



# Das Cyber-Sicherheitsnetzwerk

## Unterstützung nach IT-Sicherheitsvorfällen

Angelika Jaschob

Bonn, den 12.12.2023

# Gliederung

1. Das Cyber-Sicherheitsnetzwerk (CSN)
2. Arbeiten in der Digitalen Rettungskette  
- Unterstützung auf Augenhöhe
3. Drei Stufen der Qualifizierung
4. Schulungsanbieter und Prüfer
5. Trainingskoffer - Möglichkeit zur Vorbereitung auf den Ernstfall
6. Austauschplattform und regionale Foren zur Vernetzung alle Akteure des Cyber-Sicherheitsnetzwerks

Cyber-  
Sicherheitsnetzwerk



## Unterstützung bei IT-Sicherheitsvorfällen

Landkarte der Helfenden



Hilfe zum Einstieg in die „Digitale Rettungskette“: 0800 -274 1000  
Fragen zum Cyber-Sicherheitsnetzwerk an: [info@cyber-sicherheitsnetzwerk.de](mailto:info@cyber-sicherheitsnetzwerk.de)

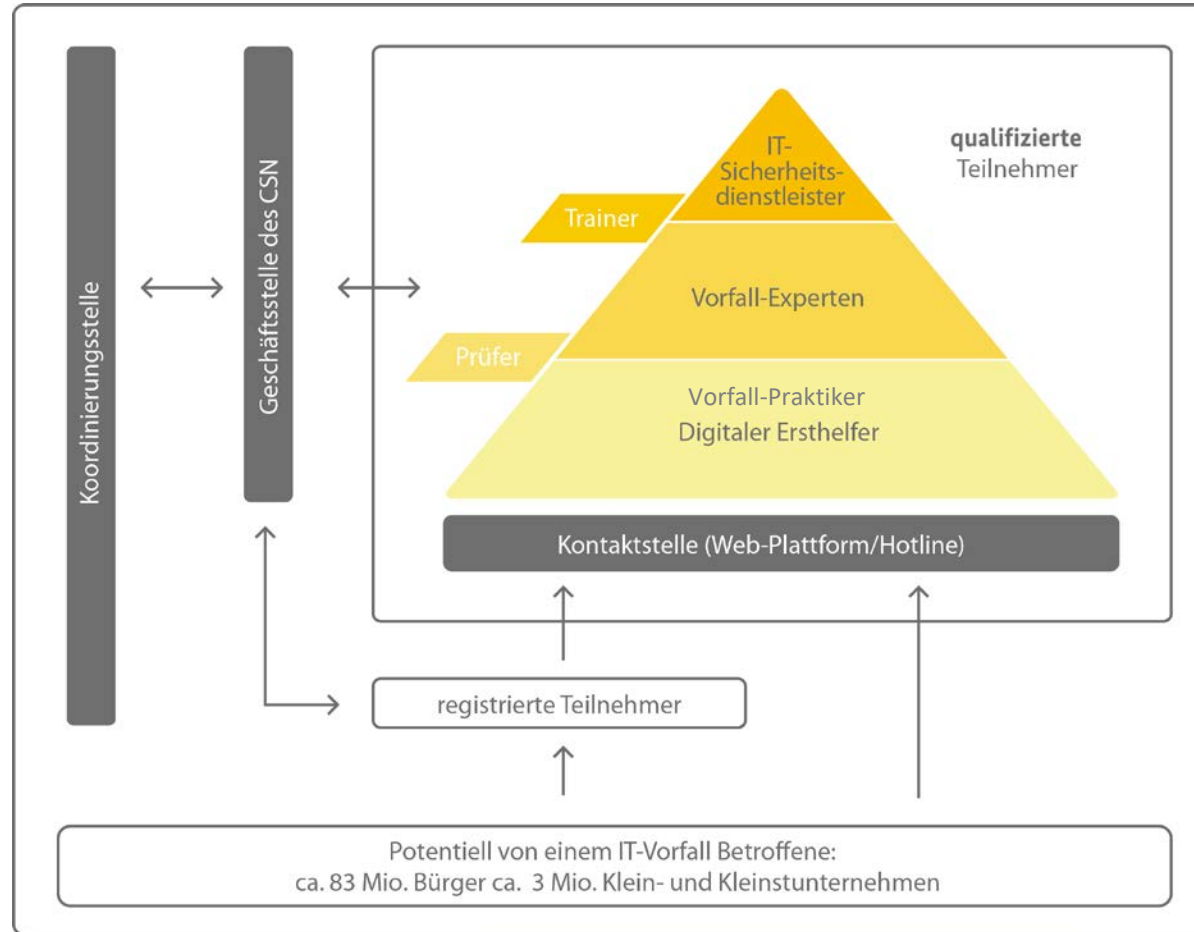


Deutschland  
Digital-Sicher-BSI

# Das Cyber- Sicherheitsnetzwerk (CSN)

**Mit dem Cyber-Sicherheitsnetzwerk soll  
eine flächendeckende dezentrale Struktur aufgebaut werden,  
die effizient und kostengünstig  
KMU und Bürger bei  
IT-Sicherheitsvorfällen Unterstützung anbietet.**

# Aufbaustruktur des Cyber-Sicherheitsnetzwerks



Weitere Informationen zum CSN:



# Arbeiten in der „Digitalen Rettungskette“

## - Unterstützung auf Augenhöhe

# Digitale Rettungskette

**Das Cyber-Sicherheitsnetzwerk**  
Für Hilfe bei IT-Sicherheitsvorfällen.

0800-274 1000

**Notfall-Hotline: 0800-274 1000**

E-Mail: [info@cyber-sicherheitsnetzwerk.de](mailto:info@cyber-sicherheitsnetzwerk.de)  
Internet: [www.cyber-sicherheitsnetzwerk.de](http://www.cyber-sicherheitsnetzwerk.de)

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•



# Kostenlose Kontaktstelle bei IT-Sicherheitsvorfällen

Deutschland  
Digital•Sicher•BSI•

## Hilfe zur Selbsthilfe

- „TOP 12 Maßnahmen“ bei Cyber-Angriffen
- Maßnahmenkatalog zum Notfallmanagement - Fokus IT-Notfälle
- Erste Hilfe bei einem schweren IT-Sicherheitsvorfall, Version 1.1

