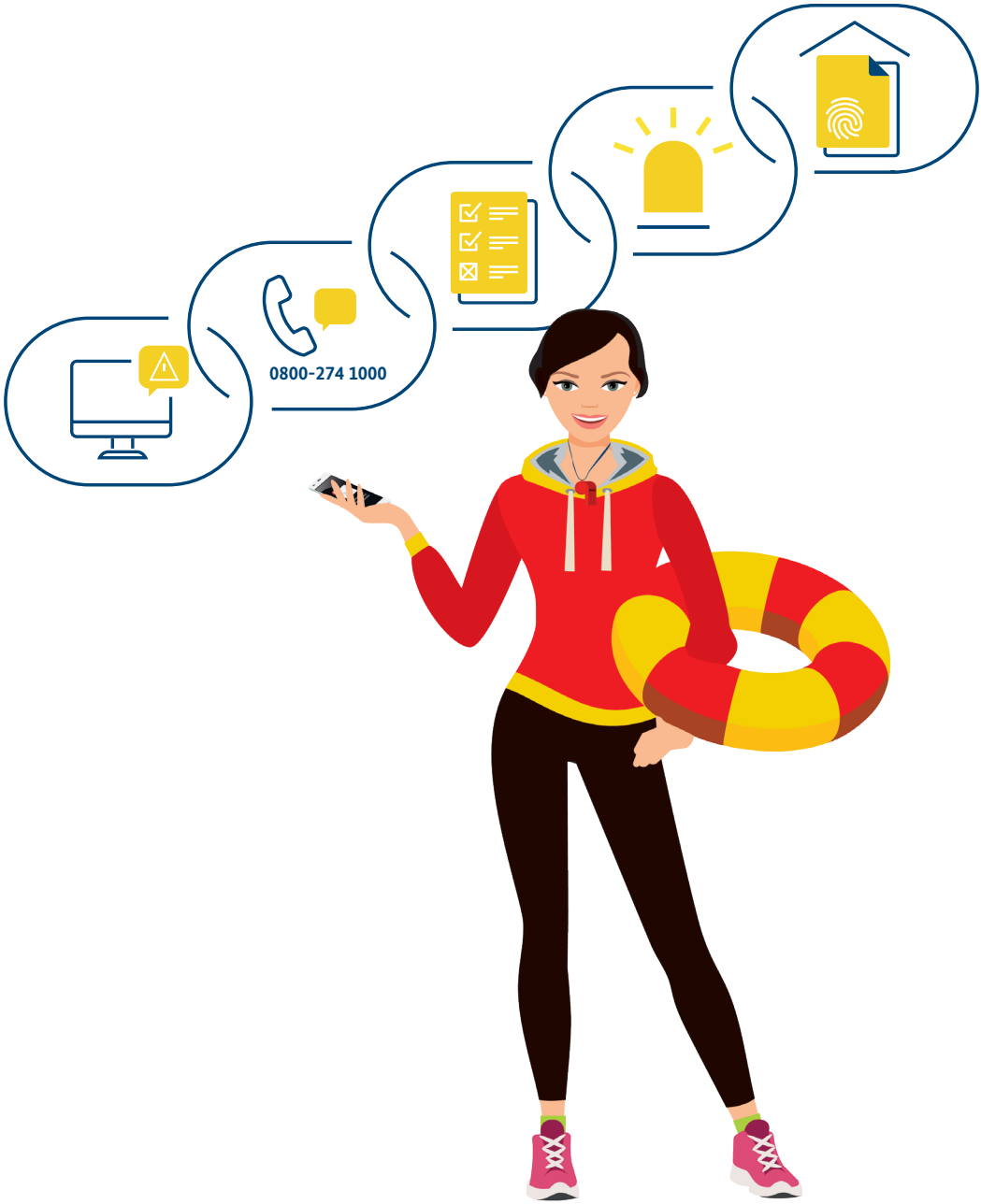
Bundesamt
für Sicherheit in der
Informationstechnik

