Dialog für Cybersicherheit

Ergebnisbericht

des Workstreams

Berichten über Cyber-Vorfälle

Handreichung für Journalist:innen

Dialog für Cybersicherheit

Stand: 28.September 2026

CC-BY-SA 4.0

Dialog für Cybersicherheit

Dieser Bericht dokumentiert den Workstream „Berichten über Cyber-Vorfälle - Eine Handreichung für Journalist:innen“, der von November 2025 bis September 2026 im Rahmen des Dialogs für Cybersicherheit aktiv war.

Eine gut informierte Gesellschaft kann Cyberbedrohungen frühzeitig erkennen und sich auf die richtige Reaktion einstellen oder vorbereiten. Deshalb sollten Journalist:innen, die über Cybersicherheit informieren, befähigt werden, über sicherheitsrelevante Themen korrekt und differenziert zu berichten, um für mehr öffentliches Verständnis der Cybersicherheit zu sorgen. Genau an dieser Stelle setzt der Workstream an und hat eine Handreichung für tagesaktuell arbeitende Journalist:innen erstellt.

Ideengeber:innen des Workstreams: Esther Ecke, Daniel Leisegang (netzpolitik.org), Anja Neubert (Journalistin), Marcel Roth (Journalist), Falk Steiner (Journalist)

Beteiligte Mitarbeiter:innen des Workstreams:
Markus Bieletzki (Stiftung Warentest), Nils Brinker, Stefanie Effner (selbständige Kommunikationsberaterin und Dozentin), Franziska Ehret, Markus Feilner (Journalist), Esther Kern (Brandenburgisches Institut für Gesellschaft und Sicherheit), Janka Kreißl (Dunkelblau GmbH & Co KG), Doris Rehn (BSI), Thilo Roscher, Markus Saborowski (dezentrale e.V., Polis180 e.V.), Vivian Simon (Hrsg. v. Militär&Milchkaffee, Digital-Magazin), Jörg Schneider, Felix Schnellbacher, Kai Schwartz

Der Dialog für Cybersicherheit des Bundesamtes für Sicherheit in der Informationstechnik ist ein partizipativ ausgerichteter gesamtgesellschaftlicher Dialog, um die Vielschichtigkeit der Perspektiven auf das Thema Cybersicherheit möglichst breit und realitätsnah abzubilden und allen Beteiligten einen Austausch bzw. eine Mitwirkung auf Augenhöhe zu ermöglichen.

Der Dialog für Cybersicherheit soll daher ausdrücklich den verschiedenen Meinungen und Ansätzen zur Annäherung an das Thema Cybersicherheit aus Sicht der Zivilgesellschaft Raum und die Möglichkeit zum Austausch geben, ohne dies durch eine engmaschige Steuerung des BSI zu beschränken.

Der vorliegende Bericht wurde von der BSI-Geschäftsstelle und den Workstream-Teilnehmer:innen eigenständig erarbeitet. Die dort wiedergegebenen Ansichten spiegeln nicht zwangsläufig die Ansicht des BSI bzw. aller Teilnehmenden wider.

Weitere Informationen zum Dialog für Cybersicherheit:
https://www.dialog-cybersicherheit.de

Kontakt Geschäftsstelle: projekt-digitalegesellschaft@bsi.bund.de

Lizenz: Dieser Bericht steht unter der Lizenz Creative Commons CC-BY-SA-Lizenz 4.0 International.

Dialog für Cybersicherheit

Inhaltsverzeichnis

1 Einleitung 3
2 Vorgehen 5
3 Ergebnis 7
Handreichung 8
Notfallblatt 9
4 Wie diese Handreichung unterstützen kann 10
5 Wie Berichterstattung gelingt 11
5.1 Tipps zur Recherche 11
5.2 Tipps zur Sprache 17
5.3 Tipps zur Bildsprache 21
6 Glossar 28
6.1 Komprimierte Liste an Begriffen 28
6.2 Quellen für Glossarerläuterungen 36
7 Weiterführende Hilfen und Materialien 37
Anlagen 40
Anlage 1: Fragebogen zu den Bedarfen in den Redaktionen 40
Anlage 2: Fragebogen zur Expert:innenbefragung zur IT-Berichterstattung 43
Anlage 3: Auswertung der Umfragen zu den Bedarfen in den Redaktionen 47
Anlage 4: Auswertung der Expert:innenbefragung zur IT-Berichterstattung 52

1 Einleitung

Die Erfahrung zeigt, dass die Berichterstattung über Cybersicherheitsvorfälle mitunter unter dem hohen Zeitdruck in Redaktionen leidet. Hinzu kommt, dass komplexe technische Vorgänge nicht immer leicht einzuordnen und die richtigen Begrifflichkeiten zu wählen sind. Ziel des Workstreams war es daher, eine Handreichung zu entwickeln, die Journalist:innen und Redaktionen dabei unterstützt, über sicherheitsrelevante Vorfälle korrekt, verständlich und differenziert zu berichten. Damit soll sie zu einem besseren öffentlichen Verständnis für Cybersicherheit und ihre Bedeutung beitragen.

Die Handreichung richtet sich an tagesaktuell arbeitende freie und festangestellte Journalist:innen aller Ressorts – von der überregionalen Publikumspresse über regionale Medien bis zur Lokalredaktion.

Gute Cybersicherheitsberichterstattung folgt denselben journalistischen Grundsätzen wie jeder andere Qualitätsjournalismus: Sie ist klar, korrekt und einordnend. Für das Publikum ist sie nachvollziehbar und relevant. Dazu gehören insbesondere folgende Aspekte:

Sachliche Einordnung: Gute Berichterstattung beschreibt einen Vorfall und seine Folgen so präzise wie möglich: Wer oder welcher Standort ist konkret betroffen? Welche Auswirkungen hat der Vorfall? Was bedeutet er für Menschen in einer Kommune, einem Landkreis oder einem Bundesland, für Beschäftigte, Kund:innen oder andere Betroffene? Worauf müssen sie nun achten und was können sie tun? Ebenso relevant sind die technischen und organisatorischen Zusammenhänge: Auf welchem Weg erfolgte der Angriff? Welche kurz-, mittel- und langfristigen Folgen sind zu erwarten? Welche Gegenmaßnahmen wurden ergriffen? Und wie hätte der Vorfall möglicherweise verhindert oder seine Auswirkungen begrenzt werden können?

Verständliche Sprache: Cybersicherheit ist ein technisches Feld mit zahlreichen Fachbegriffen. Das bedeutet jedoch nicht, dass die Berichterstattung darüber unverständlich sein muss – im Gegenteil. Gute Beiträge erklären Fachbegriffe kurz und anschaulich, ohne Sachverhalte unzulässig zu vereinfachen oder zu verharmlosen. Ziel ist es, die relevanten Fakten auch für technische Laien verständlich zu vermitteln, ohne den Sachverhalt zu verfälschen.

Fokus auf die Betroffenen: Cyberangriffe haben häufig sehr konkrete Auswirkungen auf Menschen: Fahrgäste können keine Bahntickets kaufen, Patient:innen müssen auf Operationen warten, weil diese verschoben werden. Mitarbeitende können vorübergehend nur mit Stift und Papier arbeiten. Solche Perspektiven schaffen Relevanz und Nachvollziehbarkeit. Sie machen greifbar, was ansonsten leicht abstrakt bleibt.

Frühe Einordnung der Angriffsart: Nicht jeder „Cyberangriff“ ist gleich. Sicherheitsvorfälle können ernst sein, unterscheiden sich aber erheblich hinsichtlich Ursache, Umfang

und Folgen. Es macht einen Unterschied, ob die Buchungswebsite der Deutschen Bahn für einige Stunden nicht erreichbar ist oder ob bei einer Krankenkasse sensible Gesundheitsdaten von Tausenden Menschen entwendet wurden. Gute Berichterstattung macht diese Unterschiede deutlich, statt Vorfälle pauschal gleichzusetzen oder zu dramatisieren.

Zu diesen und weiteren Aspekten bietet die vorliegende Handreichung Informationen, Orientierung und praktische Hinweise.

2 Vorgehen

Um die Ziele des Workstreams zu erreichen, wurde für die Laufzeit von November 2025 bis September 2026 gemeinsam ein Projektplan aufgesetzt, der folgende wesentliche Arbeitspakete beinhaltete:

- **Sammeln von Beispielen**
  Im Rahmen der initialen Recherche wurden zunächst Medienbeiträge über Cybersicherheitsvorfälle sowie über Digitalthemen mit Cybersicherheitskomponenten aus der tagesaktuellen Berichterstattung gesammelt. Anschließend wurde analysiert, welche Beispiele gut oder weniger gut umgesetzt wurden. Anhand dieser Analyse wurden Kriterien entwickelt, die eine gelungene Berichterstattung unterstützen sollen.

- **Anonyme Online-Umfragen**
  Da die Handreichung passend für die Zielgruppe entwickelt werden sollte, wurden über eine anonyme Online-Umfrage die fachlichen Voraussetzungen und Bedürfnisse von tagesaktuell arbeitenden Journalist:innen ermittelt. In einer zweiten anonymen Online-Umfrage, die sich an Expert:innen aus Pressestellen, Unternehmen, Verbänden sowie IT-Expert:innen und Datenschützer:innen richtete, wurden Muster und Probleme der gegenwärtigen Berichterstattung ermittelt und eingeschätzt. Die Fragebögen sowie die Auswertung der Antworten sind in den Anlagen (S. 40) dokumentiert.

- **Distribution und Veranstaltungen**
  Über die Workstream-Idee, die Ziele und die Arbeit wurde auf Veranstaltungen berichtet, um zusätzlichen Input zu erlangen. Beispiele hierfür:

  - **Organisation einer Podiumsdiskussion auf der re:publica am 20.5.2026 in Berlin**
    Unter dem Titel „Cyber, Cyber, Hacks, Hacks - Never gonna give up talking about Cyber“ diskutierten Marcel Roth, Anke Domscheit-Berg, Bianca Kastl, Caroline Krohn-Atug, Falk Steiner über das Thema.
  - **Organisation einer Podiumsdiskussion auf der Konferenz Datenspuren am 19.9.2026 in Dresden**
    Unter dem Titel „Cyber, cyber, hacks, hacks - Besser berichten über Cybersicherheit“ sprachen Marcel Roth, Anja Neubert, Jörg Schneider, froque (Markus Saborowski) und Caroline Krohn-Atug.
  - **Aufbau Expert:innennetzwerk und Austauschformate**
    Es gab Gespräche mit dem DJV Berlin, der Deutschen Journalistenschule München und IT-Sicherheitsexpert:innen darüber, inwieweit sich ein Netzwerk aufbauen lässt, das sowohl für aktuelle Anfragen von Journalist:innen als auch für Workshop-Angebote oder niederschwellige (Online-)Gesprächsformate zur Verfügung stehen kann.

- **Entwicklung der Handreichung**
  Die Handreichung wurde auf Basis der Fachexpertise der Teilnehmenden entwickelt. Zudem flossen die aus den Umfragen gewonnenen Erkenntnisse in die Auswahl, Strukturierung und inhaltliche Ausgestaltung der folgenden Empfehlungen ein. Die Ausarbeitung erfolgte im Gesamtworkstream und in kleineren Arbeitsgruppen mit thematischen Schwerpunkten, überwiegend in monatlichen virtuellen Meetings sowie bei zwei Präsenztreffen in Berlin. Die Handreichung ist in diesem Dokument ab Seite 8 zu finden.

3 Ergebnis

Am Ende der über neun Monate dauernden Zusammenarbeit der Workstream-Teilnehmenden wurden folgende Dokumente erarbeitet:

- **Notfallblatt** „Berichten über Cyber-Vorfälle: Berichten über Cyber-Vorfälle: Wer weiß was?“ (S. 9)
- **Die Handreichung** „Berichten über Cyber-Vorfälle – Handreichung für Journalist:innen“ (S. 8), die die Schwerpunkte „Wie gelingt eine gute Berichterstattung?“ sowie konkrete Tipps zur Recherche, Sprache und Bildsprache beinhaltet

Beide Dokumente sollen tagesaktuell arbeitende Journalist:innen dabei unterstützen, in ihrer Berichterstattung Gesamtzusammenhänge besser zu erfassen, die richtigen Nachfragen zu stellen und zuverlässig über IT-Sicherheitsvorfälle zu berichten.

Dialog für Cybersicherheit

Berichten über Cyber-Vorfälle

Handreichung für Journalist:innen

Dialog für Cybersicherheit

Stand: Oktober 2026

Dialog für Cybersicherheit

Notfallblatt
Berichten über Cyber-Vorfälle: Wer weiß was?

Erste Recherchefragen, nachdem Sie von einem IT-Sicherheitsvorfall in Ihrem Berichtsgebiet erfahren haben. Die große Leitfrage kann lauten: Was funktioniert und was funktioniert nicht - und das nicht nur unter technischen Gesichtspunkten! Unsere Empfehlung: IT-Vorfälle eng begleiten und immer wieder nachfragen.

Recherchefragen an die betroffene Organisation

- Welche Systeme sind ausgefallen? Wie reagieren Sie darauf?
- Was heißt das für Ihre Organisation (Standorte, Produktionsausfall, Lieferketten, Beschäftigte)?
- War es ein Angriff oder ein Fehler (extern oder intern)?
- Gilt Ihre Organisation als kritische Infrastruktur (KRITIS)? Müssen/haben Sie den Vorfall an Behörden gemeldet (Landesdatenschutzbehörden, Bundesamt für Sicherheit in der Informationstechnik)?
- Haben Sie Anzeige erstattet?
- Sind personenbezogene Daten betroffen? (Artikel 33 & 34 Datenschutz-Grundverordnung)
- Was empfehlen Sie Ihren Kund:innen und Geschäftspartner:innen?
- Welchen Fragen gehen Sie derzeit nach?
- Bearbeiten Sie den Vorfall gemeinsam mit spezialisierten IT-Dienstleistern (Incident Response/Forensik)? Wie sehen Ihre nächsten Schritte aus?
- Gab es bereits ähnliche Vorfälle in Ihrer Organisation/Ihrem Unternehmen?

Recherchefragen zu den Auswirkungen des Vorfalls

an Mitarbeitende

- Wie arbeiten Sie derzeit? Sind Sie freigestellt, müssen Sie Urlaub nehmen?
- Welche Arbeit können Sie nicht erledigen, wofür brauchen sie Ausweich-Lösungen, wie kommunizieren Sie derzeit?
- Wie sind die Auswirkungen? (Abgleich zu Unternehmensangaben)
- Haben Sie Sorgen, dass Sie Ihr Gehalt nicht bekommen?
- Hat es bereits ähnliche Vorfälle im Vorfeld gegeben?

an Kund:innen oder Bürger:innen

- Was fehlt Ihnen? Wie gehen Sie damit um? Wann haben Sie davon erfahren?
- Welche behördlichen Dienstleistungen können Sie nicht in Anspruch nehmen (Antrag auf Personalausweis, Führerschein o.ä.)?
- Bekommen Sie gerade keine behördlichen Leistungen, auf die Sie Anspruch haben (Wohngeld, Asylleistungen, Grundsicherung o.ä.)? Was heißt das für Ihr Leben?

an Geschäftspartner:innen

- Haben Sie Maßnahmen zum Schutz Ihrer eigenen Systeme ergriffen?
- Wie lange können Sie diesen Zustand mitgehen, ohne sich nach neuen Partnerunternehmen umzusehen?

an IT-Sicherheitsexpert:innen, Datenschützer:innen, Polizei, et al.

- Was empfehlen Sie Kund:innen oder Bürger:innen der betroffenen Organisation, worauf sollten sie achten (Passwortwechsel, Kommunikationskanäle)?
- Gab es schon frühere vergleichbare Vorfälle? Ist es ein Einzelfall?
- Hat sich ein:e Täter:in bekannt?

4 Wie diese Handreichung unterstützen kann

Aus der Perspektive der Betroffenen kann ein IT-Sicherheitsvorfall ein Gefühl von Ohnmacht auslösen. Dabei zeigt sich die Verletzlichkeit von Technik und gesellschaftlichen Institutionen – und zuvorderst die Verletzlichkeit der einzelnen Menschen. Sie stehen im Mittelpunkt des konkreten Geschehens in einer immer stärker von Technik geprägten Welt.

Cyberangriffe und IT-Sicherheitsvorfälle werden jedoch oft als abstrakte Größen oder gar als apokalyptische Erzählung behandelt. In der Bildsprache dominieren beliebige Zahlencodes und Aufnahmen aus Rechenzentren. Übermäßige Dramatik und unreflektierter Alarmismus können dabei zusätzlich verunsichern. Dies verhindert eine nüchterne und realistische Einschätzung der Situation oder aber auch eine nachvollziehbare Einordnung des entsprechenden Vorfalls.

Oftmals entsteht eine Erzählung von der unausweichlichen Macht mysteriöser Angreifergruppen, unabhängig davon, ob sie kriminell oder politisch motiviert sind. Das kann den Angreifer:innen in die Hände spielen. Sie buhlen um Aufmerksamkeit und nutzen ihre Aktionen nicht zuletzt, um sich mit ihren Taten als Marke zu etablieren.

Diese Handreichung soll eine differenzierte Berichterstattung unterstützen und richtet sich vor allem an **tagesaktuell arbeitende Journalist:innen in Publikumsmedien**.

5 Wie Berichterstattung gelingt

Im Folgenden werden zentrale Aspekte einer gelungenen Berichterstattung über IT-Sicherheitsvorfälle betrachtet. Die einzelnen Abschnitte zeigen, worauf bei der Recherche, der sprachlichen Darstellung und der Auswahl von Bildern geachtet werden sollte.

- Das **Notfallblatt** bietet auf einen Blick wichtige Recherchefragen.
- **Abschnitt „Tipps zur Recherche“** beschreibt, welche Fragen im Fall eines IT-Sicherheitsvorfalls an betroffene Organisationen und weitere relevante Stellen gerichtet werden können.
- **Abschnitt „Tipps zur Sprache“** widmet sich dem sprachlichen Umgang mit IT-Sicherheitsvorfällen. Erläutert wird unter anderem, bei welchen Begriffen besondere Sorgfalt geboten ist, welche wiederkehrenden Deutungsmuster auftreten und wie eine verständliche Einordnung gelingt.
- **Abschnitt „Tipps zur Bildsprache“** zeigt, wie eine gute visuelle Darstellung aussehen kann.
- **Kapitel 6** stellt ein **Glossar** mit wichtigen Begriffen zum Nachschlagen bereit.
- **Kapitel 7** verweist auf **weiterführende Hilfen, Materialien und Informationsangebote**.

5.1 Tipps zur Recherche

Die folgenden Absätze liefern einen Überblick über mögliche erste Fragen an betroffene Stellen sowie deren Mitarbeitende, Kund:innen und Partner:innen. Damit Journalist:innen die vorgeschlagenen Fragen und die darin verwendeten Begriffe richtig einordnen können, empfiehlt sich ergänzend ein Blick in das Glossar. Darin werden u.a. unterschiedliche Arten von Cyberangriffen und Vorfällen erläutert und voneinander abgegrenzt, was auch Einfluss auf die Art der Fragen hat.