## Kontakt zum Service Center (Hotline)

- Kostenlose Hotline-Nummer
- Zentrale Anlaufstelle, deutschlandweite Hotline
- Ersteinschätzung des IT-Sicherheitsvorfalls, um im richtigen Glied der Rettungskette einzusteigen





# Schnelle Hilfe bei IT-Sicherheitsvorfällen

Deutschland  
Digital•Sicher•BSI•

## Schnelle und einfache Ersthilfe durch Digitale Ersthelfer (DEH) für Verbraucherinnen und Verbraucher

- DEH löst kleine IT-Störungen und IT-Sicherheitsvorfälle (telefonische Ersthilfe)
- Leitplanken gibt ein Leitfaden mit konkreten Handlungsempfehlungen

## Schnelle Ersthilfe für KMU durch Vorfall-Praktiker (VP)

- VP löst kleine IT-Sicherheitsvorfälle (telefonische Ersthilfe)

## Umfangreiche IT-Vorfallsanalyse durch personenzertifizierte Vorfall-Experten (VE)

- Tiefgehende Analysegespräche
- Vor-Ort-Unterstützung möglich, falls erforderlich

## Lösung komplexer IT-Sicherheitsvorfälle durch einen IT-Sicherheitsdienstleister mit einem Team von Vorfall-Experten



**Kartenansicht** **Suchen nach**

**Aktivierung notwendig**

Wenn Sie die interaktive Karte nutzen möchten, wird Ihre IP-Adresse an den Kartenanbieter OpenStreetMap übertragen. Dieser ist selbst für die Verarbeitung verantwortlich. Alle Informationen dazu finden Sie in der [OpenStreetMap Privacy Policy](#)

**EINVERSTANDEN**

- Digitaler Ersthelfer
- Vorfall-Praktiker
- Vorfall-Experte
- IT-Sicherheitsdienstleister



**Kartenansicht** **Suchen nach**

- Digitale Ersthelfer
- Vorfall-Praktiker
- Vorfall-Experten
- IT-Sicherheitsdienstleister

**Suche Digitale Ersthelfer**

Mit der Suchfunktion können Sie nach Namen, Ort oder PLZ filtern. Durch Eingabe von mehr oder weniger Buchstaben des Ortes bzw. des Namens oder Ziffern der PLZ können Sie Ihre Suche entsprechend einschränken oder ausweiten.

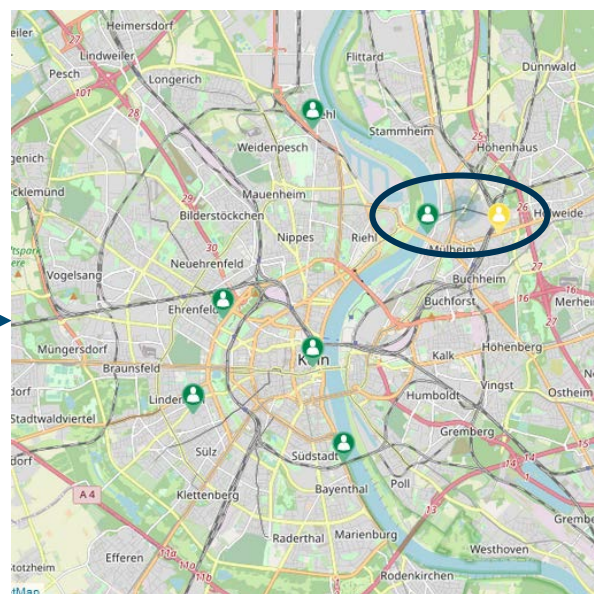
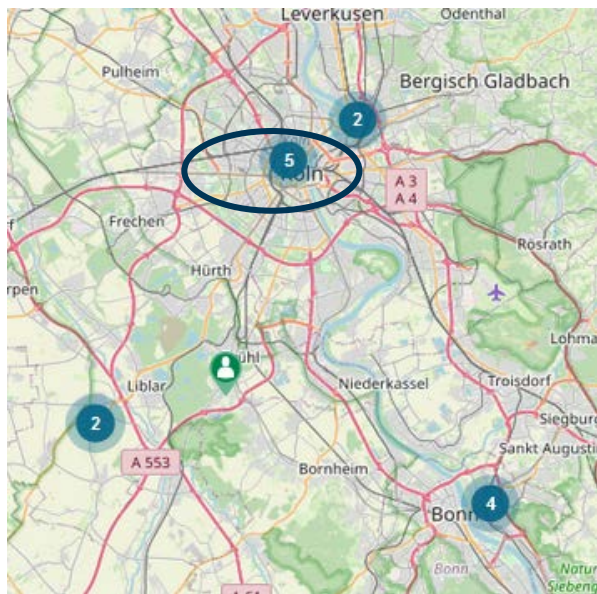
Ohne Sucheintrag, werden Ihnen alle eingetragenen "Digitale Ersthelfer" ausgegeben.

**Name**  
**Ort**  
**PLZ**

**Senden**

**1 bis 1 von 1 Ergebnissen für Ihre Suche nach ""**

Name	Ort	PLZ
Subotta, Michel	Köln	51063



**Max Mustermann**  
54321 Musterstadt  
+49 123456789  
[Beispiel@csn.de](mailto:Beispiel@csn.de)

**Mehr**

**Max Mustermann**

**Max Mustermann**

**Servicezeiten:**  
Montag-Donnerstag: 10:00 – 17:00 Uhr  
Freitag: 10:00 – 15:00 Uhr  
54321 Musterstadt  
Telefon: +49 123456789  
E-Mail: [Beispiel@csn.de](mailto:Beispiel@csn.de)

# Broschüren zum Nachlesen



Die Broschüre befindet sich hier:

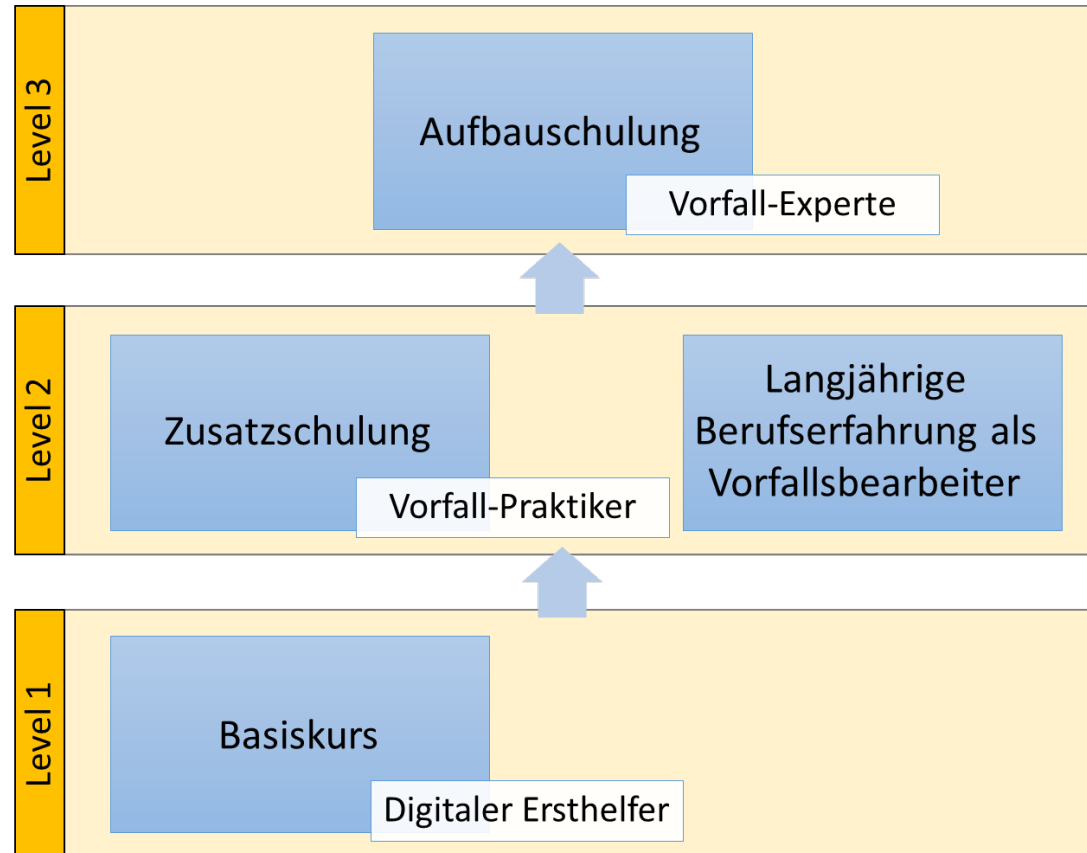


Die Broschüre befindet sich hier:



# Drei Stufen der Qualifizierung im Cyber-Sicherheitsnetzwerk

# Qualifizierungsprogramm



# Anforderungen



# Digitale Ersthelfer

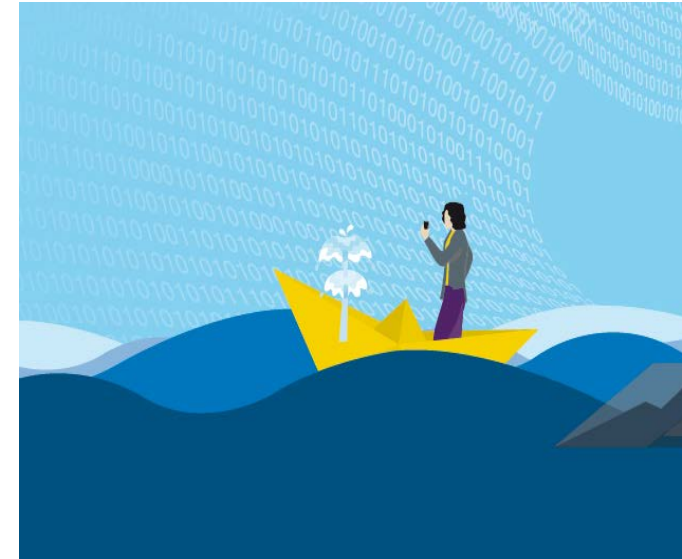
# Kostenloser Basiskurs für Digitale Ersthelfer

## 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



Der Basiskurs für  
Digitale Ersthelfer  
befindet sich hier:





# Inhalte des Basiskurs für Digitale Ersthelfer

## Modul 1

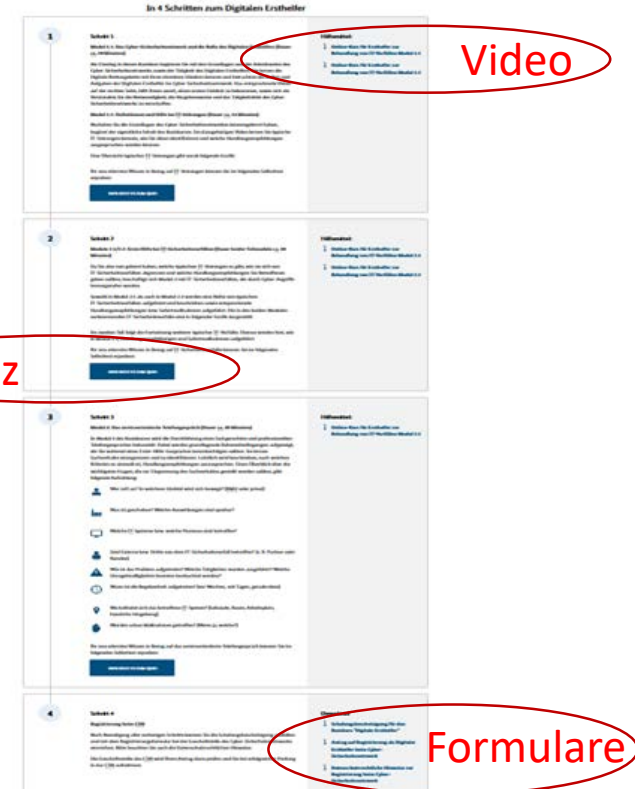
- Grundlagen des Cyber-Sicherheitsnetzwerks
- Unterschiede IT-Störung vs. IT-Vorfall
- Handlungsempfehlungen für typische IT-Störungen

