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

Bild: © AdobeStock/Liudmyla

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

Querschnittsthemen des Digitalen Verbraucherschutzes und Kooperationen (K 11)

Technischer Verbraucherschutz und Marktbeobachtung (K 12)

Informations-vermittlung und Verbraucher-sensibilisierung (K 13)

Zentrales Service-Center (K 15)

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)

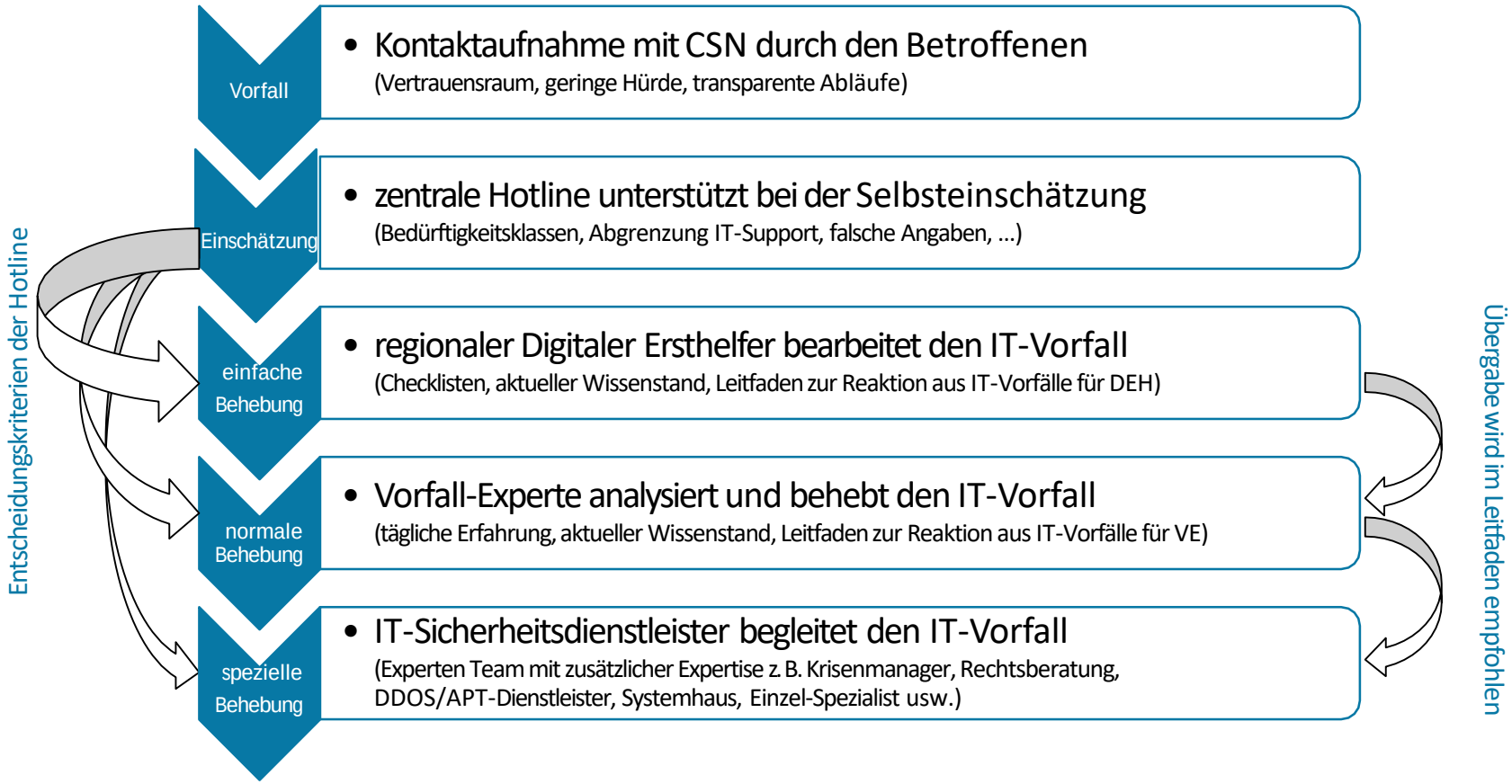
Herausforderung: Technische und psychosoziale Beratung am Bedarf der Betroffenen ausrichten und barrierefrei und kostengünstig anbieten.