Nachfragen können sich auch bei der **örtlichen Polizei**, dem **Landeskriminalamt** (**LKA)** oder der **zuständigen Landesdatenschutzbehörde** lohnen. Das sind zu Beginn oft Quellen, die einen Vorfall, eine Anzeige oder eine Meldung bestätigen können.

5.1.1 Erste Beispiel-Fragen, adressiert an Kommunikationsverantwortliche und Führungskräfte im betroffenen Unternehmen/in der Organisation

Allgemeine Infos zum Vorfall

- Wann wurde der Vorfall entdeckt? Wie sind Sie darauf aufmerksam geworden?

- Um welche Art von IT-Vorfall handelt es sich? Ist es ein externer Angriff oder gibt es interne Ursachen?
- Handelt es sich um einen Ransomware-Angriff? Wird Ihr Unternehmen erpresst/wird Lösegeld gefordert? Wenn ja, werden Sie Kontakt zu den Angreifer:innen aufnehmen und in Verhandlungen treten?
- Inwieweit haben Sie einen Notbetrieb aufgenommen, gibt es Behelfslösungen/manuelle Prozesse?
- Was wurde unternommen, um den Vorfall zu stoppen? Wie wurde auf den Vorfall reagiert?

Arbeits-/Betriebsfähigkeit, Erreichbarkeit

- Welche Standorte/Unternehmensbereiche sind betroffen – alle oder nur ein Teil?
- Welche Arbeitsabläufe/-prozesse sind durch den Vorfall derzeit nicht möglich?
- Wie wirkt sich das auf Ihre Kund:innen, Geschäftspartner:innen, Mitarbeiter:innen oder die Bevölkerung aus? (Erreichbarkeit, Produktionsstopp, gestrandete Kund:innen, Kommunikation)
- Was können oder müssen Betroffene (Kund:innen, Bürger:innen, Zulieferer:innen, Mitarbeiter:innen) jetzt tun?
- Wie ist die Prognose zur weiteren Entwicklung und der damit verbundenen Erreichbarkeit Ihrer Dienstleistungen? Bis wann werden die Einschränkungen Ihrer Einschätzung nach anhalten?
- Sind Kommunikationskanäle betroffen, verfügbar und sicher nutzbar (E-Mail, Telefonie)?

Meldepflichten/-fristen

- Fallen Sie unter NIS-2 bzw. ist Ihr Unternehmen Teil der kritischen Infrastruktur (KRITIS)? Wurde der Vorfall bereits an die zuständige/n Behörde/n gemeldet? Wenn nicht, warum nicht?
- Wurde der Vorfall bereits an die zuständige Datenschutzbehörde gemeldet?
- Wurde Anzeige erstattet?

Betroffenheit personenbezogener Daten

- Wurde auf personenbezogene Daten im Sinne der DSGVO zugegriffen?
- Haben die Angreifer:innen personenbezogene Daten im Sinne der DSGVO abgeleitet? Oder: Konnten Angreifer:innen Daten auf ihre eigenen Systeme kopieren?
- Drohen die Angreifer:innen bereits mit einer Veröffentlichung dieser personenbezogenen Daten, läuft ein Countdown?
- Wurden Daten manipuliert, verschlüsselt oder verändert?
- Werden Sie von externen Expert:innen unterstützt?

Hinweis: Für die Angriffsarten **DDoS und Ransomware** gibt es unten noch detaillierte Fragen (siehe Abschnitt „Fragen zum Vorfall DDos“ und Abschnitt „Fragen zum Vorfall Ransomware“).

5.1.2 Erste Beispiel-Fragen, adressiert an Mitarbeitende im betroffenen Unternehmen/in der Organisation und ggf. Informant:innen

Mitarbeitende in betroffenen Organisationen können eine weitere Perspektive auf den IT-Sicherheitsvorfall bieten. Möglicherweise ergeben sich daraus weitere Ansätze für eine anschaulichere Berichterstattung.

- Wann wurden Sie informiert? Von wem?
- Können Sie derzeit wie gewohnt arbeiten?
- Wenn nicht, sind Sie freigestellt worden oder müssen Sie Überstunden abbauen oder Urlaub nehmen?
- Helfen Sie in anderen Abteilungen mit?
- Wissen Sie schon, ob Ihr Lohn/Gehalt pünktlich gezahlt werden kann? Was hat man Ihnen dazu gesagt, wie lange das voraussichtlich dauern wird?
- Hatten Sie Schulungen zu IT-Sicherheit, Awareness-Trainings etc.? Aus heutiger Sicht: Waren diese hilfreich?
- Wie ist die Stimmung im Unternehmen, fühlen Sie sich gut informiert und wissen Sie, was Sie tun bzw. nicht tun sollen oder dürfen?

5.1.3 Mögliche Fragen an nicht beteiligte Expert:innen

Um die Tragweite eines Vorfalls abschätzen und die Angaben der betroffenen Unternehmen/Organisationen abgleichen zu können, können folgende Fragen an Expert:innen gestellt werden:

- Welche Schäden sind für diese Art von Vorfall typisch?
- Kann typischerweise bei dieser Art Vorfall der Verursacher bestimmt werden?
- Ist der Verursacher bereits am Anfang identifiziert oder erst nach intensiverer Untersuchungen?
- Wie lange dauern Einschränkungen bei dieser Art von Vorfall typischerweise an?
- Welche Schritte sind für die Eindämmung der Schäden und Wiederherstellung der Systeme bei dieser Art von Vorfall notwendig und relevant?
- Sind im Rahmen der digitalen Vernetzung möglicherweise auch Partnerunternehmen oder Behörden betroffen?

5.1.4 Mögliche spätere Nachfragen an die Unternehmen, Organisationen und betroffenen Personengruppen

Bei Vorfällen kann sich die Lage immer wieder ändern, und einige Informationen liegen den betroffenen Unternehmen/Organisationen erst nach einer Weile vor. Es lohnt sich also, regelmäßig nachzufragen und Updates zu aktuellen Entwicklungen einzuholen.

Größere IT-Sicherheitsvorfälle können den Betriebsablauf noch Wochen oder Monate nach dem Primärereignis beeinträchtigen. Selbst wenn in einigen Bereichen wieder Normalität hergestellt ist (z. B. Online-Dienste wieder funktionieren), kann es intern weiterhin Behelfslösungen geben, die Wiederherstellung andauern und die Analyse noch nicht abgeschlossen sein. Auch in dieser späteren Phase lohnt es sich, nachzufragen, da betroffene Unternehmen dann oft zugänglicher für Gespräche zu Ursachen sowie zu ergriffenen und geplanten Maßnahmen und Verbesserungen sind.

Aktuelle Bedrohungslage und Erkennung

- Gibt es aktuell noch eine Bedrohungslage?
- Gab es Monitoringsysteme, die den Vorfall angezeigt haben, oder wurde er erst entdeckt, als bereits nichts mehr ging? Konnte der Angriff frühzeitig detektiert und ggf. unterbrochen werden?

Ursache und Angriffsweg

- Was genau war die Ursache für den Vorfall – zum Beispiel ein nicht ordnungsgemäß ausgeführtes Update, eine Fehlkonfiguration, schwaches Passwort, fehlende Multi-Faktor-Authentifizierung?
- Wurde eine bekannte Schwachstelle in einer Software oder einem Gerät ausgenutzt? Wurde eine Schwachstelle ausgenutzt, die zum Vorfallzeitpunkt nicht öffentlich bekannt war (ZeroDay)?
- Haben mögliche Angreifer:innen zuvor erbeutete Daten genutzt (z. B. Passwörter, Interna für Social Engineering, Phishing-Mail)?
- Wurden von Angreifer:innen Techniken des Social Engineerings genutzt? Wenn ja: Waren die Mitarbeitenden geschult, gewarnt und wurde das Mitarbeitertraining regelmäßig aktualisiert? Waren die betroffenen Mitarbeitenden auf dem aktuellen technischen Stand?

Meldepflichten und Zusammenarbeit mit Behörden, betroffene Daten

- Wurden gesetzliche Vorgaben eingehalten? (z. B. Meldung nach DSGVO, Meldepflichten nach Aktiengesetz, NIS-2 oder gesetzliche Regelungen der Länder wie Informationssicherheitsgesetze)
- Wurden personenbezogene Daten im Sinne der DSGVO veröffentlicht oder droht jemand damit, dies zu tun?

Vorsorge und Krisenreaktion

- Mit wem wurde zur Behebung des Vorfalles zusammengearbeitet? (Externe IT-Dienstleister, LKA/BKA, weitere Fachexpert:innen)
- Welche Schutzmaßnahmen gab es vor dem Angriff/dem Vorfall?
- Hatten Sie einen Notfallplan für solche Fälle? Hat er gegriffen bzw. wurde er umgesetzt?
- Gab es Testläufe, was im solchen oder ähnlichen Fällen passiert und wie das Unternehmen darauf reagiert oder reagieren sollte?

Konsequenzen und weitere Maßnahmen

- Welche mittel- und langfristigen Maßnahmen werden ergriffen?
- Warum hat der Vorfall am Ende diese Dimension angenommen?
- Kann sich der Vorfall wiederholen?

5.1.5 Mögliche Fragen für konkrete Angriffsszenarien

Wenn die Art des Vorfalls bekannt ist, kann vorfallspezifisch gefragt werden. Bei anderen Arten können auch Fachexpert:innen helfen, die richtigen Fragen an die Betroffenen zu finden.
Im Folgenden gibt es Fragenkataloge zu diesen Vorfällen.

- Abschnitt zu DDoS
- Abschnitt zu Ransomware

5.1.5.1 Fragen zum Vorfall - Details für DDoS

Bei einem DDoS-Angriff (Distributed Denial of Service) werden angebotene Dienste durch Anfragen überlastet. Das kann einzelne Dienste oder auch die gesamte Außenkommunikation betreffen. Interne Abläufe sind häufig nicht direkt betroffen.

Fragen:

- Welche Dienste oder Angebote sind betroffen und welche nicht? Sind die Dienste gar nicht mehr erreichbar oder nur langsam?
- Gibt es Einschränkungen bei der internen Kommunikation oder Arbeitsweise?
- Sind die Einschränkungen dauerhaft oder sporadisch?
- Wo können sich Kund:innen über den Status informieren, wenn die Website des Unternehmens oder der Behörde ebenfalls betroffen ist?
- Was können Kund:innen tun, wenn sie den Dienst dringend benötigen? Gibt es analoge Alternativen oder Fristaufschübe?
- Sind auch Dritte betroffen, die zum Beispiel Daten des betroffenen Unternehmens nutzen?
- Welche DDoS-Gegenmaßnahmen haben Sie ergriffen – und bis zu welcher Angriffsstärke (z. B. Datenvolumen oder Anzahl Anfragen pro Sekunde) sind diese wirksam? Warum haben die Maßnahmen im konkreten Fall nicht ausgereicht?

5.1.5.2 Fragen zum Vorfall - Details für Ransomware

Bei einem Vorfall mit Ransomware werden in der Regel viele oder alle Daten der betroffenen Organisation verschlüsselt und der Schlüssel nur gegen Zahlung eines Lösegeldes herausgegeben. Inzwischen kopieren die meisten Angreifergruppen die Daten vorher, um zusätzlich mit deren Veröffentlichung drohen zu können, und kontaktieren teilweise Geschäftspartner:innen, Kund:innen und Mitarbeitende telefonisch oder per Mail.

Angreifergruppe, Erpressung und mögliche Lösegeldzahlung

- Wird Ihr Unternehmen erpresst oder wird Lösegeld gefordert? Wenn ja, werden Sie Kontakt zu den Angreifer:innen aufnehmen und in Verhandlungen treten?
- Ziehen Sie eine Lösegeldzahlung in Betracht, um den Decryption Key oder die Entschlüsselungsoftware von den Angreifer:innen zu erhalten und zu nutzen?
- Ziehen Sie eine Lösegeldzahlung in Betracht, um die Veröffentlichung abgeflossener Daten zu verhindern? Wenn nein, warum nicht?
- Wer sind die Angreifer:innen? Mit dieser Information kann das Veröffentlichungsportal der Gruppe identifiziert und so auch unabhängig geprüft werden, ob Daten veröffentlicht wurden.

Wiederherstellung der Systeme

- Können alle Systeme und Daten wiederhergestellt werden?
- Wie lange wird die Wiederherstellung schätzungsweise dauern bzw. wie sieht der Zeitplan aus? Wie wird beim Wiederaufbau priorisiert?
    - Die IT-Systeme werden in der Regel neu aufgesetzt, da auch bei einer Zahlung von Lösegeld für die Entschlüsselung nicht sichergestellt ist, dass die Angreifer:innen nicht doch noch technische „Hintertüren“ eingebaut haben, die einen erneuten Angriff ermöglichen.
    - Für den Wiederaufbau wird oft eine sogenannte Waschstraße aufgebaut: Alle betroffenen Laptops werden formatiert („plattgemacht“) und neu aufgesetzt.
    - Sofern Backups/Datensicherungen nicht verschlüsselt wurden, werden auch diese sorgfältig geprüft und dann wieder eingespielt. All diese Prozesse können Tage bis Wochen, bei großen Organisationen sogar Monate dauern.

Datenabfluss und Veröffentlichung

- Wurde auf Daten zugegriffen? Wenn ja, auf welche Art von Daten?
- Sind (personenbezogene) Daten im Sinne der DSGVO abgeflossen, z. B. von Mitarbeitenden, Kund:innen oder Partner:innen? Wenn ja, welche?
- Drohen die Angreifer:innen bereits mit einer Veröffentlichung dieser Daten? Läuft ein Countdown?
- Wurden bereits Daten veröffentlicht? Wie viele GB/TB/wie groß ist die Menge (auch in Relation zum Gesamt-Datenbestand)?

Information und Schutz der Betroffenen

- Wann und wie kontaktieren bzw. kontaktierten Sie die Betroffenen (Mitarbeiter:innen, Kund:innen, Partner:innen), um sie über die Risiken, die durch den Datenabfluss entstehen, zu informieren?
- Wie sollen bzw. können sich Betroffene jetzt schützen? Müssen sie etwas tun?
    - Z. B. Partnerunternehmen: Verbindung zu gemeinsamen Portalen trennen, Passwörter zurücksetzen etc.?

    - Mitarbeiter:innen, Kund:innen: Kontobewegungen prüfen, Passwörter ändern etc.?
- Haben die Angreifer:innen die Kunden:innen, Lieferant:innen oder Mitarbeitende per Mail oder Telefon kontaktiert und über den Angriff informiert bzw. versucht, die Personen einzuschüchtern oder ebenfalls zu erpressen?

Meldung an Behörden

- Wurde der Vorfall fristgerecht an die zuständigen Behörden gemeldet (z. B. Polizei, Datenschutzaufsicht des jeweiligen Bundeslandes)?
- Wurde Strafanzeige gestellt?

Prinzipien für die Berichterstattung über Ransomwaregruppen
In seinem Buch „Ransom War: How Cyber Crime became a Threat to National Security“ schlägt der Sicherheitsexperte Max Smeets (ETH Zürich) vier Prinzipien für die Berichterstattung über Ransomwaregruppen vor: 1) Accuracy over speed - Genauigkeit kommt vor Geschwindigkeit. 2) Sensible Sprache, die Gruppen nicht glorifiziert, jedoch auch nicht zu einem allzu „gefährlichen“ Image beiträgt. 3) Balance zwischen Berichten über erfolgreiche Angriffe und erfolgreich abgewehrte Attacken. 4) Abwägung bei der Beschreibung technischer Details hinsichtlich des potenziellen Schadens durch Nachahmende und ihrer präventiven Wirkung.

5.2 Tipps zur Sprache

Cybersicherheit ist ein vorwiegend technisches Themenfeld mit vielen Fachbegriffen. Gute Artikel erklären Fachbegriffe kurz und anschaulich. Ziel ist es, vor allem Laien technische Zusammenhänge verständlich zu vermitteln, ohne das Thema zu verfälschen.

Viele Berichte über Cyberangriffe sind mitunter ungenau und tragen nicht ausreichend zur Aufklärung der Leserschaft, Zuschauer:innen und Zuhörer:innen bei. Schlagwörter und Formulierungen wie „Cyberangriff auf die IT-Infrastruktur“, „Angriff auf die digitale Infrastruktur“, „Hacking“ oder schlicht „Cyber“ sagen wenig darüber aus, was tatsächlich passiert ist, und sollten daher um weitere Details ergänzt werden.

5.2.1 Differenzieren

Wissen Menschen nicht, ob eine Website vorübergehend überlastet war oder ob einer Behörde oder einem Unternehmen sensible Daten gestohlen wurden, können sie nicht einschätzen, ob für sie ein Risiko besteht. Unklare Begriffe können entweder unnötige Angst schüren oder tatsächlich schwerwiegende Vorfälle verharmlosen. „DDoS-Attacke auf die Buchungssysteme der Deutschen Bahn“ oder „Ransomware-Angriff auf das Netzwerk des Universitätsklinikums – Patientendaten verschlüsselt“ sind deshalb bessere

Überschriften als „Cyberangriff auf Firma XY“. Der technische Begriff muss dabei nicht vorausgesetzt werden. Er sollte jedoch im Text vorkommen und erklärt werden. Die Angriffsart sollte möglichst früh im Artikel benannt und kurz erläutert werden.

Tipps
• Unterschiedliche Angriffsszenarien nicht unter dem Begriff „Cyberangriff“ zusammenfassen, ohne zu differenzieren. • Ist die Angriffsart zunächst noch unklar, sollte dies explizit kommuniziert werden. Wird die Angriffsart später bekannt, sollte eine Verlaufsberichterstattung folgen. • „Die kriminellen Hacker:innen / Angreifer:innen“ ist besser als „der Hacker“, denn häufig handelt es sich um organisierte Kriminalität.

5.2.2 Obacht bei Begriffen, die Betroffene nutzen

Pressemitteilungen, Statements von Behörden und Polizei sowie Aussagen aus der Privatwirtschaft werden in Berichten über Cybersicherheit mitunter ungeprüft übernommen. Dabei spiegeln sie stets auch die Perspektive und Interessen des jeweiligen Absenders wider. Eine unkritische Übernahme kann die Qualität der Berichterstattung beeinträchtigen.

Konkrete Beispiele für Aussagen, die hinterfragt gehören:

- „In enger Abstimmung mit dem BSI” - Steckt dahinter eine tatsächliche operative Zusammenarbeit oder war es ein kurzes Gespräch am Rande einer Veranstaltung? Hat das BSI den Vorfall bestätigt und eingeordnet?
- „Der Chaos Computer Club (CCC) ist eingebunden” oder „Sicherheitsforscher:innen wurden konsultiert” - Wer genau? In welcher Rolle? Kann die Redaktion das verifizieren?
- „Unser Dienstleister kümmert sich darum” - Was genau tut dieser Dienstleister? Welche Maßnahmen werden ergriffen? Bis wann?