## Modul 2

- Definition, Reaktion und Handlungsempfehlungen für typische IT-Sicherheitsvorfälle

## Modul 3

- Durchführung fachgerechter und professioneller Telefongespräche, anhand praxisnaher Beispiele



# Handlungsempfehlungen für Digitale Ersthelfer

### HANDLUNGSEMPFEHLUNGEN für Digitale Ersthelfer des Cyber-Sicherheitsnetzwerkes

**Keine Internet-Verbindung**

- Netzwerktafel/WLAN-Verbindung kontrollieren
- Router prüfen
- Router neu starten
- Netzwerktafel tauschen/WLAN Adapter/Netzwerktafel aktivieren\*

**Wechseldatenträger werden nicht erkannt**

- Verwendung eines anderen USB-Ports
- Andere USB-Medien/CD nutzen
- Treibersoftware des CD-Laufwerks aktualisieren\*
- Laufwerksschleife des USB-Mediums ändern\*

**Gerät startet nicht**

- Netztafel kontrollieren
- Geräte verriegeln, neu starten/ Kontrollschalter am Netzteiler kontrollieren (nur bei Stand-PC)
- Andere Steckdose verwenden
- Netztafel tauschen

**E-Mail-Probleme**

- Internetverbindung/Spam-Filter prüfen
- Anwendung/Computer neu starten
- Speicher leeren

**IT-Störung**



**Fehlermeldung wird angezeigt**

- Gerät neu starten
- Gerät strecken machen

**Drucker druckt fehlerhaft**

- Drucker neu starten
- Toner/Tinte ersetzen
- Verbindung überprüfen
- Verbindungsbeleg austauschen
- Papier auflegen
- Aktuelle Treiberversion installieren\*

**Drucker druckt nicht**

- Drucker neu starten
- Druckkopf reinigen/Drucker/Tintenpatrone austauschen
- Verbindungsbeleg austauschen
- Papier auflegen
- Aktuelle Treiberversion installieren\*

\*IT-Kenntnisse erforderlich

Weiterführende Unterstützung durch den IT-Support.




Deutschland Digital-Sicher-BSI

### HANDLUNGSEMPFEHLUNGEN für Digitale Ersthelfer des Cyber-Sicherheitsnetzwerkes

**Virencanner erkennt Viren**

- Virencanner arbeiten lassen
- Computer vom Netz nehmen
- Dokumente schützen
- Programme beenden
- Weiterführende Überprüfung von Dateien

**Dateiverschlüsselung durch Ransomware**

- Berechtigungen kontrollieren (bei Firmennetzwerk)
- Computer vom Netz isolieren
- Zahlungsaufforderung nicht nachkommen.

**Kontomissbrauch Soziale Netzwerke**

- Aktive Sitzungen kontrollieren
- Zugangsdaten (Passwort) ändern
- Kontakte informieren
- An den Betreiber der Plattform wenden

**Ausspionieren**

- Passwortänderung
- Sicherheitssoftware kontrollieren
- Updates installieren
- Webcam/Mikrofon deaktivieren oder deaktivieren

**IT-Vorfall**



**Botnetz**

- Computer vom Netz nehmen
- Virencan durchführen
- Internet-Datenverkehr kontrollieren\*

**Diebstahl eines Mobilgerätes**

- Gerät lokalisieren
- SIM-Karte sperren
- Benutzer deaktivieren (bei Firmennetzwerk)
- Daten aus der Ferne löschen

**Merkwürdige Weiterleitungen**

- Browser neu starten
- Alternativen Browser verwenden
- Gerät neu starten
- Virencan durchführen
- Browser neu installieren\*

\*IT-Kenntnisse erforderlich

Weiterführende Unterstützung durch einen Vorfall-Experten.




Deutschland Digital-Sicher-BSI

### HANDLUNGSEMPFEHLUNGEN für Digitale Ersthelfer des Cyber-Sicherheitsnetzwerkes

**Misbrauch der E-Mail-Adresse**

- Zugangsdaten (Passwort) ändern
- Kontakte informieren

**Fälschliche Aufforderung zur Passwortänderung**

- Bei Aufforderung Passwort nicht ändern
- E-Mail-Absender verifizieren\*
- Support kontaktieren
- Zugangsdaten ändern

**Kontomissbrauch Online-Banking**

- Zugangsdaten (Passwort) ändern
- An den Betreiber der Plattform wenden
- Transaktion widerrufen

**Ungewöhnliche Warnhinweise**

- Aufforderungen nicht nachkommen
- Virencan durchführen

**IT-Vorfall**



**Anwendungen installieren sich von selbst**

- Computer vom Netz nehmen
- Virencan durchführen
- Computer zurücksetzen

**Datenverlust durch Schadsoftware**

- Computer vom Netz nehmen
- Virencan durchführen
- Datensicherung wiederherstellen

**Gerät agiert eigenständig**

- Computer vom Netz nehmen
- Virencan durchführen

\*IT-Kenntnisse erforderlich

Weiterführende Unterstützung durch einen Vorfall-Experten.




Deutschland Digital-Sicher-BSI



Deutschland Digital-Sicher-BSI

## Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Digitale Ersthelfer



Version 1.0






Deutschland Digital-Sicher-BSI

# Vorfall-Praktiker



# In 6 Schritten zum Vorfall-Praktiker

- 1. Schritt:** Grundlegendes IT-Verständnis mitbringen
- 2. Schritt:** Erste Erfahrungen bei der Vorfallsbearbeitung gesammelt
- 3. Schritt:** Den Basiskurs zum Digitalen Ersthelfer (Selbstlernkurs) absolvieren
- 4. Schritt:** Eine zweitägige Zusatzqualifikation zum Vorfall-Praktiker besuchen
- 5. Schritt:** Die Kompetenz, durch eine theoretische und „praktische“ Prüfung bei einem registrierten Schulungsanbieter, nachweisen
- 6. Schritt:** Registrierungsantrag incl. Nachweisen zum Vorfall-Praktiker beim CSN einreichen



Informationen  
zum Vorfall-  
Praktiker befinden  
sich hier:



# Inhalte der Zusatzqualifikation zum Vorfall-Praktiker

## Zusatzschulung 2 tägig + ½ Prüfungsworkshop

- Einführung in das Cyber-Sicherheitsnetzwerk incl. Rahmenbedingungen für Digitale Ersthelfer, Vorfall-Praktiker und Vorfall-Experten
- Verhalten am Telefon inkl. nicht technischer Maßnahmen
- Gefährdungen, Angriffsformen und Übersicht über die aktuelle Gefährdungslage
- Ablauf des Standardvorgehens, Behandlung von IT-Sicherheitsvorfällen
- Remote-Unterstützung
- Vorfallsbearbeitung bei IT-Systemen „abseits der üblichen Büroanwendung“
- „Nach dem Vorfall ist vor dem Vorfall“–Präventive Maßnahmen

**Begleitmaterial:** Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Vorfall-Praktiker und Vorfall-Experten



# Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Vorfall-Praktiker und Vorfall-Experten

1 Einführung in das Cyber-Sicherheitsnetzwerk (VP&VE)

## 1 Einführung in das Cyber-Sicherheitsnetzwerk (VP&VE)

Der vorliegende Leitfaden ersetzt den Leitfaden „Reaktion auf IT-Sicherheitsvorfälle für Vorfall-Experten“. Mit der Einführung der neuen Rolle des Vorfall-Praktikers wurden die Inhalte erweitert.



Dieser Leitfaden ist Grundlage für die Schulung zum Vorfall-Praktiker, bzw. die Schulung zum Vorfall-Experten. Die jeweilige Relevanz der Kapitel für die Prüfung ist durch die farblichen Abkürzungen VP (= Vorfall-Praktiker) und VE (=Vorfall-Experte) in der jeweiligen Kapitelüberschrift gekennzeichnet.

6 Behandlung von speziellen IT-Sicherheitsvorfällen (VP&VE)

## 2 Verhalten am Telefon und nichttechnische Maßnahmen (VP)

### 2.1 Intention und Lernziele

Nach Abschluss dieses Moduls sind die Schulungsteilnehmerinnen und Schulungsteilnehmer in der Lage:

-  Professionalität geübt
-  Sicher und kompetent

6 Behandlung von speziellen IT-Sicherheitsvorfällen (VP&VE)

## 9 Vor-Ort-Unterstützung: Überblick verschaffen (VE)

### 9.1 Einführung

Aufgrund von fehlenden Voraussetzungen oder Rahmenbedingungen kann es manchmal unumgänglich sein, einen Betroffenen vor Ort zu unterstützen, um einen IT-Sicherheitsvorfall ordnungsgemäß zu behandeln. Jedoch müssen auch bei der Vor-Ort-Unterstützung bestimmte Voraussetzungen erfüllt sein, damit eine reibungslose und gesetzeskonforme Behandlung gewährleistet werden kann. Betroffene sollten dabei bedenken, dass der Vorfall-Experte direkten Zugriff auf organisationsinterne Informationen erhalten kann und



Den Leitfaden finden Sie hier:



# Vorfall-Experte



# In 5 Schritten zum Vorfall-Experten

**Schritt 1:** dreitägige Aufbauschulung besuchen

**Schritt 2:** Zertifizierungsantrag mit Nachweisen

**Schritt 3:** Prüfung beim BSI ablegen und Zertifikat

**Schritt 4:** Registrierung im Cyber-Sicherheitsnetzwerk

**Schritt 5:** Aufrechterhaltung der Kompetenzen



Informationen  
zum Vorfall-  
Experten  
befinden sich  
hier:





# Inhalte der Aufbauschulung zum Vorfall-Experten

## Aufbauschulung 3-tägig

- Einführung und Rahmenbedingungen für den Vorfall-Experten
- Ablauf des Standardvorgehens mit Übungen
- Angriffsszenarien und Forensik mit Übungen
- Remote-Unterstützung
- Vor-Ort-Unterstützung: „Überblick verschaffen“ und Übungen
- Vor-Ort-Unterstützung: „Vorfallsbearbeitung“ und Übungen
- „Nach einem Vorfall ist vor einem Vorfall“ und Fazit

**Begleitmaterial:** Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Vorfall-Praktiker und Vorfall-Experten



# Anforderungen der Personenzertifizierung

## Aufbauschulung bei registrierten Schulungsanbietern

- 3-tägige Schulung

## Begleitmaterial

- Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Vorfall-Experten

## Personenzertifizierung durch die Zertifizierungsstelle des BSI

- Nachweis über Bildungsabschluss und Berufserfahrung
- Nachweis von Praxiserfahrung (Projekte)
- Schulungsbescheinigung
- Kompetenzprüfung im BSI



Weitere Informationen zum Programm für die Personenzertifizierung zum Vorfall-Experten befinden sich hier:

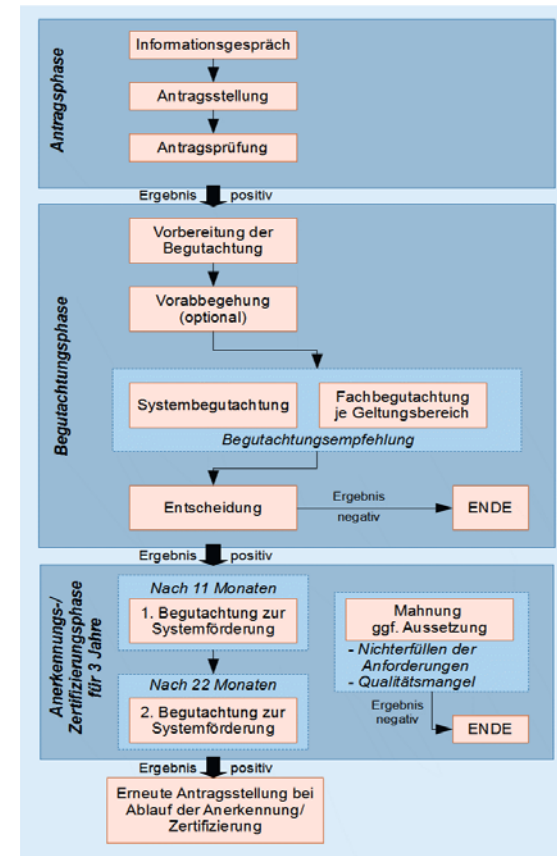


# IT-Sicherheitsdienstleister Vorfallsbearbeitung

# Zertifizierung IT-Sicherheitsdienstleister Vorfallsbearbeitung

## Erforderliche Nachweise für den IT-Sicherheitsdienstleister

- Systemdokumentation Qualitätsmanagement:  
Prozessbeschreibung Vorfallsbehandlung
- Informationssicherheitsmanagement: Informationsverbund zur Durchführung einer Vorfallsbehandlung
- Personenzertifikate von mindestens 2 Vorfall-Experten **oder** 1 Vorfall-Experte und 2 Vorfall-Praktiker
- Sicherheitskonzept auf der Basis von IT-Grundschutz, mindestens für den Bereich der Vorfallsbehandlungen durchgeführt
- Bereitschaft zur Aufnahme in die Geheimschutzbetreuung



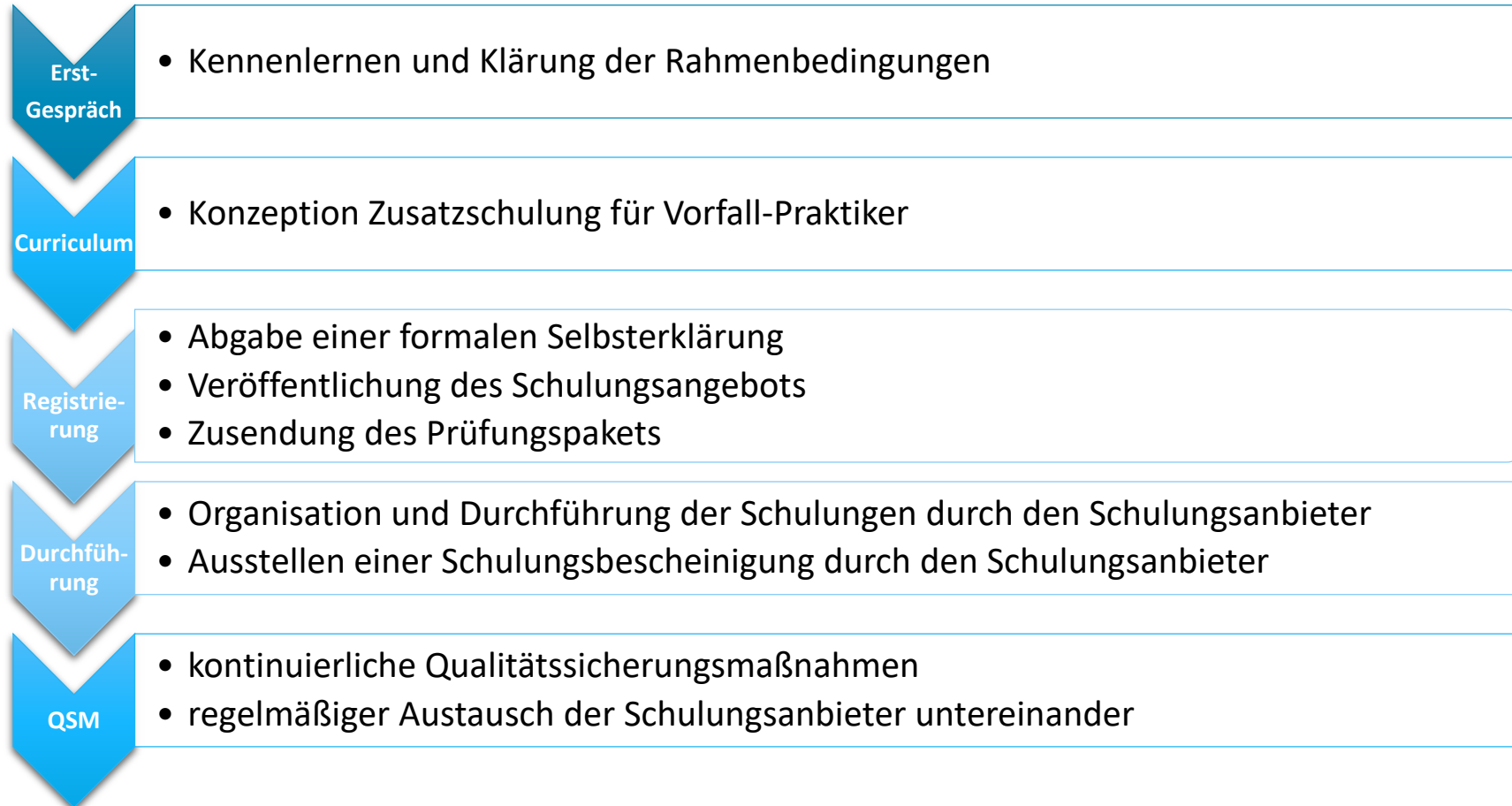
Verfahrensbeschreibung zur Zertifizierung für IT-Dienstleister für den Bereich Vorfallsbearbeitung finden Sie hier:



# Schulungsanbieter



# Prozessablauf für qualifizierte Schulungsanbieter (VP)



Eine Liste aller Schulungsanbieter finden Sie hier:



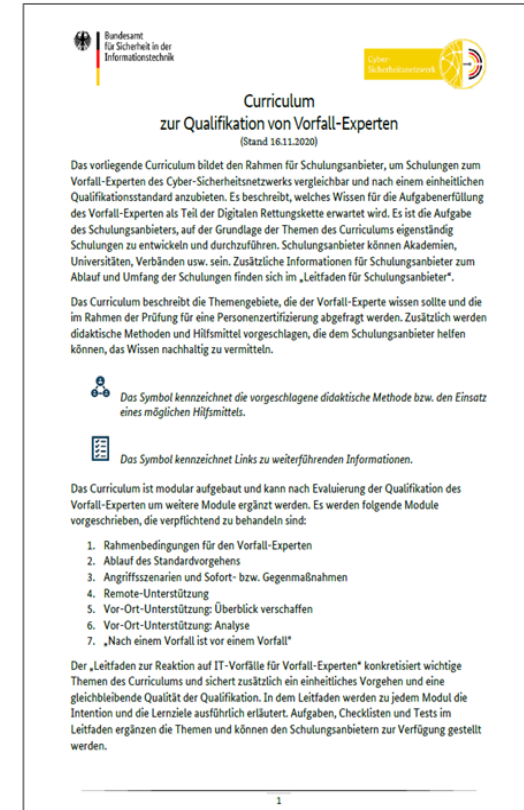
# Registrierte Schulungsanbieter

Bei Interesse wird das Informationspaket jedem Schulungsanbieter oder Trainer nach einem kurzen Informationsgespräch zugesandt.