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

Das Cyber-Sicherheitsnetzwerk

Kontaktstelle bei IT-Sicherheitsvorfällen

Ablauf der Digitalen Rettungskette



Kostenloser Basiskurs für Digitale Ersthelfer

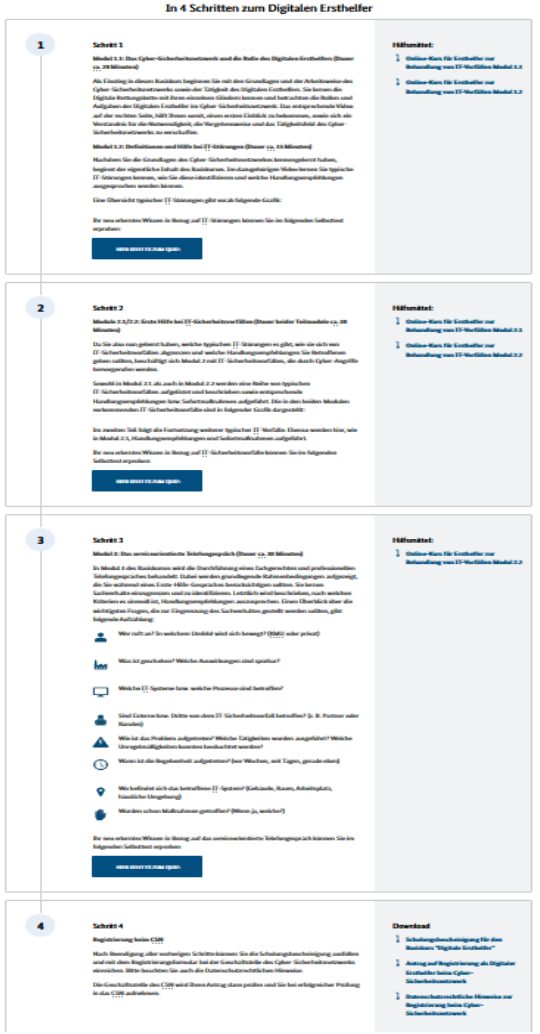
Basiskurs im Selbststudium

- 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

Zahlen, Daten, Fakten Cyber-Sicherheitsnetzwerk

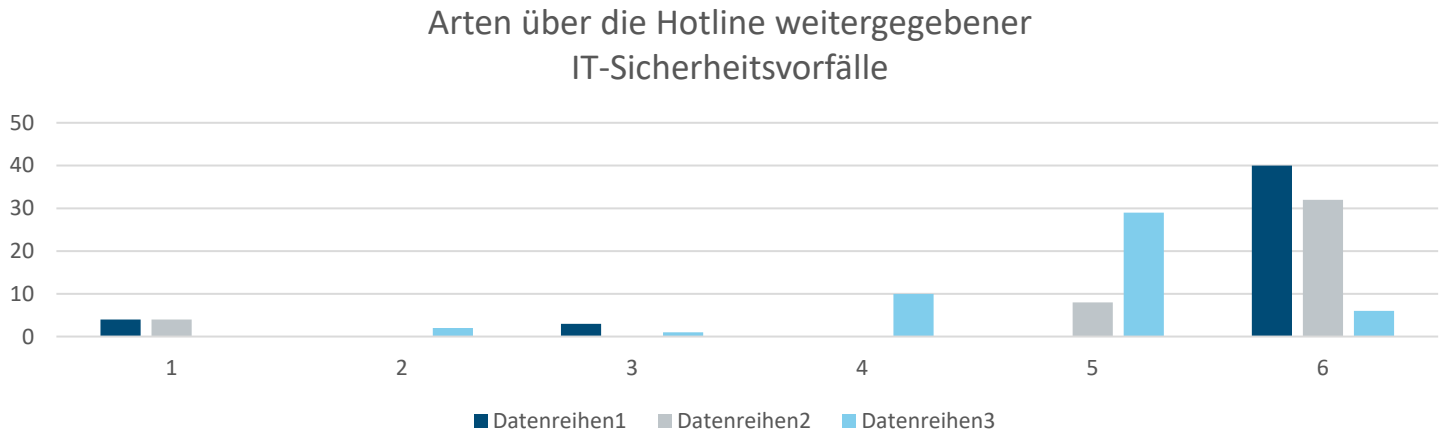
660	36	18	32
Digitale Ersthelfer	Vorfall-Praktiker	Vorfall-Experten	IT-Sicherheits-dienstleiter