Tipps
• Statements von Behörden und Unternehmen als das behandeln, was sie sind: interessengeleitete Aussagen. • Texte von Presseagenturen vor der Übernahme auf ihre Grundlage hin prüfen: Woher stammen die darin genannten Informationen? • Unabhängige Expertise einholen, etwa von Wissenschaftler:innen, zivilgesellschaftlichen Organisationen oder nicht beteiligten Sicherheitsforscher:innen.

5.2.3 Schuld und Verantwortung

Cyberangriffe haben drei relevante Ebenen: die der Angreifenden, die der Angegriffenen und der dadurch Mitbetroffenen. Alle Ebenen verdienen journalistische Aufmerksamkeit.

Wer hat angegriffen und mit welchem Motiv? Aber auch: Hat das betroffene Unternehmen oder die betroffene Institution die erforderlichen Sicherheitsvorkehrungen getroffen? Wurden branchenübliche Standards eingehalten? Hätte der Angriff durch bessere Prävention abgemildert oder gar verhindert werden können? Oder hätten zumindest die Folgen schneller behoben werden können?

Oft dominiert eine passive Sprache, die betroffene Unternehmen oder Organisationen als hilflose Opfer darstellt: „Die Deutsche Bahn ist von einem DDoS-Angriff betroffen." Dieses Beispiel lässt aber unerwähnt, dass Unternehmen - insbesondere Betreiber kritischer Infrastrukturen - auch Verantwortung für angemessene Präventions- und Schutzmaßnahmen tragen.

Das schließt die Frage ein: War es tatsächlich ein besonders ausgefeilter Angriff oder hat mangelnde Vorbereitung die Folgen verschlimmert? Im Fall des Angriffs auf das Universitätsklinikum Düsseldorf 2020 wurde beispielsweise später bekannt, dass die Angreifer:innen eine bereits bekannte Sicherheitslücke ausnutzen konnten, für die ein Sicherheitsupdate zur Verfügung stand.

Tipps
• Alle Ebenen – Angreifende, Angegriffene und Mitbetroffene - im Blick behalten. • Verantwortlichkeiten präzise benennen und passive Formulierungen nicht unreflektiert übernehmen. Vergleiche etwa: „Die Bahn hatte ihre Server nicht ausreichend gegen DDoS-Angriffe abgesichert" und „Die Bahn wurde Opfer einer DDoS-Attacke".

5.2.4 Frühe und klare Einordnung der Angriffsart

Cyberangriffe sind unterschiedlich. Ob es sich um eine DDoS-Attacke (Systeme vorübergehend überlastet, kein Datendiebstahl), Ransomware (Systeme verschlüsselt, Daten abgeflossen, Lösegeld gefordert) oder einen gezielten Einbruch in Netzwerke handelt, ist für die Einschätzung der Schwere und der Konsequenzen des Vorfalls relevant und sollte benannt werden.

Zu beachten ist, dass Cyberangriffe der gleichen Art unterschiedliche Auswirkungen haben können: Ein stundenlanger Ausfall nach einem DDoS-Angriff auf die Website einer Behörde kann zwar die Außenkommunikation stören, aber nicht deren grundsätzliche Funktionsfähigkeit. Der gleiche Angriff auf den Webshop eines kleinen Unternehmens hingegen kann zu massiven wirtschaftlichen Verlusten und somit zur Existenzgefährdung führen. Eine gute Berichterstattung sollte diese Unterschiede reflektieren, statt pauschal zu dramatisieren.

Zu beachten ist auch: Wie müssen oder sollten sich sekundär Betroffene (z. B. Kund:innen oder Geschäftspartner:innen) verhalten? Welche Rechte haben sie? Wurden sie infor-

miert und wenn ja, wann? Wurden Fristen gewahrt oder sind möglicherweise Schadensersatzansprüche entstanden? Hier können Einschätzungen von IT-Sicherheitsexpert:innen, Daten- und Verbraucherschützer:innen sowie Jurist:innen hilfreich sein.

5.2.5 Unsicherheiten benennen

Gerade wenn ein Sicherheitsvorfall erst wenige Stunden zurückliegt, ist die **Lage oftmals unklar**. Belastbare Informationen liegen dann häufig noch nicht vor, oder betroffene Unternehmen können noch keine Informationen geben, weil sie selbst Zeit für die interne Aufklärung benötigen. Gleichzeitig kann sich die **Lage dynamisch** entwickeln.

Die Recherche und Berichterstattung ist in solchen Situationen von Unsicherheiten geprägt. Deshalb sollten Journalist:innen hier besonders behutsam und besonders genau vorgehen.

Ein besonderes Risiko liegt in der **(Weiter-)Verbreitung von Fehlinformationen**. Erste Gerüchte, etwa in sozialen Medien, können auf unvollständigen Informationen oder einer falschen Wiedergabe von Ereignissen beruhen.

Ebenso ist nicht auszuschließen, dass betroffene Unternehmen oder Behörden mit Formulierungen wie „technische Störung“ oder „Sicherheitsprüfung“ vom **tatsächlichen Geschehen ablenken**. Oftmals benötigen aber auch sie zunächst Zeit, um das tatsächliche Ausmaß eines Vorfalls zu erfassen.

Fehlen belastbare Fakten zu Tathergang und Schadensausmaß, kann der Druck auf die Medien wachsen, **Spekulationen von (vermeintlichen) Expert:innen** ungeprüft zu veröffentlichen.

Redaktionen und Fachleute sollten dabei berücksichtigen, dass falsche Beschuldigungen bezüglich Sicherheitsrisiken oder Datenlecks **rechtliche und politische Konsequenzen** haben können. Auch einzelne Aussagen können rechtlich relevant sein.

Das voreilige Veröffentlichen von Details kann zudem l**aufende IT-Forensik, Verhandlungen bei Erpressungen oder behördliche Ermittlungen** gefährden. Damit sollten Journalist:innen verantwortungsvoll umgehen.

Empfohlenes Vorgehen für Journalist:innen

Journalist:innen sollten **präzise und transparent formulieren**. Sie sollten exakt benennen, was als gesicherte Information gilt. Zum Beispiel sollten sie klar unterscheiden zwischen „System ist nicht erreichbar“ und „Daten wurden gestohlen“. Außerdem sollten sie etwa bei den Presseabteilungen **hartnäckig und zielgerichtet nachfassen**. Sie sollten sich nicht mit ausweichenden Antworten zufriedengeben und konkrete Fragen stellen (z. B. „Sind Kundendaten betroffen?“, „Wann genau wurde der Vorfall bemerkt?“).

Gleichzeitig sollten sich Journalist:innen **nicht ausschließlich auf die Informationen der Presse- bzw. PR-Abteilungen betroffener Unternehmen oder Behörden verlassen**. Es ist sinnvoll, auch Fachleute für Cybersecurity, Betroffene vor Ort oder offizielle Stellen wie das Bundesamt für Sicherheit in der Informationstechnik zu befragen. So erhalten Journalist:innen und Lesende ein umfassenderes Bild.

Bei alledem sollten Journalist:innen ihr Publikum **stets wissen lassen, was derzeit noch unbekannt oder unklar ist** und welche Gründe dies hat. Ein Grund könnte etwa sein, dass die IT-Forensik noch andauert. Damit können Journalist:innen auch der Verbreitung von Gerüchten und Falschinformationen vorbeugen.

Die Berichterstattung über Cyber-Vorfälle sollte bestenfalls **fortlaufend** erfolgen. Werden bereits bestehende (Online-)Berichte aktualisiert, empfehlen wir, Änderungen klar zu kennzeichnen. Alternativ können mehrere, aufeinander aufbauende Beträge erstellt werden.

5.3 Tipps zur Bildsprache

Cybersicherheit ist ein technisches und komplexes Thema, das schwer zu bebildern ist: Kriminelle wollen unentdeckt bleiben. Betroffene Unternehmen oder Organisationen scheuen sich davor, Verletzbarkeit zu zeigen. Sie fürchten um ihre Reputation und vermeiden daher häufig ein öffentliches Auftreten in den Medien.

Journalist:innen nutzen häufig eine ähnliche Bildsprache, z. B. Serverschränke mit Kabeln, Bildschirm mit unverständlichen Zeilen, Zahlenkolonnen oder eine nicht zu erkennende Gestalt im Hoodie vor dem Computer.

Das kann zur Mystifizierung des Angriffs und der Angreifenden führen. Was dabei zu kurz kommt: **Bei Cybersicherheit geht es vor allem um Bürger:innen des Gemeinwesens bzw. um Mitarbeitende, Kund:innen und Partner:innen von Unternehmen**. Ziel einer vermittelnden Bildsprache ist es, den Vorfall für Leser:innen verständlicher und greifbarer zu machen und ihnen relevante Informationen zu möglichen Schutzmaßnahmen zu vermitteln.

5.3.1 Konkrete Vorschläge

Bei Cybersicherheit geht es letztlich um Menschen und konkrete Folgen, die für sie entstehen. Dies sollte sich auch in der Bildsprache wiederfinden. Dabei sollten möglichst authentische Bilder von vor Ort statt KI-Kollagen zum Einsatz kommen. Im Folgenden einige Beispiele:

- Eine Reha-Klinik ist Opfer einer Cyber-Attacke geworden. Zeigen Sie ein Bild der Reha-Klinik oder Menschen, die zum Beispiel am Rollator gehen (aus Gründen des Persönlichkeitsschutzes bitte von hinten).

- Eine Cyber-Attacke legt die IT einer staatlichen Kunstsammlung lahm. Nutzen Sie ein Bild der enttäuschten Besucher:innen, die vor der Eingangstür stehen.

- Wird bei Unternehmen auf „Notbetrieb“ umgestellt, z. B. mit einer Bargeld-Kassette oder handgeschriebenen Aushängen - zeigen Sie diese.

- Bei Ransomware-Vorfällen können Expert:innen ggf. Bildmaterial zuliefern.

- Eine Quelle für Screenshots bietet die Seite https://ransomware.live

Neben den Betroffenen lässt sich auch die **Motivation der Cyber-Kriminellen** illustrieren.

- Bei einem **Ransomware-Angriff** wäre eine Bildcollage denkbar, z. B. aus der betroffenen Region oder dem Unternehmen in Kombination mit einem echten Erpresserschreiben oder dem stilisierten Wort „ERPRESSUNG“.

- **Cyberspionage** spielt sich nicht für das bloße Auge sichtbar ab. Hier können symbolische Darstellungen zum Einsatz kommen, z. B. eine Hand ragt mit einer Lupe aus dem Computer und untersucht neben der Tastatur liegende Dokumente.

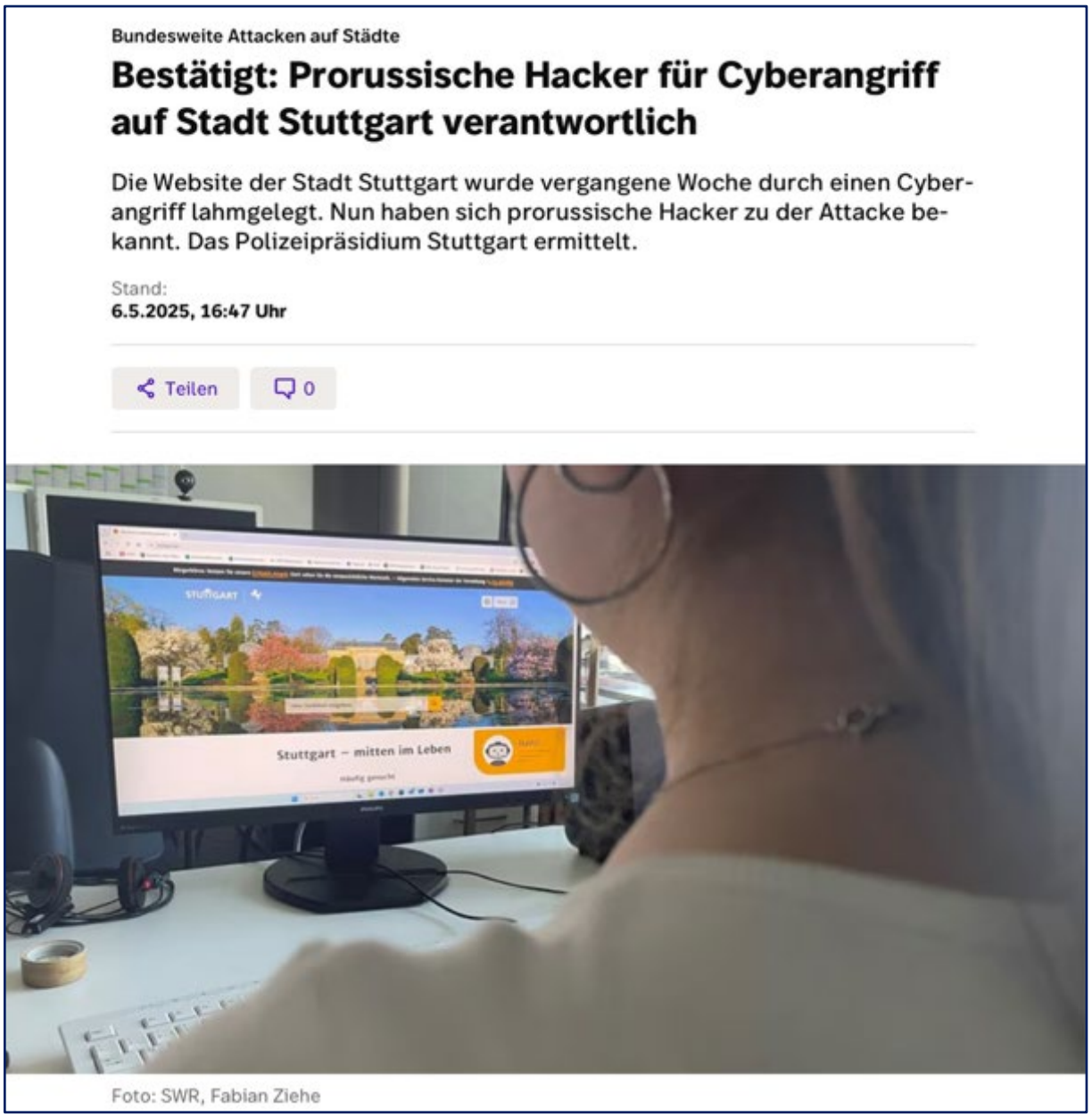
Verdeutlichen Sie die Folgen für Betroffene, indem Sie abstrakte Zahlen anschaulich übersetzen, z. B. durch Vergleiche mit der Fläche von Archiven oder der Länge von Bücherregalen, die nicht mehr zugänglich sind.

Neben den Betroffenen gibt es auch Menschen, die als „Rettungsteam“ die Herausforderungen bewältigen und die Folgen des Cybervorfalls begrenzen. Optimal wäre es, den Krisenstab oder IT-Dienstleister bei der Arbeit zu zeigen, z. B. gemeinsam in einem Raum. Die Chancen, dass dies gelingt, sind allerdings erfahrungsgemäß gering. Haben Sie Verständnis für betroffene Unternehmen, Behörden oder andere Organisationen, wenn sie in einer solchen Ausnahmesituation keinen Zugang gewähren.

5.3.2 Beispiele für gelungene Bebilderung

Im Folgenden werden ausgewählte Screenshots aus journalistischen Beiträgen zitiert, die Beispiele für eine gelungene Bebilderung von IT-Sicherheitsvorfällen darstellen.

Positivbeispiel für die Bebilderung: Die Bildmontage stellt die betroffene Stadt Berlin durch die zentrale Berlin-Symbolik in den Mittelpunkt und schafft damit unmittelbar einen lokalen Bezug zum Vorfall. Gleichzeitig vermittelt die originelle und aufmerksamkeitsstarke Gestaltung die digitale Dimension des Ereignisses: Die im Hintergrund dargestellten Binärziffern („0“ und „1“) und der farblich in Komplementärkontrasten dargestellete Glitch-Effekt stellen einen klaren Bezug zu IT und Daten her und lassen den Kontext eines IT-Sicherheitsvorfalls unmittelbar erkennen. Die Stadt Berlin ist ins wanken geraten, es gab eine reale Verzerrung. Damit verbindet die Bebilderung die konkrete Betroffenheit vor Ort mit dem zunächst abstrakten Thema eines Datenlecks und weckt zugleich Interesse am Beitrag.
Quelle: Screenshot aus: Donheiser, Max & Nina Breher: „Das Berliner Datenleck in Grafiken: Wie viele Menschen betroffen und welche Dateien brisant sind“, Tagesspiegel. Bild: © [M] Tagesspiegel/Material: IMAGO / NurPhoto. Zuletzt abgerufen am 11. September 2026, hier: https://www.tagesspiegel.de/interaktiv/das-berliner-datenleck-in-grafiken-wie-viele-menschen-betroffen-und-welche-dateien-brisant-sind-16021746.html;
Weitere Beispiele gelungener grafischer Aufbereitung finden sich hier: https://www.tagesspiegel.de/berlin/rekonstruktion-des-berliner-hackerangriffs-wahrend-das-ultimatum-verstreicht-durchsuchen-mitarbeiter-per-hand-dokumente-16023082.html; https://www.nzz.ch/deutschland/politik/144-millionen-dateien-veroeffentlicht-die-folgen-des-hackerangriffs-auf-berlin-koennten-gravierend-sein-ld.10022627



Positivbeispiel für die Bebilderung: Die Aufnahme zeigt über die Schulter einer Person den Blick auf einen Bildschirm, auf dem die Webseite der Stadt Stuttgart zu sehen ist. Dadurch wird der Cyberangriff mit seinem konkreten Ziel verknüpft und für Betrachter:innen unmittelbar greifbar. Die Perspektive stellt zugleich den Bezug zwischen Mensch und betroffenem digitalem Angebot her und erleichtert die Perspektivübernahme.

Quelle: Screenshot aus: Ziehe, Fabian; Neuhausen, Verena & Spöcker, Christian: „Bestätigt: Prorussische Hacker für Cyberangriff auf Stadt Stuttgart verantwortlich“, *SWR*. Foto: SWR, Fabian Ziehe. Zuletzt abgerufen am 16. September 2026. https://www.swr.de/swraktuell/baden-wuerttemberg/stuttgart/hackerangriff-auf-website-stadt-stuttgart-pro-russische-hacker-cybercrime-100.html .

Ein weiteres Beispiel für den „Blick über die Schulter“ findet sich hier: https://www.polizei.hessen.de/praevention/beratung-hilfe-und-unterstuetzung/betrugsdelikte/betrugsmasche-ceo-fraud

Positivbeispiel für die Bebilderung: Die Bildmontage verbindet den konkreten Unternehmensbezug, unter anderem durch die Darstellung eines Volkswagen-Werks, mit der persönlichen Dimension des Datenlecks. Eingeblendete Begriffe wie „Last Name“, „First Name“ und „Phone Number“ veranschaulichen, welche personenbezogenen Informationen von einer Datenpanne betroffen sein können. Dadurch wird das abstrakte Thema Datenleck greifbarer und der mögliche Bezug zum Leben einzelner Menschen sichtbar. Die Bebilderung vermittelt somit nicht nur den technischen Vorfall, sondern unterstützt Leser:innen dabei, dessen mögliche Bedeutung und Auswirkungen nachzuvollziehen.
Quelle: Screenshot aus: Beuth, Patrick; Flüpke; Hoppenstedt Heinrichs, Max; Kreil, Michael; Rosenbach, Marcel & Wilkin, Rina: „Wir wissen, wo dein Auto steht“, *DER SPIEGEL*. Bildunterschrift: „Volkswagen-Datenpanne: Rückschlüsse auf das Leben der Menschen am Lenkrad“. Foto/Montage: [M] DER SPIEGEL; Fotos: Paul Langrock, Thomas Starck /

AUTO BILD, picture alliance / dpa / Audi AG. Zuletzt abgerufen am 16. September 2026. https://www.spiegel.de/netzwelt/web/volkswagen-konzern-datenleck-wir-wissen-wo-dein-auto-steht-a-e12d33d0-97bc-493c-96d1-aa5892861027

Flughäfen in Europa

Auch Sonntag Wartezeiten nach Cyberattacke an Flughäfen

Nach einem Cyberangriff auf eine Flughafensoftware müssen Passagiere sich länger gedulden. In Deutschland ist von der Attacke Berlin betroffen.

Quelle: DIE ZEIT, AFP, dpa, hoe 21. September 2025, 5:55 Uhr

▶ 3 Min. 73 Zusammenfassen

Passagiere warten in einem Terminal am Berliner Flughafen. Nach einem Cyberangriff auf einen Softwareanbieter gibt es am BER weiterhin Einschränkungen. © picture alliance/dpa | Carsten Koall

Positivbeispiel für die Bebilderung: Die Aufnahme zeigt wartende Passagier:innen am Berliner Flughafen und macht damit die konkreten Auswirkungen des IT-Sicherheitsvorfalls sichtbar. Es rücken die tatsächlich betroffenen Menschen und die Folgen für ihren Alltag in den Mittelpunkt.
Quelle: Screenshot aus: DIE ZEIT, AFP, dpa, hoe: „Auch Sonntag Wartezeiten nach Cyberattacke an Flughäfen“, *DIE ZEIT*, 21. September 2025. Foto: picture alliance/dpa | Carsten Koall. Zuletzt abgerufen am 16. September 2026, hier: https://www.zeit.de/digital/2025-09/cyberattacke-flughaefen-check-in-luftverkehr-verspaetung

Ein weiteres Beispiel für die bildliche Verdeutlichung der Betroffenenperspektive findet sich hier: https://www.spiegel.de/netzwelt/miniatur-wunderland-in-hamburg-daten-schuetzer-raet-nach-hackerangriff-zu-vorsicht-a-f814ad95-f3ea-4de4-8b8f-7b0ff0553690

6 Glossar

Wer zu Cybersicherheit und konkret zu IT-Sicherheitsvorfällen recherchiert, stößt schnell auf Fachbegriffe und Abkürzungen, die den Zugang zum Thema erschweren können. Dieses Glossar erklärt verständlich und praxisnah die gängigsten technischen Begriffe aus diesem Bereich. Das Wörterverzeichnis erhebt keinen Anspruch auf Vollständigkeit, sondern versteht sich als Orientierungshilfe: Es soll Journalist:innen dabei unterstützen, relevante Informationen für die eigene Einordnung eines Falls zu erkennen und einzuschätzen, an wen sie sich für kompetente Auskünfte wenden können.

Ergänzend zu dieser Handreichung wurde deshalb ein Glossar entwickelt, das zentrale Begriffe aus dem Bereich der IT-Sicherheitsvorfälle verständlich definiert und erläutert. Das Glossar kann auch unter folgendem Link abgerufen werden: https://cooperation.dialog-cybersicherheit.de/s/B3LDfREpjwQJCtc

6.1 Komprimierte Liste an Begriffen

Agentic AI
Agentic AI bezeichnet KI-Systeme, die Aufgaben selbstständig planen und ausführen können. Sie treffen dabei innerhalb vorgegebener Grenzen eigenständig Entscheidungen.
Solche Systeme werden oft mit Chatbots verwechselt. Agentic AI reagiert jedoch nicht nur, sondern agiert proaktiv und passt ihre Strategie selbstständig an.
Sie können die IT-Sicherheit verbessern, aber auch Angriffe beschleunigen. Ihre Bedeutung für die Cybersicherheit nimmt derzeit deutlich zu.

Advanced Persistent Threat (APT)
Ein APT ist ein gezielter und langfristig angelegter Cyberangriff. Die Angreifer:innen versuchen, möglichst lange unentdeckt in einem IT-System zu bleiben. APTs richten sich häufig gegen Behörden, Unternehmen oder kritische Infrastrukturen. Sie grenzen sich von Cyberangriffen im Allgemeinen durch hohe Professionalität, Ressourcenstärke und eine langfristige Verweildauer im Netzwerk ab. Meist dienen sie der Spionage oder Sabotage und nicht der schnellen Erpressung. Bei dieser Art von Angriffen gibt es anfangs häufig keine öffentlich sichtbaren Einschränkungen, obwohl bereits Informationen ausgeleitet werden.

Advanced-Persistent-Threat-Gruppe (APT-Gruppe)
Eine Advanced-Persistent-Threat-Gruppe (APT-Gruppe) ist eine professionell organisierte Angreifergruppe, die gezielt bestimmte Organisationen oder Staaten über einen längeren Zeitraum ausspäht oder angreift.
Häufig wird die APT-Gruppe staatlichen oder staatlich unterstützten Akteur:innen zugerechnet. Allerdings ist eine solche Zuordnung nicht immer sicher nachweisbar.

Awareness
Awareness beschreibt die Wachsamkeit und das Sicherheitsbewusstsein etwa von Beschäftigten. Sie hilft dabei, Risiken zu erkennen und auf verdächtige Situationen richtig zu reagieren.
Viele Sicherheitsvorfälle beginnen mit menschlichen Fehlern. Deshalb ist Awareness wichtig, damit es erst gar nicht zu Sicherheitsvorfällen kommt.

Backup und Recovery
Ein Backup ist eine Sicherheitskopie von Daten. Recovery bezeichnet die Wiederherstellung von Daten und Systemen nach einem Ausfall oder Angriff.
Backups sind eine reaktive Maßnahme zur Schadensminimierung, wohingegen Datensicherheit den präventiven Schutz vor Manipulation und Verlust umfasst. Funktionierende Backups sind oft entscheidend, um nach einem Sicherheitsvorfall den Betrieb schnell wieder aufnehmen zu können. Daten sollten regelmäßig gesichert werden und die Backups in mehrfacher Kopie vorliegen. Eine Wiederherstellung des Backups sollte ebenfalls regelmäßig getestet werden.

Business E-Mail Compromise (BEC)
Beim Business E-Mail Compromise täuschen Angreifer:innen vertrauenswürdige E-Mails vor. Sie verfolgen damit das Ziel, an Geld oder vertrauliche Informationen zu erlangen. Konkret sollen die E-Mails etwa Mitarbeitende dazu verleiten, Überweisungen zu tätigen oder Daten herauszugeben.
BEC gehört weltweit zu den wirtschaftlich erfolgreichsten Betrugsformen. Oft werden dabei keine Schadprogramme eingesetzt, weshalb technische Filter auch nur eingeschränkt helfen. Anders als Spam sind BEC als spezifische Form des Social Engineering personalisiert und zielgerichtet.

Cyberangriff
Ein Cyberangriff ist ein gezielter Versuch, IT-Systeme oder Daten anzugreifen, zu manipulieren oder unbefugt darauf zuzugreifen.
Der Begriff sollte nur verwendet werden, wenn tatsächlich ein absichtlicher Angriff vorliegt. Nicht jeder IT-Ausfall ist ein Cyberangriff. So kann ein IT-Sicherheitsvorfall auch durch menschliche Fehler oder technische Defekte ohne Angriffsabsicht entstehen. Gleichzeitig ist ein Cyberangriff in der Regel mehr als ein technischer Sabotageakt, da er auch Spionage, Datendiebstahl und Erpressung umfasst.

Cybersicherheit
Cybersicherheit umfasst den Schutz von IT-Systemen, Netzwerken, Programmen, digitalen Diensten und Daten vor Angriffen und Missbrauch im global vernetzten Datenraum. Der Begriff wird oft deckungsgleich mit IT-Sicherheit verwendet, er bezieht allerdings den gesamten vernetzten Raum ein. Informationssicherheit umfasst hingegen den Schutz von Informationen jeglicher Art, auch auf Papier.

Datenabfluss
Datenabfluss bedeutet, dass vertrauliche Informationen unbefugt kopiert oder weitergegeben werden. Das kann personenbezogene Daten, Unternehmens- oder Betriebsdaten betreffen.
Ob Daten abgeflossen sind, ist oft wichtiger als der Angriff selbst. Davon hängen Meldepflichten, mögliche Schäden und Strafen ab (DSGVO). Der physische Verlust von Datenkontrolle ist etwas anderes als eine Datenschutzverletzung, bei der gegen Datenschutzgesetze verstoßen wird.

Datenschutzverletzung
Eine Datenschutzverletzung liegt vor, wenn personenbezogene Daten verloren gehen, verändert oder unbefugt offengelegt werden. Sie löst gesetzliche Pflichten (wie die Meldepflicht gemäß DSGVO) aus und kann schwere Bußgelder nach sich ziehen.
Der Begriff stammt aus dem Datenschutzrecht. Eine Datenschutzverletzung liegt nicht nur dann vor, wenn Daten gestohlen werden, sondern auch wenn Daten unberechtigt gelöscht oder eingesehen werden.

Datensicherheit
Datensicherheit umfasst technische und organisatorische Maßnahmen zum Schutz von Daten vor Verlust, Veränderung oder unbefugtem Zugriff.
Datensicherheit schützt alle Arten von Daten. Sie ist die technische Grundlage für Informationssicherheit und Datenschutz.

DDoS (Distributed Denial of Service)
Bei einem DDoS-Angriff werden Onlinedienste durch sehr viele gleichzeitige Anfragen überlastet. Durch die gezielt herbeigeführte Überlast ist das Online-Angebot zwar sichtbar eingeschränkt (Webseiten oder Anwendungen zeitweise nicht erreichbar), es fließen jedoch keine Daten ab. Interne Systeme funktionieren meist uneingeschränkt. DDoS-Angriffe zielen also meist auf die Verfügbarkeit von Diensten und führen nicht automatisch dazu, dass Daten gestohlen oder Systeme übernommen werden. Ziel ist meist Sabotage oder Erpressung. Eine technische Zuordnung ist in der Regel nur schwer möglich. Viele Zuordnungen basieren auf Bekennerschreiben und teilweise sehr vagen Indizien.

Defense in Depth
Defense in Depth bedeutet, dass mehrere Sicherheitsmaßnahmen kombiniert werden. Fällt eine Schutzmaßnahme aus, greifen weitere Schutzebenen (gestaffelte Verteidigung).
Das Prinzip soll verhindern, dass ein einzelner Fehler, etwa das Versagen einer Firewall, sofort zu einem schweren Sicherheitsvorfall führt, etwa der vollständigen Kompromittierung eines Netzwerks. Es ist ein Grundprinzip moderner IT-Sicherheit und umfasst Technologie, Prozesse und die Awareness der Menschen.

Einfallsvektor/Indicator of Compromise (IoC)
Der Einfallsvektor/IoC beschreibt den Weg, über den Angreifer:innen in ein IT-System gelangen. Häufig geschieht dies über Phishing, Schwachstellen oder gestohlene Zugangsdaten.
Die Kenntnis des Einfallsvektors hilft, einen Angriff zu verstehen und geeignete Schutzmaßnahmen ab- und einzuleiten. Zum Beispiel ist die E-Mail der Vektor, die Unachtsamkeit des Mitarbeitenden die Schwachstelle.

Exploit
Ein Exploit ist eine Methode oder ein Programm, mit dem eine Schwachstelle in Software oder Systemen ausgenutzt wird.
Ein Exploit wird oft mit einer Schwachstelle gleichgesetzt. Der eingesetzte Schadcode (s. auch Malware) ist aber so etwas wie ein aktiver Angriffsbaustein, mit dem eine Schwachstelle in einem System ausgenutzt wird.

Forensik, auch IT-Forensik
IT-Forensik untersucht digitale Spuren nach einem Sicherheitsvorfall. Sie soll klären, was passiert ist, wann es passiert ist und wer beteiligt war. Forensik hilft bei der Aufklärung von Angriffen. So lassen sich das Ausmaß eines Angriffs besser verstehen, Beweise etwa für Gerichtsverfahren sichern und künftige Angriffe verhindern.

Hacker:innen und Hacking
Hacking bezeichnet das technische Untersuchen, Verändern oder Eindringen in IT-Systeme. Hacker:innen können dabei legal oder illegal handeln.
Der Begriff „Hacker:in“ ist nicht per se negativ. Sicherheitsforschende nutzen ähnliche Methoden, um Schwachstellen zu finden und zu beheben. Generell werden böswillige Hacker:innen ("black hat") von gutwilligen Hacker:innen ("white hat") unterschieden.

Incident Response
Incident Response bezeichnet die geplante, strukturierte Reaktion auf einen IT-Sicherheitsvorfall. Dazu gehören Erkennung, Eindämmung, Beseitigung und Wiederherstellung.
Ein Incident Response ist ein unverzichtbarer Teil des Notfallmanagements, um im Ernstfall Chaos zu verhindern und die Ausfallzeiten so kurz wie möglich zu halten. Backup und Recovery regeln die anschließende technische Wiederherstellung.

Informationssicherheit
Informationssicherheit schützt Informationen jeglicher Art (digital, auf Papier oder in den Köpfen) vor Verlust, Manipulation und unbefugtem Zugriff.
Informationssicherheit ist das übergeordnete Schutzziel im Risikomanagement einer Organisation, das über die reine IT hinausgeht. Der Begriff schließt IT-Sicherheit (Fokus auf Systeme) und Cybersicherheit (Fokus auf das Netz) als Teilbereiche ein.

IT-Grundschutz
IT-Grundschutz ist eine vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelte Methode zum Aufbau eines angemessenen Sicherheitsniveaus.
Der Ansatz wird besonders von Behörden und Unternehmen genutzt, um Sicherheitsmaßnahmen systematisch zu planen und umzusetzen. Er basiert auf der internationalen Norm ISO 27001, konkretisiert diese aber durch detaillierte und praxisnahe Maßnahmenkataloge.

IT-Sicherheitsvorfall
Ein IT-Sicherheitsvorfall ist ein Ereignis, das die Vertraulichkeit, Integrität oder Verfügbarkeit von IT-Systemen beeinträchtigt.
Der Begriff ist der Oberbegriff für Cyberangriffe, aber auch für technische Fehler, Fehlkonfigurationen oder Bedienfehler. Auch ein Serverraum-Brand oder das versehentliche Löschen wichtiger Datenbanken ist ein IT-Sicherheitsvorfall.

IT-Sicherheit
IT-Sicherheit umfasst Maßnahmen zum Schutz von IT-Systemen, Netzwerken und Anwendungen vor Störungen, Missbrauch und Angriffen.
Sie ist ein Teilbereich der Informationssicherheit und konzentriert sich auf technische Systeme und deren Schutz.

ISO 27001
ISO 27001 ist eine internationale Norm für den Aufbau eines Informationssicherheits-Managementsystems (ISMS).
Die Norm beschreibt Anforderungen an Prozesse, Verantwortlichkeiten und Maßnahmen, mit denen Organisationen Informationssicherheit systematisch verbessern können. Unternehmen nutzen diese Zertifizierung, um Kunden und Regulierungsbehörden ein standardisiertes, hohes Sicherheitsniveau nachzuweisen.

Kill Chain
Die Kill Chain beschreibt die verschiedenen Schritte und Phasen eines Cyberangriffs, von der Vorbereitung über die Ausspähung bis zur Umsetzung des Angriffs und der Vollendung des Schadens.
Das Modell hilft dabei, Angriffe besser zu verstehen und Schutzmaßnahmen an verschiedenen Stellen der Angriffskette aufzubauen.

Lateral Movement
Lateral Movement bezeichnet die Bewegung eines Angreifenden innerhalb eines bereits kompromittierten Netzwerks.
Angreifer:innen nutzen diese Technik, um weitere Systeme zu erreichen, Rechte auszuweiten und wertvolle Daten zu finden. Lateral Movement folgt zeitlich auf den erfolgreichen Einfallsvektor und dient dazu, den Angriff innerhalb der Kill Chain auszuweiten.

Malware (Schadsoftware)
Malware ist ein Sammelbegriff für Programme, die Systeme beschädigen, überwachen oder unbefugt Daten verarbeiten.
Zu Malware gehören unter anderem Ransomware, Trojaner und Spionageprogramme. Sie ist ein häufiger Bestandteil von Cyberangriffen. Ein Computervirus ist eine Untergruppe moderner Schadsoftware.

Meldepflicht
Eine Meldepflicht verpflichtet Organisationen dazu, bestimmte Sicherheitsvorfälle an Behörden oder betroffene Personen zu melden.
Ob eine Meldung erforderlich ist, hängt vom Vorfall, den betroffenen Daten und den geltenden gesetzlichen Regelungen ab. Die Maßnahme dient der Transparenz und ermöglicht es Aufsichtsbehörden (zum Beispiel dem BSI oder Datenschutzbeauftragten), das allgemeine Bedrohungsniveau zu überwachen.

Metadaten
Metadaten sind Informationen über Daten, zum Beispiel Erstellungszeit, Speicherort oder Absender einer Datei.
Metadaten sind keine harmlosen Daten. Sie können vertrauliche Informationen enthalten und für Angreifende wie auch Ermittler:innen relevant sein. Aus ihnen lassen sich präzise Verhaltensprofile erstellen. In der Forensik werden sie zur Rekonstruktion genutzt, um bei einer Datenschutzverletzung festzustellen, wann und wie Daten abgeflossen sind.

Notbetrieb
Notbetrieb ist der zeitlich begrenzte, kontrollierte Betriebszustand nach einem schwerwiegenden IT-Ausfall oder Cyberangriff.
Er beginnt in der Regel nach der unmittelbaren Eindämmung eines Vorfalls und dauert an, bis der reguläre Betrieb sicher wiederhergestellt ist. Während dieser Übergangsphase werden nur kritische Geschäftsprozesse und IT-Dienste mit meist eingeschränkter Funktionalität aufrechterhalten.

Phishing
Phishing bezeichnet den Versuch, durch gefälschte Nachrichten an vertrauliche Informationen wie Passwörter oder Zugangsdaten zu gelangen. Es ist eine Form des Social Engineerings und einer der häufigsten Wege, über den Angreifer:innen in Unternehmen oder private Konten eindringen. Phishing ist einer der häufigsten und erfolgreichsten Einfallsvektoren für Ransomware- und Spionageangriffe.