## Inhalt des Schulungspaketes

- Curriculum
- „Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Vorfall-Praktiker und Vorfall-Experten“
- Übungspaket mit 10 Übungsideen
- Leitfaden für Schulungsanbieter und Trainer
- Ggf. Prüfungsfragen und Fallbeispiele

**Alle Schulungsanbieter sind auf den Webseiten veröffentlicht.**



# Trainingskoffer

- Möglichkeit zur Vorbereitung auf den Ernstfall



# Der digitale Trainingskoffer

- Trainingseinheiten und Spiele zum Thema
  - Cyber-Sicherheitsnetzwerk und
  - Vorfallsbehandlung
- Keine allgemeinen Awareness-Maßnahmen für IT-Sicherheit
- „Gamification“ zur Motivation der Aufrechterhaltung der Kompetenzen und Weiterbildung
- einzelne Trainingseinheiten kostenlos zum Herunterladen und Ausdrucken auf der BSI-Website



Den Trainingskoffer  
finden Sie hier:



# Spiele und Trainingseinheiten aus dem Trainingskoffer

- **Störung oder Vorfall** (Zuordnungsspiel)
- **Vor-Ort-Unterstützung** (Memory)
- **Digitale Rettungskette** (Domino)
- **Vorfallsbearbeitungs-Quiz** (Quizspiel)
- **Trainingszirkel** (Trainingsstationen)
- **Tutorium** (Karten-/Quizspiel)
- **Protect & Hack** (Brettspiel)



Deutschland  
**Digital•Sicher•BSI**



# Rollenspiele

- Störung
- Social Engineering
- Phishing
- Ransomware
- Fernzugriff
- Webshop
- Bots

# Deutschland Digital•Sicher•BSI•

CSN TRAININGS-KOFFER: Social Engineering & CEO-Fraud  
Rollenspiel: Rollenkarte 4

Herr Rath S. 1/4

### 🛡️ Rolle: Herr Rath, Geschäftsführer der Lions IT GmbH

Du bist Herr Rath, Geschäftsführer der Lions IT GmbH.

Du bist seit 20 Jahren auf deiner jetzigen Position, nachdem du bei der frisch gegründeten Lions IT GmbH bereits deine kaufmännische Ausbildung absolviert hast und über die Jahre in die Geschäftsleitung aufgestiegen warst.

Du bist lokal sehr engagiert, unter anderem in Gemeindefarbeit deiner katholischen Kirche und als Trainer bzw. in der Jugendarbeit des lokalen Hockeyvereins und daher lokal bekannt und sehr beliebt.

Deine weiteren Hobbys sind Rennradfahren, Restaurantbesuche, Kochen und Social Media.

Gestern warst du bei einem Vorstandessen des Hockeyvereins, der gerade Spenden für ein neues Trainingszentrum akquiriert.

Abends hast du von der Security Managerin, Frau Schmitt, erfahren, dass es einen Versuch eines gerade noch vereitelten CEO-Fraud gegeben haben soll und auch deine Assistenz, Frau Miller, sensible Informationen am Telefon vermutlich gegenüber einem Fremden preisgegeben hat, der sich als dein „alter Schulfreund“, Herr Merkel, ausgeben hatte.

Du kennst Merkel tatsächlich aus der Schule, hast ihn aber seitdem nicht mehr getroffen oder gesprochen.

Diese Informationen haben dich erinnern lassen, dass es zuletzt auf den Social Media-Kanalen eine ungewöhnliche Häufung von Kontaktanfragen dir fremder Personen gegeben hat – normalerweise erhältst du beinahe ausschließlich Anfragen aus dem geschäftlichen Umfeld oder dem deines sozialen Engagements bzw. deiner Hobbys. Du kannst dich nicht genau erinnern, von wem bzw. ob du Anfragen von Fremden angenommen hast, weil es gegebenenfalls Überschneidungen mit deinen geschäftlichen oder freizeithlichen Aktivitäten gegeben haben könnte.



Deutschland  
Digital-Sicher-BSI

bsi@bundesamt-sicherheit.de - http://www.bsi.bund.de

CSN TRAININGS-KOFFER: Social Engineering & CEO-Fraud  
Rollenspiel: Rollenkarte 4

Herr Rath S. 3/4

In der Spielsituation geht es unter anderem darum, dass einer Mitarbeitenden, die als Assistentin der Geschäftsführung tätig ist, nach einem Telefonat mit einer ihr unbekannt Person gewährt worden ist, dass sie möglicherweise von einem Social Engineer ausgehört wurde und potenziell Informationen über ihren Chef preisgegeben hat.

Außerdem hat sich ein Mitarbeitender aus der Finanzbuchhaltung gemeldet und einen Verdacht in Richtung eines versuchten CEO-Fraud geäußert.

Durch die Meldung bei Frau Schmitt wurde der Geschäftsführer zu weiteren Auffälligkeiten befragt.

### 😊 Emotionaler Hintergrund

Du denkst: „Mensch, dass ausgerechnet uns als IT-Berater so etwas passieren muss – das ist schon peinlich. Aber gut, dass es erstmal keine schlimmen Konsequenzen hatte. Und gerade ich als Geschäftsführer muss besser aufpassen, dass mir so etwas nicht mehr passiert.“

Du wirst jedoch auch zunehmend bewusst, dass du als Chef möglicherweise kein gutes Vorbild warst und alle Mitarbeitenden zu einer sehr offenen Informationskultur eingeladen hast – vielleicht keine gute Idee bei fortschreitender Digitalisierung mit all den Risiken des Informationsverlustes bei hoher Verfügbarkeit von Informationen.