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



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

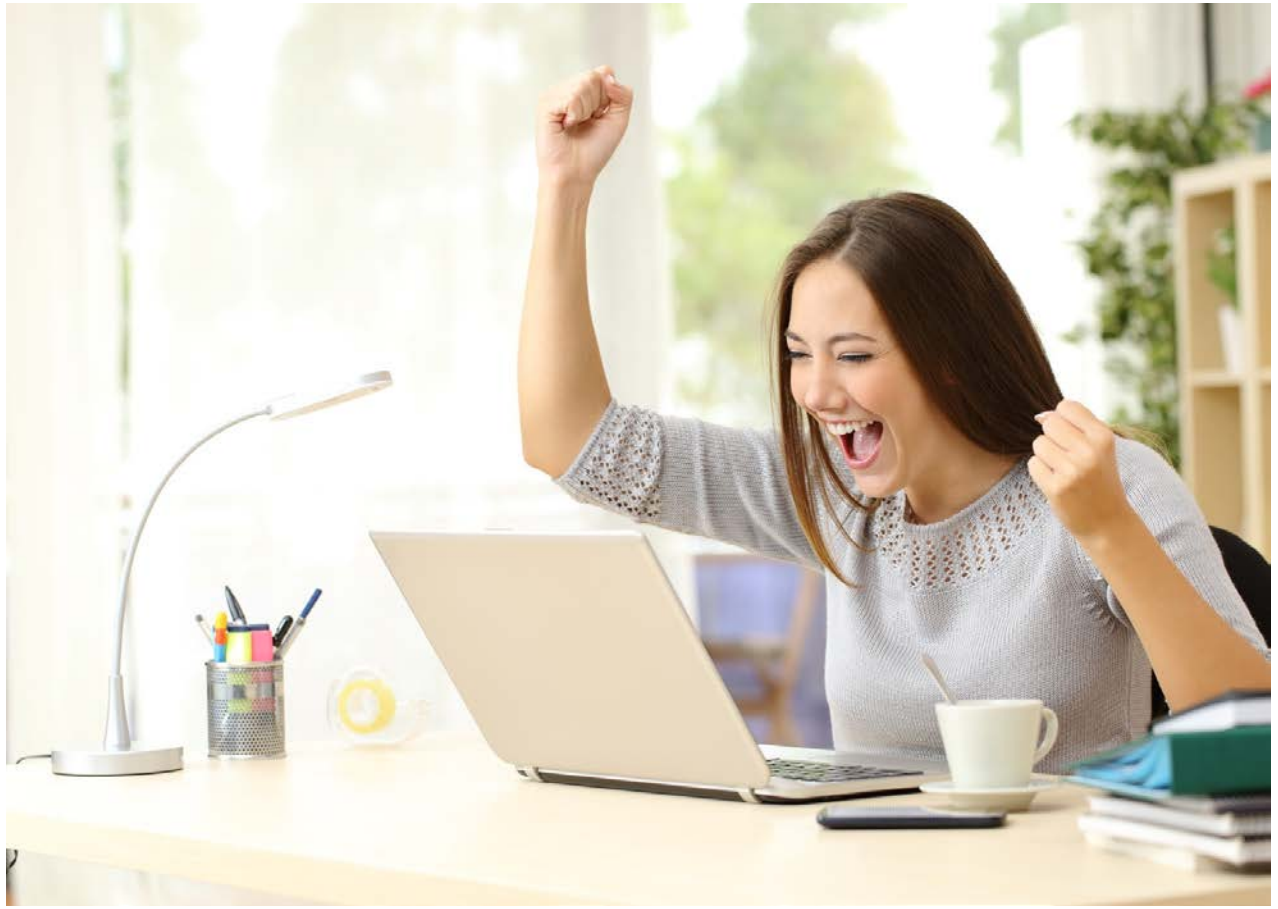


Abb. Fotolia_99777403

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: