

Technische Unterstützung bei Digitaler Gewalt im sozialen Nahraum

Düsseldorf, 27.05.2025



Bundesamt
für Sicherheit in der
Informationstechnik

Agenda

- Auftrag und Zuständigkeit
- Produktportfolio und technische Beratung
- Entwicklungsperspektiven

01. Aufgaben und Zuständigkeit





Bundesamt
für Sicherheit in der
Informationstechnik

MISSION STATEMENT

**Wir machen Deutschland resilient
gegen Cyberbedrohungen
und Sicherheit zum Erfolgsfaktor
für die Digitalisierung.**



Gesetzlicher Auftrag für den Digitalen Verbraucherschutz

§ 2 Absatz 2 BSIG Informationen sowie informationsverarbeitende Systeme, Komponenten und Prozesse sind besonders schützenswert. Der Zugriff auf diese darf ausschließlich durch autorisierte Personen oder Programme erfolgen. Die Sicherheit in der Informationstechnik und der damit verbundene Schutz von Informationen und informationsverarbeitenden Systemen vor Angriffen und unautorisierten Zugriffen im Sinne dieses Gesetzes erfordert die Einhaltung bestimmter Sicherheitsstandards zur Gewährleistung der informationstechnischen Grundwerte und Schutzziele. Sicherheit in der Informationstechnik im Sinne dieses Gesetzes bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen

1. in informationstechnischen Systemen, Komponenten oder Prozessen oder
2. bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen.

§ 3 Absatz 14a BSIG Verbraucherschutz und Verbraucherinformation im Bereich der Sicherheit in der Informationstechnik, insbesondere durch Beratung und Warnung von Verbrauchern in Fragen der Sicherheit in der Informationstechnik und unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen;



Fachbereich K 1 Digitaler Verbraucherschutz



Wir haben die Cybersicherheit der Verbraucherinnen und Verbraucher in Deutschland im Blick.

Technologiemissbrauch im sozialen Nahraum

Angreifermodell des Innentäters bei unseren Angeboten mitdenken

- **K 11: Kooperation und Standardisierung**

Vernetzung und Kooperation, u.a. „BSI im Dialog“ am 11.2.2025 in Berlin

- **K 12: Produktuntersuchungen und Warnungen**

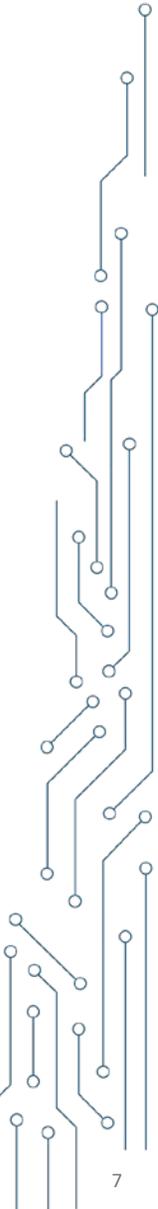
Nächstes Projekt in der Reihe „IT-Sicherheit auf dem digitalen Verbrauchermarkt“: Missbrauch im Smart Home

- **K 13: Verbraucherinformation via Webseite, Social Media, Unterrichtsmaterialien, Podcasts, Newsletter**

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Digitale-Gewalt/digitale-gewalt_node.html

- **K 15 Service-Center und Cyber-Sicherheitsnetzwerk**

0800 274 1000



Praktische Unterstützung für Betroffene

Angebote für technische Beratung

1. Digitale Angebote zur Selbsthilfe (Webseiten oder Apps z.B. Gewaltfrei in die Zukunft)
2. Persönliche technische Beratung (bislang vorwiegend regional z.B. Frauensoftwarehaus Frankfurt e.V.)
3. Technische Beratung über gezielte Weiterbildung der Frauenberatungsstellen (z.B. Baden-Württemberg)
4. Technische Beratung über Frauenberatungsstellen in Abstimmung mit IT-Experten (z.B. Kompetenzstelle gegen Cyber-Gewalt der Stadt Wien)
5. Technische Beratung durch IT-Experten in Abstimmung mit Frauenberatungsstellen (z.B. CETA)
6. Mix aus digitalen Informationsangeboten und kostenfreien Smart Phones (WESNET)

Herausforderung: Technische und psychosoziale Beratung am Bedarf der Betroffenen ausrichten und barrierefrei und kostengünstig anbieten.