Cyber-
Sicherheitsnetzwerk

Deutschland
Digital•Sicher•BSI•

Das Cyber-Sicherheitsnetzwerk

Dezentrale Unterstützung bei IT-Sicherheitsvorfällen


0800-274 1000

Kurzüberblick über das Cyber-Sicherheitsnetzwerk

Heutzutage werden in fast allen Unternehmen wichtige und sensible Verfahren mithilfe moderner Informationstechnik (IT) durchgeführt. Aber was passiert, wenn sich unberechtigte Dritte Zugang zu den digitalen Systemen verschaffen? Wenn Daten abfließen, Schadsoftware eingespielt wird oder erpresserische Forderungen gestellt werden und die Nutzung der IT nicht mehr möglich ist? Ein solcher Vorfall kann eine existenzbedrohende Situation für ein Unternehmen bedeuten!

Das Risiko, dass Ihr Unternehmen von einem Cyber-Angriff betroffen sein könnte, ist nicht gering und wird sehr oft unterschätzt. Doch was ist zu tun, wenn dieser Fall eintritt?

Das CSN steht als erste Anlaufstelle bei IT-Sicherheitsvorfällen zur Verfügung und bietet eine effektive Unterstützung bei der Behandlung von IT-Sicherheitsvorfällen.

Die Helfenden der „Digitalen Rettungskette“ unterstützen dabei mit ihrer fachlichen Expertise. Die Art und Weise der Unterstützung unterscheidet sich je nach Vorfall und Zielgruppe. Ziel des CSN ist es, den Betroffenen passgenaue Unterstützungsangebote anzubieten. Zielgruppe dabei sind vor allem KMU sowie Verbraucherinnen und Verbraucher.

Das CSN ist ein immer größer werdender Zusammenschluss qualifizierter Helferinnen und Helfer. Sie alle stellen ihre vielfältige Expertise und ihr individuelles Knowhow bei der Behebung von IT-Sicherheitsvorfällen zur Verfügung, um diese zu bearbeiten und den Schaden bei den Betroffenen möglichst gering zu halten.

Die Digitale Rettungskette ist die Kernkomponente des CSN. Sie legt ein abgestimmtes Arbeiten der Helfenden im CSN fest und gibt so einen strukturierten und nachvollziehbaren Handlungsrahmen vor. Mit diesem wird eine Kette unterschiedlicher, reaktiver Hilfsangebote definiert, beginnend bei der Identifizierung des geeigneten Helfenden über konkrete fachliche Hilfestellung bis hin zur umfassenden Lösungsbetreuung und Klärung des Vorfalls.

Eine qualitativ hochwertige Vorfallsbearbeitung durch die qualifizierten Helfenden wird mit einem einheitlichen und qualitätsgesicherten Qualifizierungsprogramm sichergestellt. Dieses verbindet eine niedrige Eintrittshürde durch einen onlinebasierten Basiskurs zum Digitalen Ersthelfer mit der fachlich fundierten Ausbildung und BSI-Zertifizierung von IT-Spezialisten.

Das Angebot eines Wissens- und Erfahrungsaustauschs in regionalen Foren oder das jährlich stattfindende Forum des CSN runden die Angebotspalette ab. Durch diese regelmäßigen Treffen bleiben alle aktiven Helfenden auf dem neuesten Stand und werden anhand von Best Practices auf die immer neuen Herausforderungen der IT-Sicherheit vorbereitet.

Aufbau und Struktur

Das CSN ist als flächendeckende, dezentrale Struktur aufgebaut, die effektiv und kostengünstig KMU, aber auch Verbraucherinnen und Verbrauchern, Unterstützung bei IT-Sicherheitsvorfällen anbietet.

Organisatorische Anlaufstelle

Die Geschäftsstelle des CSN ist im BSI angesiedelt und per E-Mail unter **info@cybersicherheitsnetzwerk.de** zu erreichen. Sie ist für die Registrierungen der Teilnehmenden des Cyber-Sicherheitsnetzwerks zuständig und beantwortet alle prozessualen und organisatorischen Fragen.