Privacy by Default
Privacy by Default bedeutet, dass Systeme standardmäßig datenschutzfreundliche Einstellungen verwenden. Der Begriff bezieht sich auf die Standard-Vorauswahl der Einstellungen bei der Auslieferung, nicht auf die strukturelle Architektur.

Privacy by Design
Privacy by Design bedeutet, dass Datenschutz und der Schutz der Privatsphäre bereits bei der Entwicklung von IT-Systemen, Software oder Prozessen von Anfang an strukturell berücksichtigt wird.
Der präventive Qualitätsansatz soll verhindern, dass Datenschutzmaßnahmen nachträglich ergänzt werden müssen. Er bildet die architektonische Grundlage, aus der die datenschutzfreundlichen Voreinstellungen von Privacy by Default resultiert.

Ransomware/Ransomware-Angriffe
Ransomware ist Schadsoftware, mit der Angreifende Daten auf einem IT-System verschlüsseln oder von dort stehlen, um vom Opfer anschließend ein Lösegeld für die Freigabe zu fordern. Ransomware gehört zu den häufigsten und folgenreichsten Cyberbedrohungen für Unternehmen und öffentliche Einrichtungen. Es ist eine spezialisierte Unterform von Malware, die im Gegensatz zu reiner Spionage-Schadsoftware auf sofortige Erpressung setzt.
Bei Ransomware-Angriffen wird in der Regel automatisch ein Erpresserschreiben auf den betroffenen Systemen abgelegt, über das die Angreifergruppe häufig identifizierbar ist. Es gibt allerdings auch Trittbrettfahrer, die sich als bekannte Angreifergruppen ausgeben. Eine eindeutige Zuordnung der Tat gelingt selten und oftmals erst nach aufwändigen digital-forensischen Untersuchungen.

Risikobewertung (Risk Assessment)
Eine Risikobewertung untersucht, wie wahrscheinlich ein Schaden ist und wie groß seine möglichen Auswirkungen sein können.
Sie ist das Fundament für jedes Sicherheitsmanagementsystem (siehe: ISO 27001), um Ressourcen dort einzusetzen, wo die Gefahren am größten sind. Sie hilft Organisationen, Sicherheitsmaßnahmen dabei, zu priorisieren und Risiken gezielt zu reduzieren.

Root Cause Analysis (Ursachenanalyse)
Die Root Cause Analysis untersucht systematisch die eigentliche Ursache eines Sicherheitsvorfalls und nicht nur seine sichtbaren Folgen.
Die Methode behandelt nicht nur die Symptome, sondern geht an die Wurzel eines Sicherheitsvorfalls. Damit sollen Fehler dauerhaft behoben und ähnliche Vorfälle in Zukunft verhindert werden. Sie stützt sich somit auf die Resultate der IT-Forensik, zielt aber strategisch darauf ab, die zugrundeliegende Schwachstelle nachhaltig zu beheben.

Schwachstelle
Eine Schwachstelle ist eine Sicherheitslücke in Software, Hardware oder Prozessen, die Angreifende ausnutzen können.
Schwachstellen sind häufig die Grundlage für erfolgreiche Cyberangriffe. Sie werden erst dann gefährlich, wenn ein passender Exploit existiert und angewendet wird. Nicht jede Schwachstelle wird tatsächlich ausgenutzt.

Social Engineering
Social Engineering bezeichnet die gezielte Manipulation von Menschen, um Informationen, Zugänge oder andere Vorteile zu erlangen.
Da technische Hürden immer höher werden, greifen Angreifer:innen vermehrt den “Faktor Mensch" über Social Engineering an. Angreifer:innen nutzen dabei Vertrauen, Hilfsbereitschaft oder Unachtsamkeit mit Hilfe psychologischer Tricks aus. Social Engineering ist der Oberbegriff, unter den spezifische Methoden wie Phishing oder Business E-Mail Compromise fallen.

Stand der Technik
Der Stand der Technik beschreibt das Sicherheitsniveau, das nach aktuellem Wissen und verfügbaren Methoden als angemessen gilt.
Der Begriff dient häufig als Maßstab, um zu bewerten, ob Schutzmaßnahmen ausreichend sind. Als rechtlich-technisches Mindestniveau verlangt er nach Praxiserprobung und nachgewiesene Zuverlässigkeit.

Triple Extortion
Triple Extortion bezeichnet eine Ransomware-Strategie mit drei Druckmitteln: 1. Verschlüsselung der Systeme, 2. die Drohung, gestohlene Daten zu veröffentlichen, 3. direkte Erpressung von Dritten wie Kunden/Partnern oder Androhung von DDoS-Angriffen.
Angreifende wollen mit Triple Extortion den Erpressungsdruck auf Unternehmen, Kund:innen oder Geschäftspartner:innen erhöhen. Triple Extortion wird oft fälschlicherweise für einen normalen Ransomware-Angriff gehalten, erweitert diesen aber um zusätzliche Erpressungselemente.

TTP (Tactics, Techniques and Procedures)
TTP beschreibt die Vorgehensweisen, Methoden und Werkzeuge, die Angreifende bei Cyberangriffen nutzen.
Die Analyse von TTP hilft Sicherheitsfachleuten, Angriffe zu erkennen und besser abzuwehren. TTP beschreibt das individuelle Verhalten der Angreifenden, während die Kill Chain den allgemeinen Ablauf eines Angriffs strukturiert.

Zero-Day (auch “Zero-Day-Schwachstelle” und “Zero-Day-Exploit”)
Ein Zero-Day bezeichnet eine bisher unbekannte Schwachstelle, die dem Software-Hersteller noch unbekannt ist (daher bleiben "0 Tage" Zeit für einen Patch).
Zero-Day-Schwachstellen sind besonders kritisch, weil Betroffene zum Zeitpunkt des Angriffs oft unvorbereitet sind. Die spezifische Unterart einer Schwachstelle ist extrem gefährlich und auf dem Schwarzmarkt überaus wertvoll.

6.2 Quellen für Glossarerläuterungen

Im Folgenden sind die Quellen aufgeführt, die für die Definition und Erläuterung der Begriffe im Glossar herangezogen wurden.

- https://medien.bsi.bund.de/lagebericht/de/glossar/
- https://www.staedtebund.gv.at/fileadmin/USERDATA/landesgruppen/steiermark/7_BSI_-_Glossar_und_Begriffsdefinition-1.pdf
- https://www.fu-berlin.de/sites/it-sicherheit/downloads/Glossar/index.html
- https://www.pd-g.de/assets/Aktuell-im-Fokus/Informationssicherheit/240904_Informationssicherheit_Glossar.pdf
- https://www.uni-muenster.de/Informationssicherheit/glossar/index.html

7 Weiterführende Hilfen und Materialien

Im Folgenden sind weiterführende Hilfen und Materialien zusammengestellt, die Journalist:innen bei der Berichterstattung über IT-Sicherheitsvorfälle unterstützen und bei Bedarf zur weiteren Vertiefung herangezogen werden können.

ARD/ZDF-Medienakademie: Fakten finden in Zeiten von Desinformation und KI - Seminar: https://www.ard-zdf-medienakademie.de/seminar/51212.html.

Berliner Journalisten Schule: Power-Input Datensicherheit im Internet – Webinar: https://www.berliner-journalisten-schule.de/webinare/datensicherheit-im-internet/

BSI: DoS- und DDoS-Attacken: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/DoS-Denial-of-Service/dos-denial-of-service_node.html

BSI Glossar: Glossar und Abkürzungsverzeichnis zum BSI Standard 200-4 (Business-Continuity Management): https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Standard200_4_BCM/Standard_200-4_BCM_Glossar.pdf?__blob=publicationFile&v=4 (Stand Dezember 2023)

BSI Publikation: Maßnahmenkatalog Ransomware: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.pdf?__blob=publicationFile&v=3

BSI - IT-Notfallkarte: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Notfallkarte/IT-Notfallkarte/it-notfallkarte_node.html

BSI Publikation: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall, Arbeitspapier – Version 1.2: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.pdf?__blob=publicationFile&v=3

BSI Publikation: IT-Notfallkarte „Verhalten bei IT-Notfällen“: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Notfallkarte/IT-Notfallkarte/it-notfallkarte_node.html

BSI Webseite - Checkliste Technik: https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Unternehmen/Ich-habe-einen-IT-Sicherheitsvorfall-Checkliste-Technik/ich-habe-einen-it-sicherheitsvorfall-checkliste-technik_node.html

BSI-Webseite: Liste zertifizierter IT-Sicherheitsdienstleister in den Geltungsbereichen IS-Revision und IS-Penetrationstests: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Anerkennung-von-Stellen-und-Zertifizierung-IT-Sicherheitsdienstleister/IS-Rev/Liste-IT-Sicherheitsdienstleister/liste-is-revi-is-pentester_node.html

BSI-Veröffentlichung: Liste der qualifizierten APT-Response-Dienstleister; Stand: 01.08.2024: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.html

CSBW - Glossar: https://www.cybersicherheit-bw.de/glossar

Deutscher Journalisten-Verband NRW mit Digital.Sicher.NRW: Jährliche Kooperationsveranstaltung zum Thema Cybersicherheit, zuletzt im Mai 2026 zum Thema Inside Cybercrime: Was Journalist:innen wissen müssen (https://www.djv-nrw.de/event-detail/inside-cybercrime-was-journalistinnen-wissen-muessen/)

Ergebnisbericht zum Workstream "Cyberresilience-Framework. In IT-Krisen schneller agieren. (Kurz: RESI)" kommunales Ransomware-Szenario“: https://www.dialog-cybersicherheit.de/storage/uploads/ws24-endprodukte/2024_Ergebnisbericht_RESI.pdf

Ergebnisbericht der AG RESI: Handreichung kommunales DDoS-Szenario: https://www.dialog-cybersicherheit.de/storage/uploads/resi-ddos/2026-03-RESI_DDoS-Handreichung.pdf

IT-Forensik „Was tun bei einem DDoS-Angriff? Leitfaden für Unternehmen“: https://it-forensik.de/facts-storys/news/ddos-angriff/

Journalisten Werkstatt: Digitale Sicherheit Warum sich Redaktionen und Freie heute anders schützen müssen als früher – und wie das klappt: https://shop.oberauer.com/werkstatt/journalisten-werkstatt/852/digitale-sicherheit?number (Stand Oktober 2025)

PD: Begriffe im Kontext der Informationssicherheit (Glossar): https://www.pd-g.de/assets/Aktuell-im-Fokus/Informationssicherheit/240904_Informationssicherheit_Glossar.pdf (Stand 04.09.2024)

Porath,Ron: „Internet, Cyber- und IT-Sicherheit von A-Z“
https://doi.org/10.1007/978-3-662-60911-8

Reporterfabrik: Workshop 128 Digitale Sicherheit: https://akademie.reporterfabrik.org/courses/course-v1:Reporterfabrik+128+2023/about

Reporterfabrik: Workshop 325 Hacken für Anfänger: https://akademie.reporterfabrik.org/courses/course-v1:Reporterfabrik+Workshop108+2018/about

Verbraucherzentrale „Starke Passwörter erstellen: So schützen Sie Ihre Online-Konten effektiv: https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/starke-passwoerter-erstellen-so-schuetzen-sie-ihre-onlinekonten-effektiv-11672

Anlagen

Die Anlagen umfassen die Fragebögen zu den Bedarfen in den Redaktionen (Anlage 1) und zur Expert:innenbefragung zur IT-Berichterstattung (Anlage 2) sowie die jeweiligen Auswertungen der beiden Befragungen (Anlagen 3 und 4).

Anlage 1: Fragebogen zu den Bedarfen in den Redaktionen

Berichten über IT-Sicherheitsvorfälle

Im **Dialog für Cybersicherheit** entwickelt eine Gruppe von Journalist:innen zusammen mit dem BSI und weiteren Mitwirkenden eine **Handreichung für Redaktionen**, die eine differenziertere **Berichterstattung zu IT-Sicherheitsvorfällen** unterstützen soll. Dieser Fragebogen soll uns helfen, die Handreichung an den Bedürfnissen der Redaktionen auszurichten.
Die Teilnahme ist **anonym**: Geben Sie am Ende Ihre **E-Mail-Adresse** an, ist die Umfrage **nicht mehr anonym**. Bei der Veröffentlichung der Ergebnisse wird aber kein Personenbezug hergestellt.

Sie können uns jederzeit unter **projekt-digitalegesellschaft@bsi.bund.de** kontaktieren.
Die Umfrage dauert etwa **5 Minuten** und ist **bis zum 30.04.2026** geöffnet.
Vielen Dank für Ihre Unterstützung!

Weitere Informationen finden Sie hier.

Definition IT-Sicherheitsvorfälle

Im Fragebogen verwenden wir den Begriff „**IT-Sicherheitsvorfälle**“ als Sammelbegriff für Ereignisse, die IT-Systeme, Netzwerke oder Daten beeinträchtigen. Dazu zählen sowohl gezielte Angriffe wie Hackerangriffe, Ransomware oder DDoS-Attacken als auch andere Ursachen wie Software- oder Hardwarefehler, Fehlkonfigurationen oder Stromausfälle. Gemeint sind damit alle Situationen, in denen Systeme nicht mehr richtig funktionieren, Daten verändert werden oder unbefugt eingesehen werden können.

Q1: In welchem Bereich arbeiten Sie hauptsächlich?

- Lokaljournalismus
- Regionaljournalismus
- Überregional
- Investigativ
- Wirtschaft
- Technik / IT

- Sonstiges: _____

Q2: Wie gut fühlen Sie sich in Ihrer Redaktion auf die Berichterstattung zu IT-Sicherheitsvorfällen vorbereitet?
[Skala von 1 (sehr schlecht vorbereitet) bis 5 (sehr gut vorbereitet)]

Q3: Wie oft berichten Sie oder Ihre Redaktion über IT-Sicherheitsvorfälle?
- Wöchentlich
- Mehrmals im Monat
- Monatlich
- Mehrmals pro Jahr
- Jährlich
- Seltener
- Nie

Q4: Wer berichtet typischerweise über IT-Sicherheitsvorfälle?
Mehrere Antworten sind möglich.
- Tagesaktuell arbeitende Reporter:innen
- Redaktionseigene Spezialist:innen für IT-Themen
- Investigativteam
- Externe Expert:innen
- Sonstiges: _____

Q5: Wie erfahren Sie in der Regel von IT-Sicherheitsvorfällen in Ihrem Berichtsgebiet?
Mehrere Antworten sind möglich.
- Pressemitteilungen
- Betroffene Organisationen
- Sicherheitsbehörden
- IT-Sicherheitsunternehmen
- Social Media
- Fachmedien
- Hinweise von Informant:innen
- Sonstiges: _____

Q6: Welche der folgenden Ressourcen stehen Ihnen (zur Recherche) zur Verfügung?
Mehrere Antworten sind möglich.
- Zugang zu IT-Expert:innen
- internes Fachwissen in der Redaktion
- technische Analyse-Tools

- ausreichend Zeit für Recherche
- Schulungen / Weiterbildungen zu IT-Sicherheitsvorfällen
- Zugang auf Darknet-Seiten
- keine speziellen Ressourcen
- Sonstiges: _____

Q7: Welche Herausforderungen treten bei der Berichterstattung zu IT-Sicherheitsvorfällen besonders häufig auf?
Mehrere Antworten sind möglich.

- fehlendes technisches Verständnis
- redaktionelles Unverständnis
- schwierige Quellenlage, Verifikation von Angaben
- mangelnde Transparenz von Unternehmen
- Zeitdruck
- komplizierte Fachbegriffe
- rechtliche Unsicherheiten
- Einordnung der Angriffe
- Mangelnde Kontakte zu Expert:innen
- Sonstiges:_____

Q8: Welche der folgenden Angebote wären hilfreich für Ihre Arbeit?
Mehrere Antworten sind möglich.

- Vorlage für sinnvollen KI-Prompt für IT-Sicherheitsvorfälle
- Leitfaden für passende Fotos und Bildsprache zu IT-Sicherheitsvorfällen
- Regelmäßige Austauschformate zum Berichten zu IT-Sicherheitsvorfällen
- Schulungen zur Berichterstattung zu IT-Sicherheitsvorfällen
- Checkliste für IT-Sicherheitsvorfälle
- Zugang zu Expert:innen der IT-Sicherheit
- Leitfaden für Berichterstattung zu IT-Sicherheitsvorfällen
- Glossar wichtiger Begriffe der IT-Sicherheit

Q9: Was sollte eine Handreichung für Journalist:innen zum Thema IT-Sicherheitsvorfälle enthalten, damit diese für Ihre Arbeit hilfreich ist?
(offenes Feld)

Q10: Wenn Sie die Handreichung nach Fertigstellung erhalten möchten, tragen Sie bitte hier Ihre E-Mail-Adresse ein:
Wenn Sie dies tun, ist diese Umfrage jedoch nicht mehr anonym.
(offenes Feld)

Vielen Dank für Ihre Teilnahme und Ihre Unterstützung!
Ihre Antworten helfen uns, eine praxisnahe Handreichung für die Berichterstattung über IT-Sicherheitsvorfälle zu entwickeln.

Wenn Sie weitere Fragen, Anmerkungen oder Erfahrungen teilen möchten, können Sie uns **gern jederzeit über diese E-Mail-Adresse kontaktieren: projekt-digitalegesellschaft@bsi.bund.de**

Wenn Sie uns sonst direkt noch etwas mitgeben wollen, können Sie das hier tun:
(offenes Feld)

Anlage 2: Fragebogen zur Expert:innenbefragung zur IT-Berichterstattung

Eine Expert:innenbefragung zur Berichterstattung über IT-Sicherheitsvorfälle

Im Workstream entwickelt eine Gruppe von Journalist:innen zusammen mit dem BSI und weiteren Mitwirkenden eine **Handreichung für Redaktionen**, die eine differenziertere **Berichterstattung zu IT-Sicherheitsvorfällen in Publikumsmedien** unterstützen soll. Dabei helfen uns Ihre Antworten.

Die Teilnahme ist **anonym**, dauert etwa **fünf Minuten** und ist **bis zum 31.05.2026** geöffnet.
Vielen Dank für Ihre Unterstützung!

Sie können uns jederzeit unter **projekt-digitalegesellschaft@bsi.bund.de** kontaktieren.

IT-Sicherheitsvorfälle
Wir verwenden „**IT-Sicherheitsvorfälle**“ als Sammelbegriff für Ereignisse, die IT-Systeme, Netzwerke oder Daten beeinträchtigen. Dazu zählen gezielte Angriffe und Ursachen wie Software- oder Hardwarefehler, Fehlkonfigurationen oder Stromausfälle. Gemeint sind alle Situationen, in denen Systeme nicht mehr richtig funktionieren, Daten verändert werden oder unbefugt eingesehen werden können.

Hinweis

Unsere Fragen beziehen sich ausschließlich auf Publikumsmedien. Publikumsmedien sind journalistische Angebote, die sich an eine breite, allgemeine Öffentlichkeit richten; insbesondere überregionale und regionale Zeitungen, Online-Nachrichtenportale,

Fernsehen, Radio und reichweitenstarke journalistische Social-Media-Angebote. Es geht nicht um Fachmedien, die sich an IT- oder Sicherheitsexpert:innen richten.

Q1: In welcher Funktion sind Sie derzeit hauptsächlich tätig?

- IT-Sicherheits- oder IT-Expert:in
- Pressesprecher:in / Kommunikationsverantwortliche:r (Behörde oder Unternehmen)
- IT-Fachjournalist:in
- IT-Wissenschaftler:in
- Sonstiges: _____

Q2: Haben Sie in Ihrer beruflichen Praxis bereits persönliche Erfahrungen mit IT-Sicherheitsvorfällen gemacht?

- Ja
- Nein
- Weiß nicht / keine Angabe

Q3: Wenn Sie die tagesaktuelle Berichterstattung über IT-Sicherheitsvorfälle in Publikumsmedien verfolgen: Wie bewerten Sie insgesamt die Qualität dieser Berichterstattung?
[Skala von 1 (sehr schlecht) bis 5 (sehr gut)]

Q4: Woran machen Sie Ihre Bewertung fest?
Bitte erläutern Sie kurz die Gründe für Ihre Einschätzung.
(offenes Feld)

Q5: Sehen Sie Unterschiede in der Berichterstattung über IT-Sicherheitsvorfälle zwischen lokalen, regionalen und überregionalen Medien?

- Ja
- Nein
- Weiß nicht / keine Angabe

Q6: Welche Fehler sehen Sie häufig in der Berichterstattung über IT-Sicherheitsvorfälle?
Mehrere Antworten sind möglich.

- Nicht sauber verwendete Fachbegriffe
- Oberflächliche Beschreibung von Vorfällen
- Fehlende Beschreibung von grundsätzlichen IT-Zusammenhängen
- Täter-Darstellung als übermächtig
- Opfer-Darstellung als unschuldig
- Klischeehafte Bildsprache
- Fehlende nachhaltige Berichterstattung
- Fehlende Beschreibung von politischen Zuständigkeiten

- Weiß nicht / keine Angabe
- Sonstiges: _____

Q7: Was sind aus Ihrer Sicht die Hauptgründe für Fehler in der Berichterstattung über IT-Sicherheitsvorfälle?
Mehrere Antworten sind möglich.

- Zeitdruck in Redaktionen
- Wirtschaftlicher / Klick- bzw. Verkaufsdruck
- Fehlendes Wissen zu IT-Sicherheit
- Komplexität des Themas / schwer verständlich
- Fehlende Einordnung oder Kontextualisierung
- Sensationalisierung / Dramatisierung
- Unreflektierte Nutzung von Agenturmeldungen, Sekundärquellen oder Pressemitteilungen
- Unklare oder unvollständige Informationslage bei Vorfällen
- Weiß nicht / Keine Angabe
- Sonstiges: _____

Q8: Halten Sie den Begriff „Cyber" für problematisch?
[Skala von 1 (gar nicht problematisch) bis 5 (sehr problematisch)]

Q9: Was glauben Sie, mit welchen Angeboten für Journalist:innen von Publikumsmedien ließe sich die Berichterstattung verbessern?
Mehrere Antworten sind möglich.

- Vorlage für sinnvollen KI-Prompt für IT-Sicherheitsvorfälle
- Leitfaden für passende Fotos und Bildsprache zu IT-Sicherheitsvorfällen
- Regelmäßige Austauschformate zum Berichten zu IT-Sicherheitsvorfällen
- Schulungen zur Berichterstattung zu IT-Sicherheitsvorfällen
- Checkliste für IT-Sicherheitsvorfälle
- Zugang zu Expert:innen der IT-Sicherheit
- Leitfaden für Berichterstattung zu IT-Sicherheitsvorfällen
- Auf Redaktionen zugeschnittenes Glossar wichtiger Begriffe der IT-Sicherheit
- Sonstiges:_____

Q10. Welche Inhalte sollten Ihrer Meinung nach in einer Handreichung zur Berichterstattung zu IT-Sicherheitsvorfällen für Journalist:innen von Publikumsmedien enthalten sein?
(offene Frage)

Q11: Welche drei Begriffe rund um IT-Sicherheitsvorfälle sollten Ihrer Meinung nach unbedingt in einem Glossar für Redaktionen enthalten sein?
(offene Frage)

Ihre weitere Hilfe und Erhalt der Handreichung

Möchten Sie die **fertige Handreichung** erhalten? Oder **können wir Sie kontaktieren, um Sie gegebenenfalls in unser Expert:innennetzwerk aufzunehmen?** Dann können Sie Ihre Kontaktdaten separat hinterlassen. Ihre Antworten hier bleiben anonym.

WICHTIG: Bitte öffnen Sie die Umfrage in einem neuen Fenster. Vergessen Sie aber nicht, diese Befragung unten abzuschließen. **Hier Kontaktdaten hinterlassen.**

Vielen Dank für Ihre Teilnahme und Ihre Unterstützung!
Wenn Sie weitere Fragen, Anmerkungen oder Erfahrungen teilen möchten**: projekt-digitalegesellschaft@bsi.bund.de**

Wenn Sie uns sonst anonym noch etwas mitteilen wollen, können Sie das hier tun:
(offenes Feld)

[Ende der Befragung 1]

[Zweite nicht-anonyme separate Befragung]

Kontaktmöglichkeit und Versand der Handreichung
Vielen Dank für Ihre Teilnahme an unserer Umfrage zur Berichterstattung über IT-Sicherheitsvorfälle.

Wenn Sie möchten, können Sie uns im Folgenden **freiwillig Ihre Kontaktdaten hinterlassen**. Diese werden **getrennt von Ihren Antworten aus der Hauptumfrage gespeichert** und lassen keine Rückschlüsse auf Ihre dortigen Angaben zu.

Q1: Sind Sie damit einverstanden, dass wir Sie kontaktieren, um Sie gegebenenfalls in unser Expert:innennetzwerk aufzunehmen?
Ihre Kontaktdaten werden ausschließlich für den Zweck verwendet, Sie für unser Expert:innennetzwerk zu kontaktieren und nicht an andere weitergegeben.

- Ja
- Nein

Q2: Falls „Ja“: Wie können wir Sie am besten erreichen?
Geben Sie Ihren Namen und Ihre präferierten Kontaktmöglichkeiten an.
(offenes Feld)

Q3: Wenn Sie die Handreichung nach Fertigstellung erhalten möchten, tragen Sie bitte hier Ihre E-Mail-Adresse ein:
(offenes Feld)

[Nach Abschicken der Umfrage]
Vielen Dank für Ihre Teilnahme!
Bitte vergessen Sie nicht, auch die Hauptbefragung abzuschicken, sofern Sie das noch nicht getan haben.

[Ende der Befragung]

Anlage 3: Auswertung der Umfragen zu den Bedarfen in den Redaktionen

An der Umfrage nahmen vom 30. März 2026 bis zum 20. April 2026 insgesamt 23 Personen teil. Die Ergebnisse sind in den folgenden Diagrammen dargestellt:

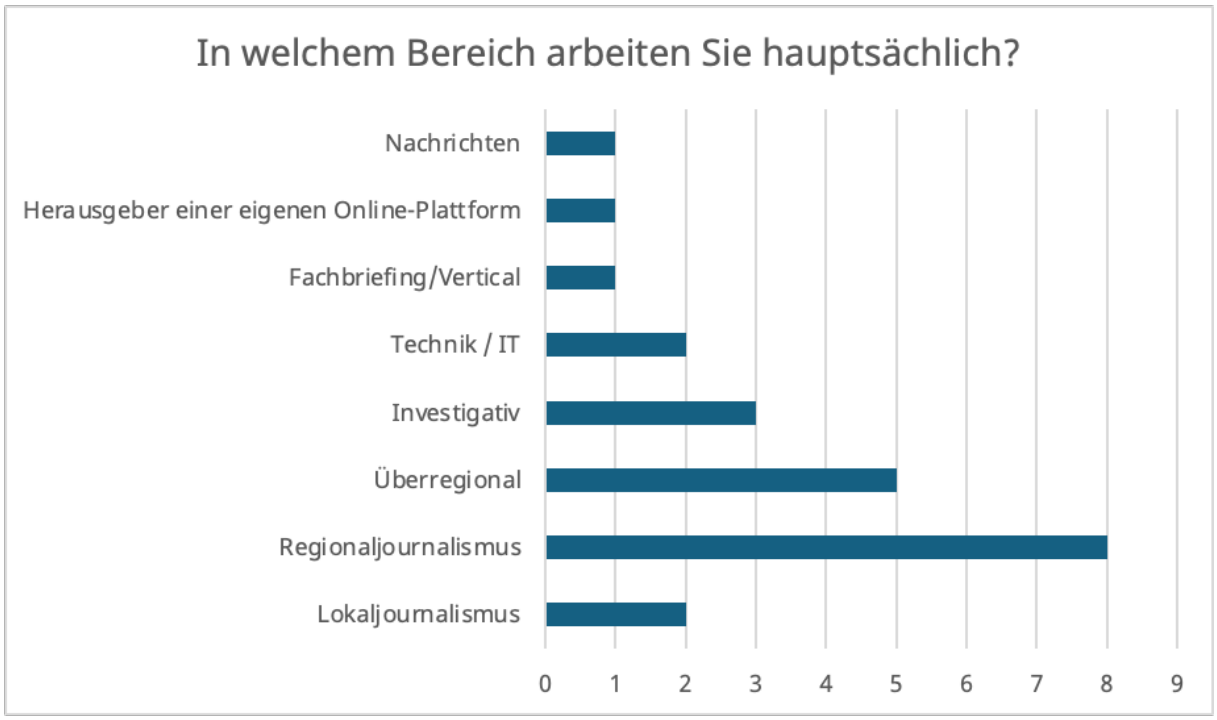


Diagramm: Anzahl der Antworten (Einfachantworten, 23 Teilnehmende)

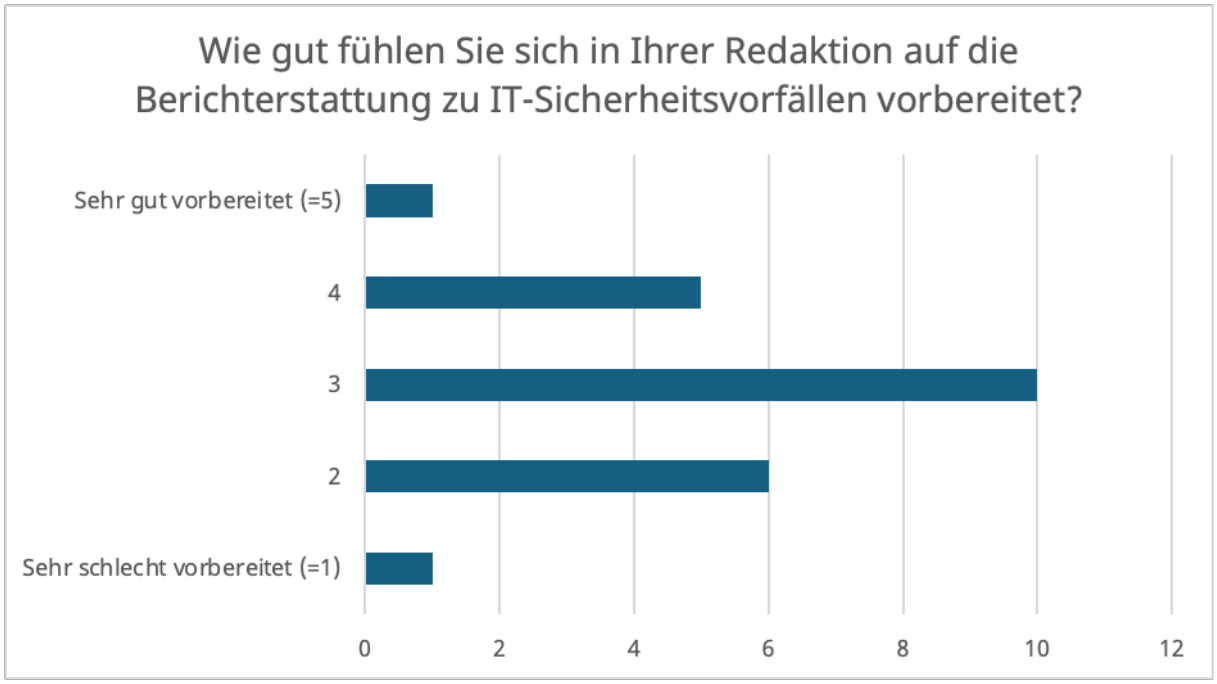


Diagramm: Anzahl der Antworten (Einfachantworten, 23 Teilnehmende)

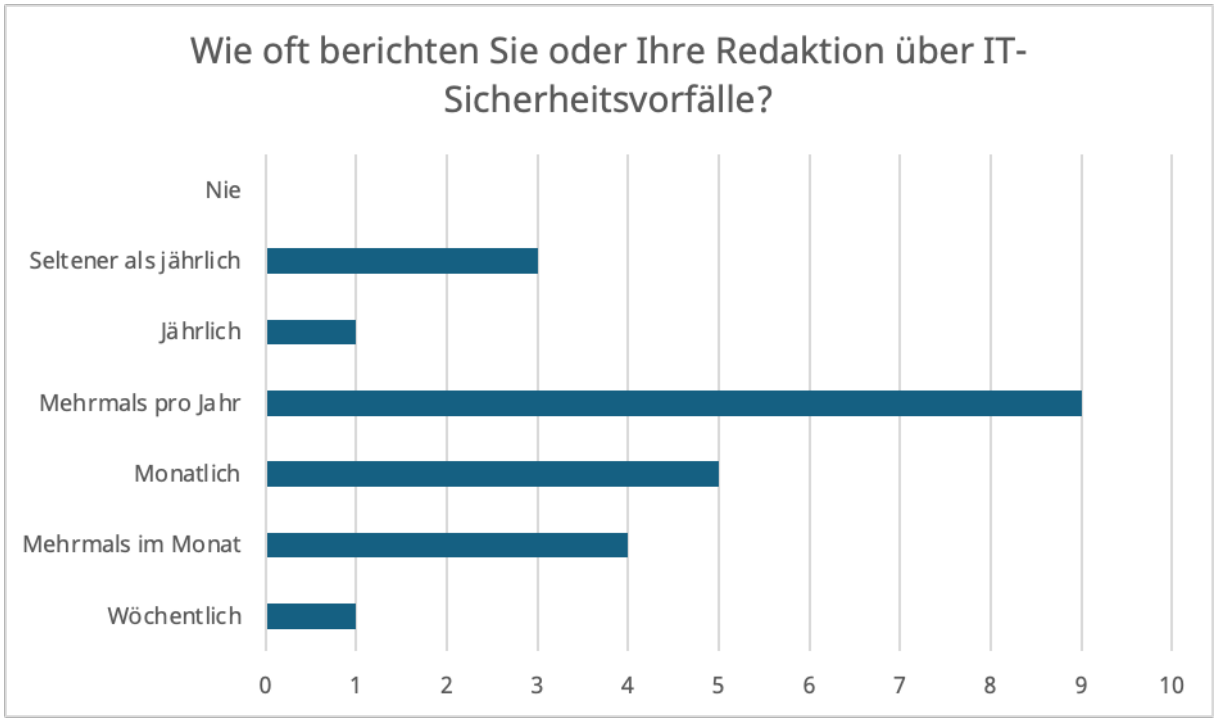


Diagramm: Anzahl der Antworten (Einfachantworten, 23 Teilnehmende)

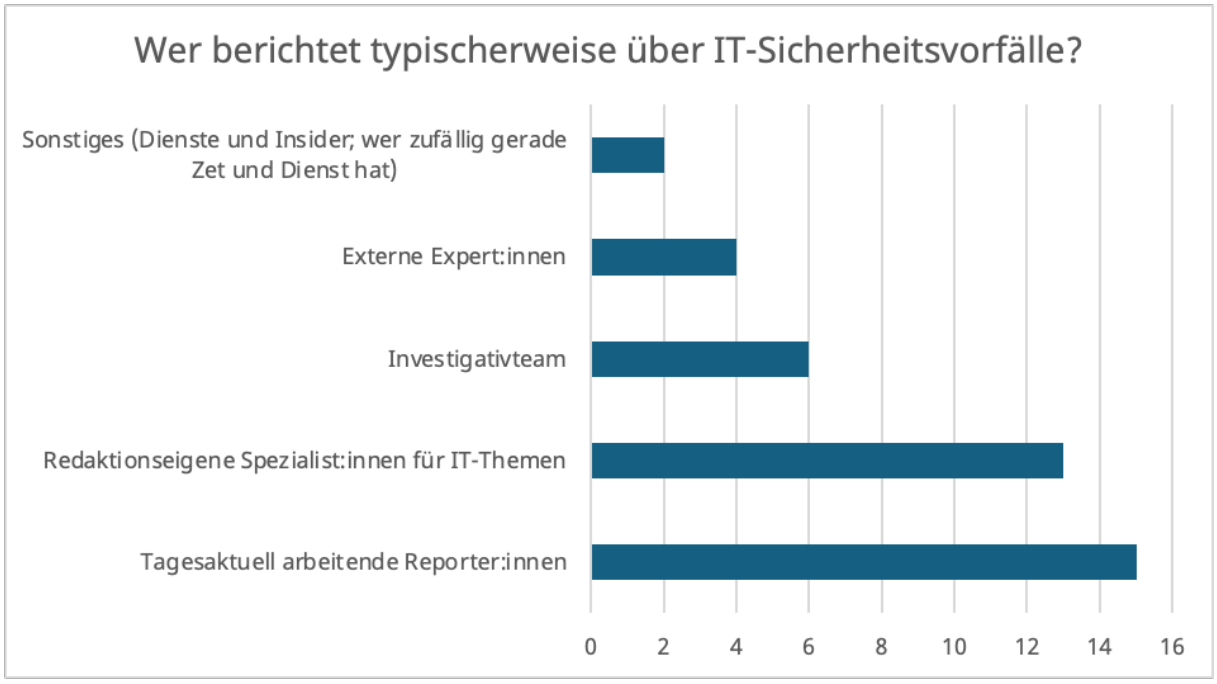


Diagramm: Anzahl der Antworten pro Antwortoption (Mehrfachantworten möglich, 22 Teilnehmende)

