Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Benutzerhandbuch MIP für CSN

Anleitungen für Registrierung und Vorfallsbericht

Änderungshistorie

Version	*Datum*	*Name*	*Beschreibung*
1.0	04.12.2023	CSN	Erste Veröffentlichungsversion
1.1	19.01.2024	CSN	Ergänzte Veröffentlichungsversion

Tabelle 1: Änderungshistorie

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
E-Mail: info@cyber-sicherheitsnetzwerk.de
Internet: https://www.bsi.bund.de, www.cyber-sicherheitsnetzwerk.de

Inhalt

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@cybersicherheitsnetzwerk.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?

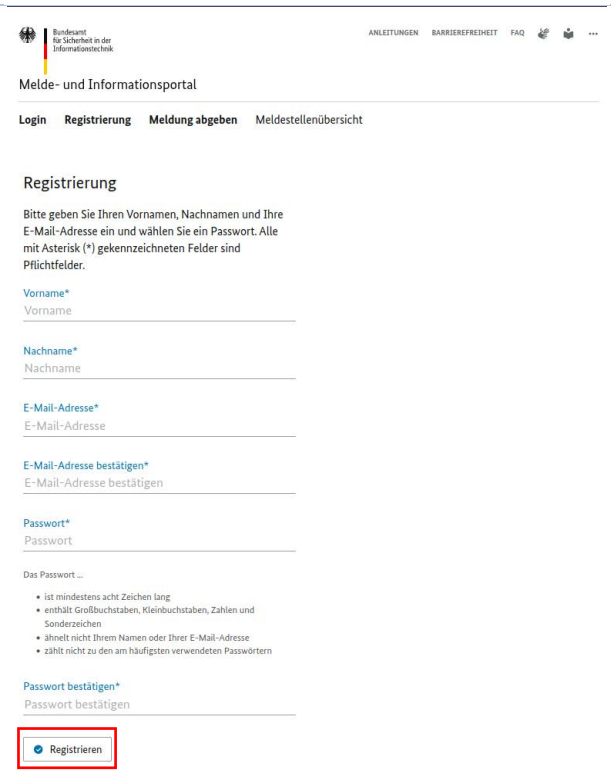
Bei Fragen hilft Ihnen die CSN-Geschäftsstelle gerne weiter (info@cyber-sicherheitsnetzwerk.de). Bitte senden Sie uns Ihre Anfrage zu. Wir melden uns so schnell wie möglich bei Ihnen.

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

2 Benutzerverwaltung

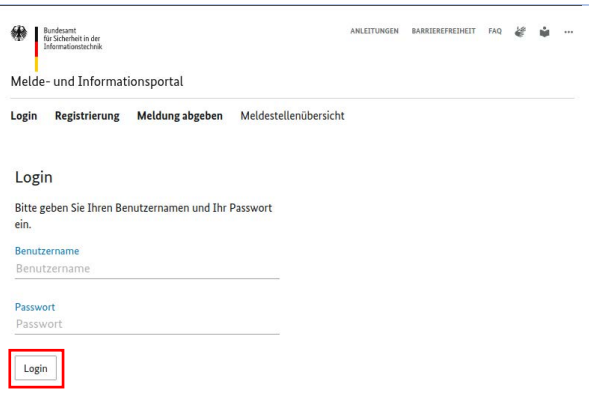
Jede Person und jedes Unternehmen, die/das Zugang zum MIP erhalten möchte, hat exakt ein Benutzerkonto. Der Login erfolgt mit der User-ID und einem Passwort, ggf. ergänzt durch eine Zwei-Faktor-Authentisierung.

2.1 Anlegen eines neuen Benutzers

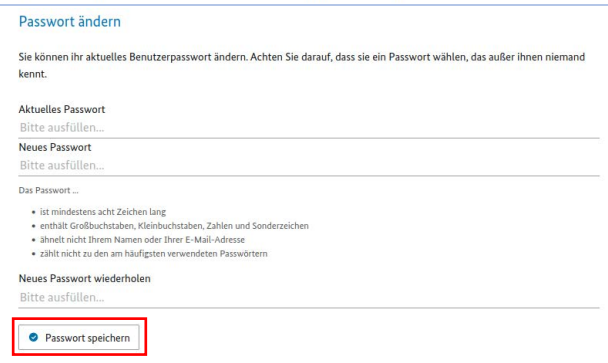
Schritt	Anleitung
1	Zum Anlegen eines neuen Benutzerkontos klicken Sie im unteren Bereich der Startseite (https://mip2.bsi.bund.de/) auf **Registrieren**. 
2	Füllen Sie mindestens alle mit einem Stern (*) gekennzeichneten Felder aus. Beachten Sie bei der Passwortvergabe die auf der Seite beschriebenen Regeln. Später können Sie das Konto durch einen zweiten Faktor (z. B. Passkey) zusätzlich absichern. Wenn Sie alle Daten eingegeben haben, bestätigen Sie dies mit Klick auf **Registrieren**. 
3	Im nächsten Fenster wird Ihnen eine Registrierungsbestätigung und die automatisch generierte User-ID angezeigt. 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.

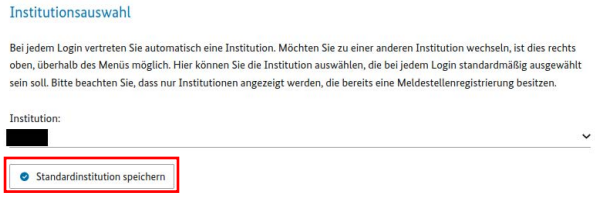
2.2 Login

Schritt	Anleitung
1	Rufen Sie die Seite zum Login des MIP auf: https://mip2.bsi.bund.de/authentifizierung/login/

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

2.3 Weitere Optionen der Benutzerverwaltung

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

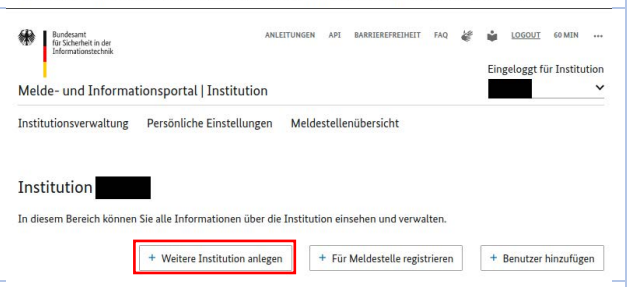
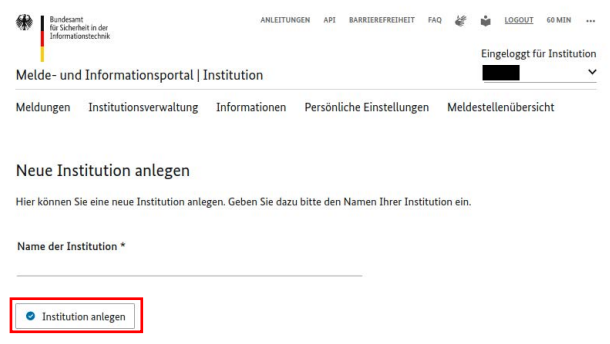
	entsprechenden Eintrag auf **Token löschen**.	
4	Sie können festlegen, welche Institution beim Login standardmäßig aktiv sein soll. Wählen Sie die Institution über das Dropdown-Menü aus und bestätigen Sie durch Klick auf **Standardinstitution speichern**.	

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.