Quelle: Ergebnisbericht „Technische Anlaufstelle für Betroffene von digitaler Gewalt in Partnerschaften“ <https://www.dialog-cybersicherheit.de/media/>

Das Cyber-Sicherheitsnetzwerk

Kontaktstelle bei IT-Sicherheitsvorfällen

Das Cyber-Sicherheitsnetzwerk
Für Hilfe bei IT-Sicherheitsvorfällen.
0800-274 1000

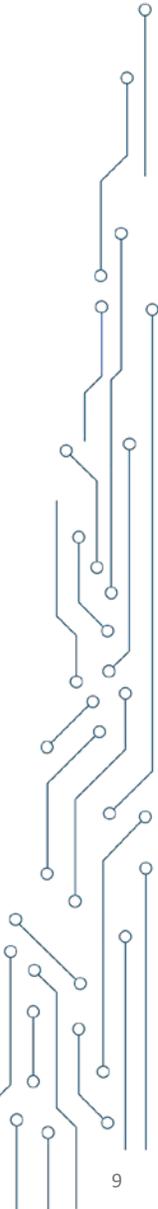
Cyber-Sicherheitsnetzwerk

Bundesamt für Sicherheit in der Informationstechnik

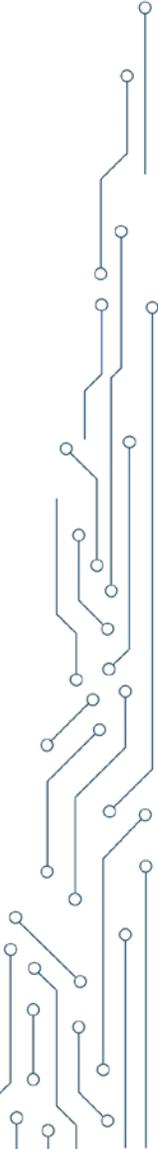
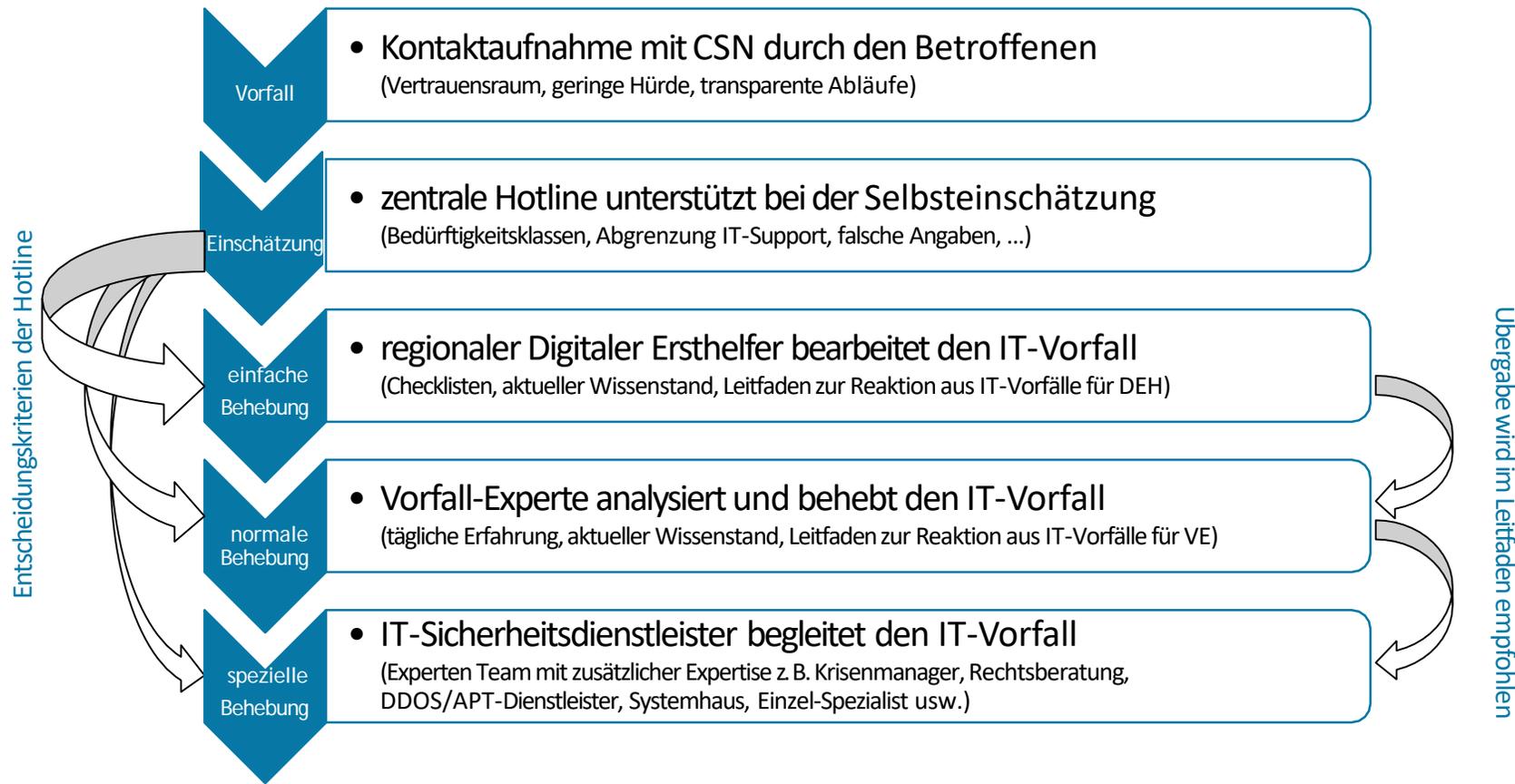
Notfall-Hotline: 0800-274 1000

E-Mail: info@cyber-sicherheitsnetzwerk.de
Internet: www.cyber-sicherheitsnetzwerk.de

Deutschland
Digital•Sicher•BSI



Ablauf der Digitalen Rettungskette



Kostenloser Basiskurs für Digitale Ersthelfer

Basiskurs im Selbststudium

- kostenloser Onlinekurs, bestehend aus drei Modulen in fünf Videos à ca. 20 Minuten
- Selbsttest als Lernkontrolle nach jedem Modul

Begleitmaterial

- Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Digitale Ersthelfer
- Umfang von 60 Seiten mit Aufgaben nach jedem Kapitel, Checklisten zum Ausdrucken.
- Schulungsbescheinigung zum Ausfüllen und Ausdrucken
- Registrierungsformular für das CSN

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Onlinekurs/Onlinekurs_node.html

In 4 Schritten zum Digitalen Ersthelfer

1	<p>Schritt 1</p> <p>Modul 1.1: Das Cyber-Sicherheitsnetzwerk und die Rolle des Digitalen Ersthelfers (Dauer: 17, 19 Minuten)</p> <p>Als Einstieg in diesen Basiskurs begrüßen Sie sich mit dem Grundlagen und der Architektur des Cyber-Sicherheitsnetzwerks sowie der Tätigkeit des Digitalen Ersthelfers. Sie lernen die digitale Berichterstattung und deren verschiedenen Ebenen und Funktionen des Netzes und Aufgaben der Digitalen Ersthelfer im Cyber-Sicherheitsnetzwerk. Ein entsprechende Video auf dem ersten Teil, falls Ihnen etwas von dem Inhalt des Basiskurses, sowie auch die Verantwortlichkeiten, die Verantwortlichkeiten und die Tätigkeiten des Cyber-Sicherheitsnetzwerks zu verstehen.</p> <p>Modul 1.2: Handlungsempfehlungen zum Cyber-Sicherheitsnetzwerk (Dauer: 19, 24 Minuten)</p> <p>Markieren Sie die Grundlagen des Cyber-Sicherheitsnetzwerks kennengelernt haben, beginnt der eigentliche Inhalt des Basiskurses. Im darauffolgenden Video lernen Sie typische IT-Sicherheitsvorfälle, wie die Identifizierung und weitere Handlungsempfehlungen angeschlossen werden können.</p> <p>Eine Übersicht typischer IT-Sicherheitsvorfälle wird folgende Liste:</p> <p>Es sind erlernte Wissen in Bezug auf IT-Sicherheitsvorfälle können Sie im folgenden Selbsttest überprüfen:</p> <p>www.bsi.bund.de/onlinekurs</p>	<p>Ergebnis:</p> <ol style="list-style-type: none"> 1. Online-Kurs für Ersthelfer zur Bekämpfung von IT-Sicherheitsvorfällen 1. Online-Kurs für Ersthelfer zur Bekämpfung von IT-Sicherheitsvorfällen
2	<p>Schritt 2</p> <p>Modul 2.1: Erste Hilfe bei IT-Sicherheitsvorfällen (Dauer: basale Teilnehmende: 19, 20 Minuten)</p> <p>Sie sind also nun gebildet haben, welche typischen IT-Sicherheitsvorfälle es gibt, wie sie sich mit IT-Sicherheitsvorfällen auseinandersetzen und welche Handlungsempfehlungen Sie beschreiben können, beschließen sich Modul 2 mit IT-Sicherheitsvorfällen, die durch Cyber-Angriffe hervorgerufen werden.</p> <p>Somit in Modul 2.2, die auch in Modul 2.2 werden eine Hilfe von typischen IT-Sicherheitsvorfällen aufgeführt und beschrieben werden entsprechende Handlungsempfehlungen von Cyber-Sicherheitsvorfällen aufgeführt. Sie sind also basale Module von Cyber-Sicherheitsvorfällen sind in folgenden Liste dargestellt:</p> <p>Es sind erlernte Wissen in Bezug auf IT-Sicherheitsvorfälle können Sie im folgenden Selbsttest überprüfen:</p> <p>www.bsi.bund.de/onlinekurs</p>	<p>Ergebnis:</p> <ol style="list-style-type: none"> 1. Online-Kurs für Ersthelfer zur Bekämpfung von IT-Sicherheitsvorfällen 1. Online-Kurs für Ersthelfer zur Bekämpfung von IT-Sicherheitsvorfällen
3	<p>Schritt 3</p> <p>Modul 3: Das verteilte Netzwerke (Dauer: 19, 20 Minuten)</p> <p>In Modul 3 des Basiskurses wird die Identifizierung eines Cyberangriffs und professionellen Handlungsempfehlungen beschrieben. Dabei werden grundlegende Netzwerkstrukturen aufgeführt, die Sie während eines Cyber-Angriffs berücksichtigen sollten. Sie lernen auch die verschiedenen IT-Sicherheitsvorfälle, die durch Cyber-Angriffe hervorgerufen werden können, sowie die Handlungsempfehlungen angeschlossen. Eine Übersicht über die wichtigsten IT-Sicherheitsvorfälle, die durch Cyber-Angriffe hervorgerufen werden können, gibt folgende Liste:</p> <p>Wie oft? In welchem Umfang wird sich bewegt? (Häufigkeit oder selten)</p> <p>Wie ist geschaltet? Welche Auswirkungen sind typischer?</p> <p>Wie ist? (Systeme bzw. welche Prozesse sind betroffen?)</p> <p>Sind Experten bzw. Dritte von einem IT-Sicherheitsvorfälle betroffen? (z. B. Partner oder Kunden)</p> <p>Welche der Probleme aufgetreten? Welche Tätigkeiten werden angestrebt? Welche Lösungsmaßnahmen können beschleunigt werden?</p> <p>Wann ist die Regelhaftigkeit aufgetreten? (per Wochen, mit Tagen, gerade eben)</p> <p>Wie schließt sich das Netzwerke? (per Netzwerke, Server, Antivirus, Hardwaredatensicherung)</p> <p>Wirden schon Maßnahmen getroffen? (Wann ja, wann nicht)</p> <p>Es sind erlernte Wissen in Bezug auf das verteilte Netzwerke können Sie im folgenden Selbsttest überprüfen:</p> <p>www.bsi.bund.de/onlinekurs</p>	<p>Ergebnis:</p> <ol style="list-style-type: none"> 1. Online-Kurs für Ersthelfer zur Bekämpfung von IT-Sicherheitsvorfällen
4	<p>Schritt 4</p> <p>Registrierung beim CSN</p> <p>Nach Beendigung aller vorherigen Schritte können Sie die Schulungsbescheinigung ausfüllen und mit dem Registrierungsformular bei dem Cyber-Sicherheitsnetzwerk eintragen. Bitte beachten Sie auch die Datenschutzrichtlinien des Cyber-Sicherheitsnetzwerks. Das Registrierungsformular des CSN wird Ihnen bereitgestellt und Sie bei erfolgreicher Prüfung in der CSN aufgenommen.</p>	<p>Download</p> <ol style="list-style-type: none"> 1. Schulungsbescheinigung für den Basiskurs "Digitale Ersthelfer" 1. Antrag auf Registrierung als Digitaler Ersthelfer im Cyber-Sicherheitsnetzwerk 1. Datenblatt des Cyber-Sicherheitsnetzwerks