Strategische Unterstützung

Die strategische Ausrichtung sowie die Koordinierung des CSN übernimmt die Koordinierungsstelle im BSI. Diese wird unterstützt von einem „Round Table", bestehend aus Vorfall-Experten sowie Vertretern von Behörden, Bildungsinstitutionen und unterschiedlichen Interessensgruppen. Hier werden strategische Entscheidungen zur Weiterentwicklung des CSN vorbereitet und Ideen für Prozesse und Produkte diskutiert.

Von einem Vorfall Betroffene

Betreiber kritischer Infrastrukturen und größere Unternehmen stehen nicht im Fokus des CSN, da diese über individuelle Prozesse und eigenes Knowhow für die Vorfallsbehandlung verfügen. Die Zielgruppe des CSN sind in erster Linie von einem IT-Sicherheitsvorfall betroffene Verbraucherinnen und Verbraucher, Kleinstunternehmen (KKU) sowie kleinere und mittlere Unternehmen (KMU).

Diese Zielgruppen sind bei IT-Sicherheitsvorfällen häufig besonders anfällig, wenn sie technisch überfordert und passende Ansprechpartner nicht bekannt sind. Für diesen Fall ist eine vertrauenswürdige Stelle erforderlich, die ihnen mit Rat und Tat zur Seite steht. Das CSN soll deutschlandweit diese zentrale Anlaufstelle für Betroffene nach einem IT-Sicherheitsvorfall sein.

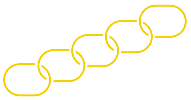
Registrierte Teilnehmende

Für jedes Unternehmen besteht zusätzlich die Möglichkeit, sich als registrierter Teilnehmender in das CSN aufnehmen zu lassen. Registrierten Teilnehmenden bieten sich zusätzliche Möglichkeiten. Zum Beispiel erhalten sie vom CSN ein Willkommenspaket und einen regelmäßigen Newsletter. Sie können an regionalen Foren teilnehmen und werden zu Veranstaltungen des CSN eingeladen. Sie können sich also fortlaufend weiterbilden und Teil eines großen, kompetenten Netzwerks sein.

Aktive Helfende und Experten

Die erste persönliche Anlaufstelle des CSN in der Digitalen Rettungskette ist die Kontaktstelle. Eine zentrale Hotline vermittelt die Betroffenen an Helfende in ihrer Region und stellt die passenden Kontaktlisten zur Verfügung. Zudem verweist sie auf die „Hilfe zur Selbsthilfe"-Angebote auf der Webseite des BSI.

Mithilfe der auf den Webseiten des BSI bereitgestellten Landkarte aller registrierten Helfenden, ist es für Betroffene schnell möglich, einen geeigneten, regionalen Ansprechpartner zu finden, der sie bei der Vorfallsbearbeitung effektiv und gezielt unterstützt.



Digitale Rettungskette

Um allen Betroffenen die passenden Unterstützungsleistungen anbieten zu können, sieht das CSN die „Digitale Rettungskette“ vor. Sie besteht aus mehreren Eskalationsstufen und verfolgt das Ziel, Betroffenen nach einem IT-Sicherheitsvorfall schnell die passende, qualifizierte Hilfe zu vermitteln.

An erster Stelle der Digitalen Rettungskette steht die „Hilfe zur Selbsthilfe“. Wichtige „Erste-Hilfe-Maßnahmen zur Selbsthilfe“ finden Betroffene auf der Webseite des CSN. Diese enthalten in folgenden Paketen die wichtigsten Erste-Hilfe-Maßnahmen:

- TOP-12-Maßnahmen bei Cyber-Angriffen
- Maßnahmenkatalog zum Notfallmanagement – Fokus IT-Notfälle
- Erste Hilfe bei einem schweren IT-Sicherheitsvorfall

Die Checklisten „Organisatorisches“ und „Technik“ führen online kurz und knapp durch die ersten Schritte zur Bewältigung eines IT-Sicherheitsvorfalls.

