maßnahmen anpassen	Weitere Sitzungen Krisenstab/ Kommunikation		
Folge-Information an Mitarbeiter aktualisieren/versenden	Kommunikation		
FAQ intern/Sprechzettel anpassen/versenden	Kommunikation		
Folge-Information an Bürger aktualisieren/publizieren	Kommunikation		
Folge-Information an Medien	Kommunikation		

¹ Auf den Abschnitt „Evaluierung“ wird hier aus Platzgründen verzichtet.

aktualisieren/versenden			
Mediananfragen bündeln/beantworten			
FAQ extern aktualisieren/ggf. publizieren	Kommunikation		
Ggf. Information an weitere Partner aktualisieren/versenden	Kommunikation		

Notfall-Kontaktliste: Wichtige Ansprechpartner im Krisenfall

Notfall-Kontaktliste: Wichtige Ansprechpartner im Krisenfall						
Ansprechpartner	Name	Telefon dienstl.	Mobil dienstl.	E-Mail dienstl.	ggf. Telefon (privat)	ggf. E-Mail (privat)
Krisenstab						
Verwaltungsleitung (HVB, Landrat/Bürgermeister)						
Recht & Compliance						
Datenschutz und Datensicherheit						
IT-Abteilung/IT-Dienstleister						
Kommunikation/Pressestelle						
Arbeitssicherheit						
Weitere Mitglieder des Krisenstabs						
Behörden und Verwaltung						
Polizei						

Feuerwehr						
Rettungsdienst						
Kommunales Amt für Brand- /Katastrophenschutz, Rettungsdienst						
Kommunale Unternehmen (Stadtwerke o.ä.)						
Landeskriminalamt/LKA						
Zentrale Ansprechstelle Cyberkriminalität/ZAC	-					
Landesdatenschutzbeauftragter/LDI						
Bundesamt für Sicherheit in der Informationstechnik						
LandesCERT						
Kreisverwaltung (für kreisangehörige Gemeinden)						
Ansprechpartner	Name	Telefon dienstl.	Mobil dienstl.	E-Mail dienstl.	ggf. Telefon privat	ggf. E-Mail privat
Meldung nach Sicherheitsgesetz Bundesland						
(Haupt)-Stadtverwaltung						

Aufsichtsbehörden (falls vorhanden)						
Regierung/Parteien						
Landrat						
Nachbarlandkreis/e für Amtshilfe						
Nachbarkommune/n für Amtshilfe						
Politische Parteien						
Externe Dienstleister						
IT-Dienstleister für Incident Response/Forensik						
Krisenmanagement						
Krisenkommunikation						
Rechtsberatung						
Cyberversicherung						
Gasversorger						
Stromversorger						

Wasserversorger						
Medien						
Lokalmedien (Print, Online-Portale, TV, Hörfunk)						
Informationsstand: bitte für Kommune spezifisch ausfüllen und aktualisieren						

Merkblätter Behördliche Meldepflichten

Merkblatt Meldepflichten Allgemein

Übersicht

- Im Falle einer Cyberattacke, z.B. bei einem Ransomware-Angriff oder eines DDoS-Angriffs, kann eine Kommune unterschiedlichen gesetzlichen Meldepflichten unterliegen.
- **Neben Pflichten** besteht die Möglichkeit zu **freiwilligen Meldungen**
- Zu beachten ist, dass die folgende Übersicht nicht abschließend ist. Im Krisenfall ist eine individuelle Prüfung notwendig.
- Die beigefügten Steckbriefe enthalten die wichtigsten Informationen zu den relevantesten Meldepflichten.

Wichtigste Meldepflichten				
Rechtgrundlage	Wer	Wann	An wen	Wichtigsten Fristen
DSGVO	Sämtliche öffentliche und nicht öffentlichen Stellen (Ausnahme etwa Strafverfolgungsbehörden)	Verletzung des Schutzes personenbezogener Daten	Landes Datenschutz-aufsicht	Meldung unverzüglich, spätestens nach 72 Stunden
BSIG	Betreiber wichtiger und wesentlicher Dienste (ehemals KRITIS), Kommunalverwaltung i.d.R. nicht	erheblicher Sicherheitsvorfall	BSI	gestaffelte Meldung, Erstmeldung unverzüglich, spätestens nach 24 Stunden

Landesgesetze	i.d.R. kommunale Verwaltungen (Landesspezifisch)	Sicherheitsvorfall oder Informationen zur Abwehr von Cyberrisiken	Landesspezifisch	i.d.R. unverzüglich
eIDAS				
Sonstiges	Betreiber spezieller Dienste oder Verarbeitung von besonders sensiblen Inhalten	Ausfall des speziellen Dienstes oder Verletzung des Schutzes der konkreten Inhalte	Dezierte Aufsichtsbehörden oder konkret Verantwortliche Stellen	-

Welche Meldepflichten können bestehen?

- Es existieren sowohl allgemeine Meldepflichten (bspw. DSGVO), als auch spezielle, welche die sich aus einer konkreten Tätigkeit ergeben.
- Im Rahmen der Evaluation, welche Meldepflichten bestehen, kommt es demnach auf die konkreten Tätigkeiten an, die durch eine Kommune wahrgenommen werden.

Leitfragen für die Evaluierung können dabei sein:

- Übt die Betroffene Stelle eine Tätigkeit im Rahmen des Anwendungsbereichs der Meldepflicht aus?
- Wirkt sich der Vorfall ausreichend schwerwiegend auf die entsprechende Tätigkeit aus?

Meldepflichten müssen sich dabei nicht explizit auf das Vorliegen einer Cyberattacke beziehen. Entscheidend ist das Bestehen einer Auswirkung auf einen bestimmten Dienst.

Neben den hier aufgeführten Meldepflichten können noch weitere Meldepflichten bestehen. **Leitfragen zur Identifizierung solcher hierfür können sein:**

- Werden durch die Kommune sensible Dokumente (etwa zur Strafverfolgung, Verfassungsschutz usw.) verarbeitet?
- Ist die Kommune an Behördennetze (wie das Netz des Bundes) angeschlossen?

Meldung an die Polizei?

Neben gesetzlichen Meldepflichten kann es grundsätzlich sinnvoll sein, im Falle einer Cyberattacke wie einem Ransomware-Angriff oder eines DDoS-Angriffs Anzeige bei der Polizei zu erstatten. Die meisten Landeskriminalämter verfügen für diese Fälle i.d.R. über spezialisierte Abteilungen. Eine Übersicht hierzu finden Sie im Anhang.

Freiwillige Meldungen

Gesetzliche Meldepflichten können gewissermaßen als das „notwendige Minimum“ an Informationsflüssen angesehen werden. Über die verpflichtenden Meldungen hinaus kann es aus operativer Sicht dennoch sinnvoll sein, bestimmte Informationen über einen erfolgreichen Angriff mit weiteren externen Stakeholdern zu teilen. Grundsätzlich ist es sinnvoll zu evaluieren, inwiefern eine Meldung bzw. die Kommunikation zu folgenden Stakeholdern angebracht ist:

1. Andere Stellen
 - a. sofern sie bei der Erbringung ihrer eigenen Dienste von denjenigen der Verwaltung abhängig sind, oder
 - b. im Falle eines Angriffes auf einen Dienstleister (o. sonstige Drittorganisationen) andere von diesem Dienstleister abhängige Stellen (Kommunen);
 - c. ggf. zur gemeinsamen Bewältigung des Vorfalls,
 - d. zur Begrenzung der Auswirkungen sowie
 - e. zum Austausch über Reaktionsmaßnahmen.
2. Gefahrenabwehr- und Katastrophenschutzbehörden
 - a. zur Abschätzung und Koordination ggf. notwendiger Gefahrenabwehrmaßnahmen, etwa durch Polizei und Feuerwehr;
3. die Strafverfolgung
 - a. sofern der IT-Sicherheitsvorfall auf eine Straftat zurückzuführen sein könnte, sowie

4. das Bundesamt für Sicherheit in der Informationstechnik (BSI)
 - a. zur Ausübung ihrer Aufgaben als zentrale Meldestelle (Vorgehensweisen und potenzielle Auswirkungen analysieren, Lagebilderstellung, überregionale Unterrichtung).
5. Landes CERTS
 - a. Zur Evaluierung ggf. bestehender Unterstützungsmöglichkeiten

Merkblatt Meldepflicht nach DSGVO nach einem erfolgreichen Cyberangriff für KRITIS-Betreiber

Übersicht

Wann besteht eine Meldepflicht?	Bei erheblichen Auswirkungen auf die Bereitstellung der kritischen Dienstleistung
Fristen:	unverzüglich, spätestens 72 Stunden nach Bekanntwerden (an die Aufsichtsbehörde)
Empfangende Stelle:	an die zuständige Datenschutzaufsichtsbehörde (siehe folgende Tabelle),

Für wen besteht eine Meldepflicht?

Eine Meldepflicht nach der DSGVO gilt für sämtliche datenverarbeitenden Stellen, mit Ausnahme von zuständigen Behörden, welche etwaige Daten zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung verarbeiten.

Mit Ausnahme der Strafverfolgungsbehörden wird demnach i.d.R. eine Meldepflicht bestehen.

Wann besteht eine Meldepflicht?

Grundsätzlich besteht eine Meldepflicht, sofern eine Verletzung des Schutzes personenbezogener Daten erfolgt. Eine solche Verletzung liegt vor, sofern personenbezogene Daten unbeabsichtigt oder unrechtmäßig vernichtet, verloren, verändert oder unbefugt offengelegt wurden bzw. sich unbefugter Zugang verschafft wurde.

Im Falle eines erfolgreichen Ransomware-Angriffs liegt i.d.R. eine solche Verletzung vor. Dabei ist es unwesentlich, ob bereits festgestellt werden kann ob etwa Daten abgeflossen sind. Der Zugang durch den Angreifer und eine Verletzung der Verfügbarkeit durch die Verschlüsselung reichen hier bereits aus. Bei einem DDoS-Angriff muss man ebenfalls prüfen, ob die Angreifer möglicherweise Zugriff auf Daten gehabt haben. Dann besteht hier ebenfalls eine Meldeverpflichtung.

Die weiteren Meldepflichten sind im Weiteren zweistufig aufgebaut:

- sofern ein Risiko für die Rechte und Freiheiten der betroffenen Person nicht ausgeschlossen werden kann, ist eine Meldung an die zuständige Aufsichtsbehörde abzugeben. **Hiervon ist im Falle eines Ransomware-Angriffs i.d.R. auszugehen.**

- sofern voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen besteht, sind diese ebenfalls zu informieren.

Welche Fristen bestehen?

- Meldepflicht an die Aufsichtsbehörde: **unverzüglich, spätestens 72 Stunden nach Bekanntwerden der Verletzung.**
- Meldepflicht an die betroffenen Personen: **unverzüglich nach Bekanntwerden der Verletzung**

Rechtsgrundlagen

- Art. 4 Nr. 12 DSGVO (Definition Verletzung des Schutzes personenbezogener Daten)
- Art. 32 DSGVO (Meldepflicht an die Aufsichtsbehörde)
- Art. 33 DSGVO (Meldepflicht an die betroffenen Personen)

FAQ:

- **Muss das von den Aufsichtsbehörden bereitgestellte Meldeformular genutzt werden?**

Die meisten Landesaufsichtsbehörden stellen ein Standardformular (als PDF oder Webformular) zur Verfügung. Die dort abgefragten Informationen richten sich im Wesentlichen nach Art. 33 Abs. 3 DSGVO (u.a. Kategorien der Betroffenen-Daten, wahrscheinliche Folgen/Schäden, ergriffene Mitigation-Maßnahmen), können jedoch im Detail unterschiedlich sein. Grundsätzlich ist eine Nutzung der bereitgestellten Formulare jedoch nicht zwingend. Nicht über das Standardformular abgefragte Informationen können ggf. von der Aufsicht nachgefordert werden, weshalb es ggf. sinnvoll sein kann, eine umfassende Bestandsaufnahme anhand einer „Konsolidierten Fassung – Datenschutz-Meldung“ (bspw. [hier](#)) vorzunehmen, und eine Meldung ggf. anhand der dort erfassten Angaben auf dem elektronischen Postweg vorzunehmen.

- **Wann besteht eine Meldepflicht bzw. was bedeutet „Verletzung des Schutzes personenbezogener Daten“?**

Als Verletzung des Schutzes personenbezogener Daten gilt die Verletzung der Sicherheit, ob unbeabsichtigt oder unrechtmäßig, die zum Verlust, der Veränderung, oder unbefugten Offenlegung bzw. unbefugten Zugang personenbezogener Daten geführt hat.

- **Im Falle eines Ransomware-Angriffs wird dies i.d.R. der Fall sein, daher wird i.d.R. eine Meldepflicht bestehen. Ab wann läuft die Frist der „72“ Stunden?**

Die meisten Aufsichtsbehörden interpretieren die 72 Stundenfrist als 72 Zeitstunden ab Bekanntwerden der Verletzung. Unerheblich sind hier die üblichen Arbeitszeiten der verantwortlichen Stelle sowie etwaige Feiertage. Die Frist beginnt mit der Kenntnisnahme der Verletzung innerhalb der verantwortlichen Stelle, d.h. nicht etwa erst, wenn der Datenschutzbeauftragte in Kenntnis gesetzt wurde.

Grundsätzlich sollte eine Meldung so schnell wie möglich (d.h. unverzüglich) erfolgen, wobei die 72 Stunden als Höchstfrist anzunehmen sind.

- **Kann ich eine Meldung an die Aufsichtsbehörde abgeben, bevor ich die Lage/ Auswirkungen eines Vorfalls abschließend beurteilt habe?**

Eine abschließende Beurteilung eines Vorfalls ist nicht notwendig. Im Zweifel ist es i.d.R. möglich, eine Erstmeldung durch eine spätere Nachreichung zu konkretisieren. Ggf. fragt die zuständige Datenschutzbehörde diese Nachreichung an.

Übersicht Anschriften Landesdatenschutzbeauftragte

Anschriften und Erreichbarkeit Landesdatenschutzbeauftragte

(Informationen finden Sie auch hier: <https://www.bfdi.bund.de/DE/Service/Anschriften/Laender/Laender-node.html>)

Übersicht Landesaufsichtsbehörden für Datenschutz			
Land	Behörde	Kontakt	Link Formular Meldung
Baden-Württemberg	Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Pro. Dr. Tobias Keber Lautenschlagerstraße 20 70173 Stuttgart Postanschrift Postfach 10 29 32 70025 Stuttgart	Telefon: 07 11/61 55 41-0 Montag bis Freitag von 10 bis 12 Uhr, außer Mittwoch, da von 14 bis 15.30 Uhr. Telefax: 07 11/61 55 41-15 E-Mail: poststelle@lfd.bwl.de Homepage: https://www.baden-wuerttemberg.datenschutz.de	https://www.baden-wuerttemberg.datenschutz.de/datenpanne-melden/ https://www.baden-wuerttemberg.datenschutz.de/kontakt-aufnehmen/
Bayern	Der Bayerische Landesbeauftragte für den Datenschutz Prof. Dr. Thomas Petri Wagmüllerstraße 18 80538 München Postanschrift Postfach 22 12 19 80502 München	Telefon: 089/21 26 72-0 Telefax: 089/21 26 72-50 E-Mail: poststelle@datenschutz-bayern.de Homepage: https://www.datenschutz-bayern.de	https://www.lida.bayern.de/de/datenpanne.html https://www.datenschutz-bayern.de/service/data_breach.html
Berlin	Berliner Beauftragte für Datenschutz und Informationsfreiheit Meike Kamp Alt-Moabit 59-61 10555 Berlin	Telefon: 030/13 88 9-0 Telefax: 030/21 55 050 E-Mail: mailbox@datenschutz-berlin.de Homepage: https://www.datenschutz-berlin.de	https://www.datenschutz-berlin.de/datenschutz/datenpanne/datenpannenformular/

Brandenburg	Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Dagmar Hartge Stahnsdorfer Damm 77 14532 Kleinmachnow	Telefon: 03 32 03/356-0 Telefax: 03 32 03/356-49 E-Mail: poststelle@lda.brandenburg.de Homepage: https://www.lda.brandenburg.de	https://www.lda.brandenburg.de/lda/de/service/formulare-und-musterschreiben/meldung-einer-datenschutzverletzung/
Bremen	Die Landesbeauftragte für Datenschutz und Informationsfreiheit Dr. Timo Utermark. Georgstraße 122-124 27570 Bremerhaven	Telefon: 04 21/361-2010 oder 04 71/596-2010 E-Mail: office@datenschutz.bremen.de Homepage: https://www.datenschutz.bremen.de/	https://www.datenschutz.bremen.de/wir-ueber-uns/online-meldungen/datenschutzverletzung-melden-15665
Hamburg	Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit Thomas Fuchs Ludwig-Erhard-Str 22, 7. OG 20459 Hamburg	Telefon: 040/428 54 - 4040 Telefax: 040/4279 - 4000 E-Mail: mailbox@datenschutz.hamburg.de Homepage: https://datenschutz-hamburg.de/	https://datenschutz-hamburg.de/service-information/datenpanne-melden
Hessen	Der Hessische Beauftragte für Datenschutz und Informationsfreiheit Prof. Dr. Alexander Roßnagel Gustav-Stresemann-Ring 1 65189 Wiesbaden Postanschrift Postfach 3163 65021 Wiesbaden	Telefon: 06 11/14 08-0 Telefax: 06 11/14 08-611 E-Mail: poststelle@datenschutz.hessen.de De-Mail: poststelle@datenschutz.hessen.de-mail.de Homepage: https://datenschutz.hessen.de/	https://datenschutz.hessen.de/service/meldung-nach-art-33-ds-gvo
Mecklenburg-Vorpommern	Der Landesbeauftragte für Datenschutz und Informationsfreiheit Sebastian Schmid Werderstraße 74a 19055 Schwerin Postanschrift Schloss Schwerin Lennéstraße 1 19053 Schwerin	Telefon: 03 85/594 94-0 Telefax: 03 85/594 94-58 E-Mail: info@datenschutz-mv.de (PGP Key) Homepage: https://www.datenschutz-mv.de	https://www.datenschutz-mv.de/kontakt/meldung-einer-datenpanne/

Niedersachsen	Die Landesbeauftragte für den Datenschutz Niedersachsen Denis Lehmkemper Prinzenstraße 5 30159 Hannover Postanschrift Postfach 221 30002 Hannover	Telefon: 05 11/120-45 00 Telefax: 05 11/120-45 99 E-Mail: poststelle@lfd.niedersachsen.de Homepage: https://www.lfd.niedersachsen.de	https://www.lfd.niedersachsen.de/verletzung
Nordrhein-Westfalen	Die Landesbeauftragte für Datenschutz und Informationsfreiheit Bettina Gayk Kavalleriestraße 2-4 40213 Düsseldorf Postanschrift Postfach 20 04 44 40102 Düsseldorf	Telefon: 02 11/384 24-0 Telefax: 02 11/384 24-999 E-Mail: poststelle@ldi.nrw.de Homepage: https://www.ldi.nrw.de	https://www.ldi.nrw.de/kontakt/meldeformular-fuer-datenpannen
Rheinland-Pfalz	Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Prof. Dr. Dieter Kugelmann Hintere Bleiche 34 55116 Mainz Postanschrift Postfach 30 40 55020 Mainz	Telefon: 061 31/208-2449 Telefax: 061 31/208-2497 E-Mail: poststelle@datenschutz.rlp.de Homepage: https://www.datenschutz.rlp.de/	https://www.datenschutz.rlp.de/themen/online-services/meldeformular-datenpanne-art-33-ds-gvo
Saarland	Unabhängiges Datenschutzzentrum Saarland Die Landesbeauftragte für Datenschutz und Informationsfreiheit Monika Grethel Fritz-Dobisch-Straße 12 66111 Saarbrücken	Telefon: 06 81/947 81-0 Telefax: 06 81/947 81-29 E-Mail: poststelle@datenschutz.saarland.de Homepage: https://www.datenschutz.saarland.de	

Sachsen	Sächsische Datenschutzbeauftragte Dr. Juliane Hundert Devrientstraße 5 01067 Dresden Postanschrift Postfach 11 01 32 01330 Dresden	Telefon: 03 51/85 471 101 Telefax: 03 51/85 471 109 E-Mail: saechsdsb@slt.sachsen.de Homepage: https://www.saechsdsb.de	https://www.datenschutz.saarland.de/online-dienste/meldung-datenpanne
Sachsen-Anhalt	Landesbeauftragter für den Datenschutz Sachsen-Anhalt Maria Christina Rost Leiterstraße 9 39104 Magdeburg Postanschrift Postfach 1947 39009 Magdeburg	Telefon: 03 91/81 803-0 Telefax: 03 91/81 803-33 E-Mail: poststelle@lfd.sachsen-anhalt.de Homepage: https://datenschutz.sachsen-anhalt.de	https://datenschutz.sachsen-anhalt.de/service/online-formulare/datenschutzverletzung
Schleswig-Holstein	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein Dr. h.c. Marit Hansen Landesbeauftragte für Datenschutz Schleswig-Holstein Holstenstraße 98 24103 Kiel Postanschrift Postfach 71 16 24171 Kiel	Telefon: 04 31/988-1200 Telefax: 04 31/988-1223 E-Mail: mail@datenschutzzentrum.de Homepage: https://www.datenschutzzentrum.de	https://www.datenschutzzentrum.de/meldungen/#panne
Thüringen	Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit Tino Melzer Häßlerstraße 8 99096 Erfurt Postanschrift Postfach 900455 99107 Erfurt	Telefon: 03 61/57 311 29 00 Telefax: 03 61/57 311 29 04 E-Mail: poststelle@datenschutz.thueringen.de Homepage: https://www.tlfdi.de/	

Stand: November 2024 (muss regelmäßig aktualisiert werden)

Merkblatt Meldepflicht an das BSI nach einem erfolgreichen Ransomware-Angriff nach BSIG (Stand: Nach Bundestagsversion des NIS2UmseCG, Drucksache 20/13184)

Übersicht

Wann besteht eine Meldepflicht?	Bei erheblichen Auswirkungen auf die Bereitstellung der kritischen Dienstleistung
Fristen:	<ul style="list-style-type: none"> • Erstmeldung: unverzüglich, spätestens 24 Stunden nach Bekanntwerden (an die Meldestelle) • Konkretisierung: unverzüglich, spätestens innerhalb 72 Stunden nach Bekanntwerden (an die Meldestelle) • Abschlussmeldung: spätestens einen Monat nach Übermittlung der Konkretisierung
Empfangende Stelle:	<ul style="list-style-type: none"> • Meldestelle des BSI und dem Bundesamt für Bevölkerungsschutz

Für wen besteht eine Meldepflicht?

Eine Meldepflicht nach § 32 BSIG besteht für wesentliche und wichtige Einrichtungen.

Kommunen und kommunale Verwaltungen sind grundsätzlich nicht vom Anwendungsbereich des BSIG betroffen. Für diese können jedoch Meldepflichten nach Landesgesetzen bestehen.

Stellen der Bundesverwaltung sowie kommunale Dienstleister (Stadtwerke, Verkehrsbetriebe etc.) fallen jedoch ggf. in den Anwendungsbereich des BSIG.

Als wesentliche bzw. wichtige Einrichtung besteht eine Registrierungspflicht. Daher sollte i.d.R. bereits bekannt sein, ob die betroffene Stelle unter den Anwendungsbereich fällt.

Wann besteht eine Meldepflicht?

Eine Meldepflicht besteht im Falle eines erheblichen Sicherheitsvorfalls, d.h. Sicherheitsvorfall, der (potentiell) eine schwerwiegende Betriebsstörung oder finanzielle Verluste einer betreffenden Einrichtung verursacht oder anderen natürlichen oder juristischen Personen erhebliche materielle oder immaterielle Schäden zufügen kann.

Entscheidend ist somit eine Risikobewertung der Auswirkungen des Vorfalls. Sofern die wesentlichen bzw. kritischen Dienstleistungen aufgrund eines Ransomware-Angriffs über Tage nicht erbracht werden können, kann i.d.R. von einer Meldepflicht ausgegangen werden.

Welche Fristen bestehen?

- **Erstmeldung:** unverzüglich, spätestens 24 Stunden nach Bekanntwerden (an die Meldestelle), Inhalt: Beschreibung und Begründung, ob ein Verdacht besteht, dass der Sicherheitsvorfall auf eine rechtswidrige oder böswillige Handlung zurückzuführen ist oder ob grenzüberschreitende Auswirkungen bestehen könnten
- **Konkretisierung:** unverzüglich, spätestens innerhalb 72 Stunden nach Bekanntwerden (an die Meldestelle): Aktualisierung der in der Erstmeldung angegebenen Informationen sowie erste Einschätzung des Schweregrads der Auswirkungen sowie ggf. Hinweise der Kompromittierung (Indicators of Compromise/IoC)
- **Abschlussmeldung:** spätestens einen Monat nach Übermittlung der Konkretisierung, Inhalt: Ausführlicher Bericht und Beschreibung, Auswirkungsanalyse, Mitigationsmaßnahmen, ggf. grenzüberschreitende Auswirkungen

Rechtsgrundlagen

- Art. 23 Abs. 3 NIS2, § 2 Nr. 11 BSIG (Definition Erheblicher Sicherheitsvorfall)
- § 28 BSIG (Anwendungsbereich/ Definition von wesentlichen und wichtigen Einrichtungen)
- § 29 BSIG (Anwendungsbereich/ Definition von Einrichtungen der Bundesverwaltung)
- Art. 23 Abs. 4 NIS2, § 32 BSIG (Meldepflicht in Falle eines erheblichen Sicherheitsvorfalls)

FAQ:

- **Bin ich als Kommune KRITIS?**

Kommunen als Teil der Länder fallen nicht in den Anwendungsbereich des BSIG als Bundesgesetz und sind demnach auch nicht rechtlich als KRITIS definiert. Eine Meldepflicht an das BSI besteht demnach nicht. Jedoch können landesspezifische Sicherheitsgesetze bestehen, welche eine **Meldepflicht an entsprechende Landesbehörden begründen. Das Nichtbestehen einer Pflicht schließt weiterhin eine freiwillige Meldung an das BSI nicht aus.**

- **Bestehen weitere Meldeverpflichtungen?**

Weiterhin können analoge Meldepflichten für Kommunen bestehen, sofern die jeweilige Landesregierung diese per Landesgesetz oder Verwaltungsverordnung (aktuell nur Niedersachsen) festgelegt hat. In diesem Fall sind die formalen Vorschriften hinsichtlich Fristen und Inhalt der Meldung i.d.R. vergleichbar. **Jedoch muss statt an das BSI i.d.R. eine entsprechende Landesbehörde als Stelle benannt an die zu melden ist.**

Merkblatt Meldepflicht an das BSI nach einem erfolgreichen Cyberangriff nach Landesgesetzen

Übersicht

Grundsätzlich können **Meldepflichten** für Kommunen auch über **Landesgesetze** umgesetzt sein. Bundesweit ist dies innerhalb der Länder unterschiedlich geregelt. **Eine Übersicht** über die landespezifischen IT-Sicherheitsgesetze finden Sie in der folgenden Tabelle.

Grundsätzlich ist hierbei zu beachten, dass sowohl die Stelle, an die eine Meldung abzugeben ist, das begründende Ereignis einer Meldepflicht (bspw. die Definition eines Sicherheitsvorfalls), der Adressatenkreis als auch etwaige Fristen **uneinheitlich geregelt** sind.

Im Krisenfall müssen etwaige Meldepflichten daher anhand der einschlägigen Landesgesetze evaluiert werden.

Dabei sind innerhalb der vorhandenen IT-Sicherheitsgesetze, welche eine Meldepflicht formulieren, zwei Arten von Meldepflichten auszumachen:

- Meldepflicht bei Bestehen eines IT-Sicherheitsvorfalls.
- Meldepflicht sämtlicher Informationen, die für die Abwehr von Cybersicherheits-Risiken relevant sind.

Im Fall **einer erfolgreichen Cyberattacke** (wie einem Ransomware-Angriff oder DDos-Angriff) kann davon ausgegangen werden, dass eine **Meldepflicht in beiden Fällen besteht**.

Freiwillige Meldung an das CERT

Auch wenn **keine Meldepflicht** besteht, kann **grundsätzlich eine freiwillige Meldung** an zuständige **Landes-CERT** abgegeben werden. Eine Meldung an das CERT erfüllt dabei weniger aufsichtstypische Zwecke, sondern dient dazu, die Möglichkeit einer **operativen Unterstützung** durch das jeweilige CERT abzuschätzen.

Rechtsgrundlagen

- Landesgesetze und Verwaltungsverordnungen

Übersicht:

Meldepflichten Länder

Land	Landeseigenes IT-Sicherheitsgesetz Verwaltungsvorschrift mit NIS2 Bezug	Meldepflicht	
		Im Fall eines Sicherheitsvorfalls	Informationen relevant zur Cyberabwehr
Baden-Württemberg	ja (Egov BW; CSG BW)	nein	ja (§ 4 Abs. 4 CSG BW)
Bayern	ja (BayDiG)	nein	ja (Art. 43 BayDiG)
Berlin	nein	-	-
Bremen	nein (in Planung)	-	-
Brandenburg	nein	-	-
Hamburg	nein (Spezialgesetz für Gerichte HmbITJG)	verpflichtend für Gerichte (§ 4 HmbITJG)	-
Hessen	ja (HITSig)	ja (§ 18 HiTSig)	nein
Mecklenburg- Vorpommern	nein (in Planung)	-	-

Niedersachsen	ja (NDIG Verwaltungsvorschrift mit NIS2 Bezug NIS2UmsRdErl)	ja (§ 14 Abs. 2 NDIG), sofern Anschluss an das Landesnetz besteht. ja für Kommunen, ähnlich Meldepflichten nach NIS2 (Abschnitt 6 NIS2UmsRdErl)	-
Nordrhein-Westfalen	nein (in Planung)	-	-
Rheinlandpfalz	nein	-	-
Saarland	ja (IT-SiG SL)	Verpflichtend in Bezug auf allgemeine Informationen zur Abwehr von Gefahren der Informationssicherheit (§ 3 Saar)	ja (§3 IT-SiG SL)
Sachsen	ja (SächLSichG)	ja (§ 16 SächLSichG)	nein
Sachsen-Anhalt	nein (in Planung)	-	-
Schleswig-Holstein	nein	-	-
Thüringen	nein	-	-

Notfall-Kontaktliste: Zentrale Ansprechstellen Cybercrime (ZAC) der Polizeien in den Ländern

Land/ Bund	Telefonnummer	E-Mail	Link Website	Adresse Website
Baden-Württemberg	+49 711 5401-2444	cybercrime@polizei.bwl.de	ZAC Baden-Württemberg	https://lka.polizei-bw.de/zentrale-ansprechstelle-cybercrime/
Bayern	+49 89 1212-3300	zac@polizei.bayern.de	ZAC Bayern	https://www.polizei.bayern.de/kriminalitaet/interne-kriminalitaet/002464/index.html
Berlin	+49 30 4664-972972	zac@polizei.berlin.de	ZAC Berlin	https://www.berlin.de/polizei/aufgaben/praevention/cybercrime/artikel.854755.php
Brandenburg	+49 3334 388-8686	zac@polizei.brandenburg.de	ZAC Brandenburg	https://polizei.brandenburg.de/seite/internetkriminalitaet/2460110
Bremen	+49 421 362-19820	cybercrime@polizei.bremen.de	ZAC Bremen	https://www.polizei.bremen.de/praevention/cybercrime-60310
Hamburg	+49 40 4286-75455	zac@polizei.hamburg.de	ZAC Hamburg	https://www.polizei.hamburg/zentrale-ansprechstelle-cybercrime-556368
Hessen	+49 611 83-8377	zac.hlka@polizei.hessen.de	ZAC Hessen	https://www.polizei.hessen.de/praevention/gemeinsam-sicher-in-hessen/sicher-im-internet-1
Mecklenburg-Vorpommern	+49 3866 64-9494	cybercrime.lka@polmv.de	ZAC Mecklenburg-Vorpommern	https://behoerdenverzeichnis.mv-serviceportal.de/?ouId=144692325
Niedersachsen	+49 511 9873-6230	zac@lka.polizei.niedersachsen.de	ZAC Niedersachsen	https://www.zac-niedersachsen.de/
Nordrhein-Westfalen	+49 211 939-4040	cybercrime.lka@polizei.nrw.de	ZAC Nordrhein-Westfalen	https://www.sta-koeln.nrw.de/aufgaben/geschaefte-stak_1_zac/index.php

Rheinland-Pfalz	+49 6131 65-64760	lka.cybercrime@polizei.rlp.de	ZAC Rheinland-Pfalz	https://www.polizei.rlp.de/die-polizei/dienststellen/landeskriminalamt-rheinland-pfalz/service-und-ansprechstellen/zentrale-ansprechstelle-cybercrime-zac
Saarland	+49 681 962-2448	cybercrime@polizei.slpol.de	ZAC Saarland	https://www.saarland.de/polizei/DE/themen-aufgaben/kriminalitaet/zac/zac_node.html
Sachsen	+49 351 855 3226	zac.lka@polizei.sachsen.de	ZAC Sachsen	https://www.polizei.sachsen.de/de/47792.htm
Sachsen-Anhalt	+49 391 250-2909	zac.lka@polizei.sachsen-anhalt.de	-	-
Schleswig-Holstein	+49 431 160 42727	cybercrime@polizei.landsh.de	ZAC Schleswig-Holstein	https://www.schleswig-holstein.de/DE/landesregierung/ministerien-behoerden/POLIZEI/DasSindWir/LKA/cybercrime/_artikel/_fachinhalte/zac_startseite
Thüringen	+49 361 57431-4545	cybercrime.lka@polizei.thueringen.de	ZAC Thüringen	https://polizei.thueringen.de/landeskriminalamt/zentrale-ansprechstelle-cybercrime
		-		
Bundeskriminalamt	+49 611 55-15037			https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html
<p>Quellen: https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html sowie eigene Recherche Informationsstand: 05.12.2025</p>				