Zahlen, Daten, Fakten Cyber-Sicherheitsnetzwerk



20 Trainingseinheiten im neuen Trainingskoffer

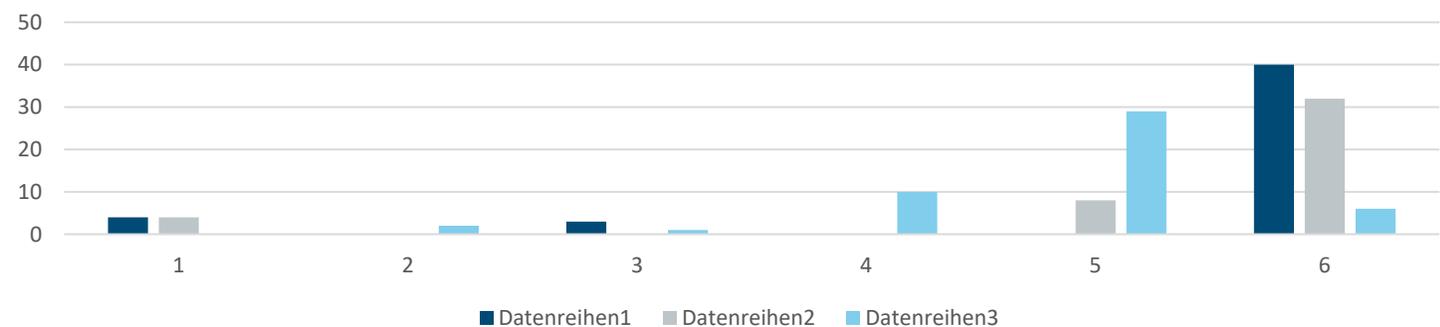
44 Anzahl der Schulungsanbieter

1029 durch die Hotline weitergeleitete IT-Sicherheitsvorfälle

1301 Teilnehmerinnen und Teilnehmer an Schulungen zum Vorfall-Praktiker bzw. Vorfall-Experten

660	36	18	32
Digitale Ersthelfer	Vorfall-Praktiker	Vorfall-Experten	IT-Sicherheitsdienstleister

Arten über die Hotline weitergegebener IT-Sicherheitsvorfälle



Neukonzeption des Cyber-Sicherheitsnetzwerks

Beratungsschwerpunkte und -konzepte

- Über zwei Drittel der Hilfesuchenden kommt aus dem Bereich Verbraucherinnen und Verbraucher
- Weiterentwicklung des Cyber-Sicherheitsnetzwerks zu einer Unterstützungsstruktur nur für diese Zielgruppe
- Erfolgt durch entsprechende Qualifizierung der Digitalen Ersthelferinnen und Ersthelfer, um am Bedarf der Zielgruppe optimal anzusetzen



Abb. Fotolia_99777403

Optionen zur Weiterentwicklung

Vermittlungs- und Verweisungssystem zwischen technischer, (straf-)rechtlicher und psychosozialer Beratung aufbauen

Optionen:

- a) Technische Expertise in Beratungsstellen aufbauen?
- b) Psychosoziale Expertise bei IT-Experten aufbauen?
- c) Kooperativer Beratungsansatz
 - Aufbau von Basiskompetenzen bei Berater*innen (Identifizierung technischer Gewalt) über entsprechenden Kurs des BSI
 - Integration ins Cyber-Sicherheitsnetzwerk als Expert*innen für Digitale Gewalt
 - Zusammenarbeit mit Kolleg*innen aus dem Cyber-Sicherheitsnetzwerk bei anspruchsvollen Fällen



Raum für Diskussion und Ihre Fragen

- z.B. Welche Inhalte müssen vermittelt werden? Was sind die häufigsten Angriffsvektoren?
- Wie können wir mit der Polizei zusammenarbeiten?
- Was wünschen sich Betroffene und wie können sie erreicht werden?
- Welche Hürden bestehen aktuell?

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Katharina Witterhold
Referentin Digitaler Verbraucherschutz

digitalegewalt@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87
53175 Bonn

www.bsi.bund.de



Bundesamt
für Sicherheit in der
Informationstechnik

Follow us:

