Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Das Cyber-Sicherheitsnetzwerk

Unterstützung nach IT-Sicherheitsvorfällen

Angelika Jaschob

Bonn, den 02.11.2023

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. Best Practices
   Wie gut ist mein Unternehmen auf einen IT-Sicherheitsvorfall vorbereitet?

Cyber-
Sicherheitsnetzwerk

Das Cyber-Sicherheitsnetzwerk (CSN)

Mit dem Cyber-Sicherheitsnetzwerk soll

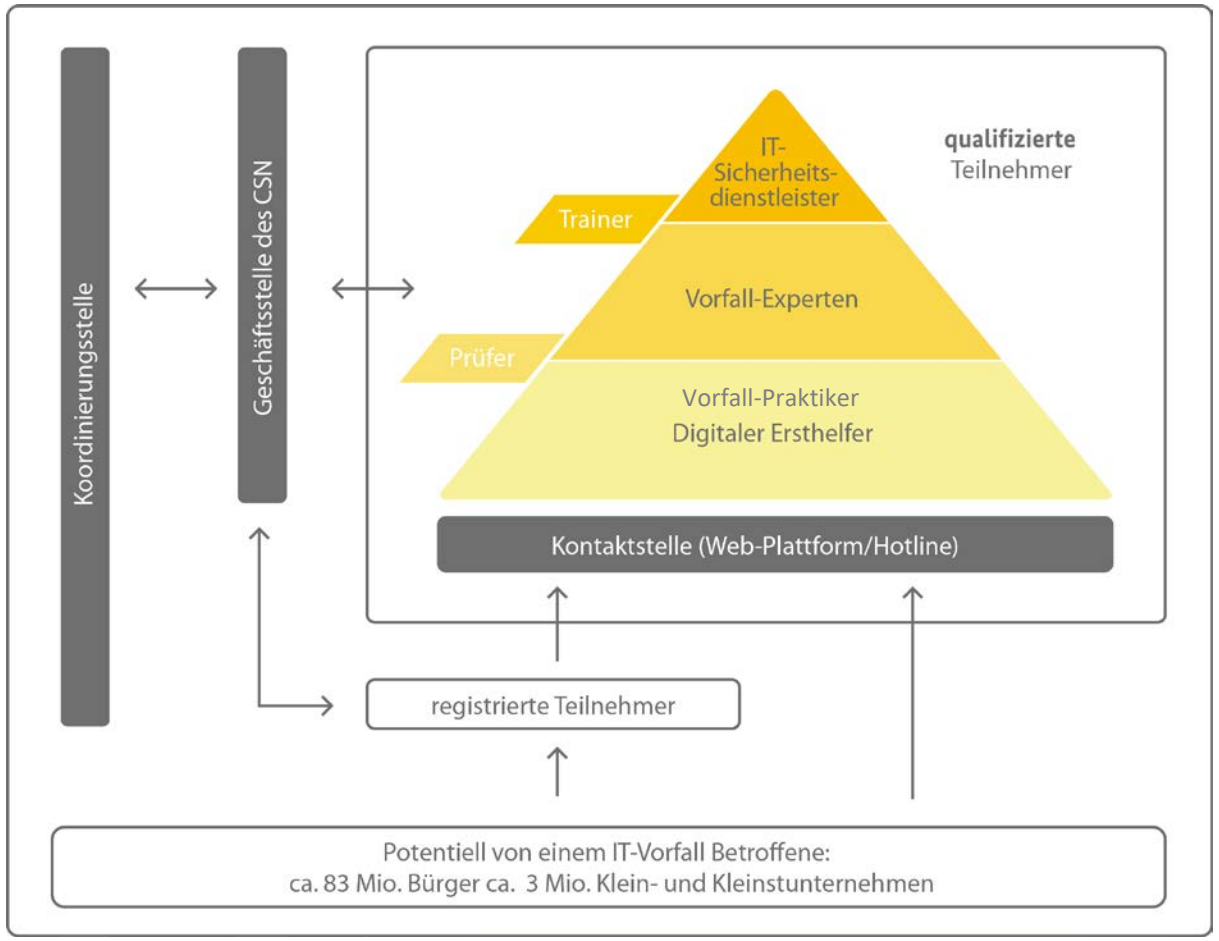
eine flächendeckende dezentrale Struktur aufgebaut werden,

die effizient und kostengünstig

KMU und Bürger bei

IT-Sicherheitsvorfällen Unterstützung anbietet.

Aufbaustruktur des Cyber-Sicherheitsnetzwerks



Weitere Informationen zum CSN:

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•

Arbeiten in der „Digitalen Rettungskette“

- Unterstützung auf Augenhöhe

Digitale Rettungskette

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)

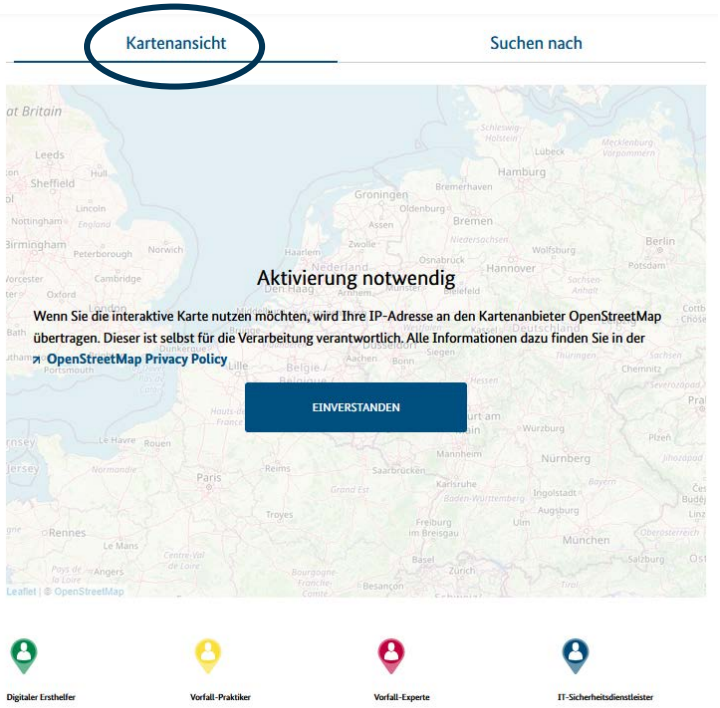
- VP löst kleine IT-Sicherheitsvorfälle (telefonische Ersthilfe)

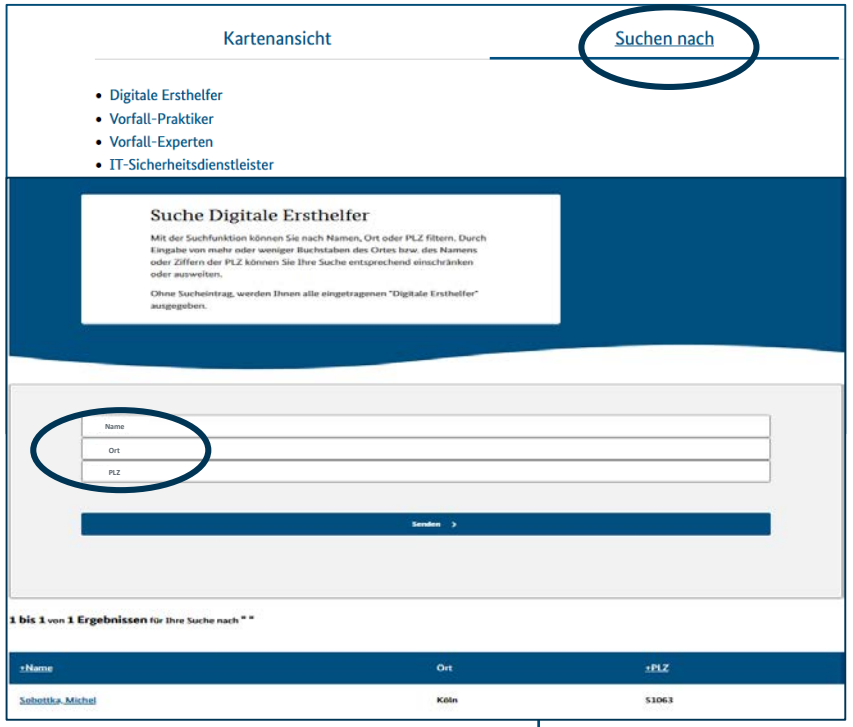
Umfangreiche IT-Vorfallsanalyse durch personenzertifizierte Vorfall-Experten (VE)

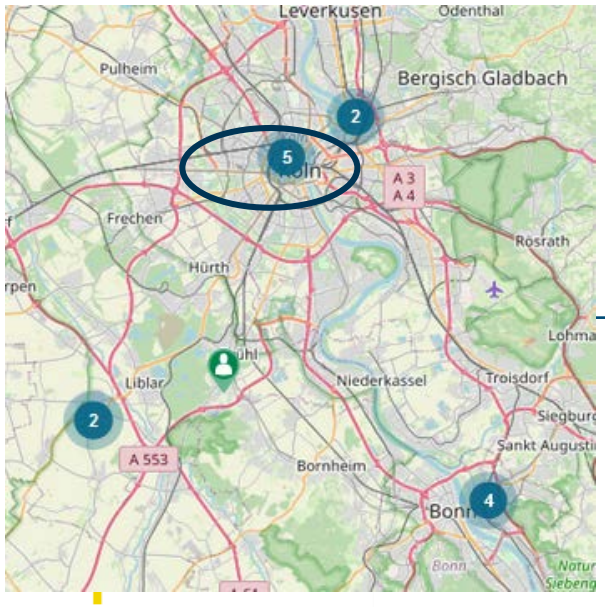
- Tiefergehende Analysegespräche
- Vor-Ort-Unterstützung möglich, falls erforderlich

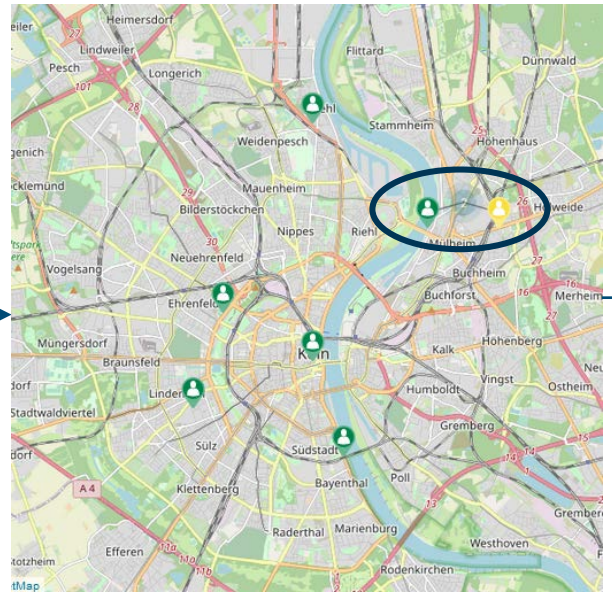
Lösung komplexer IT-Sicherheitsvorfälle durch einen IT-Sicherheitsdienstleister mit einem Team von Vorfall-Experten

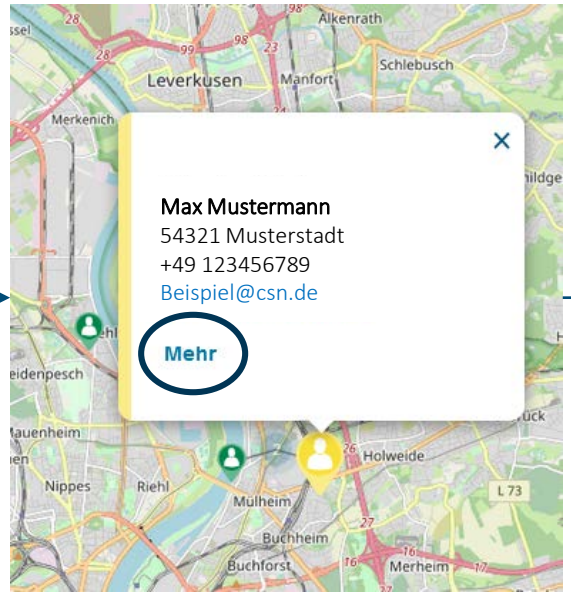
Bundesamt
für Sicherheit in der
Informationstechnik

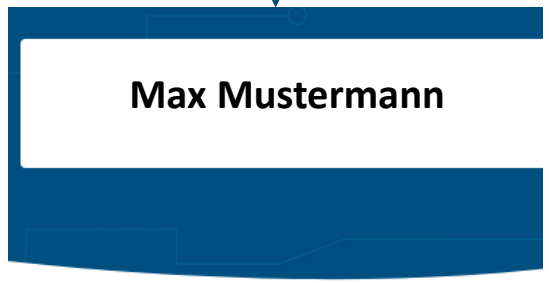












Max Mustermann

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

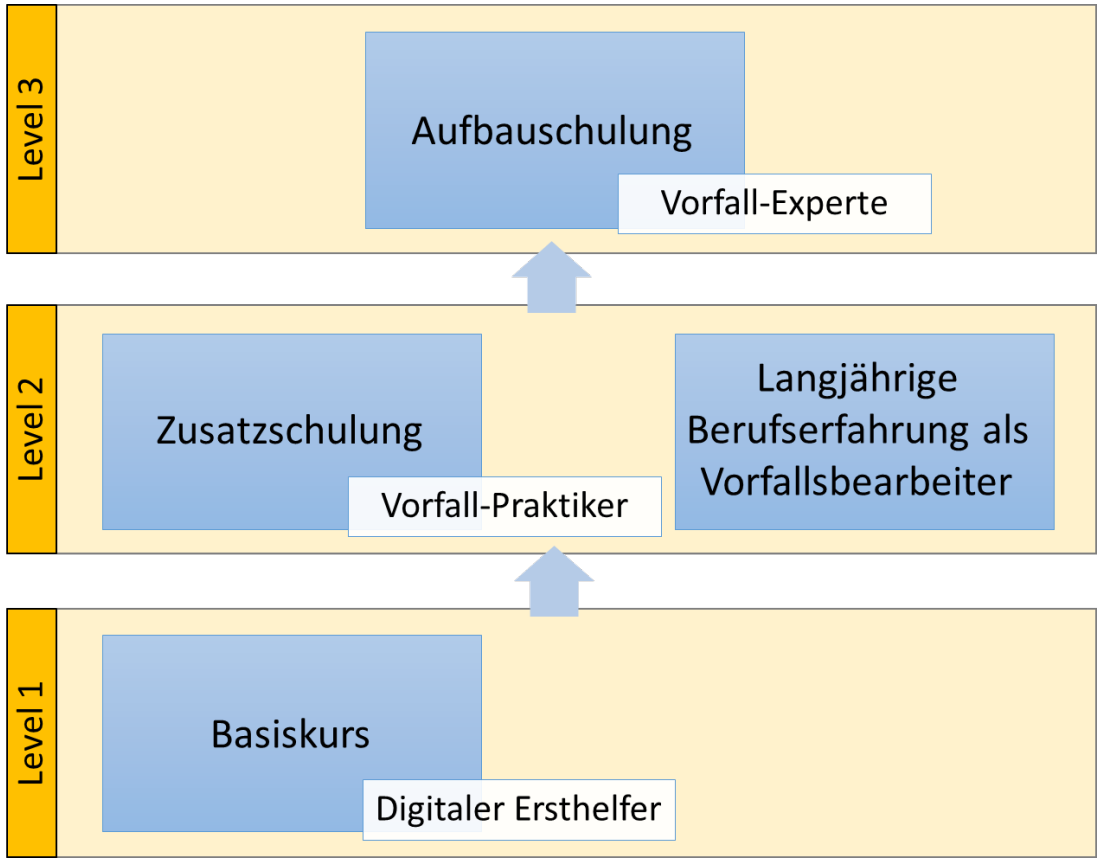
Broschüren zum Nachlesen

Die Broschüre befindet sich hier:

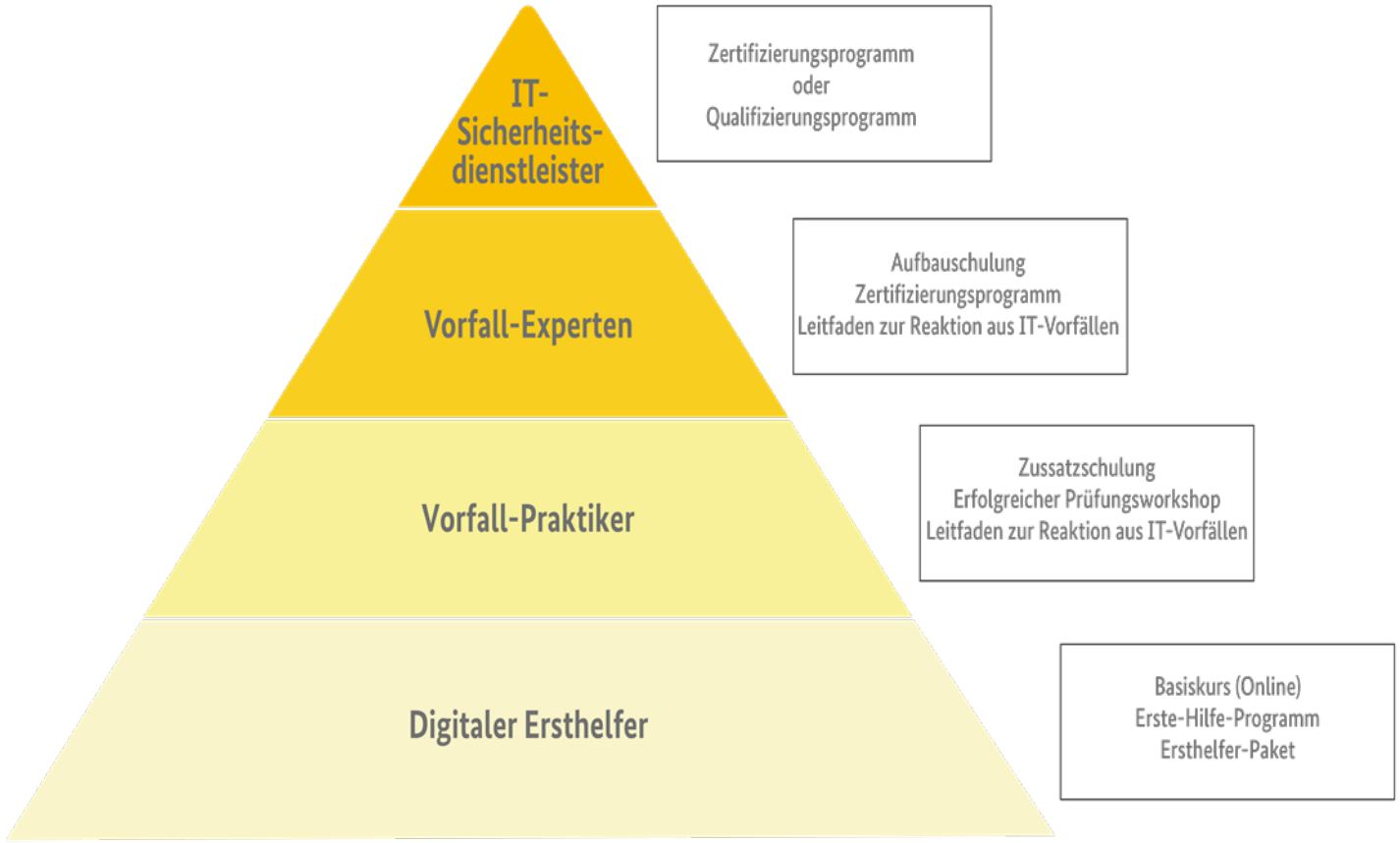
Die Broschüre befindet sich hier:

Drei Stufen der Qualifizierung im Cyber-Sicherheitsnetzwerk

Qualifizierungsprogramm



Anforderungen



Digitale Ersthelfer

Cyber-Sicherheitsnetzwerk

Kostenloser Basiskurs für Digitale Ersthelfer

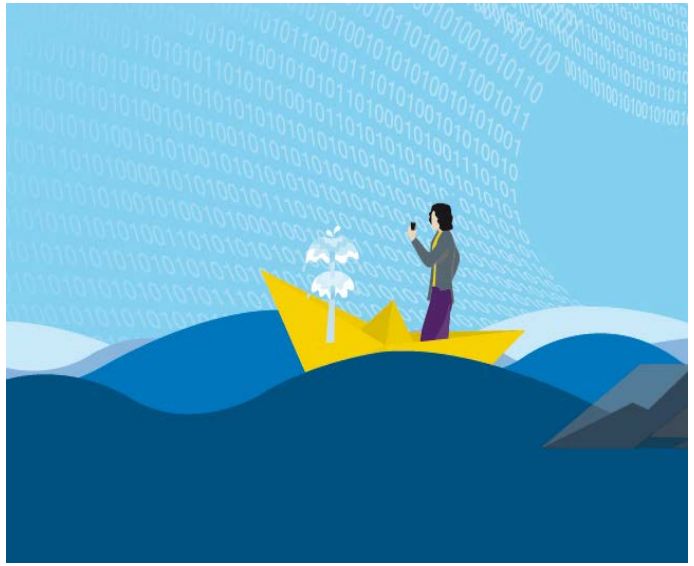
Basiskurs im Selbststudium

- 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:

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•

Inhalte des Basiskurs für Digitale Ersthelfer

Modul 1

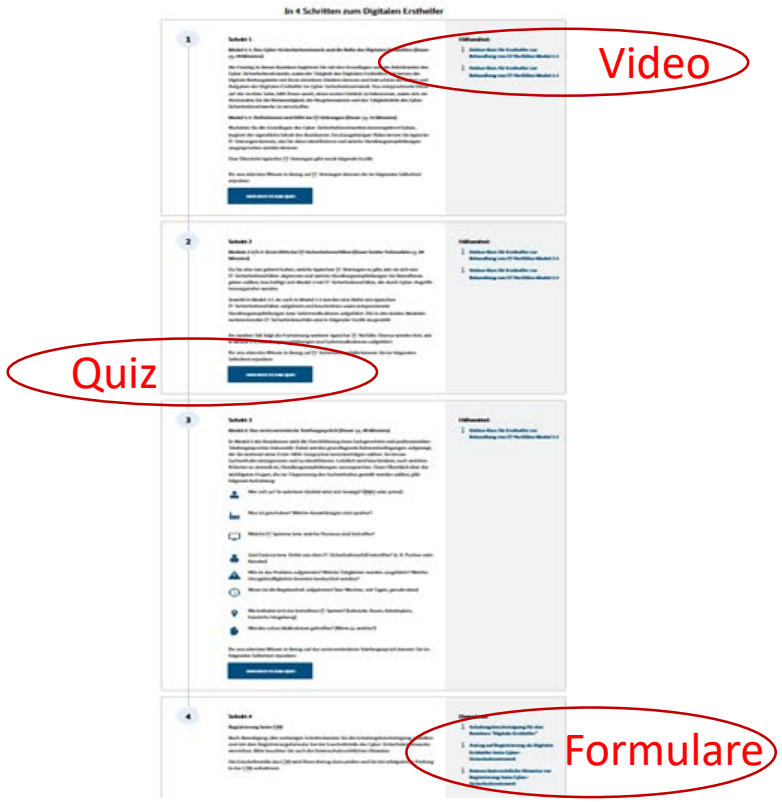
- Grundlagen des Cyber-Sicherheitsnetzwerks
- Unterschiede IT-Störung vs. IT-Vorfall
- Handlungsempfehlungen für typische IT-Störungen

Modul 2

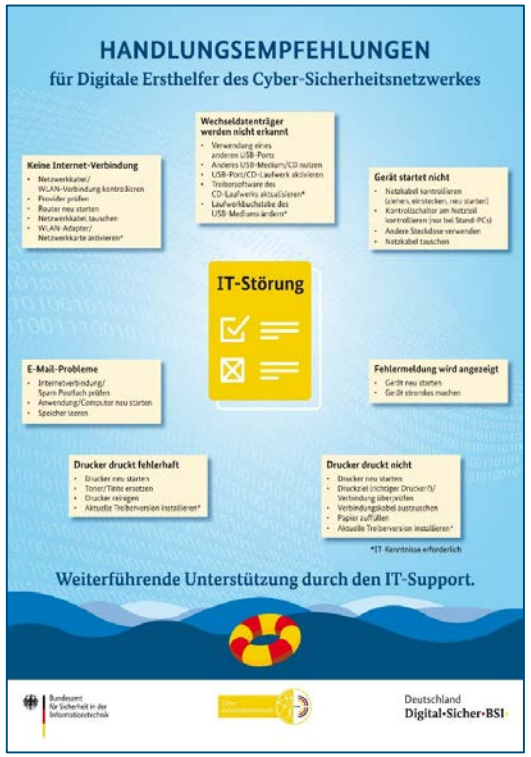
- Definition, Reaktion und Handlungsempfehlungen für typische IT-Sicherheitsvorfälle

Modul 3

- Durchführung fachgerechter und professioneller Telefongespräche, anhand praxisnaher Beispiele



Handlungsempfehlungen für Digitale Ersthelfer



Vorfall-Praktiker

Cyber-Sicherheitsnetzwerk

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:

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•

Inhalte der Zusatzqualifikation zum Vorfall-Praktiker

Deutschland Digital•Sicher•BSI•

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

Den Leitfaden finden Sie hier:

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•

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

Deutschland
Digital•Sicher•BSI•

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:

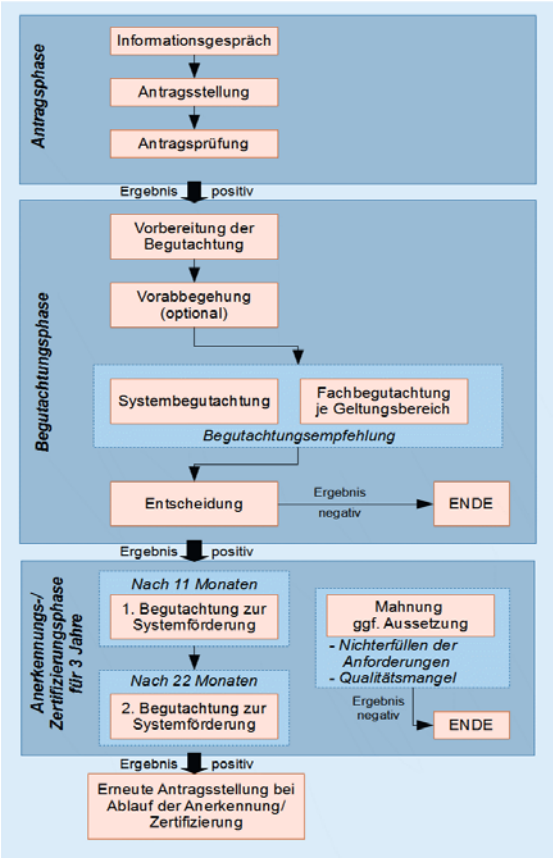
IT-Sicherheitsdienstleister Vorfallsbearbeitung

Cyber-Sicherheitsnetzwerk

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:

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•

Schulungsanbieter

Prozessablauf für qualifizierte Schulungsanbieter (VP)

Erst-Gespräch
- Kennenlernen und Klärung der Rahmenbedingungen

Curriculum
- Konzeption Zusatzschulung für Vorfall-Praktiker

Registrierung
- Abgabe einer formalen Selbsterklärung
- Veröffentlichung des Schulungsangebots
- Zusendung des Prüfungspakets

Durchführung
- Organisation und Durchführung der Schulungen durch den Schulungsanbieter
- Ausstellen einer Schulungsbescheinigung durch den Schulungsanbieter

QSM
- kontinuierliche Qualitätssicherungsmaßnahmen
- regelmäßiger Austausch der Schulungsanbieter untereinander

Eine Liste aller Schulungsanbieter finden Sie hier:

Registrierte Schulungsanbieter

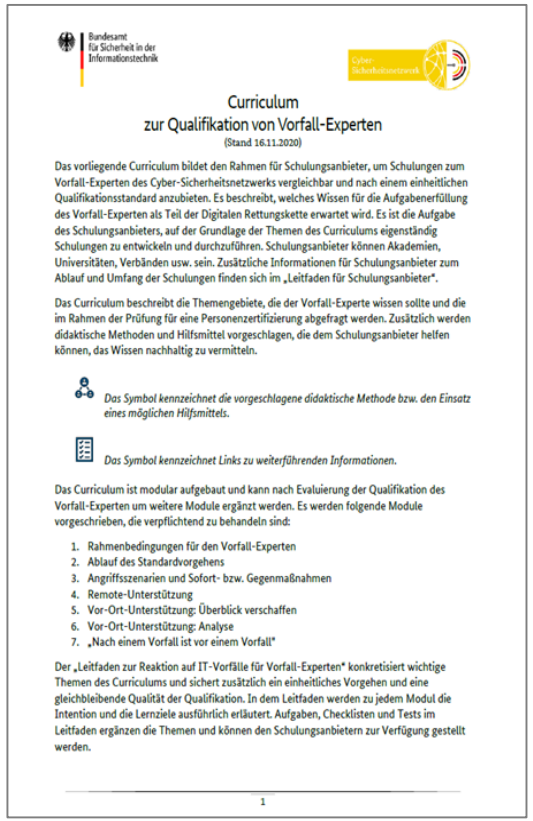
Deutschland
Digital•Sicher•BSI•

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.



Bundesamt für Sicherheit in der Informationstechnik

Curriculum
zur Qualifikation von Vorfall-Experten
(Stand 16.11.2020)

Das vorliegende Curriculum bildet den Rahmen für Schulungsanbieter, um Schulungen zum Vorfall-Experten des Cyber-Sicherheitsnetzwerks vergleichbar und nach einem einheitlichen Qualifikationsstandard anzubieten. Es beschreibt, welches Wissen für die Aufgabenerfüllung des Vorfall-Experten als Teil der Digitalen Rettungskette erwartet wird. Es ist die Aufgabe des Schulungsanbieters, auf der Grundlage der Themen des Curriculums eigenständig Schulungen zu entwickeln und durchzuführen. Schulungsanbieter können Akademien, Universitäten, Verbänden usw. sein. Zusätzliche Informationen für Schulungsanbieter zum Ablauf und Umfang der Schulungen finden sich im „Leitfaden für Schulungsanbieter“.

Das Curriculum beschreibt die Themengebiete, die der Vorfall-Experte wissen sollte und die im Rahmen der Prüfung für eine Personenzertifizierung abgefragt werden. Zusätzlich werden didaktische Methoden und Hilfsmittel vorgeschlagen, die dem Schulungsanbieter helfen können, das Wissen nachhaltig zu vermitteln.

Das Symbol kennzeichnet die vorgeschlagene didaktische Methode bzw. den Einsatz eines möglichen Hilfsmittels.

Das Symbol kennzeichnet Links zu weiterführenden Informationen.

Das Curriculum ist modular aufgebaut und kann nach Evaluierung der Qualifikation des Vorfall-Experten um weitere Module ergänzt werden. Es werden folgende Module vorgeschrieben, die verpflichtend zu behandeln sind:

1. Rahmenbedingungen für den Vorfall-Experten
2. Ablauf des Standardvorgehens
3. Angriffsszenarien und Sofort- bzw. Gegenmaßnahmen
4. Remote-Unterstützung
5. Vor-Ort-Unterstützung: Überblick verschaffen
6. Vor-Ort-Unterstützung: Analyse
7. „Nach einem Vorfall ist vor einem Vorfall“

Der „Leitfaden zur Reaktion auf IT-Vorfälle für Vorfall-Experten“ konkretisiert wichtige Themen des Curriculums und sichert zusätzlich ein einheitliches Vorgehen und eine gleichbleibende Qualität der Qualifikation. In dem Leitfaden werden zu jedem Modul die Intention und die Lernziele ausführlich erläutert. Aufgaben, Checklisten und Tests im Leitfaden ergänzen die Themen und können den Schulungsanbietern zur Verfügung gestellt werden.

1

Trainingskoffer

- Möglichkeit zur Vorbereitung auf den Ernstfall

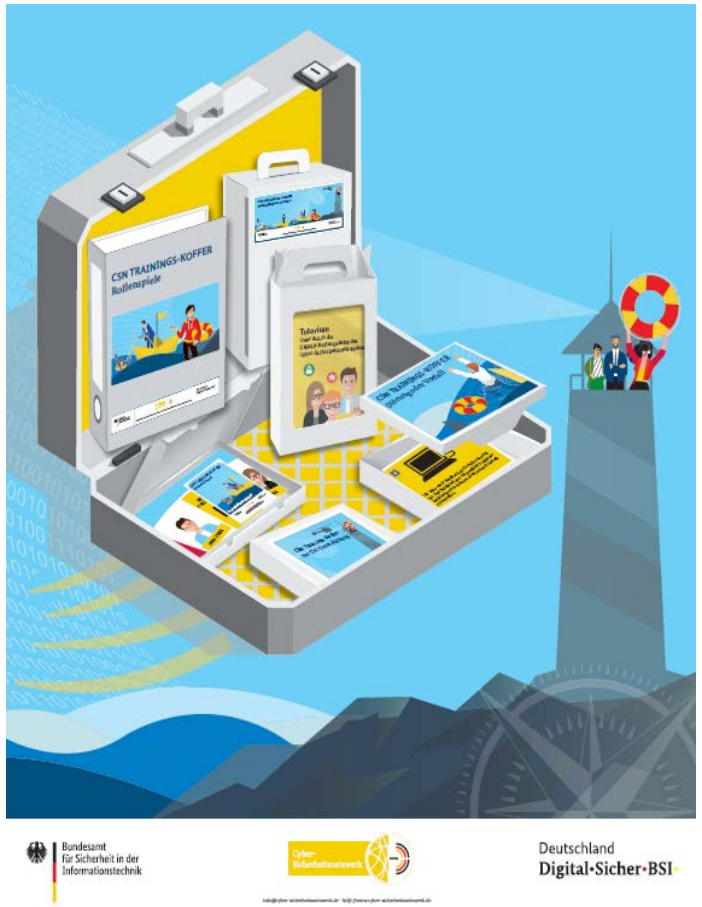
Der digitale Trainingskoffer

- 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:

Bundesamt für Sicherheit in der Informationstechnik

Deutschland
Digital•Sicher•BSI•

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•

Bundesamt
für Sicherheit in der
Informationstechnik

Rollenspiele

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

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 hattest und über die Jahre in die Geschäftsleitung aufgestiegen warst.

Du bist lokal sehr engagiert, unter anderem in Gemeindearbeit 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.

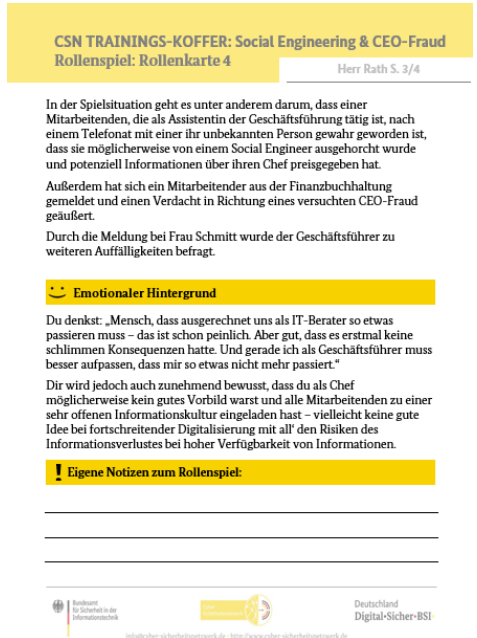
Gestern warst du bei einem Vorstandsessen des Hockeyvereins, der gerade Spenden für ein neues Trainingszentrum akquiriert.

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 einen 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-Kanälen 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 freizeitlichen Aktivitäten gegeben haben könnte.

Deutschland Digital•Sicher•BSI



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 unbekannten Person gewahr geworden ist, dass sie möglicherweise von einem Social Engineer ausgehorcht 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.

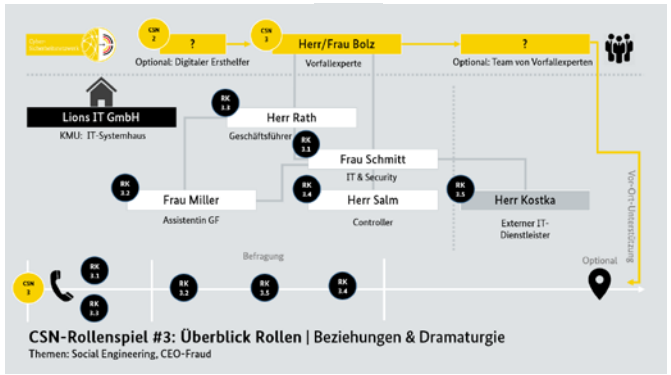
Durch die Meldung bei Frau Schmitt wurde der Geschäftsführer zu weiteren Auffälligkeiten befragt.

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."

Dir wird 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:



Bundesamt für Sicherheit in der Informationstechnik

Escape-Game

Deutschland
Digital•Sicher•BSI•

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

Zeitumfang: ca. 90 Minuten

Bundesamt
für Sicherheit in der
Informationstechnik

Zusammenfassung

Zahlen, Daten, Fakten des Cyber-Sicherheitsnetzwerks

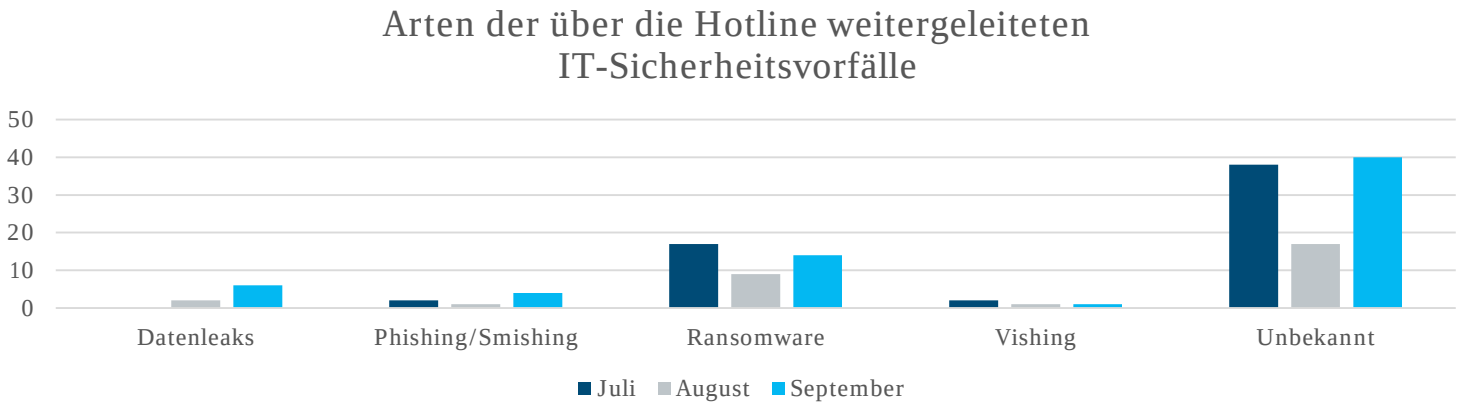
345	22	13	16
Digitale Ersthelfer	Vorfall-Praktiker	Vorfall-Experten	IT-Sicherheits-dienstleiter

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



Bundesamt für Sicherheit in der Informationstechnik

Cyber-Sicherheitsnetzwerk

Deutschland Digital•Sicher•BSI•

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.

Best Practices und Selbsteinschätzungstest

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:

3. Forum Cyber-Sicherheitsnetzwerk

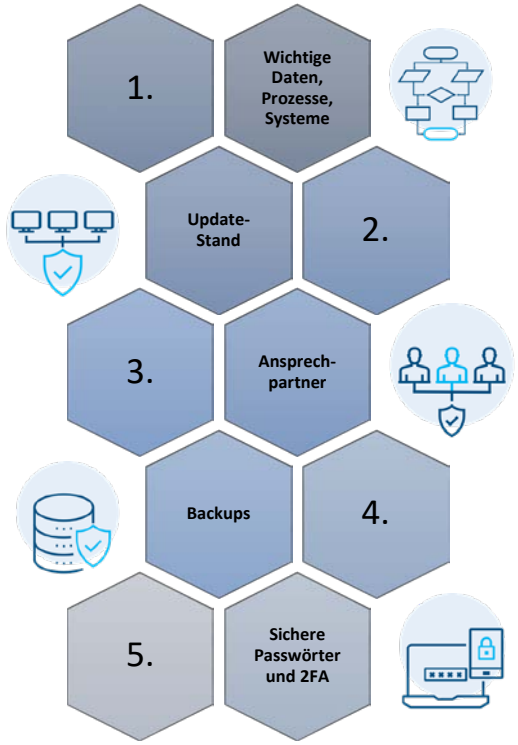
- Dienstag, den 14.11.2023
- Kostenlose digitale Veranstaltung
  https://www.bsi.bund.de/SharedDocs/Termine/DE/2023/CSN_Forum.html

Die Agenda finden Sie hier:

Cyber-Sicherheitsnetzwerk

Wie gut sind Sie auf einen IT-Sicherheitsvorfall vorbereitet?

Nutzen Sie die Möglichkeit und
machen Sie jetzt den Selbsteinschätzungstest!



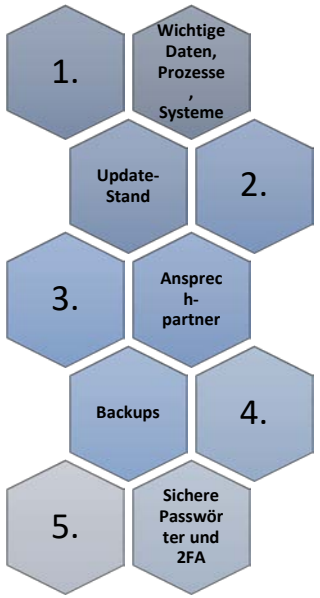
https://bsi.sslsurvey.de/CSN-selbsteinschaetzungstest/

Cyber-Sicherheitsnetzwerk

Wie gut sind Sie auf einen IT-Sicherheitsvorfall vorbereitet?

Damit Sie und Ihr Unternehmen bei einem IT-Sicherheitsvorfall besser reagieren kann, sollten Sie die folgenden Punkte beachten:

1. Überblick über die Datenspeicherorte und Datenströme verschaffen (Notfallunterlagen),
2. Geräte regelmäßig auf Updates prüfen und diese einspielen,
3. Zuständigkeiten für den Notfall festlegen, Mitarbeiterinnen und Mitarbeiter schulen und sensibilisieren,
4. Datenbestände regelmäßig sichern und Backups getrennt aufbewahren,
5. Sichere Passwörter, Passwort-Manager und, wenn möglich, 2FA (2-Faktor-Authentisierung) nutzen.



Melden Sie sich zum 3. Forum Cyber-Sicherheitsnetzwerk an und erfahren Sie wie Ihr Unternehmen im Vergleich zu anderen aufgestellt ist.

Das Anmeldeformular finden Sie hier:

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•

Vielen Dank für Ihre Aufmerksamkeit!

Deutschland
Digital•Sicher•BSI•

Angelika Jaschob

Projektleiterin CSN

Cyber-Sicherheitsnetzwerk

Bundesamt
für Sicherheit in der
Informationstechnik

Bundesamt
für Sicherheit in der
Informationstechnik
Digital•Sicher•BSI•