### ! Eigene Notizen zum Rollenspiel:

---



---

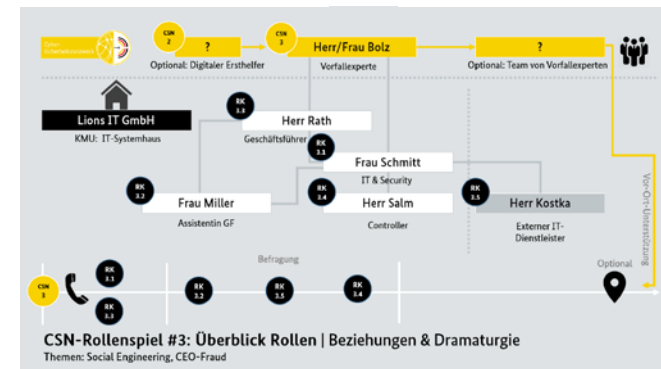


---



Deutschland  
Digital-Sicher-BSI

bsi@bundesamt-sicherheit.de - http://www.bsi.bund.de



Bundesamt  
für Sicherheit in der  
Informationstechnik

# Escape-Game

Fiktive Spielsituation zu existenz-bedrohendem Cyber-Angriff auf ein kleines Unternehmen.

**Ziel:** gemeinsam mit einer Vorfall-Praktikerin einen IT-Sicherheitsvorfall zu lösen.

## Zielgruppe:

- Digitale Ersthelfer
- Vorfall-Praktiker
- Vorfall-Praktiker des Unternehmen

**Gruppengröße:** 4 bis 12 Personen

**Zeitungfang:** ca. 90 Minuten



Deutschland  
**Digital•Sicher•BSI•**



# Zusammenfassung

# Zahlen, Daten, Fakten des Cyber-Sicherheitsnetzwerks



**19** Trainingseinheiten im neuen Trainingskoffer

**38** Anzahl der Schulungsanbieter

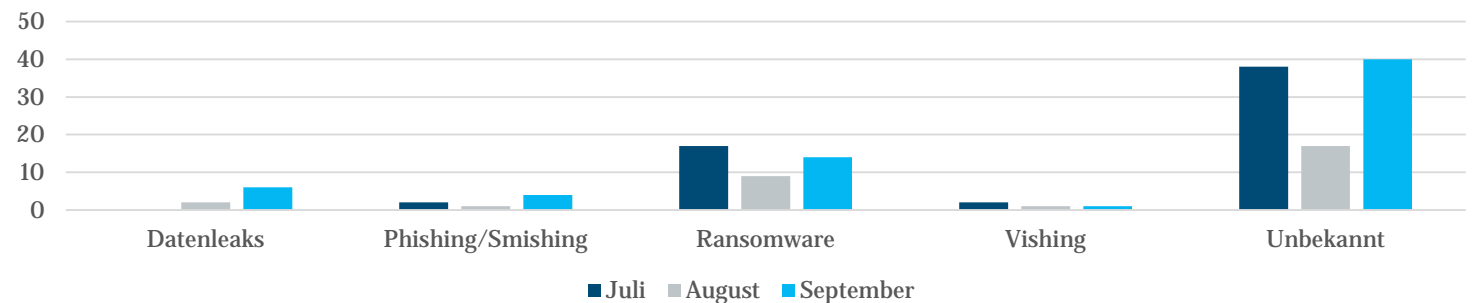
**555** durch die Hotline weitergeleitete IT-Sicherheitsvorfälle

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

<b>345</b>	<b>22</b>	<b>13</b>	<b>16</b>
Digitale Ersthelfer	Vorfall-Praktiker	Vorfall-Experten	IT-Sicherheitsdienstleiter



Arten der über die Hotline weitergeleiteten IT-Sicherheitsvorfälle



## Fazit

1. Das Ergebnis der Evaluierung zeigt den großen Bedarf schneller und verlässlicher Unterstützung nach IT-Sicherheitsvorfällen sowohl bei Verbraucherinnen und Verbrauchern als auch bei KMU.
2. Ziel muss es sein das CSN regional auszurollen. In der
  - ersten Phase sind die Helfer zu qualifizieren und in der
  - zweiten Phase kann die Digitale Rettungskette ausgerollt werden.

Nur so kann das Cyber-Sicherheitsnetzwerk als Public Private Partnership (PPP) zu einem Erfolg werden und eine bundesweite Akzeptanz erlangen.

# Austauschplattform und regionale Foren zur Vernetzung alle Akteure des CSN





# Netzwerk und Austauschplattform

## Regionale Foren

- Vertrauensvolles Netzwerk (keine wirtschaftlichen Interessen)
- Austausch über aktuelle Themen (Best Practices)
- Anlaufstelle und Trainingsumgebung für Mitglieder der Digitalen Rettungskette



Eine Liste der Regionalen Foren finden Sie hier:



# Vielen Dank für Ihre Aufmerksamkeit!

**Angelika Jaschob**

Projektleiterin CSN  
*Cyber-Sicherheitsnetzwerk*



Deutschland  
**Digital•Sicher•BSI•**

## Unterstützung bei IT-Sicherheitsvorfällen

Landkarte der Helfenden



Hilfe zum Einstieg in die „Digitale Rettungskette“: 0800 -274 1000  
Fragen zum Cyber-Sicherheitsnetzwerk an: [info@cyber-sicherheitsnetzwerk.de](mailto:info@cyber-sicherheitsnetzwerk.de)



Deutschland  
**Digital•Sicher•BSI•**

# Links zu den Themen

Deutschland  
**Digital•Sicher•BSI**

Flyer Digitale-Rettungskette

<https://www.bsi.bund.de/dok/974514>

Landkarte der Helferinnen und Helfer des CSN

<https://www.bsi.bund.de/dok/Landkarte>

Basiskurs für die Qualifikation als Digitaler Ersthelfer

<https://www.bsi.bund.de/dok/947558>

Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle  
für Vorfall-Praktiker und Vorfall Experten

<https://www.bsi.bund.de/dok/896968>

Liste der Schulungsanbieter

[https://www.bsi.bund.de/CSN\\_Schulungsanbieter](https://www.bsi.bund.de/CSN_Schulungsanbieter)

Selbsteinschätzungstest

<https://www.bsi.bund.de/dok/Selbsteinschaetzungstest>

Trainingskoffer

<https://www.bsi.bund.de/dok/Trainingskoffer>

Liste der Regionale-Foren

<https://www.bsi.bund.de/dok/RegionaleForen>