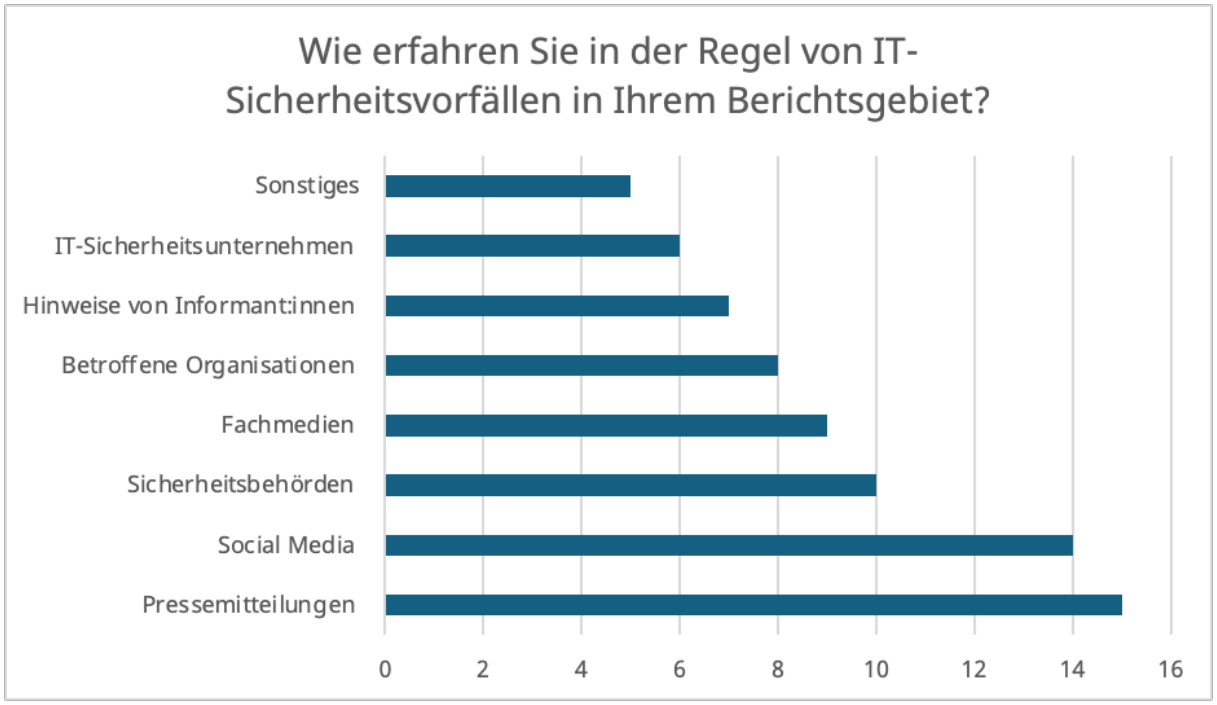


Diagramm: Anzahl der Antworten pro Antwortoption (Mehrfachantworten möglich, 23 Teilnehmende)

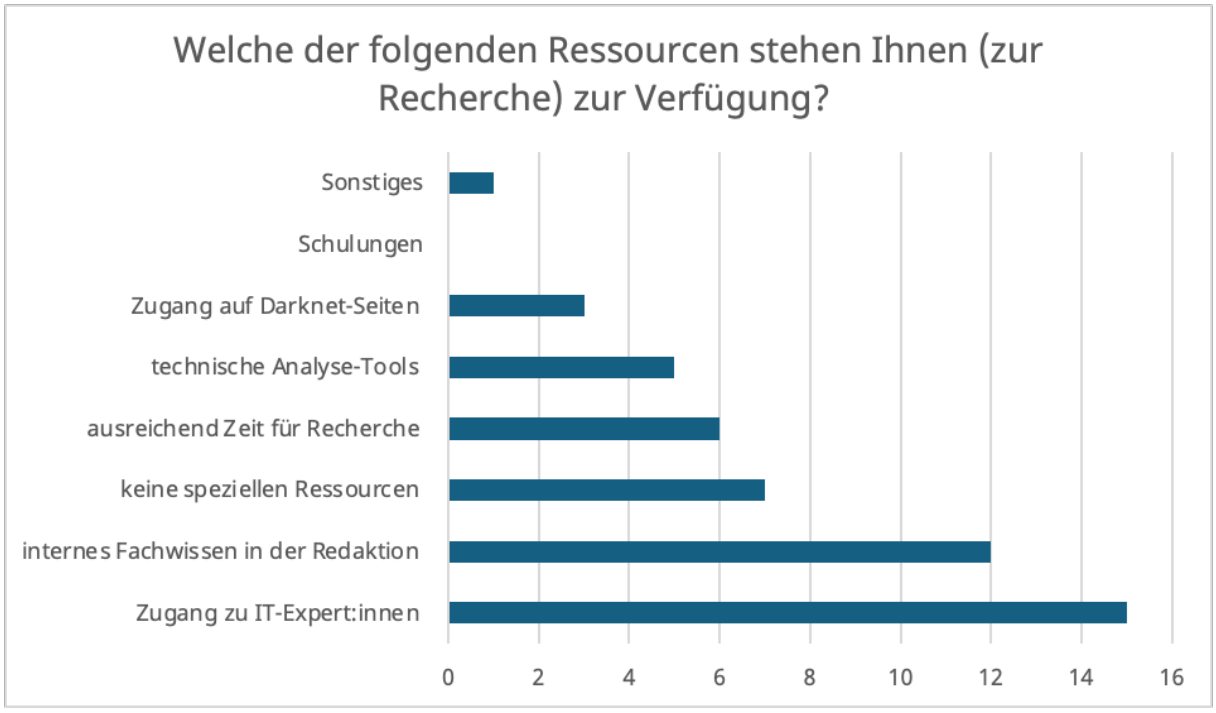


Diagramm: Anzahl der Antworten pro Antwortoption (Mehrfachantworten möglich, 23 Teilnehmende)

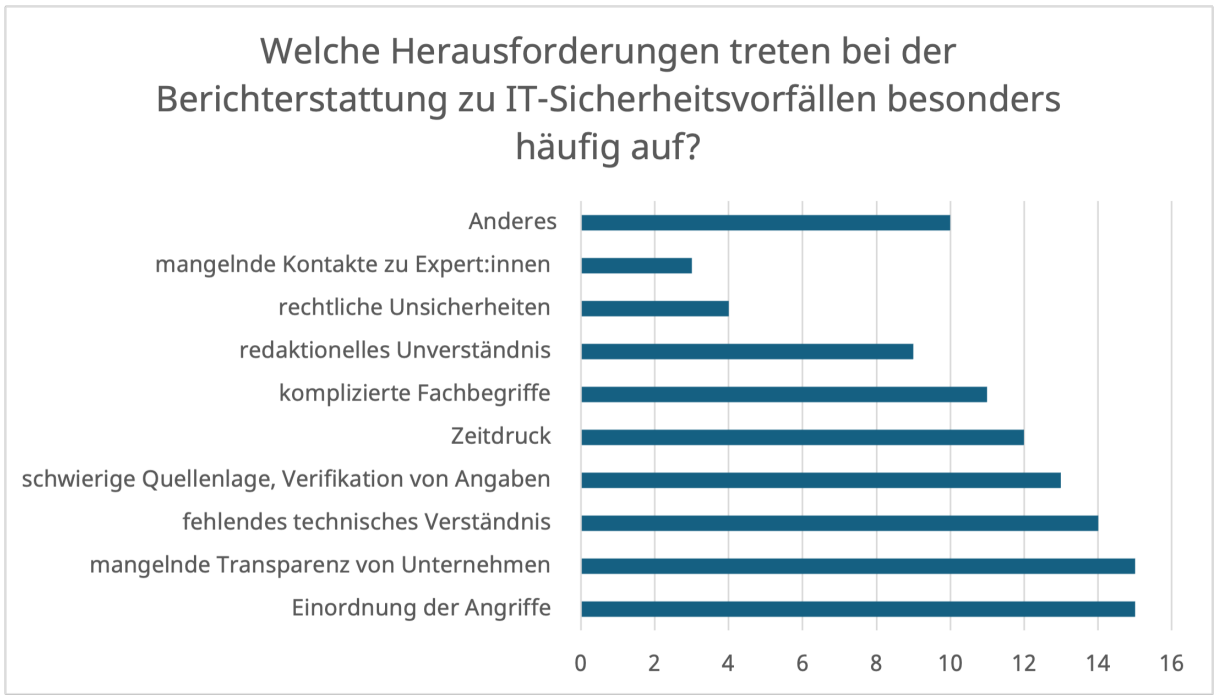


Diagramm: Anzahl der Antworten pro Antwortoption (Mehrfachantworten möglich, 22 Teilnehmende)

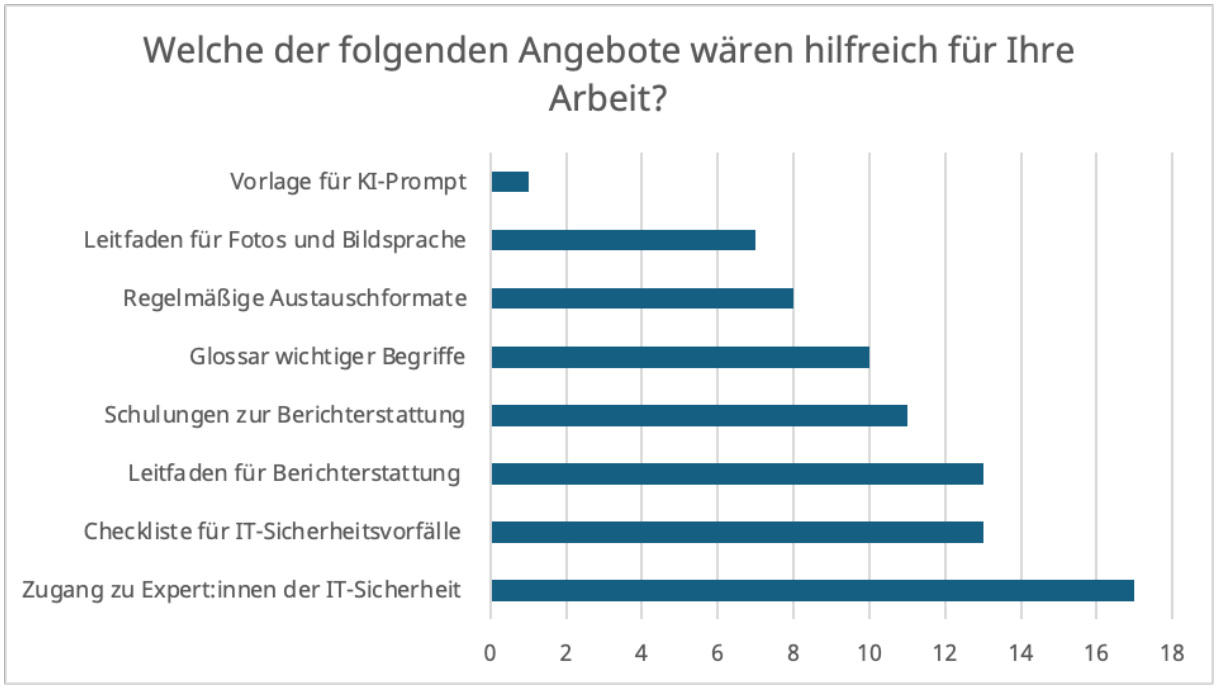


Diagramm: Anzahl der Antworten pro Antwortoption (Mehrfachantworten möglich, 23 Teilnehmende)

Offene Frage: Was sollte eine Handreichung für Journalist:innen zum Thema IT-Sicherheitsvorfälle enthalten, damit diese für Ihre Arbeit hilfreich ist?

In den Antworten auf die offenen Fragen kristallisierte sich ein Wunsch klar heraus: der nach einem **Werkzeugkasten**, der den Journalist:innen auch eine schnelle Bewertung von IT-Sicherheitsvorfällen hinsichtlich Ausmaß und Bedeutung erlaubt.

Der Werkzeugkasten sollte eine Liste mit Kontakten von Ansprechpersonen, themenbezogenen Expert:innen sowie staatlichen und nichtstaatlichen Quellen für Hintergrundinformationen enthalten. Letztere können Redaktionen helfen, die Tragweite eines Angriffs oder einer Störung sowie die Relevanz für Wirtschaft, Gesellschaft und einzelne Bürger:innen einzuordnen. Gerade bei Vorfällen wie einer nicht erreichbaren Website stellt sich für Journalist:innen die Frage, ob tatsächlich ein Angriff vorliegt, welche Folgen für Nutzer entstehen und ob der Fall eine ausreichende journalistische Fallhöhe besitzt.

Die Befragten wünschen sich außerdem ein **Glossar**: Erklärungen zu wichtigen Begriffen, Angriffskategorien und relevanten Akteuren, möglichst einfach, präzise und auf Deutsch. Das Glossar sollte demnach technische Definitionen liefern und aufzeigen, wer bei welchen Vorfällen kompetent Auskunft geben kann. Zudem soll es bei der Einordnung helfen, welche Informationen für die journalistische Bewertung eines Falls relevant sind und wie bestimmte Begriffe klar voneinander abgegrenzt werden können.

In diesem Zusammenhang wird auch die **Bedeutung von Kennzahlen und Einschätzungen**, etwa CVSS-Scores oder Angaben von Sicherheitsanbietern und Behörden, angesprochen. Die Handreichung sollte daher erklären, wie solche Angaben zu lesen sind und welche Aussagekraft sie für die journalistische Einordnung tatsächlich haben.

Die Befragten wünschen sich außerdem **praktische Beispiele**, Alltagssituationen und Hinweise auf typische Missverständnisse. Sie könnten dabei helfen, Unterschiede zwischen IT-Sicherheitsvorfällen sichtbar zu machen und die Berichterstattung verständlicher zu gestalten.

Bei der Einordnung der Ergebnisse ist zu berücksichtigen, dass in den offenen Antworten einzelne Perspektiven aus größeren Redaktionen stärker vertreten sein oder bestimmte Redaktionstypen überrepräsentiert sein könnten. Dennoch decken sich die Rückmeldungen insgesamt mit den Annahmen des Workstreams. Die vermuteten Schwachstellen im Journalismus – insbesondere der Bedarf an verständlicher Orientierung, schneller Einordnung, verlässlichen Ansprechpartner:innen und einer klaren Erklärung der gesellschaftlichen Relevanz von IT-Sicherheitsvorfällen – werden durch die Antworten weitgehend bestätigt.

Aufgrund der Vielzahl der Antworten und Wünsche bei den offenen Fragen konnten im Rahmen der Handreichung leider nicht alle Anregungen berücksichtigt werden.

Anlage 4: Auswertung der Expert:innenbefragung zur IT-Berichterstattung

Zur Berichterstattung über IT-Vorfälle gibt es mindestens eine weitere Perspektive: die derjenigen, die beruflich mit IT befasst sind. Welche Lücken und Bedarfe sie in der journalistischen Berichterstattung ausmachen, wurde ab dem 29. April 2026 in einer „Expert:innenbefragung zur Berichterstattung über IT-Sicherheitsvorfälle“ erhoben. Bis zur Schließung der Befragung am 1. Juni 2026 hatten insgesamt 59 Personen teilgenommen. 25 Personen hinterlegten ihre Kontaktdaten für eine mögliche Aufnahme in ein Expert.

Die Ergebnisse der anonymen Befragung sind in den folgenden Diagrammen dargestellt:

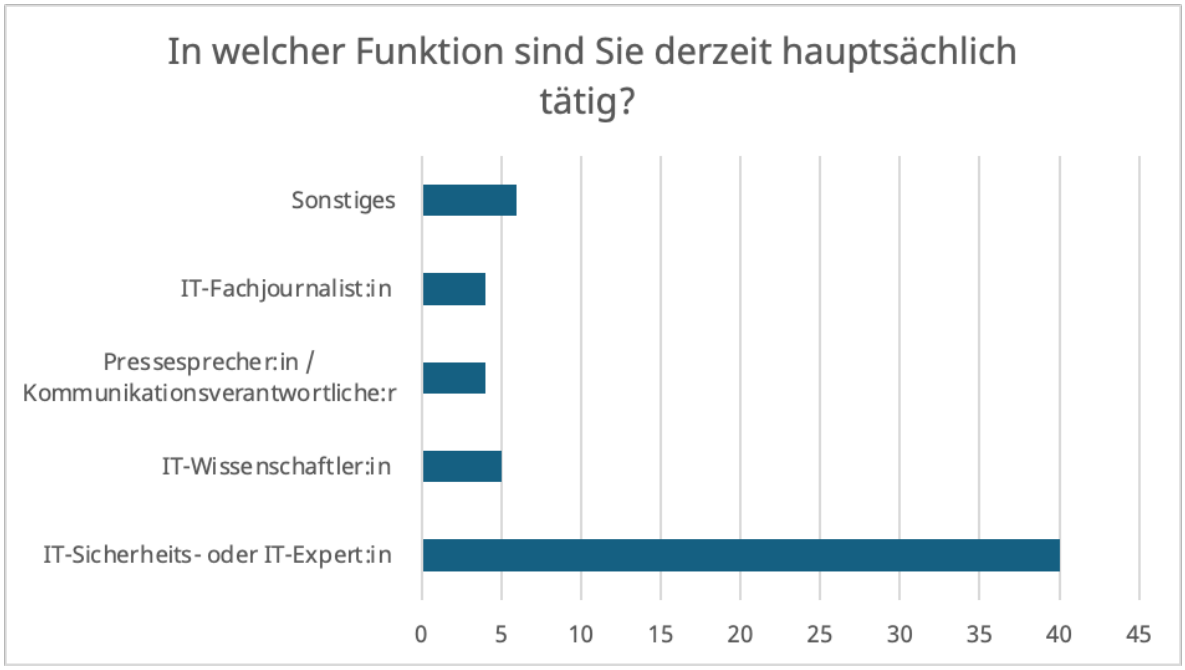


Diagramm: Anzahl der Antworten pro Antwortoption (Einfachantworten, 59 Teilnehmende)

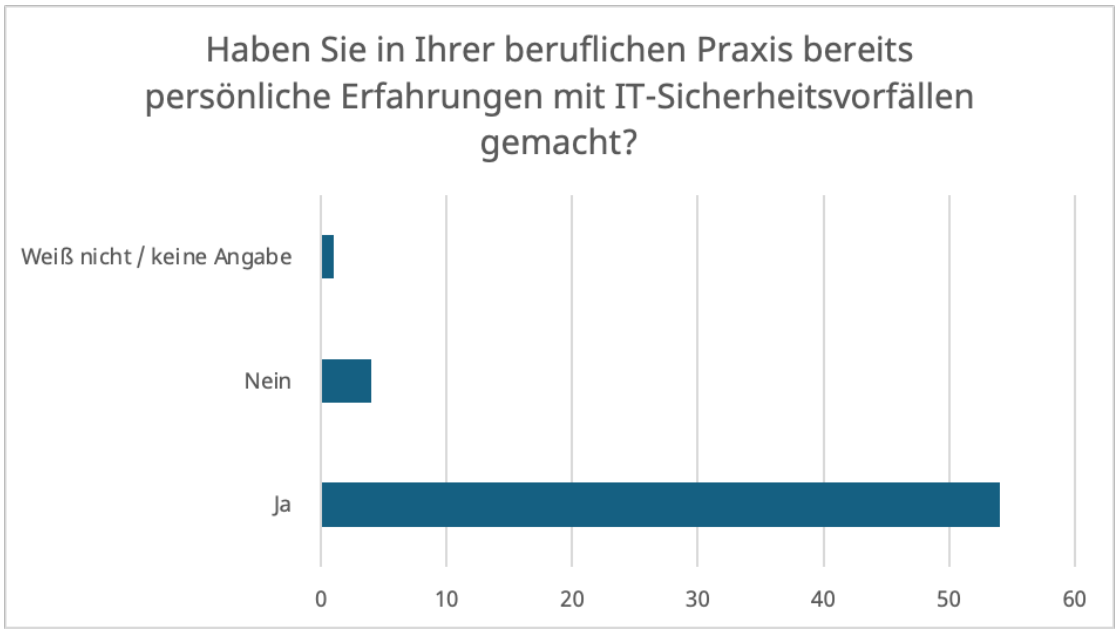


Diagramm: Anzahl der Antworten pro Antwortoption (Einfachantworten, 59 Teilnehmende)