Hilfe zum Einstieg in die Digitale Rettungskette

Erste persönliche Anlaufstelle der Digitalen Rettungskette ist die Kontaktstelle des CSN (dies ist derzeit das Service Center des BSI). Zwischen 8:00 Uhr und 18:00 Uhr ist dieses über eine kostenfreie Hotline (Tel. 0800-274 1000) erreichbar. Mitarbeitende der Kontaktstelle unterstützen Betroffene, den IT-Sicherheitsvorfall richtig einzuschätzen, und helfen ihnen bei der Auswahl des richtigen Glieds der Digitalen Rettungskette (Eskalationsstufe).

In der ersten Eskalationsstufe unterstützen „Digitale Ersthelfer“ Betroffene, vor allem Verbraucherinnen und Verbraucher sowie Kleinst- und Kleinunternehmen (KKU), bei der Behebung von kleineren IT-Störungen und kleinen IT-Sicherheitsvorfällen. Auf der Landkarte der Helfenden finden Betroffene registrierte Digitale Ersthelfer in der Region.

Die erste Unterstützung von kleinen und mittleren Unternehmen (KMU) übernehmen „Vorfall-Praktiker“. Auch hier stellt

das CSN eine Liste der qualifizierten und registrierten Vorfall-Praktiker bereit. Im Vergleich zum Digitalen Ersthelfer haben Vorfall-Praktiker eine zweitägige Zusatzschulung absolviert und verfügen sowohl über breiteres als auch tieferes Wissen.

Handelt es sich um einen komplexeren IT-Sicherheitsvorfall, so kann auf die nächste Eskalationsstufe verwiesen werden. Hierfür stehen zertifizierte Vorfall-Experten oder IT-Sicherheitsdienstleister zur Verfügung. Sie sind in der Lage, den jeweiligen Vorfall tiefer zu analysieren und entsprechende Hilfestellung zu geben – ggf. auch vor Ort.

Schnittstellen zu anderen Hotlines und Initiativen

Das Cyber-Sicherheitsnetzwerk bietet bestehenden kostenfreien IT-Sicherheitshotlines und -initiativen an, sich dem CSN anzuschließen. So haben Betroffene eine zentrale Anlaufstelle, aber auch die Möglichkeit, aus dem regionalen Angebot die für sie passende Unterstützungsleistung auszuwählen.

Qualifizierung und Erfahrungsaustausch

Das CSN sieht drei Qualifizierungsstufen für Helfende vor:

1. **Digitale Ersthelfer:** Sie absolvieren in einem Selbststudium den Basiskurs (kostenloser Online-Kurs).

2. **Vorfall-Praktiker:** Sie besuchen eine zweitägige Zusatzschulung mit abschließendem Prüfungsworkshop bei einem registrierten Schulungsanbieter.

3. **Vorfall-Experten:** Diese müssen als ein Nachweis für die Personenzertifizierung eine dreitägige Aufbauschulung bei einem registrierten Schulungsanbieter besuchen und eine schriftliche Wissensprüfung beim BSI bestehen. Danach haben sie die Möglichkeit, eine Personenzertifizierung beim BSI zu beantragen.

Selbststudium

Digitale Ersthelfer qualifizieren sich durch das Selbststudium des „Leitfadens zur Reaktion auf IT-Sicherheitsvorfälle für Digitale Ersthelfer“. Zur Unterstützung bietet das CSN online einen kostenfreien Basiskurs an. Dieser gliedert sich in drei Module, welche auf dem genannten Leitfaden basieren. Am Ende eines jeden Moduls steht ein Kompetenztest. Nach der Teilnahme und dem erfolgreichen Abschluss aller drei Module ist eine Registrierung als Digitaler Ersthelfer und eine Aufnahme auf die Landkarte der Helfer möglich.

Schulungen durch Trainer und Schulungsanbieter

Die Qualifikation der Vorfall-Praktiker und Vorfall-Experten erfolgt durch Schulungsanbieter. Dies können Schulungsanbieter für IT und Informationssicherheit, Verbände oder Universitäten sein. Das CSN veröffentlicht eine Liste aller registrierten Schulungsanbieter.

Aufgabe des Schulungsanbieters sind die eigenständige Konzeption und das Angebot von Schulungen sowie Prüfungen auf der Grundlage des entsprechenden Curriculums des CSN. Die Organisation und Durchführung der Schulungen obliegt ausschließlich den Schulungsanbietern.

Entsprechend dem angestrebten Qualifizierungslevel wird eine zweitägige Zusatzschulung zum Vorfall-Praktiker inkl. Prüfungsworkshop oder eine dreitägige Aufbauschulung zum Vorfall-Experten angeboten. Die Abschlussprüfung zum Vorfall-Experten wird vom BSI durchgeführt, dieses vergibt auch bei Bestehen das Personenzertifikat.

Kompetenzausbau und Weiterentwicklung

Am letzten Freitag jedes Monats erscheint regelmäßig ein kurzer Newsletter mit aktuellen Vorfällen, Neuigkeiten aus dem CSN und Veranstaltungshinweisen. Zielgruppe des Newsletters sind registrierte Teilnehmende, Digitale Ersthelfer, Vorfall-Praktiker und Vorfall-Experten.

Zusätzlich gibt es die Möglichkeit, sich über eine Online-Plattform zu aktuellen Bedrohungen oder Vorfällen auszutauschen.

Das CSN bietet regelmäßig Formate zum Erfahrungsaustausch an. Dazu gehört z. B. ein jährliches CSN-Forum im Herbst mit Vorträgen und Workshops.

Rückmeldungen können die Teilnehmenden jederzeit direkt per E-Mail oder über die regelmäßig durchgeführten Umfragen geben und so mithelfen, das CSN kontinuierlich weiterzuentwickeln und zu verbessern.

Austausch in regionalen Foren und Trainingskoffer

Mit den regionalen Foren bietet das CSN sowohl Unternehmen als auch Helfenden die Möglichkeit, in einer vertrauensvollen Umgebung die Bewältigung eines IT-Sicherheitsvorfalls zu trainieren. Hierfür stellt das CSN u. a. in seinem Trainingskoffer eine kostenfreie Übungs- bzw. Trainingssammlung zur Verfügung.

Der Trainingskoffer ist ein einfaches, spielerisches Training für die Vorfallsbearbeitung „out of the box“. Er ist so gestaltet, dass die Trainingseinheiten leicht selbstständig erstellt und schnell eingesetzt werden können.

Die regionalen Foren sind ca. zweistündige Erfahrungsaustauschformate, welche in unterschiedlicher Form in Präsenz oder virtuell stattfinden können. Sie werden in der Regel von erfahrenen Vorfall-Experten

organisiert und geleitet. In diesem Format können sich zum einen teilnehmende Unternehmen mit den Helfenden des CSN vernetzen und durch den Austausch selbst Wissen aneignen, welches in den internen Prozessen angewandt werden kann. Zum anderen bieten die regionalen Foren Digitalen Ersthelfern, Vorfall-Praktikern und Vorfall-Experten einen vertrauensvollen Rahmen, in dem Erfahrungen und Best Practices ausgetauscht sowie konkrete Szenarien geübt werden können. Die Foren verbinden also das Netzwerken mit dem fortlaufenden Lernen.

Selbsteinschätzungstest für KMU

Mithilfe des Selbsteinschätzungstests können KMU anhand von fünf Fragen überprüfen, wie gut sie auf einen IT-Sicherheitsvorfall vorbereitet sind. Bei der Auswertung der Fragen sind wichtige, themenbezogene Hinweise und Ratschläge des BSI eingebunden, sodass direkt Hilfestellung zur Schließung von organisatorischen und technischen Lücken in der Informationssicherheit angeboten wird.

Helfende des Cyber-Sicherheitsnetzwerks

Aufgabe der Helfenden des CSN ist die Unterstützung von Betroffenen bei der Bearbeitung eines IT-Sicherheitsvorfalls im Rahmen der Digitalen Rettungskette.

Digitale Ersthelfer

Digitale Ersthelfer können alle interessierten und IT-affinen Personen werden. Die Grundvoraussetzung ist das Absolvieren eines Basiskurses, der auf dem „Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Digitale Ersthelfer“ basiert und online direkt durch das Cyber-Sicherheitsnetzwerk angeboten wird.

Nach der Teilnahme am Basiskurs und dem erfolgreichen Abschluss aller Module können sich die Absolventinnen und Absolventen beim Cyber-Sicherheitsnetzwerk als Digitale Ersthelfer registrieren lassen.

Digitale Ersthelfer sind für die First-Level-Unterstützung in der Digitalen Rettungskette im CSN zuständig. Sie unterstützen vorwiegend Verbraucherinnen und Verbraucher sowie Kleinstunternehmen mit schneller, telefonischer Ersthilfe. Zu den von ihnen angegebenen Servicezeiten stehen sie Betroffenen für Anfragen zur

Verfügung. Ihre Aufgabe ist eine qualifizierte Einschätzung eines IT-Sicherheitsvorfalls. Betroffene sollen dadurch eine erste Hilfe bei kleineren IT-Störungen und kleinen IT-Sicherheitsvorfällen sowie erste Handlungsempfehlungen erhalten.

Digitale Ersthelfer sollen auf Basis ihrer Einschätzung auch die Kontaktaufnahme mit einem Vorfall-Praktiker oder Vorfall-Experten empfehlen, wenn sie es für notwendig erachten. Den Rahmen für die Mitarbeit als Digitaler Ersthelfer gibt der „Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Digitale Ersthelfer" vor. Dieser Leitfaden unterstützt den Digitalen Ersthelfer auch bei der Analyse von IT-Sicherheitsvorfällen und gibt passende Handlungsempfehlungen. Zur Dokumentation des Kontakts erstellt der Digitale Ersthelfer einen Vorfallsbericht, welchen er dem Betroffenen im Nachgang zusendet.

Vorfall-Praktiker

Vorfall-Praktiker sind IT-Fachleute, die z. B. in Unternehmen wie IT-Sicherheitsdienstleistern oder Computerfirmen arbeiten oder auch IT-Systemadministratoren von Unternehmen sind. Für die Qualifikation zum Vorfall-Praktiker wird eine zweitägige Zusatzschulung angeboten, die mit einem halbtägigen Prüfungsworkshop abschließt.

Der „Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Vorfall-Praktiker und Vorfall-Experten" bildet den Rahmen für die Qualifikation. Für die Mitarbeit als Vorfall-Praktiker im CSN ist eine Registrierung erforderlich, für welche

- die erfolgreiche Teilnahme an einem Prüfungsworkshop zum Vorfall-Praktiker und
- eine einjährige Tätigkeit als Digitaler Ersthelfer (oder eine vergleichbare Tätigkeit) oder
- eine IT-sicherheitstechnische Qualifikation, z. B. als Systemadministrator, oder
- eine gleichwertige Kompetenz nachzuweisen ist.

Vorfall-Praktiker sind die First-Level-Unterstützung vom KMU in der Digitalen Rettungskette. Sie bieten KMU schnelle, telefonische Ersthilfe an und stehen ihnen innerhalb ihrer beim CSN angegebenen Servicezeiten telefonisch oder per E-Mail zur Verfügung. Sie geben den Betroffenen eine qualifizierte Ersteinschätzung, führen ggf. eine Analyse durch und geben passende Handlungsempfehlungen.

Ist der Vorfall weder mit angemessenem Aufwand noch in einem ersten Gespräch zu beheben, empfiehlt der Vorfall-Praktiker die Kontaktaufnahme mit einem Vorfall-Experten.

Die gewonnenen Erkenntnisse und empfohlenen Maßnahmen zur Behebung des IT-Sicherheitsvorfalls werden fortlaufend in einem Vorfallsbericht dokumentiert. Dieser wird dem Betroffenen nach Beendigung der Vorfallsbehandlung und des Unterstützungsangebots zugesandt.

Vorfall-Experte

Vorfall-Experten sind in der Regel IT-Fachleute, die sich zusätzlich im Rahmen einer Aufbauschulung für das CSN als Vorfall- Experten qualifizieren. Dazu müssen sie an einer dreitägigen Aufbauschulung eines beim CSN registrierten IT-Schulungsanbieters teilnehmen.

Diese Aufbauschulung basiert auf dem „Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Vorfall-Praktiker und Vorfall-Experten". An die Schulung schließt sich eine Personenzertifizierung durch die Zertifizierungsstelle des BSI an, die neben einer Prüfung der Nachweise auch eine Kompetenzprüfung in Form einer schriftlichen Prüfung umfasst. Erst nach der erfolgreichen Zertifizierung ist es möglich, sich als Vorfall-Experte im Cyber-Sicherheitsnetzwerk registrieren zu lassen.

Zu den Aufgaben eines Vorfall-Experten gehört es, nach einer durch Digitale Ersthelfer oder Vorfall-Praktiker erstellten ersten Einschätzung eine tiefergehende Analyse oder eine Vor-Ort-Unterstützung anzubieten. Hier agiert der Vorfall-Experte als Krisenmanager und unterstützt Betroffene aktiv bei der Vorfallsbewältigung. Grundlage für die Tätigkeit ist ein individueller Dienstleistungsvertrag.

Der IT-Sicherheitsvorfall wird an einen IT-Sicherheitsdienstleister abgegeben, wenn zur Analyse und Behebung oder zu einer weitergehenden forensischen Untersuchung ein Team unterschiedlicher Spezialisten erforderlich ist, das Betroffenen über einen gewissen Zeitraum vor Ort Unterstützungsleistung anbietet.

IT-Sicherheitsdienstleister

IT-Sicherheitsdienstleister des CSN sind größere IT-Dienstleister, die überregional agieren und eine größere Anzahl zertifizierter Vorfall-Experten bereitstellen können. So können sie bei komplexeren und größeren IT-Sicherheitsvorfällen ein Team aus Vorfall-Experten mit speziellen Kenntnissen und Fähigkeiten für die Vorfallsbehandlung anbieten.

Sie werden benötigt, wenn zur Analyse und Behebung eines IT-Sicherheitsvorfalls auf der höchsten Stufe der Digitalen Rettungskette ein Team mit besonderen Kenntnissen über einen längeren Zeitraum vor Ort Unterstützung anbieten muss.

IT-Sicherheitsdienstleister mit einem Team von Vorfall-Experten besitzen spezielle Fähigkeiten wie

- Koordination und Steuerung eines größeren Notfallteams, z. B. auch in Bezug auf rechtliche und öffentlichkeitsrelevante Maßnahmen,
- Fähigkeiten im Bereich der Abwehr verschiedener Angriffsformen wie Advanced Persistent Threat (APT) oder Distributed Denial of Service (DDoS)
- Erfahrungen bzgl. der Hintergründe und Vorgehensweisen von Angreifern

IT-Sicherheitsdienstleister mit einem Team von Vorfall-Experten im CSN können entweder

- zertifizierte IT-Sicherheitsdienstleister für den Geltungsbereich Vorfallsbearbeitung oder
- qualifizierte Dienstleister für das Spezialgebiet DDoS oder APT sein.

LANDKARTE:
https://www.bsi.bund.de/dok/CSN-Karte

TRAININGSKOFFER:
https://www.bsi.bund.de/dok/Trainingskoffer

SELBSTEINSCHÄTZUNGSTEST:
https://www.bsi.bund.de/dok/Selbsteinschaetzungstest

KONTAKTDATEN:

Cyber-Sicherheitsnetzwerk (CSN)
Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn

Web: www.cyber-sicherheitsnetzwerk.de
E-Mail: info@cyber-sicherheitsnetzwerk.de
Tel.: +49 800 - 274 1000
Fax: +49 800 - 274 600