



Bundesamt  
für Sicherheit in der  
Informationstechnik

Deutschland  
**Digital•Sicher•BSI**

# Benutzerhandbuch MIP für CSN

Anleitungen für Registrierung und Vorfallsbericht



# Änderungshistorie

<i>Version</i>	<i>Datum</i>	<i>Name</i>	<i>Beschreibung</i>
1.0	04.12.2023	CSN	Erste Veröffentlichungsversion
1.1	19.01.2024	CSN	Ergänzte Veröffentlichungsversion

*Tabelle 1: Änderungshistorie*

# Inhalt

1	Kurzzusammenfassung .....	4
1.1	Was ist das MIP? .....	4
1.2	Wie ist das MIP aufgebaut?.....	4
1.3	Welche Prozesse des CSN werden im MIP abgebildet?.....	5
1.4	Erste Schritte .....	5
1.5	Wo bekomme ich Hilfe bei Fragen oder Problemem? .....	5
2	Benutzerverwaltung.....	6
2.1	Anlegen eines neuen Benutzers .....	6
2.2	Login .....	6
2.3	Weitere Optionen der Benutzerverwaltung .....	7
3	Institutionsverwaltung .....	9
3.1	Anlegen einer neuen Institution .....	9
3.2	Erzwingen der Zwei-Faktor-Authentisierung .....	10
3.3	Anderen Benutzern Zugriff auf Institution geben .....	10
3.4	Registrieren einer Institution für die Meldestelle Cyber-Sicherheitsnetzwerk .....	10
4	Erstellen eines Vorfallsberichts.....	17

# 1 Kurzzusammenfassung

Um die Registrierung und die Abgabe von Statistikberichten für Helfende (Digitale Ersthelfer, Vorfall-Praktiker, Vorfall-Experte, IT-Sicherheitsdienstleister) des Cyber-Sicherheitsnetzwerks (CSN) einfacher zu gestalten, werden die laufenden Prozesse ab dem 15.01.2024 digitalisiert. Jeder Helfende muss sich neu im Melde- und Informationsportal (MIP) registrieren, um darauf Zugriff darauf zu erhalten und Statistikberichte abgeben zu können.

Wichtig ist, dass nach Ablauf der Übergangsfrist nur noch diejenigen Helfenden im CSN als aktiv angesehen (und auf den Helferlisten veröffentlicht) werden, die sich über das MIP registriert haben. Auch bestehende Helfende müssen sich innerhalb der Übergangsfrist neu registrieren. Für die Registrierung sind etwa 10 bis 15 Minuten einzuplanen, um die Schulungsbescheinigungen (Basiskurs, Zusatzschulung, Zertifizierungsurkunde) hochzuladen. Der Registrierungsprozess ist damit für die Nutzerseite komplett digital.

## 1.1 Was ist das MIP?

Das Melde- und Informationsportal (MIP) ermöglicht, Unternehmen sowie Personen, sich beim Bundesamt für Sicherheit in der Informationstechnik (BSI) zu registrieren und Meldungen abzugeben. Die an das BSI gemeldeten Daten werden für die Anreicherung des Lagebilds Wirtschaft genutzt, sodass das CSN einen wichtigen Sensor des Lagezentrums für die IT-Sicherheitslage in Deutschland im Bereich Wirtschaft und Gesellschaft darstellt.

Das MIP unterstützt Registrierungs- und Meldeprozesse und erfüllt alle gesetzlichen Vorgaben, insbesondere die des Online-Zugangs-Gesetzes (OZG) und der Datenschutz-Grundverordnung (DS-GVO) und wird bereits in Zusammenhang mit dem IT-Sicherheitsgesetz und den Kritischen Infrastrukturen eingesetzt. Eine Zwei-Faktor-Authentisierung wird ebenfalls unterstützt.

Das MIP ist über die URL <https://mip2.bsi.bund.de/> erreichbar.

## 1.2 Wie ist das MIP aufgebaut?

Jeder Benutzer hat ein (1) Benutzerkonto mit einer User-ID. Der Benutzer entspricht Ihnen als Person, bzw. bei IT-Sicherheitsdienstleistern dem Unternehmen.

Innerhalb des Benutzerkontos können beliebig viele, sogenannte Institutionen, angelegt werden. Die CSN-Entsprechung einer Institution ist die Rolle, in der Sie agieren (also als Digitaler Ersthelfer, Vorfall-Praktiker, Vorfall-Experte, IT-Sicherheitsdienstleister). Jede Institution erhält eine eindeutige Institutions-ID und kann für jede Meldestelle genau einmal registriert und freigeschaltet werden.

Die Meldestelle ist die Schnittstelle, über die Meldungen abgegeben werden. Meldungen entsprechen im Falle des CSN den Vorfalls- oder Statistikberichten.

Jeder CSN-Helfende (DEH, VP, VE sowie IT-Sicherheitsdienstleister) muss somit einen Benutzer anlegen und innerhalb seines Benutzers eine Institution für seinen Qualifikationslevel erstellen. Helfende mit mehreren Rollen benötigen für jede Rolle eine angemeldete Institution. Auch bei Weiterqualifizierung muss eine neue Institution für die neue Rolle angelegt und registriert werden.

Im MIP werden keine personenbezogenen Daten gespeichert. Außerdem ist kein lesender Zugriff auf Kontaktdaten möglich. Dies hat zur Folge, dass Änderungen nicht selbstständig durch den Nutzer vorgenommen werden können – bei Änderungen der Telefonnummer, E-Mail-Adresse oder Servicezeiten, nehmen Sie Kontakt mit der CSN-Geschäftsstelle [info@cyber-sicherheitsnetzwerk.de](mailto:info@cyber-sicherheitsnetzwerk.de) auf.

### 1.3 Welche Prozesse des CSN werden im MIP abgebildet?

Das Cyber-Sicherheitsnetzwerk benutzt das MIP insbesondere für zwei Kernprozesse: Die Registrierung und die Abgabe von Vorfalls-/Statistikberichten (im MIP: Meldung).

Alle Rollen der digitalen Rettungskette bekommen die Möglichkeit, sich über die Registrierungsfunktion für die Meldestelle Cyber-Sicherheitsnetzwerk anzumelden und so Teil des CSN zu werden. Dies betrifft sowohl die Digitalen Ersthelfer als auch Vorfall-Praktiker und Vorfall-Experten sowie die zertifizierten IT-Sicherheitsdienstleister.

Die im MIP erstellten Meldungen können in verschiedenen Formaten heruntergeladen werden. Der Vorfallsbearbeiter ist dazu angehalten, dem Betroffenen den Vorfallsbericht im PDF- sowie im JSON-Format zur Verfügung zu stellen. Die JSON-Datei wird benötigt, wenn zu einem Vorfall Folgemeldungen erstellt werden müssen.

### 1.4 Was muss ich tun um mich zu registrieren (Erste Schritte)?

Nachdem Sie die Qualifizierung für Ihre Rolle (d.h. Digitaler Ersthelfer/DEH, Vorfall-Praktiker/VP, Vorfall-Experte/VE oder IT-Sicherheitsdienstleister) abgeschlossen und die entsprechende Bescheinigung erhalten haben, können Sie sich für das CSN registrieren. Der Ablauf ist wie folgt:

1. Einrichtung eines Benutzerkontos im MIP (siehe 2.1)
2. Anlegen einer Institution für Ihre Rolle (siehe 3.1)
3. Ausfüllen und Absenden des Registrierungsformulars (siehe 3.4)

Nachdem die CSN-Geschäftsstelle Ihre Registrierung geprüft und bestätigt hat, können Sie über die Schaltfläche **Meldungen** Vorfallsberichte erstellen (siehe 4).

### 1.5 Wo bekomme ich Hilfe bei Fragen oder Problemen?

Bei Fragen hilft Ihnen die CSN-Geschäftsstelle gerne weiter ([info@cyber-sicherheitsnetzwerk.de](mailto:info@cyber-sicherheitsnetzwerk.de)). Bitte senden Sie uns Ihre Anfrage zu. Wir melden uns so schnell wie möglich bei Ihnen.

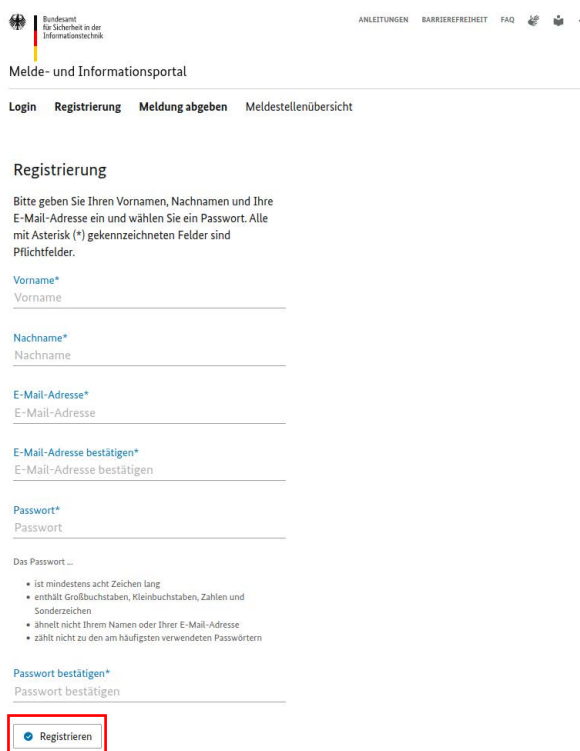
Bitte beachten Sie auch die FAQ, die für bereits registrierte Helfende auf dem BSCW-Server einsehbar ist und regelmäßig aktualisiert wird.

## 2 Benutzerverwaltung

Jede Person und jedes Unternehmen, die/das Zugang zum MIP erhalten möchte, hat exakt ein Benutzerkonto. Der Login erfolgt mit der User-ID und einem Passwort, ggf. ergänzt durch eine Zwei-Faktor-Authentisierung.

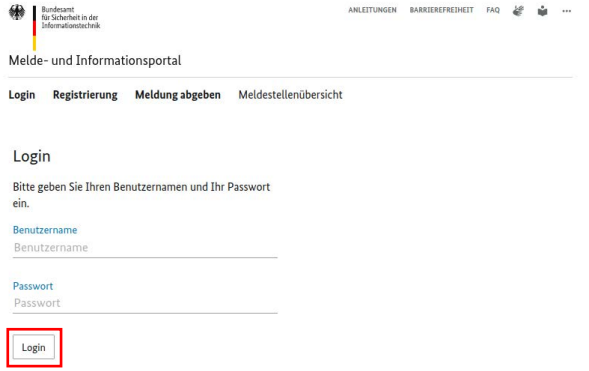
### 2.1 Anlegen eines neuen Benutzers

Schritt	Anleitung
1	<p>Zum Anlegen eines neuen Benutzerkontos klicken Sie im unteren Bereich der Startseite (<a href="https://mip2.bsi.bund.de/">https://mip2.bsi.bund.de/</a>) auf <b>Registrieren</b>.</p>
2	<p>Füllen Sie mindestens alle mit einem Stern (*) gekennzeichneten Felder aus.</p> <p>Beachten Sie bei der Passwortvergabe die auf der Seite beschriebenen Regeln. Später können Sie das Konto durch einen zweiten Faktor (z. B. Passkey) zusätzlich absichern.</p> <p>Wenn Sie alle Daten eingegeben haben, bestätigen Sie dies mit Klick auf <b>Registrieren</b>.</p>
3	<p>Im nächsten Fenster wird Ihnen eine Registrierungsbestätigung und die automatisch generierte User-ID angezeigt.</p> <p>Merken oder notieren Sie sich die User-ID gut – wir empfehlen diese zusammen mit dem in Schritt 2 vergebenen Passwort in einem Passworttresor abzulegen. Sie benötigen die User-ID zum späteren Login (siehe 2.2) in das MIP.</p>


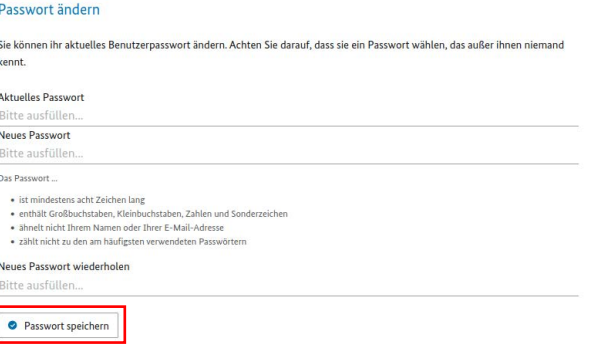



### 2.2 Login

Schritt	Anleitung
1	<p>Rufen Sie die Seite zum Login des MIP auf: <a href="https://mip2.bsi.bund.de/authentifizierung/login/">https://mip2.bsi.bund.de/authentifizierung/login/</a></p>

2	<p>Geben Sie Ihre User-ID sowie Ihr Passwort ein und bestätigen Sie per Klick auf <b>Login</b>.</p> <p>Wenn Sie <u>keine</u> Zwei-Faktor-Authentisierung (2FA) eingerichtet haben, sind Sie nun eingeloggt. Ansonsten siehe Schritt 3.</p>	
3	<p><i>Optional, wenn Sie 2FA eingerichtet haben:</i></p> <p>Bestätigen Sie im nächsten Fenster die Anmeldung über Ihren zweiten Faktor.</p>	

## 2.3 Weitere Optionen der Benutzerverwaltung

Schritt	Anleitung	
1	<p>Die Benutzerverwaltung erreichen Sie, indem Sie auf <b>Persönliche Einstellungen</b> klicken.</p>	
2	<p>Um Ihr Passwort zu ändern, geben Sie zuerst Ihr altes Passwort ein und anschließend zwei Mal das Neue.</p> <p>Bestätigen Sie durch Klick <b>Passwort speichern</b>.</p>	
3	<p>Zur Einrichtung der 2FA können Sie in der Benutzerverwaltung neue Token hinzufügen oder alte entfernen.</p> <p>Klicken Sie zum Hinzufügen auf <b>Neuen Token registrieren</b> und folgen Sie den Bildschirmanweisungen.</p> <p>Zum Entfernen von registrierten Token klicken Sie neben dem</p>	

	entsprechenden Eintrag auf <b>Token löschen</b> .
4	<p>Sie können festlegen, welche Institution beim Login standardmäßig aktiv sein soll.</p> <p>Wählen Sie die Institution über das Dropdown-Menü aus und bestätigen Sie durch Klick auf <b>Standardinstitution speichern</b>.</p> <div><p><b>Institutionsauswahl</b></p><p>Bei jedem Login vertreten Sie automatisch eine Institution. Möchten Sie zu einer anderen Institution wechseln, ist dies rechts oben, überhalb des Menüs möglich. Hier können Sie die Institution auswählen, die bei jedem Login standardmäßig ausgewählt sein soll. Bitte beachten Sie, dass nur Institutionen angezeigt werden, die bereits eine Meldestellenregistrierung besitzen.</p><p>Institution: <span>■■■■■</span> ▼</p><p><input checked="" type="button" value="Standardinstitution speichern"/></p></div>



## 3 Institutionsverwaltung

Eine Institution entspricht im CSN Ihrer Rolle, also Ihre Rolle als Digitaler Ersthelfer, Vorfall-Praktiker, Vorfall-Experte oder IT-Sicherheitsdienstleister. Jede Institution kann nur einmal für eine Meldestelle registriert werden, d. h., dass Sie für jede Rolle, in der Sie im CSN aktiv sind, eine eigene Institution registrieren müssen. Selbiges gilt, wenn Sie als aktiver Helfender eine Schulung für eine höhere Rolle absolviert haben.

Es besteht die Möglichkeit, anderen Benutzern den Zugriff auf eine Institution zu gewähren (siehe 3.3). Diese Option sollten lediglich IT-Sicherheitsdienstleister nutzen, die mehrere Vorfallsbearbeiter beschäftigen. Wichtig: Jede Person, die Zugriff erhalten soll, muss ein eigenes Benutzerkonto haben (siehe 2.1).

### 3.1 Anlegen einer neuen Institution

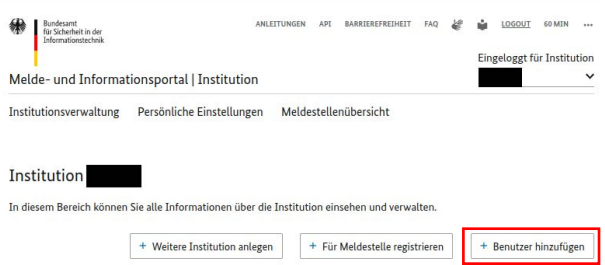

Schritt	Anleitung
1	Die <b>Institutionsverwaltung</b> erreichen Sie über den entsprechenden Menüeintrag im oberen Seitenbereich.
2	Anschließend klicken Sie auf <b>Weitere Institution</b> anlegen.
3	Geben Sie der Institution einen Namen und klicken Sie anschließend auf <b>Institution anlegen</b> .
4	Im nächsten sich öffnenden Fenster befinden Sie sich in der Institutionsverwaltung der neuen Institution und die Institutions-ID wird angezeigt.

Die Beschreibung der Registrierung für die Meldestelle Cyber-Sicherheitsnetzwerk finden Sie im Abschnitt 3.4.

## 3.2 Erzwingen der Zwei-Faktor-Authentisierung

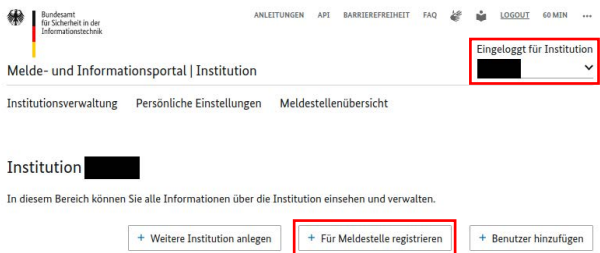
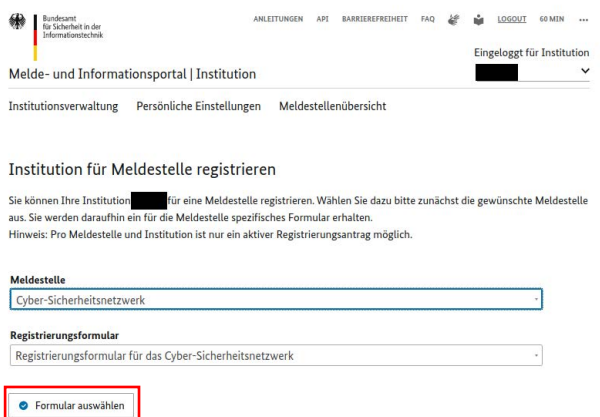

Schritt	Anleitung
1	<p>Sie können für Institutionen den Login mit 2FA erzwingen. Hierfür ändern Sie die Auswahl auf Aktiv und bestätigen per Klick auf <b>Zwei-Faktor-Einstellung</b> speichern.</p> <p><b>Zwei-Faktor-Authentisierung erzwingen</b></p> <p>Falls die Option "Aktiv" gewählt ist, müssen sich alle Benutzer dieser Institution mit einem zweiten Faktor authentisieren. Der zweite Faktor kann beispielsweise ein USB-Hardwaretoken sein. Der Token muss den FIDO2 Standard erfüllen. Durch die verpflichtende Zwei-Faktor-Authentisierung schützen sie Ihre Daten zusätzlich. Benutzer können ihre Token in den persönliche Einstellungen verwalten.</p> <p>Zwei-Faktor-Zwang</p> <p><input checked="" type="radio"/> Inaktiv <input type="radio"/> Aktiv</p> <p><b>Zwei-Faktor-Einstellung speichern</b></p>

## 3.3 Anderen Benutzern Zugriff auf Institution geben

Schritt	Anleitung
1	<p>Sie haben die Möglichkeit, einem anderen Benutzer Zugriff auf eine Institution zu geben, welche Sie verwalten. Dies ist erst möglich, wenn Ihre Registrierungsanfrage angenommen wurde.</p> <p>Klicken Sie hierfür auf <b>Benutzer hinzufügen</b>.</p> 
2	<p>Mit dem Klick auf <b>Einladungslink erzeugen</b> wird ein Link generiert, den Sie einer anderen Person zusenden können. Diese folgt dem Link und muss selbst einen Benutzer anlegen, um Zugriff auf die Institution zu erhalten.</p> <p>Nach dem Beitritt kann der Institutionsverwalter die Rolle des anderen Benutzers anpassen oder ihm den Zugriff auch wieder entziehen.</p> <p><i>Diese Funktion ist insbesondere für IT-Sicherheitsdienstleister relevant, welche mehrere Vorfallsbearbeiter beschäftigen.</i></p> 

## 3.4 Registrieren einer Institution für die Meldestelle Cyber-Sicherheitsnetzwerk

Um Zugriff auf die Meldungsschnittstelle zu erhalten, müssen Sie Ihre Institution für die Meldestelle Cyber-Sicherheitsnetzwerk registrieren. Die Registrierungsformulare unterscheiden sich je nach Rolle im Detail, daher achten Sie auf die korrekte Rollenauswahl auf der ersten Seite.

Schritt	Anleitung	
1	<p>Um eine Institution für eine Meldestelle zu registrieren, wählen Sie diese Institution über das Dropdown-Menü rechts oben aus und klicken anschließend links oben auf <b>Institutionsverwaltung</b>.</p> <p>Dort starten Sie den Registrierungsprozess über <b>Für Meldestelle registrieren</b>.</p>	
2	<p>Im nächsten Schritt wählen Sie über die Dropdown-Menüs als Meldestelle <b>Cyber-Sicherheitsnetzwerk</b> und das <b>Registrierungsformular für das Cyber-Sicherheitsnetzwerk</b> aus.</p> <p>Bestätigen Sie Ihre Auswahl mit einem Klick auf <b>Formular auswählen</b>.</p>	
3	<p>Nun wählen Sie gewünschte Rolle und die Registrierungsart aus.</p> <p><u><b>Rollenauswahl:</b></u> Wählen Sie über das Dropdown-Menü die gewünschte Rolle aus. Zur Auswahl stehen <b>Digitaler Ersthelfer</b>, <b>Vorfall-Praktiker</b>, <b>Vorfall-Experte</b> und <b>IT-Sicherheitsdienstleister</b>.</p> <p><u><b>Registrierungsart:</b></u> Wenn Sie mit Ihren Kontaktdaten öffentlich gelistet werden möchten, wählen Sie <b>öffentliche Helferlisten</b> aus. Ansonsten wählen Sie <b>nicht-öffentliches IT-Notfallregister</b>.</p> <p>Klicken Sie auf <b>Speichern &amp; Weiter</b>.</p>	

<p><b>4a</b></p>	<p><i>Diese Seite wird Ihnen nur angezeigt, wenn Sie zuvor eine der folgenden Rollen ausgewählt haben: Digitaler Ersthelfer, Vorfall-Praktiker, Vorfall-Experte.</i></p> <p>Als nächstes geben Sie Ihre persönlichen Daten an. Diese werden verschlüsselt übertragen und ausschließlich im – nur innerhalb des BSI-Netzes erreichbaren – CRM des BSI gespeichert.</p> <p>Die Felder sind weitestgehend selbsterklärend. Folgende Hinweise sind dennoch zu beachten:</p> <p>Bitte geben Sie an dieser Stelle Ihre persönlichen Kontaktdaten an, unter denen Sie vom BSI kontaktiert werden möchten. Sollten Sie sich mit speziellen Kontaktdaten in die öffentlichen Helferlisten eintragen wollen, wählen Sie bitte bei <i>Abweichende Kontaktdaten</i> für öffentliche Listen <i>ja</i> aus.</p> <p>Wenn Sie öffentlich gelistet werden möchten, aber keine abweichenden Kontaktdaten angeben, werden die hier angegebenen Kontaktdaten veröffentlicht.</p> <p>Wenn Sie sich für das nicht-öffentliche IT-Notfallregister registrieren möchten, belassen Sie die Auswahl bei der Frage nach den abweichenden Kontaktdaten bei <i>nein</i>.</p> <p>Klicken Sie auf <b>Speichern &amp; Weiter</b>.</p>	<div> <h3>Stammdaten</h3> <p>Anrede *</p> <p>Bitte auswählen ▼</p> <p>Vorname *</p> <p>Bitte ausfüllen...</p> <p>Nachname *</p> <p>Bitte ausfüllen...</p> <p>Straße + Hausnummer *</p> <p>Bitte ausfüllen...</p> <p>PLZ *</p> <p>Bitte ausfüllen...</p> <p>Ort *</p> <p>Bitte ausfüllen...</p> <p>E-Mail-Adresse *</p> <p>max@mustermann.de</p> <p>Telefonnummer *</p> <p>Bitte ausfüllen...</p> <p>alternative Telefonnummer (optional)</p> <p>Bitte ausfüllen...</p> <p>Abweichende Kontaktdaten für öffentliche Listen * Ⓞ</p> <p>Sie haben die Möglichkeit in den öffentlich einsehbaren Listen abweichende Kontaktdaten anzugeben. Dies gilt sowohl mit als auch ohne Unternehmensnennung. Möchten Sie davon Gebrauch machen?</p> <p><input checked="" type="radio"/> nein</p> <p><input type="radio"/> ja</p> <p>Bestätigung der Volljährigkeit *</p> <p>Ich versichere, dass ich eine natürliche Person und volljährig bin.</p> <p>Bitte auswählen ▼</p> </div> <div> <p>± Eingaben exportieren</p> <p>↔ Eingaben importieren</p> <p>← Zurück</p> <p><b>Speichern &amp; Weiter &gt;</b></p> </div>
<p><b>4b</b></p>	<p><i>Diese Seite wird Ihnen nur angezeigt, wenn Sie zuvor die folgende Rolle ausgewählt haben: IT-Sicherheitsdienstleister.</i></p> <p>Als nächstes geben Sie die Stammdaten Ihrer Firma an. Diese werden verschlüsselt übertragen und ausschließlich im – nur innerhalb des BSI-Netzes erreichbaren – CRM des BSI gespeichert.</p> <p>Die Felder sind weitestgehend selbsterklärend. Folgende Hinweise sind dennoch zu beachten:</p> <p>Bitte geben Sie an dieser Stelle die allgemeinen Firmenkontaktdaten an. Die Kontaktdaten der speziell für die</p>	<div> <h3>Unternehmensstammdaten</h3> <p>Unternehmensname *</p> <p>Bitte inkl. Rechtsform angeben.</p> <p>Bitte ausfüllen...</p> <p>Unternehmensgröße (Mitarbeiterzahl) *</p> <p>1-9 ▼</p> <p>Straße + Hausnummer *</p> <p>Bitte ausfüllen...</p> <p>PLZ *</p> <p>Bitte ausfüllen...</p> <p>Ort *</p> <p>Bitte ausfüllen...</p> <p>Webseite *</p> <p>https://example.de</p> <p>Allgemeine E-Mail-Adresse *</p> <p>max@mustermann.de</p> <p>Allgemeine Telefonnummer *</p> <p>Bitte ausfüllen...</p> </div>

Tätigkeit im CSN verantwortlichen Ansprechperson werden im unteren Abschnitt dieser Seite eingetragen.

Sollten Sie sich mit speziellen Kontaktdaten in die öffentlichen Helferlisten eintragen wollen, wählen Sie bitte bei **Abweichende Kontaktdaten** für öffentliche Listen **ja** aus.

Wenn Sie öffentlich gelistet werden möchten, aber keine abweichenden Kontaktdaten angeben, werden die Allgemeine Telefonnummer und die Allgemeine E-Mail-Adresse aus dem Bereich Unternehmensstammdaten veröffentlicht.

Wenn Sie sich nur für das nichtöffentliche IT-Notfallregister registrieren möchten, belassen Sie die Auswahl bei der Frage nach den abweichenden Kontaktdaten bei **nein**.

Klicken Sie auf **Speichern & Weiter**.

Abweichende Kontaktdaten für die Veröffentlichung? \* ⓘ

In den öffentlich verfügbaren CSN-Helferlisten werden Postleitzahl und Ort sowie Kontaktdaten eingetragen (E-Mail und Telefon). Möchten Sie andere als die oben angegebenen Kontaktdaten für die Veröffentlichung angeben?

☒ nein  
☐ ja

Zuständige Ansprechperson

Bitte geben Sie eine persönliche Ansprechperson für die CSN-Geschäftsstelle an. An diese werden alle das CSN betreffenden Informationen gesendet.

Anrede \*

keine ▼

Vorname \*

Bitte ausfüllen...

Nachname \*

Bitte ausfüllen...

E-Mail-Adresse der Ansprechperson \*

max@mustermann.de

Telefonnummer der Ansprechperson \*

Bitte ausfüllen...

alternative Telefonnummer der Ansprechperson

Bitte ausfüllen...

⚙ Eingaben exportieren ⚙ Eingaben importieren < Zurück **Speichern & Weiter >**

4c

*Diese Seite wird Ihnen nur angezeigt, wenn Sie zuvor ausgewählt haben, dass Sie gesonderte Kontaktdaten für die öffentlichen Helferlisten angeben möchten.*

In diesem Schritt geben Sie eine E-Mail-Adresse sowie eine Telefonnummer an, welche wir auf den Helferlisten veröffentlichen sollen.

Klicken Sie auf **Speichern & Weiter**.

#### Alternative Kontaktdaten für öffentliche Helferlisten

Hier können Sie abweichende Kontaktdaten (E-Mail und Telefon) für die Veröffentlichung in den Helferlisten des CSN an.

E-Mail-Adresse

max@mustermann.de

Telefonnummer

Bitte ausfüllen...

⚙ Eingaben exportieren ⚙ Eingaben importieren < Zurück **Speichern & Weiter >**

4d

*Diese Seite wird Ihnen nur angezeigt, wenn Sie zuvor ausgewählt haben, dass Sie öffentlich gelistet werden möchten.*

In diesem Schritt geben Sie an, zu welchen Zeiten Sie normalerweise für Hilfesuchende erreichbar sind. Diese Zeiten werden veröffentlicht.

**Wichtig:** Wir können keine temporären Änderungen vornehmen. Richten Sie daher automatische Antworten (E-Mail: Autoreply, Telefon: Mailboxansage) ein, wenn Sie z. B. im Urlaub sind.

Klicken Sie auf **Speichern & Weiter**.

#### Ihre Servicezeiten

Sie können bestimmen, wann Sie Ihre Unterstützung im CSN anbieten - so wie es zu Ihren individuellen Umständen passt.

Bitte beachten Sie, dass Änderungen nicht immer zeitnah durchgeführt werden können. Geben Sie Ihre Servicezeiten daher so allgemein wie möglich an.

- Servicezeiten \*
- ☐ rund um die Uhr (24/7)  
☐ nach 18 Uhr  
☐ nur an Wochenenden  
☐ zu regulären Geschäftszeiten (Mo.-Fr., 9-18 Uhr)  
☐ individuelle Servicezeiten (bitte unten angeben)

#### Individuelle Servicezeiten

Bitte ausfüllen...

⚙ Eingaben exportieren ⚙ Eingaben importieren < Zurück **Speichern & Weiter >**



5a

*Diese Seite wird Ihnen nur angezeigt, wenn Sie zuvor folgende Rolle ausgewählt haben: Digitaler Ersthelfer.*

Als Digitaler Ersthelfer<sup>1</sup> müssen Sie den Basiskurs<sup>2</sup> absolviert haben. An dessen Ende können Sie sich eine digitale Schulungsbescheinigung herunterladen, welche Sie in diesem Schritt der Registrierung als Nachweis hochladen.

Außerdem müssen Sie die dort stehenden Selbsterklärungen abgeben.

Klicken Sie auf **Speichern & Weiter**.

### Qualifikationsnachweis (Digitaler Ersthelfer)

#### Basiskurs für Digitale Ersthelfer \*

Hiermit bestätige ich, den Basiskurs für Digitale Ersthelfer eigenständig absolviert zu haben und somit die speziellen fachlichen Voraussetzungen für Digitale Ersthelfer erfülle. Als Nachweis füge ich die Schulungsbescheinigung bei.

Bitte auswählen

#### Upload Schulungsbescheinigung Basiskurs

Bitte laden Sie hier die Schulungsbescheinigung des Basiskurses hoch.

Keine Datei ausgewählt

#### Fach- und persönliche Kompetenz \*

Hiermit bestätige ich in Form einer Selbsterklärung, dass ich die erforderlichen allgemeinen fachlichen Voraussetzungen erfülle. Bei diesen handelt es um ein Verständnis von IT-Systemen, Netzwerken, Betriebssystemen, Internet, E-Mail, Webseiten, Servern, Clients, dedizierter Hardware sowie Kenntnisse der Gefährdungslage (d.h. Bedrohungen, Schwachstellen und Gefährdungen). Weiterhin bestätige ich in Form einer Selbsterklärung, dass ich die erforderlichen persönlichen und sozialen Kompetenzen erfülle. Bei diesen handelt es sich um ein hohes Maß an Einsatzbereitschaft, ein gutes Zeitmanagement und ein ausgeprägtes Sozialverhalten. Meiner Verantwortung als Digitaler Ersthelfer bin ich mir bewusst.

Bitte auswählen

#### Verpflichtungserklärung \*

Mir ist bewusst, dass wenn ich die Rahmenbedingung des „Leitfadens zur Reaktion auf IT-Sicherheitsvorfälle für Digitale Ersthelfer“ nicht einhalte oder meine vorgenannte Qualifikation nicht gegeben ist, ich nicht mehr Teil des Cyber-Sicherheitsnetzwerkes sein kann und auch von der Liste der Digitalen Ersthelfern genommen werde.

Bitte auswählen

⚙ Eingaben exportieren

📄 Eingaben importieren

⬅ Zurück

**Speichern & Weiter ➤**

5b

*Diese Seite wird Ihnen nur angezeigt, wenn Sie zuvor folgende Rolle ausgewählt haben: Vorfall-Praktiker.*

Als Vorfall-Praktiker<sup>3</sup> müssen Sie zum einen den Basiskurs<sup>4</sup> zum Digitalen Ersthelfer absolviert haben. Die digitale Schulungsbescheinigung ist in diesem Schritt als Nachweis hochzuladen.

Weiterhin müssen Sie die Zusatzschulung zum Vorfall-Praktiker bei einem der gelisteten Schulungsanbieter<sup>5</sup> besucht und bestanden haben. Auch hierfür erhalten Sie eine Bescheinigung, die Sie in dem dafür vorgesehenen Feld hochladen können.

Außerdem sind verschiedene Selbsterklärungen abzugeben.

Klicken Sie auf **Speichern & Weiter**.

### Qualifikationsnachweis (Vorfall-Praktiker)

#### Fachkompetenz \*

Hiermit bestätige ich in Form einer Selbsterklärung, dass ich die erforderlichen fachlichen Voraussetzungen erfülle. Bei diesen handelt es um ein Verständnis von IT-Systemen, Netzwerken, Betriebssystemen, Internet, E-Mail, Webseiten, Servern, Clients, dedizierter Hardware sowie Kenntnisse der Gefährdungslage.

Bitte auswählen

#### Selbsterklärung zur Erfahrung in der Vorfallsbearbeitung \*

Hiermit bestätige ich, dass ich mindestens ein Jahr als Digitaler Ersthelfer im Cyber-Sicherheitsnetzwerk oder vergleichbare Unterstützungsleistung erbracht habe. (Tätigkeitsnachweis)

Bitte auswählen

#### Basiskurs für Digitale Ersthelfer \*

Hiermit bestätige ich, den Basiskurs für Digitale Ersthelfer eigenständig absolviert zu haben und somit die speziellen fachlichen Voraussetzungen für Digitale Ersthelfer erfülle. Als Nachweis füge ich die Schulungsbescheinigung bei.

Bitte auswählen

#### Upload Schulungsbescheinigung Basiskurs

Keine Datei ausgewählt

#### Zusatzschulung zum Vorfall-Praktiker \*

Hiermit bestätige ich, dass ich die Zusatzqualifikation zum Vorfall-Praktiker besucht sowie die Prüfung zum Vorfall-Praktiker bestanden habe.

☒ nein

☐ ja

#### Zusatzschulung zum Vorfall-Praktiker \*

Hiermit bestätige ich, dass ich die Zusatzqualifikation zum Vorfall-Praktiker besucht sowie die Prüfung zum Vorfall-Praktiker bestanden habe.

☒ nein

☐ ja

#### Upload Prüfungsbescheinigung Zusatzqualifikation

##### Vorfall-Praktiker

Keine Datei ausgewählt

#### Verpflichtungserklärung \*

Mir ist bewusst, dass wenn ich die Rahmenbedingung des „Leitfadens zur Reaktion auf IT-Sicherheitsvorfälle für Vorfall-Praktiker“ nicht einhalte oder meine vorgenannte Qualifikation nicht gegeben ist, ich nicht mehr Teil des Cyber-Sicherheitsnetzwerkes sein kann und auch von der Liste der Vorfall-Praktiker genommen werde.

☒ nein

☐ ja

⚙ Eingaben exportieren

📄 Eingaben importieren

⬅ Zurück

**Speichern & Weiter ➤**

<p><b>5c</b></p>	<p>Diese Seite wird Ihnen nur angezeigt, wenn Sie zuvor folgende Rolle ausgewählt haben: Vorfall-Experte.</p> <p>Als Vorfall-Experte<sup>6</sup> müssen Sie die Aufbauschulung bei einem gelisteten Schulungsanbieter<sup>7</sup> besuchen und anschließend den Zertifizierungsprozess des BSI durchlaufen.</p> <p>An dessen Ende erhalten Sie ein Zertifikat, welches Sie in dem dafür vorgesehenen Feld hochladen können.</p> <p>Außerdem ist eine Verpflichtungserklärung abzugeben.</p> <p>Klicken Sie auf <b>Speichern &amp; Weiter</b>.</p>	<div> <h3>Qualifikationsnachweis (Vorfall-Experte)</h3> <p><b>Zertifizierung *</b></p> <p>Hiermit bestätige ich, vom BSI als Vorfall-Experte zertifiziert worden zu sein. Als Nachweis füge ich die Zertifizierungsurkunde bei.</p> <p>ja <input type="checkbox"/></p> <p><b>Upload Zertifizierungsnachweis</b></p> <p>Keine Datei ausgewählt <input type="button" value="Auswählen"/></p> <p><b>Verpflichtungserklärung *</b></p> <p>Mir ist bewusst, dass wenn ich die Rahmenbedingung des „Leitfadens zur Reaktion auf IT-Sicherheitsvorfälle für Vorfall-Praktiker und Vorfall-Experten“ nicht einhalte oder meine vorgenannte Qualifikation nicht gegeben ist, ich nicht mehr Teil des Cyber-Sicherheitsnetzwerkes sein kann und auch von der Liste der Vorfall-Experten genommen werde.</p> <p>ja <input type="checkbox"/></p> </div> <div> <input type="button" value="Eingaben exportieren"/> <input type="button" value="Eingaben importieren"/> <input type="button" value="Zurück"/> <input type="button" value="Speichern &amp; Weiter"/> </div>
<p><b>5d</b></p>	<p><i>Diese Seite wird Ihnen nur angezeigt, wenn Sie zuvor folgende Rolle ausgewählt haben: IT-Sicherheitsdienstleister.</i></p> <p>Für die Registrierung als IT-Sicherheitsdienstleister<sup>8</sup> geben Sie an, welche der Zulassungskriterien Ihr Unternehmen erfüllt und laden Sie anschließend den dazu passenden Nachweis hoch.</p> <p>Außerdem müssen Sie eine Selbsterklärung abgeben.</p> <p>Klicken Sie auf <b>Speichern &amp; Weiter</b>.</p>	<div> <h3>Qualifikationsnachweis (IT-Sicherheitsdienstleister)</h3> <p>Als IT-Sicherheitsdienstleister müssen Sie ein der folgenden Bedingungen erfüllen:</p> <p>a) Zertifizierung als IT-Sicherheitsdienstleister b) Qualifikation als APT-Dienstleister c) Qualifikation als DDoS-Dienstleister</p> <p><b>Zertifizierung *</b></p> <p>Wir erklären hiermit, die o.g. Voraussetzungen zu erfüllen. Folgendes können wir nachweisen (bitte Nachweis hochladen):</p> <p><input type="checkbox"/> Zertifizierung als IT-Sicherheitsdienstleister <input type="checkbox"/> Qualifikation als APT-Dienstleister <input type="checkbox"/> Qualifikation als DDoS-Dienstleister</p> <p><b>Upload Nachweis</b></p> <p>Keine Datei ausgewählt <input type="button" value="Auswählen"/></p> <p><b>Erklärung *</b></p> <p>Uns ist bewusst, dass wir sobald wir den Status eines zertifizierten bzw. qualifizierten IT-Sicherheitsdienstleisters verlieren, dies unaufgefordert der Geschäftsstelle des Cyber-Sicherheitsnetzwerkes mitteilen (info@cyber-sicherheitsnetzwerk.de) müssen.</p> <p>ja <input type="checkbox"/></p> </div> <div> <input type="button" value="Eingaben exportieren"/> <input type="button" value="Eingaben importieren"/> <input type="button" value="Zurück"/> <input type="button" value="Speichern &amp; Weiter"/> </div>
<p><b>6</b></p>	<p>Abschließend sind noch verschiedene Erklärungen notwendig:</p> <p>Verpflichtend zu bestätigen sind die Datenschutzvereinbarung und die Verpflichtung auf das Traffic Light Protocoll.</p> <p>Die Zustimmung zu den Nutzungsbedingungen des CSN-Logos sind optional, allerdings dürfen Sie das Logo nur nutzen, wenn Sie die Nutzungsbedingungen akzeptieren.</p>	<div> <h3>Abschließende Erklärungen und Verpflichtungen</h3> <p><b>Datenschutz und Datenverarbeitung</b></p> <p>Ich willige ein, dass die in Punkt 1 genannten personenbezogenen Daten zu den Zwecken der Registrierung und Veröffentlichung und zum Zwecke der Verwaltung von Kontaktdaten, für die Mitteilung von Informationen, Einladungen oder für Rückfragen vom BSI verarbeitet werden dürfen. Eine Weitergabe an Dritte findet nicht ohne weitere Zustimmung statt. Diese Einwilligungserklärung ist freiwillig und kann jederzeit per E-Mail an info@cyber-sicherheitsnetzwerk.de widerrufen werden. Nach Eingang des Widerrufs können die personenbezogenen Daten, die von dem Widerruf umfasst sind, nicht mehr durch das BSI aufgrund dieser Einwilligung weiterverwendet werden. Durch den Widerruf einer Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Verantwortliche Stelle für die Verarbeitung der oben genannten personenbezogenen Daten ist das Bundesamt für Sicherheit in der Informationstechnik, Postfach 200363, 53133 Bonn. Die von Ihnen angegebenen Daten werden ausschließlich im Rahmen der vorgenannten Zwecke verarbeitet und dies nur so lange, wie es zu den zuvor genannten Zwecken erforderlich ist, um die gesetzlichen Aufgaben zu erfüllen bzw. bis Sie Ihre Einwilligung widerrufen. Weitere Informationen darüber, wie wir Ihre personenbezogenen Daten bei uns verarbeiten und welche Rechte Ihnen diesbezüglich zustehen, können Sie der Datenschutzerklärung auf den Seiten des BSI entnehmen: <a href="https://www.bsi.bund.de/DE/Service/Datenschutz/datenschutz_node.html">https://www.bsi.bund.de/DE/Service/Datenschutz/datenschutz_node.html</a></p> <p><b>Zustimmung zur Datenverarbeitung *</b></p> <p>Bitte auswählen <input type="checkbox"/></p> </div>

	<p>Wenn Sie Interesse haben, ein Regionales Forum zu gründen oder zu leiten, wählen Sie an der entsprechenden Frage <b>ja</b> aus. Wir kontaktieren Sie diesbezüglich gesondert.</p> <p>Sie müssen außerdem erklären, dass Sie uns über Änderungen zu den vorherigen Angaben umgehend informieren.</p> <p>Optional können Sie außerdem den Empfang des CSN-Newsletters wünschen. In diesem informieren wir Sie regelmäßig (i. d. R. monatlich) über Neuigkeiten rund um das CSN.</p> <p>Klicken Sie auf <b>Speichern &amp; Vorschau</b>.</p>	<p><b>Traffic Light Protocoll (TLP)</b></p> <p>Die im Rahmen des Cyber-Sicherheitsnetzwerks verbreiteten Informationen werden, entsprechend ihres Schutzbedürfnisses, gemäß dem „Traffic Light Protocol“ (TLP) eingestuft. Die Regelungen zum TLP werden durch das „Merkblatt zum sicheren Informationsaustausch mit dem Traffic Light Protocol (TLP), Version 2.0“ festgelegt und erläutert: <a href="https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/TLP/merkblatt-ttp.html">https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/TLP/merkblatt-ttp.html</a></p> <p>Alle Zugangsberechtigten aus den teilnehmenden Institutionen haben sich persönlich dazu verpflichtet, Informationen, welche sie durch oder im Zusammenhang mit dem CSN erlangen, entsprechend den Regelungen des TLP zu behandeln und diese unbefugten Dritten nicht zugänglich zu machen. Ich verpflichte mich entsprechend den TLP Bestimmungen zu handeln. Für den Fall, dass ein Teilnehmer gegen die im TLP niedergeschriebenen Anforderungen verstößt, ist das CSN berechtigt, die Teilnahme dieses Teilnehmers in der CSN ohne Einhaltung einer Frist zu beenden.</p> <p><b>Bestätigung der Verpflichtung auf das TLP *</b></p> <p>Bitte auswählen <span>▼</span></p> <p><b>Nutzungsbedingungen des CSN-Logos</b></p> <p>Aktive Teilnehmer des Cyber-Sicherheitsnetzwerks sind berechtigt, das dafür bereitgestellte Logo des Cyber-Sicherheitsnetzwerks (CSN) nach Zustimmung zu den Nutzungsbedingungen (<a href="https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CSN/230508_Nutzungsvereinbarung_Logo.html?nn=972382">https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CSN/230508_Nutzungsvereinbarung_Logo.html?nn=972382</a>) zu nutzen, um auf die Teilnahme ihrer Person bzw. ihrer Institution an dem CSN hinzuweisen.</p> <p>Teilnehmer sind Personen bzw. Institutionen die sich beim Cyber-Sicherheitsnetzwerk mittels Registrierungsformular als Digitaler Erstherfer, Vorfälle Praktiker, Vorfälle-Experte, Leiter eines regionalen CSN-Forums, Schulungsanbieter, Hotline oder Initiative registriert haben.</p> <p><b>Zustimmung zu den Nutzungsbedingungen</b></p> <p><input checked="" type="radio"/> nein <input type="radio"/> ja</p> <p><b>Regionale Foren</b></p> <p>Ich möchte ein regionales Forum leiten. Bitte senden Sie mir diesbezüglich weitere Informationen zu.</p> <p><input checked="" type="radio"/> nein <input type="radio"/> ja</p> <p><b>Information über Änderungen *</b></p> <p>Bei Änderung meiner Kontaktdaten verpflichte ich mich, dies umgehend der Geschäftsstelle des Cyber-Sicherheitsnetzwerks (<a href="mailto:info@cyber-sicherheitsnetzwerk.de">info@cyber-sicherheitsnetzwerk.de</a>) mitzuteilen.</p> <p>Bitte auswählen <span>▼</span></p> <p><b>Empfang CSN-Newsletter</b></p> <p>Über den monatlichen CSN-Newsletter halten wir Sie auf dem Laufenden rund um die Entwicklungen des CSN. Möchten Sie den Newsletter abonnieren?</p> <p><input checked="" type="radio"/> nein <input type="radio"/> ja</p>								
7	<p>Bevor Sie den Antrag einreichen, können Sie diesen im pdf- oder html-Format für Ihre Unterlagen herunterladen.</p> <p>Zum Absenden klicken Sie auf <b>Antrag einreichen</b>. Sie können den Antrag anschließend nicht mehr bearbeiten!</p>	<p><b>Institution für Meldestelle registrieren</b></p> <p>Ihr Antrag wurde gespeichert. Bitte laden Sie die Vorschau herunter und prüfen Sie den Antrag. Sind alle Angaben korrekt, klicken Sie bitte auf "Antrag einreichen". Sobald Sie den Antrag eingereicht haben, können Sie keine weiteren Änderungen vornehmen.</p> <p>Bitte beachten Sie, dass Ihnen der Registrierungsantrag nur 48 Stunden lang im Melde- und Informationsportal zur Verfügung steht.</p> <p><a href="#">Vorschau (PDF) herunterladen</a></p> <p><a href="#">Vorschau (HTML) herunterladen</a></p> <p>⚠ Bitte beachten Sie, dass Sie nach Abgabe den Antrag nicht mehr verändern können!</p> <p><a href="#">Antrag bearbeiten</a> <a href="#">Antrag einreichen</a></p>								
8	<p>Im Bereich Institutionsverwaltung sehen Sie nun unter Offene Meldestellenregistrierungen Ihren eingereichten Antrag und den Status.</p>	<p><b>Offene Meldestellenregistrierungen</b></p> <p>Die eingegebenen Daten stehen Ihnen im Portal für 48 Stunden ab der letzten gespeicherten Änderung zur Verfügung. Bitte bearbeiten Sie den Registrierungsantrag oder übermitteln Sie diesen vor Ablauf der Frist. Die Daten werden nach Ablauf der Frist oder nach Übermittlung des Registrierungsantrags im Portal dauerhaft gelöscht.</p> <table border="1"> <thead> <tr> <th>Registrierungsformular</th> <th>Meldestelle</th> <th>Status (gespeichert bis)</th> <th>Aktionen</th> </tr> </thead> <tbody> <tr> <td>Registrierungsformular für das Cyber-Sicherheitsnetzwerk</td> <td>Cyber-Sicherheitsnetzwerk</td> <td>Abgeschickt</td> <td><a href="#">✎</a> <a href="#">🗑</a></td> </tr> </tbody> </table> <p><b>Hinweis:</b> Falls eine Zeile komplett ausgegraut sein sollte, befindet sich dieses Formular im Wartungsmodus.</p>	Registrierungsformular	Meldestelle	Status (gespeichert bis)	Aktionen	Registrierungsformular für das Cyber-Sicherheitsnetzwerk	Cyber-Sicherheitsnetzwerk	Abgeschickt	<a href="#">✎</a> <a href="#">🗑</a>
Registrierungsformular	Meldestelle	Status (gespeichert bis)	Aktionen							
Registrierungsformular für das Cyber-Sicherheitsnetzwerk	Cyber-Sicherheitsnetzwerk	Abgeschickt	<a href="#">✎</a> <a href="#">🗑</a>							
9	<p>Nach Annahme des Antrag sehen Sie in der Institutionsverwaltung, dass der Status auf <b>Angenommen</b> geändert wurde.</p> <p>Außerdem sehen Sie Ihre Nutzer-ID unter Rollenverwaltung als Institutionsverwalter und die Meldestelle unter Registrierungen.</p>	<p><b>Offene Meldestellenregistrierungen</b></p> <p>Die eingegebenen Daten stehen Ihnen im Portal für 48 Stunden ab der letzten gespeicherten Änderung zur Verfügung. Bitte bearbeiten Sie den Registrierungsantrag oder übermitteln Sie diesen vor Ablauf der Frist. Die Daten werden nach Ablauf der Frist oder nach Übermittlung des Registrierungsantrags im Portal dauerhaft gelöscht.</p> <table border="1"> <thead> <tr> <th>Registrierungsformular</th> <th>Meldestelle</th> <th>Status (gespeichert bis)</th> <th>Aktionen</th> </tr> </thead> <tbody> <tr> <td>Registrierungsformular für das Cyber-Sicherheitsnetzwerk</td> <td>Cyber-Sicherheitsnetzwerk</td> <td>Angenommen</td> <td><a href="#">✎</a> <a href="#">🗑</a></td> </tr> </tbody> </table> <p><b>Hinweis:</b> Falls eine Zeile komplett ausgegraut sein sollte, befindet sich dieses Formular im Wartungsmodus.</p>	Registrierungsformular	Meldestelle	Status (gespeichert bis)	Aktionen	Registrierungsformular für das Cyber-Sicherheitsnetzwerk	Cyber-Sicherheitsnetzwerk	Angenommen	<a href="#">✎</a> <a href="#">🗑</a>
Registrierungsformular	Meldestelle	Status (gespeichert bis)	Aktionen							
Registrierungsformular für das Cyber-Sicherheitsnetzwerk	Cyber-Sicherheitsnetzwerk	Angenommen	<a href="#">✎</a> <a href="#">🗑</a>							



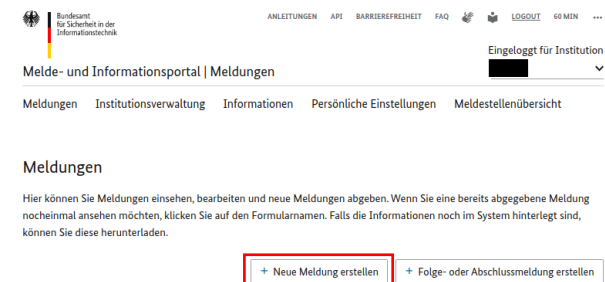
## 4 Erstellen eines Vorfallsberichts

Das Modul, mit dem Sie Ihre Vorfallsberichte erstellen können, heißt im MIP „Meldungen“. Bitte füllen Sie die Meldung nach Abschluss der Vorfallsbearbeitung vollständig aus. Notieren Sie sich die Kontaktdaten des Betroffenen. Als Hilfestellung für die Vorfallsbearbeitung können Sie die Bearbeitungsvorlagen nutzen, welche Sie von der CSN-Geschäftsstelle erhalten.

Um ein möglichst genaues Bild über die Art der Anrufe zu bekommen, bitten wir Sie, auch bei Störungen eine Meldung abzugeben.

Die gemeldeten IT-Sicherheitsvorfälle fließen in das Lagebild Wirtschaft und Gesellschaft ein und werden durch das BSI regelmäßig ausgewertet. Gemeldete Störungen ermöglichen uns die Erstellung von FAQs, welche wiederum für eine Vorfilterung der Anrufe sorgen kann.

Bitte geben Sie auf keinen Fall personenbezogene Daten ein!

Schritt	Anleitung	
1	<p>Wählen Sie über das Dropdown-Menü rechts oben die Institution aus, mit der Sie den Vorfallsbericht abgeben möchten.</p> <p>Wenn Sie mehrere Institutionen haben, wählen Sie diejenige aus, die die Rolle hat, in der Sie den Vorfall bearbeitet haben.</p> <p>Klicken Sie nun auf den Menüpunkt <b>Meldungen</b>.</p>	
2	<p>Starten Sie den Meldevorgang durch einen Klick auf <b>Neue Meldung erstellen</b>.</p>	
3	<p>Wählen Sie in den Dropdown-Menüs als Meldestelle <b>Cyber-Sicherheitsnetzwerk</b> sowie das Meldeformular <b>Vorfallsbericht des CSN</b> aus.</p> <p>Fahren Sie mit einem Klick auf <b>Meldung erstellen</b> fort.</p>	
4	<p>Wenn Sie einen Folgebericht zu einer bestehenden Meldung eingeben möchten, können Sie über <b>Eingaben importieren</b> die JSON-Datei des betreffenden Vorfalles einlesen und Ihren Bericht auf Basis der bereits erfassten Informationen eingeben. Dabei können Sie jede Angabe frei verändern, wenn dies nötig ist.</p>	

5

Die erste Seite des Vorfallsberichts umfasst allgemeine Daten, die sich teilweise auf die Anzeige der folgenden Unterseiten auswirken.

**Rollenauswahl:** Wählen Sie die Rolle aus, in der Sie den Vorfall bearbeitet haben.

**Ihre Registrierungsnummer:** Geben Sie Ihre für die Rolle zutreffende CSN-Registrierungsnummer an.

**Datum und Uhrzeit des Erstkontakts:** Wann hat die/der Betroffene Sie erstmalig kontaktiert?

**Erst- oder Folgemeldung:** Bitte geben Sie Folgemeldung an, wenn der Vorfall bereits von einem anderen Glied der Digitalen Rettungskette vorher bearbeitet wurde. Lassen Sie sich in diesem Fall den vorherigen Vorfallsbericht vom Betroffenen geben – idealerweise die json-Datei.

**Sonstiges:** Geben Sie hier an, wie man den Betroffenen eingruppieren kann, wenn die vorherigen Kategorien nicht passen.

**Vorfalls-ID:** Vergeben Sie bei Erstmeldung eine neue Vorfalls-ID (Formatvorgabe beachten). Bei Folgemeldungen geben Sie die ID an, die der vorherige Bearbeiter vergeben hat.

**Einstufung des Vorgangs:** Dies ist eine Vorwegnahme des Bearbeitungsergebnisses und dient zur Auswahl der folgenden Seiten.

Klicken Sie auf **Speichern & Weiter**.

### Vorfallsbericht des CSN

Mit diesem Formular können Digitale Ersthelfer, Vorfall-Praktiker und Vorfall-Experten die Berichte zu den von ihnen behandelten Vorfällen einreichen.  
Die erhobenen Daten gehen in die Lagebeobachtung des BSI und in statistische Auswertungen des CSN ein. Bitte beachten Sie beim Ausfüllen, insbesondere in den Freitextfeldern, dass Sie KEINE personenbezogenen Daten eingeben.

#### Allgemeine Angaben

##### Rollenauswahl \*

Bitte geben Sie hier an, in welcher Rolle Sie die Meldung abgeben.

Digitaler Ersthelfer

##### Ihre Registrierungsnummer \*

Bitte geben Sie hier Ihre CSN-Registrierungsnummer an.

Bitte ausfüllen...

##### Vorfalls-ID \*

Bitte vergeben Sie eine Vorfalls-ID. Bei Folgemeldungen geben Sie bitte die Vorfalls-ID der Erstmeldung an.

Bitte ausfüllen...

##### Erst- oder Folgemeldung \*

Bitte geben Sie an, ob es sich um eine Erst- oder eine Folgemeldung handelt. Folgemeldungen liegen vor, wenn der Vorfall vorher bereits von einem anderen Helfer bearbeitet und gemeldet wurde.

☒ Erstmeldung

☐ Folgemeldung

##### Datum des Erstkontakts \*

Bitte geben Sie hier an, an welchem Tag Sie wegen des zu meldenden Vorfalls erstmals kontaktiert wurden.

TT.MM.JJJJ

##### Uhrzeit des Erstkontakts \*

--:--

##### Art des Betroffenen \*

Bitte wählen Sie aus, zu welcher Gruppe der/die Betroffene gehört.

Privatperson

##### Art des Betroffenen: Sonstiges bitte erläutern


Bitte geben Sie KEINE personenbezogenen Daten ein!


Bitte ausfüllen...

##### Einstufung des Vorgangs \*


Bitte wählen Sie aus, welche Vorfallskategorie für diese Meldung zutrifft.

IT-Sicherheitsvorfall

 Eingaben exportieren

 Eingaben importieren

 Zurück

Speichern & Weiter 

6a

*Diese Seite wird Ihnen nur angezeigt, wenn Sie zuvor bei Art des Betroffenen folgendes ausgewählt haben: Privatperson.*

Bitte geben Sie die Postleitzahl des Betroffenen an. Diese hilft dabei, lokale Häufungen von Vorfällen zu detektieren.


Klicken Sie auf **Speichern & Weiter**.


### Zusatzangaben bei betroffenen Privatpersonen

Bei Privatpersonen benötigen wir ausschließlich die PLZ der/des Betroffenen, um Rückschlüsse auf die regionale Bekanntheit des CSN ziehen und lokale Häufungen von Vorfällen erkennen zu können.


#### Postleitzahl \*

Bitte ausfüllen...

 Eingaben exportieren

 Eingaben importieren

 Zurück

Speichern & Weiter 

6b

*Diese Seite wird Ihnen nur angezeigt, wenn Sie zuvor bei Art des Betroffenen folgendes ausgewählt haben: Unternehmen, Verein/Verband, Sonstiges (bitte erläutern).*

Bitte geben Sie die Postleitzahl des Betroffenen an. Diese hilft dabei, lokale Häufungen von Vorfällen zu dektieren.

Anschließend werden verschiedene Daten zur Organisation und der Struktur der Organisations-IT abgefragt.

Weiterhin wird gefragt, inwieweit der Vorfall bereits mit den verfügbaren Ressourcen bearbeitet wurde und ob Dritte betroffen sind.

Als Ergänzung zur Betroffenheit Dritter können Sie eine Gruppe, die nicht explizit genannt ist, per Freitext benennen. Bitte geben Sie im Erläuterungsfeld KEINE personenbezogenen Daten an!

Klicken Sie auf **Speichern & Weiter**.

### Zusatzangaben bei Organisationen

Bei Organisationen werden die PLZ sowie strukturelle Daten zur betroffenen Organisation erhoben. So können wir Rückschlüsse auf die regionale Bekanntheit sowie die Akzeptanz innerhalb der Zielgruppen des CSN ziehen. Die Strukturdaten zur IT ermöglicht uns Rückschlüsse auf den Zustand der IT-Sicherheit innerhalb der Zielgruppen. Außerdem wird eine mögliche Betroffenheit Dritter abgefragt, um Vorfälle mit weitreichenden Folgen bereits im Vorfeld erkennen zu können.

#### Postleitzahl \*

Bitte ausfüllen...

#### Organisationsgröße (Anzahl Mitarbeitende) \*

1-9

#### Rolle der/des Anrufenden \*

Management/InhaberIn

#### Tätigkeitsbereich \*

Ist die betroffene Organisation im IT-Umfeld tätig?

- ☐ nein  
☐ ja, als Dienstleister  
☐ ja, als Hersteller

#### Strukturdaten zur Organisations-IT \*

Bitte geben Sie an, welche dieser Einrichtungen in der Organisation vorhanden sind.

- ☐ keine der Genannten  
☐ externer IT-Dienstleister  
☐ eigenständige IT-Abteilung  
☐ Informationssicherheitsbeauftragter (intern)  
☐ Informationssicherheitsbeauftragter (extern)  
☐ Datenschutzbeauftragter (intern)  
☐ Datenschutzbeauftragter (extern)

#### Einbeziehung \* ⓘ

Wurde mindestens eine der vorher genannten Einrichtungen bereits in den Vorgang einbezogen?

- ☒ nein  
☐ ja  
☐ nicht zutreffend

#### Betroffenheit Dritter \*

Sind Daten oder Systeme von Dritten betroffen?

- ☐ nein  
☐ ja, von Mitarbeitenden  
☐ ja, von Lieferanten  
☐ ja, von Mitgliedern oder Kunden (Privatpersonen)  
☐ ja, von Mitgliedern oder Kunden (andere Unternehmen)  
☐ ja, von staatlichen Einrichtungen (Behörden)  
☐ ja, von anderen Gruppen (bitte erläutern)

#### Betroffene Dritte: Sonstiges bitte erläutern

Bitte geben Sie KEINE personenbezogenen Daten ein!

Bitte ausfüllen...

⚙ Eingaben exportieren

📄 Eingaben importieren

⬅ Zurück

**Speichern & Weiter ➤**

7a

*Diese Seite wird Ihnen nur angezeigt, wenn Sie auf der Startseite als Rolle Digitaler Ersthelfer und als Einstufung des Vorfalls IT-Sicherheitsvorfall ausgewählt haben.*

Bitte beschreiben Sie den Vorfall mittels den angegebenen Fragestellungen.

### Vorfall: Beschreibung der Angriffsvektoren

Es wird zwischen technischen und nicht-technischen Angriffsvektoren unterschieden. Bitte geben Sie an, was aus Ihrer Sicht zutrifft. Weiterführende Details zu diesem Bereich (z. B. der Name der verwendeten Schadsoftware) können Sie im Freitextfeld angeben.

#### Technische Angriffsvektoren

##### Schadsoftware \*

Gemeint sind nur Infektionen von Geräten/Systemen der/des Betroffenen.

- ☐ nein  
☐ ja, mit Ransomware  
☐ ja, mit anderer Art von Schadprogramm

#### Hacking und Manipulation \*

Hierunter fallen: webanwendungsbasierter Angriffe (z.B. Drive-By-Infektion), Angriff auf Webanwendungen (z.B. SQL-Injection), Kommunikationsmanipulation (z.B. Man-in-the-Middle, Spoofing), Brute-Force-Attack (z.B. systematisches Ausprobieren von Passwörtern), Fälschung von digitalen Zertifikaten, Ausnutzung von Protokollschwachstellen (z.B. DNS, SMTP) etc.

- ☒ nein  
☐ ja

#### Angriff auf die Verfügbarkeit von Diensten \*

Hier sind sowohl Systeme der/des Betroffenen als auch Systeme Dritter gemeint.

- ☐ nein  
☐ ja, durch Überflutung (z.B. DDoS)  
☐ ja, durch gezielten Systemabsturz (z.B. durch Ausnutzung von Systemschwachstellen)

Falls Sie darüberhinaus weitere Angaben machen möchten, nutzen Sie das Freitextfeld. Geben Sie KEINE personenbezogenen Daten an!

#### Nichttechnische Angriffsvektoren

##### Social Engineering und Identitätsmissbrauch \*

- ☐ nein
- ☐ Diebstahl von Zugangsdaten (z.B. Phishing)
- ☐ Missbrauch/Vortäuschung von Identitäten (z.B. Betrug beim Onlineshopping)
- ☐ Manipulation von Mitarbeitenden (z.B. CEO-Fraud)

##### Innentäter \*

Hierunter fallen alle vorsätzlichen Angriffe durch Insider - z. B. Mitarbeitende.

- ☐ nein
- ☐ ja

##### Physischer Angriff \*

- ☐ nein
- ☐ Diebstahl von IT-Komponenten
- ☐ Zerstörung/Beschädigung von IT-Komponenten
- ☐ unbefugter Zutritt

##### Lieferkettenangriff \*

Ein Lieferkettenangriff liegt vor, wenn der Angriff über Mitarbeitende oder Produkte von Zulieferern bzw. für das Unternehmen tätige Dienstleister erfolgt.

- ☐ nein
- ☐ ja

##### Sonstiges bitte erläutern

Bitte geben Sie KEINE personenbezogenen Daten ein! Hier können z. B. auch die Symptome beschreiben, die durch die/den Betroffenen bemerkt wurden.

Bitte ausfüllen...

Klicken Sie auf **Speichern & Weiter**.

⬇ Eingaben exportieren

📄 Eingaben importieren

⬅ Zurück

**Speichern & Weiter ➔**

7b

*Diese Seite wird Ihnen nur angezeigt, wenn Sie auf der Startseite als Rolle Vorfall-Praktiker, Vorfall-Experte oder IT-Sicherheitsdienstleister und als Einstufung des Vorfalls IT-Sicherheitsvorfall ausgewählt haben.*

Bitte beschreiben Sie den Vorfall mittels den angegebenen Fragestellungen.

#### Vorfall: Angriffsvektoren

Es wird zwischen technischen und nicht-technischen Angriffsvektoren unterschieden. Bitte geben Sie an, was aus Ihrer Sicht zutrifft. Weiterführende Details zu diesem Bereich (z. B. der Name der verwendeten Schadsoftware) können Sie im Freitextfeld angeben.

##### Technische Angriffsvektoren

###### Schadsoftware

- ☐ Ransomware
- ☐ Malwareinfektion (z.B. Trojaner, Spyware)
- ☐ Adware oder Scareware
- ☐ multifunktionale Schadprogramme (z.B. Viren, Würmer)

###### Hacking und Manipulation

- ☐ webanwendungsbasierter Angriff (z.B. Drive-By-Infektion)
- ☐ Angriff auf Webanwendungen (z.B. SQL-Injection)
- ☐ Kommunikationsmanipulation (z.B. Man-in-the-Middle, Spoofing)
- ☐ Brute-Force-Attack (z.B. systematisches Ausprobieren von Passwörtern)
- ☐ Fälschung von digitalen Zertifikaten
- ☐ Ausnutzung von Protokollschwachstellen (z.B. DNS, SMTP)

###### Angriffe auf die Verfügbarkeit von Dienste

- ☐ Überflutung (z.B. DDoS)
- ☐ gezielter Systemabsturz (z.B. durch Ausnutzung von Systemschwachstellen)

Falls Sie darüberhinaus weitere Angaben machen möchten, nutzen Sie das Freitextfeld. Geben Sie KEINE personenbezogenen Daten an!

#### Nichttechnische Angriffsvektoren

##### Social Engineering und Identitätsmissbrauch

- ☐ Diebstahl von Zugangsdaten (z.B. Phishing)
- ☐ Missbrauch/Vortäuschung von Identitäten (z.B. Betrug beim Onlineshopping)
- ☐ Manipulation von Mitarbeitenden (z.B. CEO-Fraud)

##### Innentäter

- ☐ Weitergabe interner Informationen
- ☐ unberechtigtes Erlangen erweiterter Zugriffsrechte
- ☐ missbräuchliche Verwendung von Zugriffsrechten
- ☐ Löschung oder Beschädigung von Daten(-trägern)

##### Physischer Angriff

- ☐ Diebstahl von IT-Komponenten
- ☐ Zerstörung/Beschädigung von IT-Komponenten
- ☐ unbefugter Zutritt

##### Lieferkettenangriff

- ☐ unkontrollierter Zugriff auf ausgelagerte Informationen (z.B. Cloud-Dienstleister)
- ☐ Ausfall von Dienstleistern (z.B. bei SaaS)
- ☐ Schwachstellen bei eingesetzter Software (z.B. Exchange-Schwachstelle)
- ☐ Schwachstellen in eingesetzter Hardware

##### Sonstiges bitte erläutern

Bitte geben Sie KEINE personenbezogenen Daten ein! Hier können z. B. auch die Symptome beschreiben, die durch die/den Betroffenen bemerkt wurden.

Bitte ausfüllen...

⬇ Eingaben exportieren

📄 Eingaben importieren

⬅ Zurück

Speichern & Weiter ➤

Klicken Sie auf **Speichern & Weiter**.

8a

*Diese Seite wird Ihnen nur angezeigt, wenn Sie auf der Startseite als Rolle Digitaler Ersthelfer und als Einstufung des Vorfalls IT-Sicherheitsvorfall ausgewählt haben.*

Beschreiben Sie die Ursachen, die Ihrer Einschätzung nach zu dem Vorfall geführt haben.

Falls Sie darüberhinaus weitere Angaben machen möchten, nutzen Sie das Freitextfeld. Geben Sie KEINE personenbezogenen Daten an!

#### Vorfall: Schwachstellen

Bitte geben Sie an, welche Schwachstelle (vermutlich) ursächlich für den Vorfall war.

##### Organisatorische Mängel

Bitte geben Sie an, welche Schwachstelle (vermutlich) ursächlich für den Vorfall war.

- ☐ unzureichendes Passwortmanagement
- ☐ nicht eingespieltes Patch/Update
- ☐ unzureichendes Backupmanagement
- ☐ mangelnde Sensibilität/Fahrlässigkeit
- ☐ Sorglosigkeit im Umgang mit Informationen

##### Technische Mängel

- ☐ fehlendes Patch/Update (Zero-Day-Exploit)
- ☐ andere technische Mängel

##### Sonstiges bitte erläutern

Falls die oben genannten Kategorien nicht ausreichen, können Sie hier weitere Informationen angeben. Bitte geben Sie KEINE personenbezogenen Daten ein!

Bitte ausfüllen...

⬇ Eingaben exportieren

📄 Eingaben importieren

⬅ Zurück

Speichern & Weiter ➤

Klicken Sie auf **Speichern & Weiter**.

8b

*Diese Seite wird Ihnen nur angezeigt, wenn Sie auf der Startseite als Rolle Vorfall-Praktiker, Vorfall-Experte oder IT-Sicherheitsdienstleister und als Einstufung des Vorfalls IT-Sicherheitsvorfall ausgewählt haben.*

Beschreiben Sie die Ursachen, die Ihrer Einschätzung nach zu dem Vorfall geführt haben.

Falls Sie darüberhinaus weitere Angaben machen möchten, nutzen Sie das Freitextfeld. Geben Sie KEINE personenbezogenen Daten an!

Klicken Sie auf **Speichern & Weiter**.

### Vorfall: Schwachstellen

Bitte geben Sie an, welche Schwachstelle (vermutlich) ursächlich für den Vorfall war.

#### Organisatorische Mängel

- ☐ unzureichende Prozesse/Regeln zur IT-Sicherheit
- ☐ Ressourcenmangel
- ☐ unzureichendes Patch-/Updatemanagement
- ☐ unzureichendes Passwortmanagement
- ☐ unzureichendes Backupmanagement
- ☐ mangelnde Sensibilität/Fähigkeit
- ☐ unzureichendes Notfallmanagement
- ☐ unzureichende Dokumentation
- ☐ Sorglosigkeit im Umgang mit Informationen
- ☐ unzureichende technische Sicherheit

#### Technische Mängel

- ☐ fehlendes Patch/Update in eingesetzter Software (Zero-Day-Exploit)
- ☐ unzureichende Datensicherung (Back-Ups)
- ☐ unzureichende Netzwerksegmentierung
- ☐ Verwendung unsicherer Protokolle oder Netze
- ☐ bauliche Mängel (z.B. bei unberechtigtem Zutritt, fehlender Brandschutz)
- ☐ unzureichende Dimensionierung der Infrastruktur (z.B. Stromversorgung)

#### Sonstiges bitte erläutern

Bitte geben Sie KEINE personenbezogenen Daten ein!

Bitte ausfüllen...

± Eingaben exportieren

≡ Eingaben importieren

< Zurück

**Speichern & Weiter >**

8c

*Diese Seite wird Ihnen nur angezeigt, wenn Sie auf der Startseite als Einstufung des Vorfalls Störung oder Fehlbedienung ausgewählt haben.*

Bitte kategorisieren Sie die Störung mittels den angegebenen Auswahlfelder.

Darüber hinaus können Sie im Textfeld beschreiben, welche Symptome vom Anrufer beschrieben wurden. Geben Sie KEINE personenbezogenen Daten an!

Klicken Sie auf **Speichern & Weiter**.

### Störung/Anwenderfehler: Beschreibung

Entsprechend der Leitfäden des CSN wird bei einer IT-Störung von einem technischen Defekt oder einem versehentlichen fehlerhaften Nutzen des IT-Systems durch den Benutzer selbst ausgegangen.

#### Einstufung \*

- ☐ technische Störung
- ☐ Fehlbedienung
- ☐ äußerer Einfluss (Wetter etc.)
- ☐ anderes

#### Beschreibung \*

Hier können Sie weitere Informationen zur Art und Ursache der Störung angeben. Bitte geben Sie KEINE personenbezogenen Daten ein!

Bitte ausfüllen...

± Eingaben exportieren

≡ Eingaben importieren

< Zurück

**Speichern & Weiter >**

9

Bitte wählen Sie aus, welche Systeme/Dienste von dem Vorfall bzw. der Störung betroffen sind.

Insbesondere bei Störungen können Sie im Freitextfeld weitere Details angeben, z. B. welche Art Kabel defekt war.

Bitte geben Sie KEINE personenbezogenen Daten an!

Klicken Sie auf **Speichern & Weiter**.

## Betroffene Systeme

Bitte geben Sie an, welches System bzw. welche Systeme betroffen sind/waren.

### Webbasierte Dienste

Hierunter fallen alle internetbasierten Dienste, bei denen Nutzerkonten zur Inanspruchnahme bestehen.

- ☐ Kommunikationsdienste (E-Mail, Messenger...)
- ☐ Netzwerkdienste (Facebook, Twitter...)
- ☐ Onlineshopping (amazon, ebay...)
- ☐ Finanzdienste (Onlinebanking, PayPal...)
- ☐ andere webbasierte Dienste

### PC/Laptop

Bitte geben Sie das Betriebssystem des betroffenen PC/Laptop an.

- ☐ Windows 10
- ☐ Windows 11
- ☐ ältere Windowsversion
- ☐ MacOS
- ☐ Linux
- ☐ anderes Betriebssystem

### Mobiles Endgerät

Bitte geben Sie das Betriebssystem des betroffenen Gerätes an.

- ☐ nicht mehr unterstützte Androidversion
- ☐ aktuelle/noch unterstützte Androidversion
- ☐ nicht mehr unterstützte iOS-Version
- ☐ aktuelle/noch unterstützte iOS-Version
- ☐ anderes Betriebssystem

### Peripheriegeräte

- ☐ Eingabegeräte (Maus, Tastatur, Mikrofon...)
- ☐ Drucker/Scanner
- ☐ Ausgabegeräte (Monitor, Lautsprecher...)
- ☐ andere Peripheriegeräte

### Netzwerkssysteme

- ☐ Router/Access Points
- ☐ Netzwerkspeicher/lokaler Datenserver
- ☐ Firewall
- ☐ andere Netzwerksysteme

### Sonstige Komponenten und Dienste

- ☐ Produktionssysteme/OT
- ☐ IoT-Geräte (Smarthome etc.)
- ☐ Verkabelung, Funkverbindungen
- ☐ lokal oder im lokalen Netzwerk installierte Software

### Infrastruktur

- ☐ Strom
- ☐ Internet/Telefon
- ☐ anderes

### Sonstiges bitte erläutern

Hier können Sie weitere Details zum betroffenen Dienst/System angeben, z. B. welcher Dienst oder welche Software betroffen ist. Bitte geben Sie KEINE personenbezogenen Daten ein!

Bitte ausfüllen...

⬇ Eingaben exportieren

⬆ Eingaben importieren

⬅ Zurück

**Speichern & Weiter ➤**

10

Bitte geben Sie nun zunächst an, ob Sie dem Betroffenen die Kontaktaufnahme mit einer anderen Stelle (welche?) empfohlen haben, und den Zeitpunkt des Endes der Vorfallsbehandlung.

Anschließend geben Sie an, ob der Ihnen vorliegende Leitfaden für die Behandlung des Vorfalls im Rahmen Ihrer Rollen ausreichend war. Sollten Sie Ergänzungen haben, geben Sie diese bitte im Freitextfeld an. Bitte geben Sie KEINE personenbezogenen Daten ein!

Klicken Sie auf **Speichern & Vorschau**.

### Empfohlenes Vorgehen

Bitte geben Sie an, welches Vorgehen Sie der/dem Betroffenen angeraten haben. Waren die Inhalte des Leitfadens für die Behandlung ausreichend oder wären mehr Informationen/Hilfestellungen notwendig gewesen. Bitte beachten Sie bei der Behandlung und der Bewertung den Handlungsrahmen, der für Ihre Rolle (DEH/VP/VE) vorgesehen ist.

#### Eskalation \*

Wurde der/dem Betroffenen empfohlen, sich mit dem Vorfall an jemand anderen zu wenden?

- ☐ nein, Vorfall erfolgreich abgeschlossen
- ☐ ja, an bsi.bund.de
- ☐ ja, an Vorfall-Praktiker
- ☐ ja, an Vorfall-Experte
- ☐ ja, an IT-Sicherheitsdienstleister (CSN)
- ☐ ja, an Strafverfolgungsbehörden
- ☐ ja, an Dritte

#### Ende Vorfallsbehandlung \*

Wann haben Sie die Bearbeitung des Vorfalls abgeschlossen?

TT. MM. JJJJ

#### Uhrzeit zum Ende der Vorfallsbehandlung \*

--:--

#### Leitfaden ausreichend \*

Waren die im Leitfaden empfohlenen Maßnahmen für die Behandlung ausreichend?

keine Maßnahmen notwendig (z. B. Fehlbedienung) ▾

#### Ergänzung

Wenn der Leitfaden nicht ausreicht hat, geben Sie hier bitte an, was ggf. gefehlt hat. Bitte geben Sie KEINE personenbezogenen Daten ein!

Bitte ausfüllen...

± Eingaben exportieren

↕ Eingaben importieren

< Zurück

Speichern & Vorschau >

11

Abschließend klicken Sie auf **Meldung abgeben**. Ihr Vorfallsbericht wird nun an das BSI übermittelt.

Bundesamt für Sicherheit in der Informationstechnik

ANLEITUNGEN API BARRIEREFREIHEIT FAQ LOGOUT 60 MIN ...

Eingeloggt für Institution

Melde- und Informationsportal | Meldungen

Meldungen Institutionsverwaltung Informationen Persönliche Einstellungen Meldestellenübersicht

### Meldung abgeben

Ihre Meldung wurde gespeichert. Bitte laden Sie die Vorschau herunter und prüfen Sie die Meldung. Sind alle Angaben korrekt, klicken Sie bitte auf "Meldung abgeben". Sobald Sie die Meldung eingereicht haben, können Sie keine weiteren Änderungen vornehmen.

± Vorschau (PDF) herunterladen

± Vorschau (HTML) herunterladen

● Bitte beachten Sie, dass Sie nach Abgabe die Meldung nicht mehr verändern können!

✎ Meldungen bearbeiten

● **Meldung abgeben**



12

Auf der abschließenden Seite laden Sie den Vorfallsbericht als **PDF**- und als **JSON**-Datei herunter. Beide Dateien stellen Sie dem Betroffenen zur Verfügung.

Abgegebene Vorfallsberichte sind nur eine bestimmte Zeit im MIP verfügbar. Sie sollten Ihre Berichte daher lokal archivieren. Es empfiehlt sich, die Vorfalls-ID (nicht die Meldungs-ID des MIP) in den Dateinamen zu integrieren.

The screenshot shows the 'Melde- und Informationsportal | Meldungen' interface. At the top, there is a navigation bar with links for 'ANLEITUNGEN', 'API', 'BARRIEREFREIHEIT', 'FAQ', 'LOGOUT', and '60 MIN'. The user is logged in as 'Eingeloggt für Institution'. Below the navigation bar, there is a breadcrumb trail: 'Meldungen > Institutionsverwaltung > Informationen > Persönliche Einstellungen > Meldestellenübersicht'. A message box states: 'Die Meldung wurde erfolgreich abgegeben'. Below this, there is a section titled 'Meldung mit ID [redacted] ansehen'. A note says: 'Hier können Sie nochmals ihre bereits abgegebene Meldung einsehen. Bitte laden Sie sich mindestens die JSON-Datei herunter, da die Daten im Portal nur temporär gespeichert werden.' The 'Meldungs-ID' is [redacted]. The 'Typ der Meldung' is 'Alleinstehende Meldung'. The 'Für Meldestelle' is 'Cyber-Sicherheitsnetzwerk'. The 'Formularname' is 'Vorfallsbericht des CSN'. There are three download buttons: 'PDF herunterladen', 'JSON herunterladen', and 'HTML herunterladen'. The 'PDF herunterladen' and 'JSON herunterladen' buttons are highlighted with red boxes. At the bottom, there is a button 'Zurück zur Meldungsübersicht'.

## Links und Verweise

---

- <sup>1</sup> [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Qualifizierung/Digitaler\\_Ersthelfer/Digitaler\\_Ersthelfer\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Qualifizierung/Digitaler_Ersthelfer/Digitaler_Ersthelfer_node.html)
- <sup>2</sup> [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Onlinekurs/Module/Onlinekurs\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Onlinekurs/Module/Onlinekurs_node.html)
- <sup>3</sup> [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Qualifizierung/Vorfall\\_Praktiker/Vorfall\\_Praktiker\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Qualifizierung/Vorfall_Praktiker/Vorfall_Praktiker_node.html)
- <sup>4</sup> [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Onlinekurs/Module/Onlinekurs\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Onlinekurs/Module/Onlinekurs_node.html)
- <sup>5</sup> [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Qualifizierung/Vorfall\\_Experten/Liste\\_Schulungsanbieter\\_Vorfall\\_Experte/liste\\_Schulungsanbieter\\_Vorfall\\_Experte\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Qualifizierung/Vorfall_Experten/Liste_Schulungsanbieter_Vorfall_Experte/liste_Schulungsanbieter_Vorfall_Experte_node.html)
- <sup>6</sup> [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Qualifizierung/Vorfall\\_Experten/Vorfall\\_Experte\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Qualifizierung/Vorfall_Experten/Vorfall_Experte_node.html)
- <sup>7</sup> [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Qualifizierung/Vorfall\\_Experten/Liste\\_Schulungsanbieter\\_Vorfall\\_Experte/liste\\_Schulungsanbieter\\_Vorfall\\_Experte\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Qualifizierung/Vorfall_Experten/Liste_Schulungsanbieter_Vorfall_Experte/liste_Schulungsanbieter_Vorfall_Experte_node.html)
- <sup>8</sup> [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Qualifizierung/Sicherheitsdienstleister/Sicherheitsdienstleister\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Qualifizierung/Sicherheitsdienstleister/Sicherheitsdienstleister_node.html)