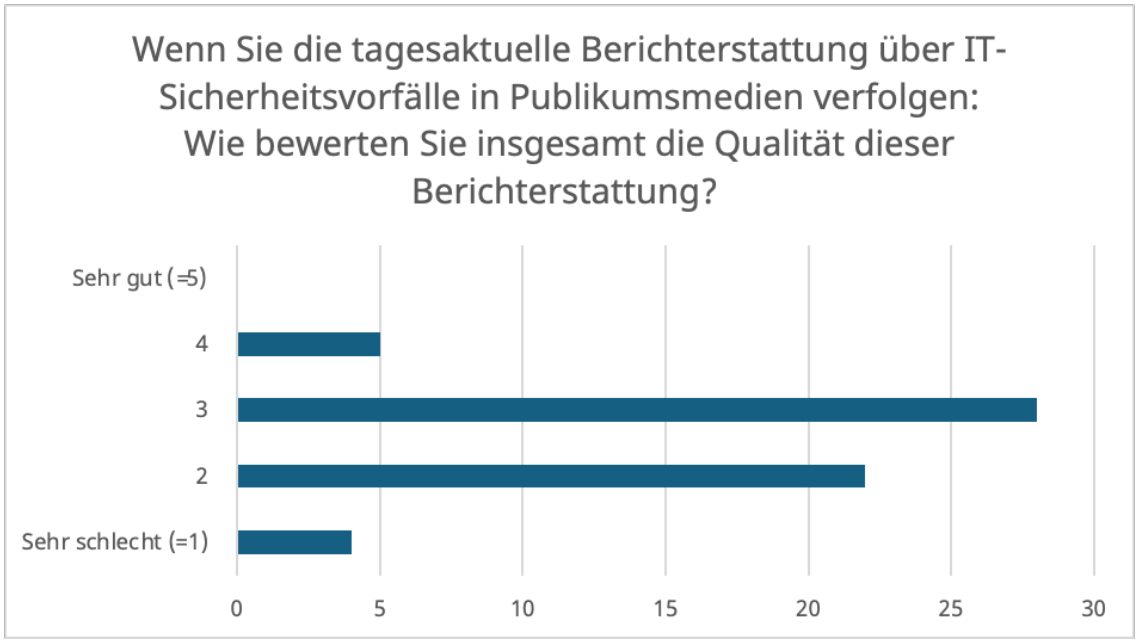


Diagramm: Anzahl der Antworten pro Antwortoption (Einfachantworten, 59 Teilnehmende)

Offene Fragen: Warum sehen Expert:innen die Berichterstattung als weitgehend verbesserungswürdig und woran machen sie dies fest?

Positiv wird vereinzelt hervorgehoben, dass entsprechende Vorfälle inzwischen häufiger aufgegriffen werden und dadurch öffentliche Aufmerksamkeit entsteht. Zudem werden einzelne Fachjournalist:innen oder Fachmedien als gute Beispiele genannt.

Kritisiert wird an der Berichterstattung vor allem Oberflächlichkeit: fehlende fachliche/technische Einordnung, keine Analyse von Ursachen, Folgen und Verantwortung, Clickbait, Alarmismus sowie unscharfe Begriffsverwendung (z. B. „Cyberangriff“ vs. „IT-Störung"), wodurch unklar bleibt, ob es sich um einen externen Angriff, technischen Ausfall oder Datenverlust handelt.

Auch die Einschätzung der Schwere von Vorfällen gilt vielen als wenig fundiert – DDoS-Attacken würden aufgebauscht, Attributionen unkritisch übernommen, ohne deren Unsicherheit zu benennen. Politisch motivierte Angriffe stünden überproportional im Fokus, obwohl finanziell motivierte Cyberkriminalität häufiger ist. Zudem würden PR- und politische Narrative oft unkritisch übernommen, etwa bei Täterzuordnungen oder der Betonung „hoher krimineller Energie".

Viele bemängeln eine fehlende Kontextualisierung: Einfallsvektoren, Auswirkungen, Schutzmöglichkeiten und Lessons Learned kämen zugunsten des reinen Ereignisses zu kurz. Als Beispiel wird die Berichterstattung zum Signal-Phishing bei Klöckner genannt, die sich auf die Sicherheit der App statt auf eine Erklärung des Phishings konzentriert

habe. Auch bei Sicherheitslücken dominiere häufig Effekthascherei statt Einordnung. Zudem fehle es oft an Follow-up-Berichten zu Folgen und Handlungsoptionen für Betroffene.

Der Anspruch der Befragten an Publikumsmedien: technische Zusammenhänge verständlich übersetzen, Risiken realistisch einordnen und zur Kompetenzvermittlung beitragen.

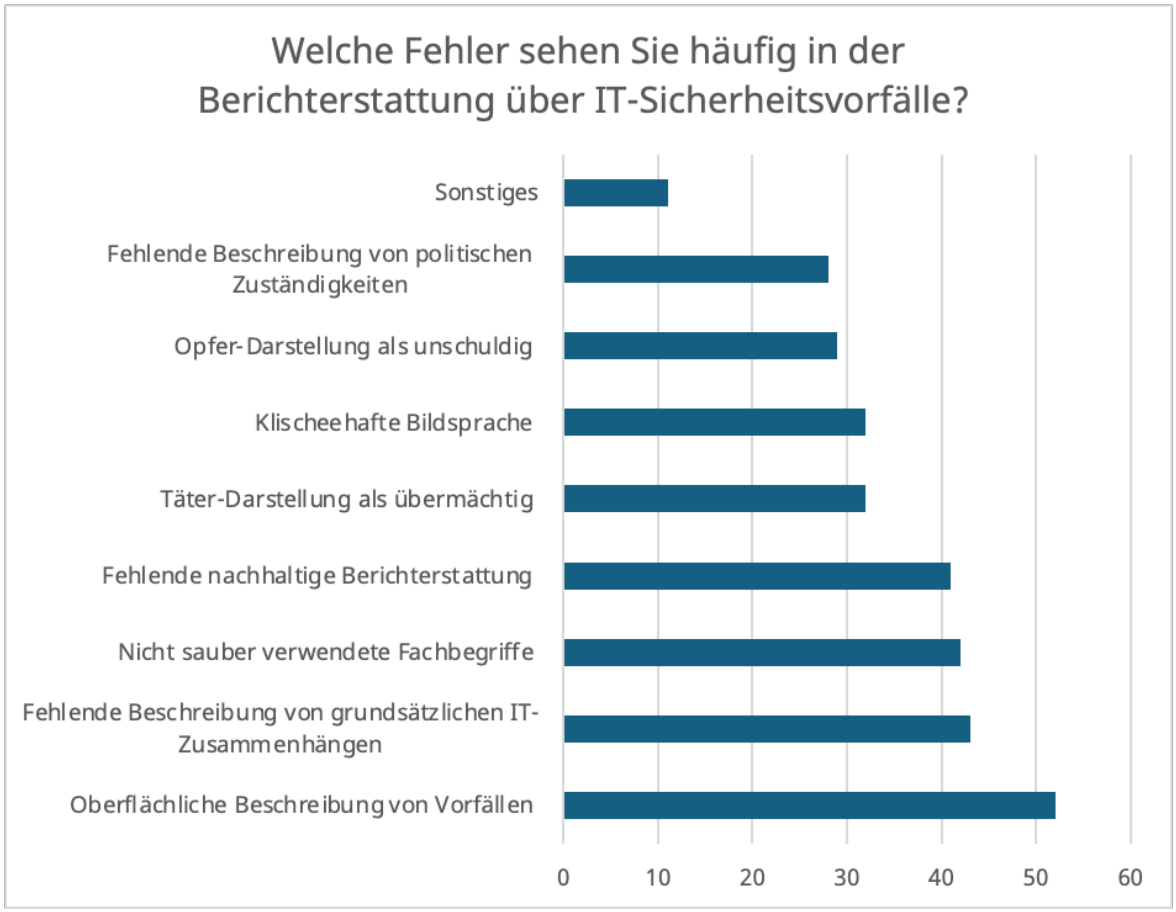


Diagramm: Anzahl der Antworten pro Antwortoption (Mehrfachantworten möglich, 59 Teilnehmende)

Welche Fehler sehen Sie häufig in der Berichterstattung über IT-Sicherheitsvorfälle?

Laut den Befragten werden Cybervorfälle häufig als News-Ereignisse erzählt, aber zu selten als komplexe Sicherheits-, Verantwortungs- und Gesellschaftsthemen eingeordnet. Häufigster Kritikpunkt ist eine zu oberflächliche Beschreibung der Vorfälle, eine fehlende Erläuterung grundsätzlicher IT-Zusammenhänge sowie die unsaubere Verwendung von Fachbegriffen. Dies könne zu weiteren Verständnisproblemen und Lücken in der Berichterstattung führen, weil falsche Begriffe und unklare technische Abläufe verkürzte oder fehlerhafte Erzählungen begünstigten.

Klischees in der Sprache werden ebenso kritisiert wie das Bild vom Mann im „Hoodie vor grünem Code“. Sie verstärkten das Narrativ von mysteriösen, übermächtigen Täter:innen und lenkten von Strukturen, Verantwortung und Prävention ab. Kritisiert wurden zudem eine überzeichnete Täter-Opfer-Darstellung beziehungsweise die Darstellung ausschließlich „unschuldiger Opfer“ sowie der Verzicht auf eine Einordnung politischer Zuständigkeiten und der Rollen von Behörden, BSI, Datenschutzaufsicht, Polizei/LKA und Kommunen.

Diagramm: Anzahl der Antworten pro Antwortoption (Mehrfachantworten möglich, 58 Teilnehmende)

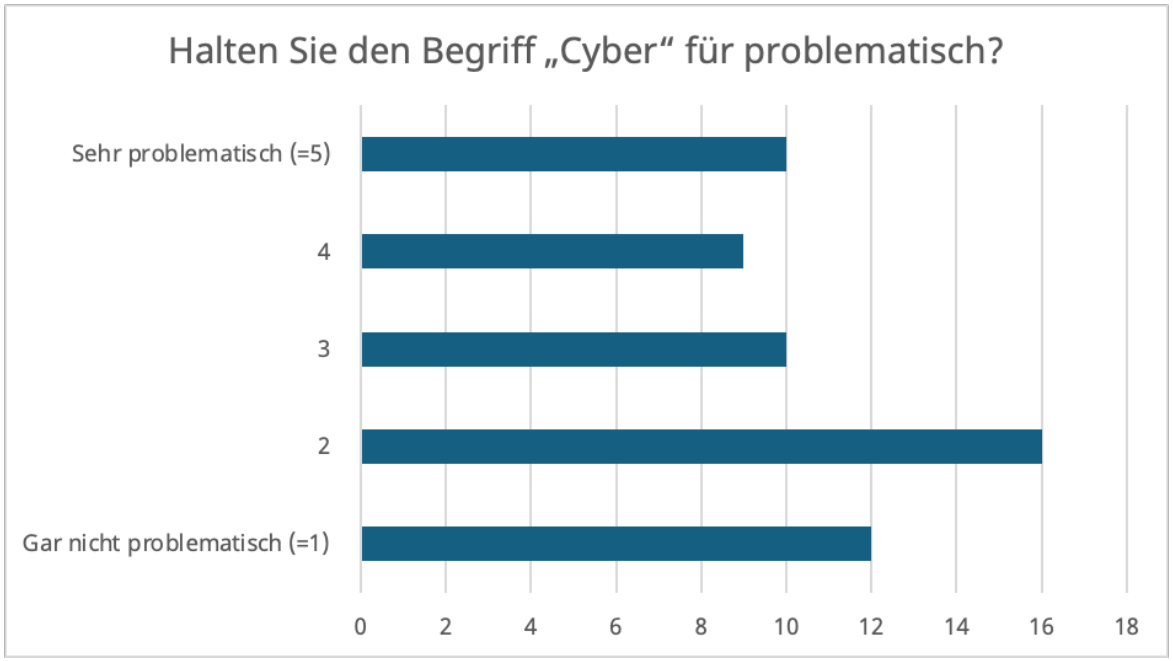


Diagramm: Anzahl der Antworten pro Antwortoption (Einfachantworten, 57 Teilnehmende)

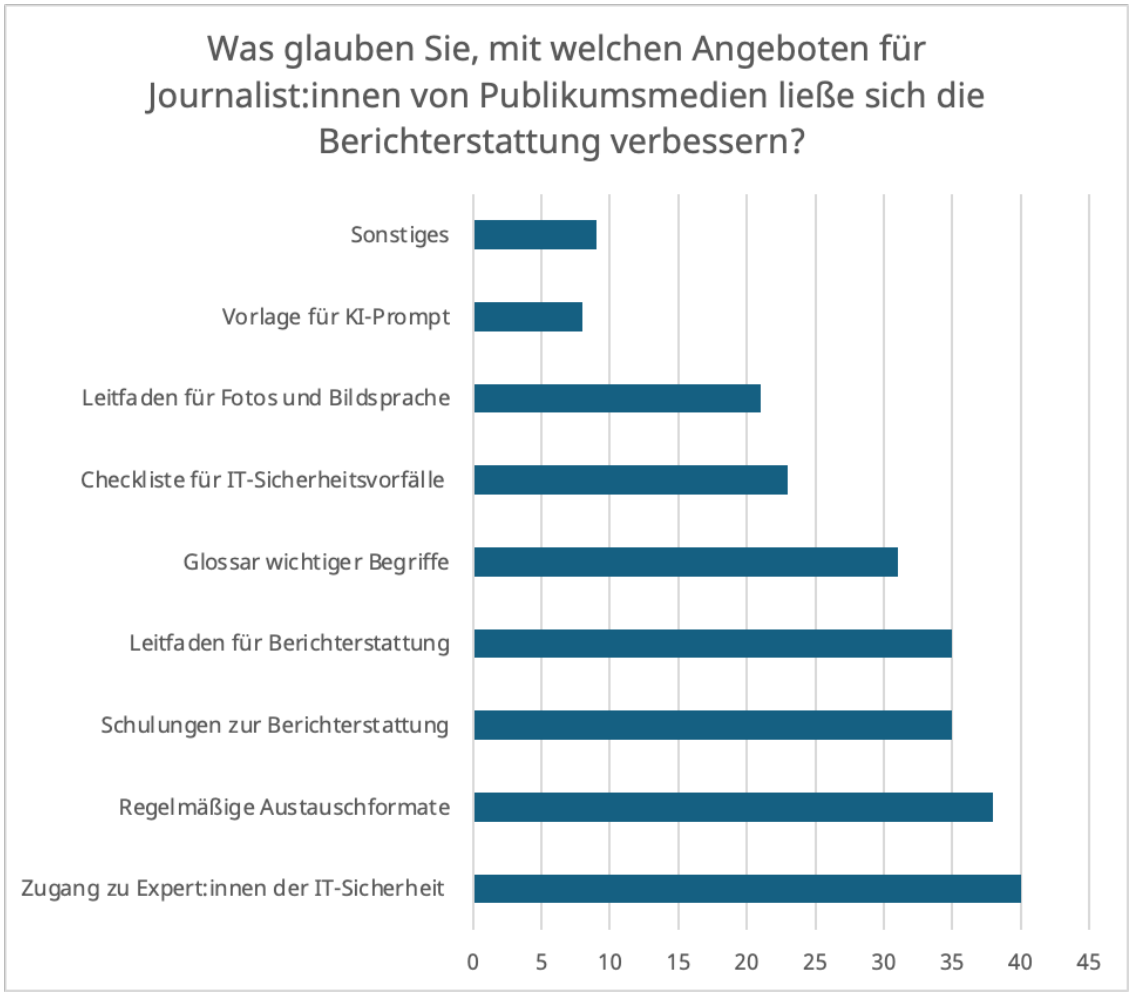


Diagramm: Anzahl der Antworten pro Antwortoption (Mehrfachantwort möglich, 58 Teilnehmende)

Offene Frage: Welche Inhalte sollten Ihrer Meinung nach in einer Handreichung zur Berichterstattung zu IT-Sicherheitsvorfällen für Journalist:innen von Publikumsmedien enthalten sein?

Die Befragten glauben, dass **redaktionelle Standards** für den Akutfall helfen können. In diesem Zusammenhang sprechen sie sich an erster Stelle für **Leitfäden** aus, gefolgt von **Checklisten** und **Glossaren** mit den wichtigsten IT-Fachbegriffen. **Schulungen** halten sie für sinnvoll. Inhalte könnten IT-forensisches Grundwissen und ein allgemeiner Aufbau von IT-Kompetenz sein. Sie wünschen sich Schulungsangebote, die es Journalist:innen ermöglichen, selbst zu urteilen. Die Vermittlung von Infos zu typischen Angriffsszenarien, Abläufen und Akteuren/Gruppen sowie eine klare Abgrenzung unterschiedlicher Vorfallsarten wie Ransomware, Phishing, Datenabfluss, DDoS-Angriff oder technische Störung wird als hilfreich gesehen. Wichtig ist den Befragten dabei, dass IT-Sicherheitsvorfälle nicht vorschnell als reine „Hackerangriffe“ dargestellt werden, sondern Ursachen, Motive und Kontexte differenziert erklärt werden.

Ein zweiter Schwerpunkt könne die Bereitstellung von Recherche- und Bewertungsfragen sein. Zur Bildsprache bei der Berichterstattung schlagen einige Befragte KI-Prompts als Hilfsmittel vor, andere lehnen dies explizit ab.

Darüber hinaus betonen viele Befragte, dass eine gute Berichterstattung nicht bei der technischen Beschreibung eines Vorfalls stehen bleiben darf. Gewünscht werden Inhalte zu gesellschaftlichen, wirtschaftlichen, politischen, rechtlichen und ethischen Folgen und Rahmenbedingungen, etwa zu Datenschutz, KRITIS, NIS-2, DSGVO, Verantwortlichkeiten, Präventionsmaßnahmen und Hilfsangeboten für Betroffene.