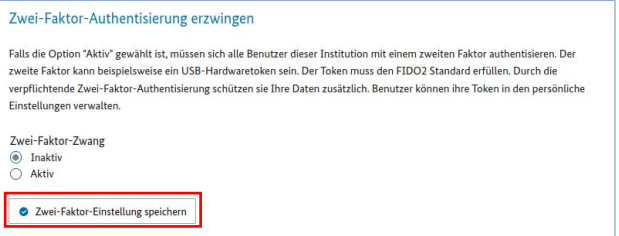
Es besteht die Möglichkeit, anderen Benutzern den Zugriff auf eine Institution zu gewähren (siehe 3.3). Diese Option sollten lediglich IT-Sicherheitsdienstleister nutzen, die mehrere Vorfallsbearbeiter beschäftigen. Wichtig: Jede Person, die Zugriff erhalten soll, muss ein eigenes Benutzerkonto haben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

3.1 Anlegen einer neuen Institution

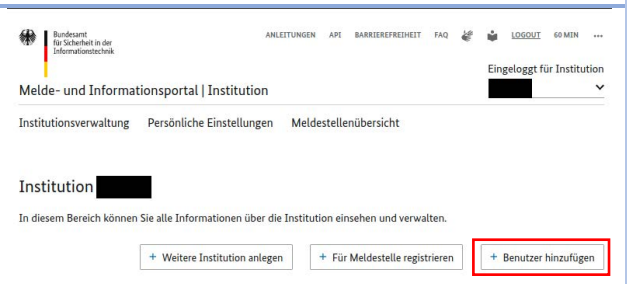
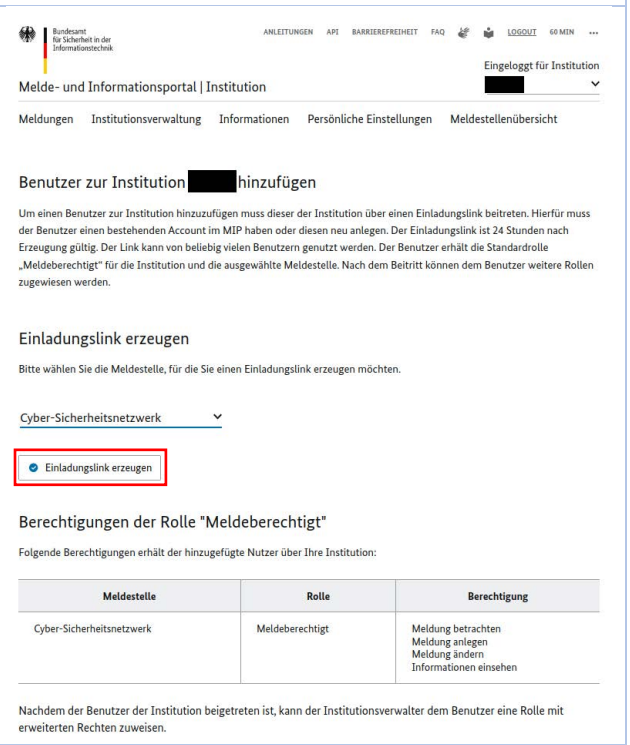
Schritt	Anleitung	
1	Die **Institutionsverwaltung** erreichen Sie über den entsprechenden Menüeintrag im oberen Seitenbereich.	
2	Anschließend klicken Sie auf **Weitere Institution** anlegen.	
3	Geben Sie der Institution einen Namen und klicken Sie anschließend auf **Institution anlegen**.	
4	Im nächsten 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	Sie können für Institutionen den Login mit 2FA erzwingen. Hierfür ändern Sie die Auswahl auf Aktiv und bestätigen per Klick auf **Zwei-Faktor-Einstellung** speichern.	

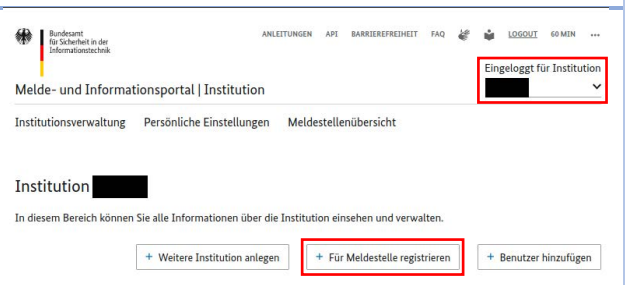
3.3 Anderen Benutzern Zugriff auf Institution geben

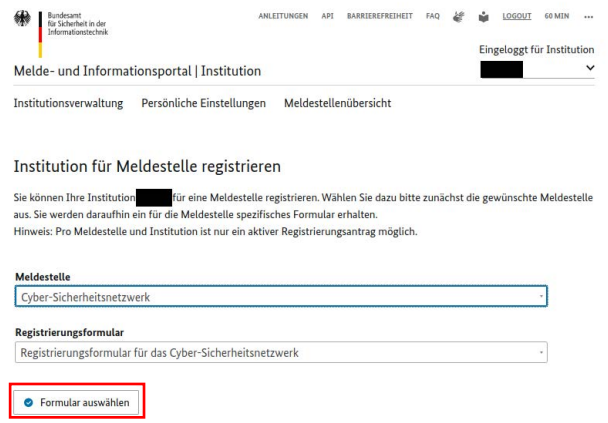
Schritt	Anleitung	
1	Sie haben die Möglichkeit, einem anderen Benutzer Zugriff auf eine Institution zu geben, welche Sie verwalten. Dies ist erst möglich, wenn Ihre Registrierungsanfrage angenommen wurde. Klicken Sie hierfür auf **Benutzer hinzufügen**.	
2	Mit dem Klick auf **Einladungslink erzeugen** 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. Nach dem Beitritt kann der Institutionsverwalter die Rolle des anderen Benutzers anpassen oder ihm den Zugriff auch wieder entziehen. *Diese Funktion ist insbesondere für IT-Sicherheitsdienstleister relevant, welche mehrere Vorfallsbearbeiter beschäftigen.*	

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.

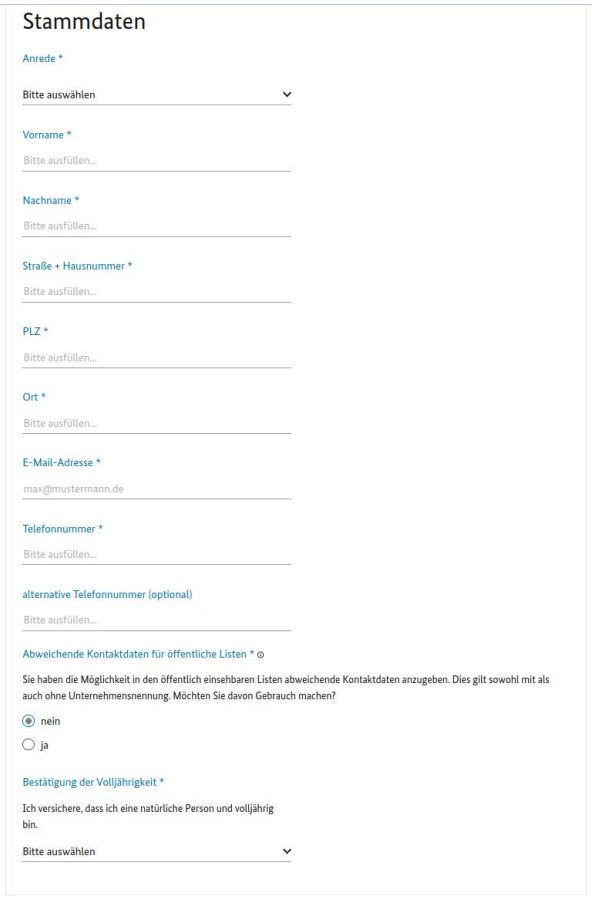
Schritt	Anleitung
1	Um eine Institution für eine Meldestelle zu registrieren, wählen Sie diese Institution über das Dropdown-Menü rechts oben aus und klicken anschließend links oben auf **Institutionsverwaltung**. Dort starten Sie den Registrierungsprozess über **Für Meldestelle registrieren**.
2	Im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





4a

Diese Seite wird Ihnen nur angezeigt, wenn Sie zuvor eine der folgenden Rollen ausgewählt haben: Digitaler Ersthelfer, Vorfall-Praktiker, Vorfall-Experte.



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.

Die Felder sind weitestgehend selbsterklärend. Folgende Hinweise sind dennoch zu beachten:

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 *Abweichende Kontaktdaten* für öffentliche Listen *ja* aus.

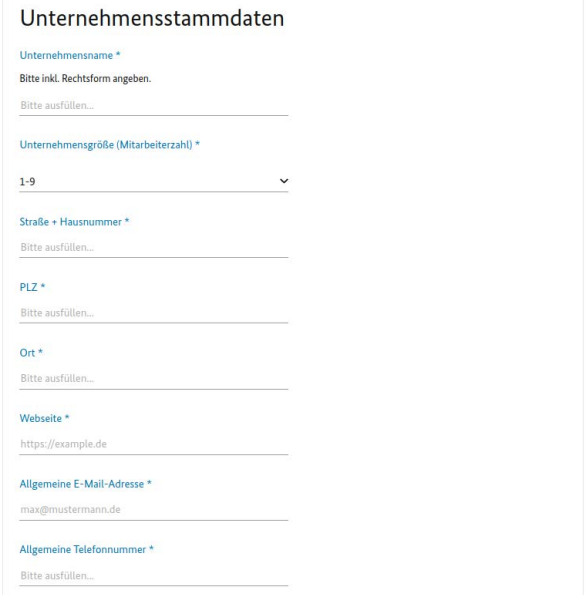
Wenn Sie öffentlich gelistet werden möchten, aber keine abweichenden Kontaktdaten angeben, werden die hier angegebenen Kontaktdaten veröffentlicht.

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

Klicken Sie auf **Speichern & Weiter**.

4b

Diese Seite wird Ihnen nur angezeigt, wenn Sie zuvor die folgende Rolle ausgewählt haben: IT-Sicherheitsdienstleister.



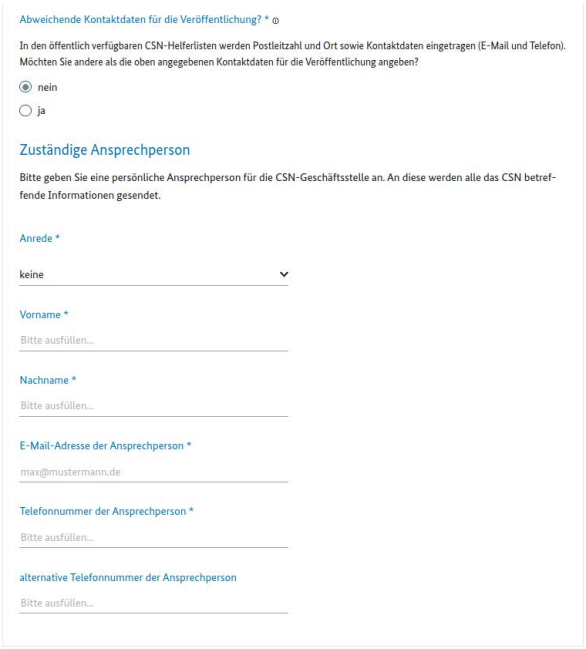
Als nächstes geben Sie die Stammdaten Ihrer Firma an. Diese werden verschlüsselt übertragen und ausschließlich im – nur innerhalb des BSI-Netzes erreichbaren – CRM des BSI gespeichert.

Die Felder sind weitestgehend selbsterklärend. Folgende Hinweise sind dennoch zu beachten:

Bitte geben Sie an dieser Stelle die allgemeinen Firmenkontaktdaten an. Die Kontaktdaten der speziell für die

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**.

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**.

4d

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

<u>Wichtig</u>: 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**.

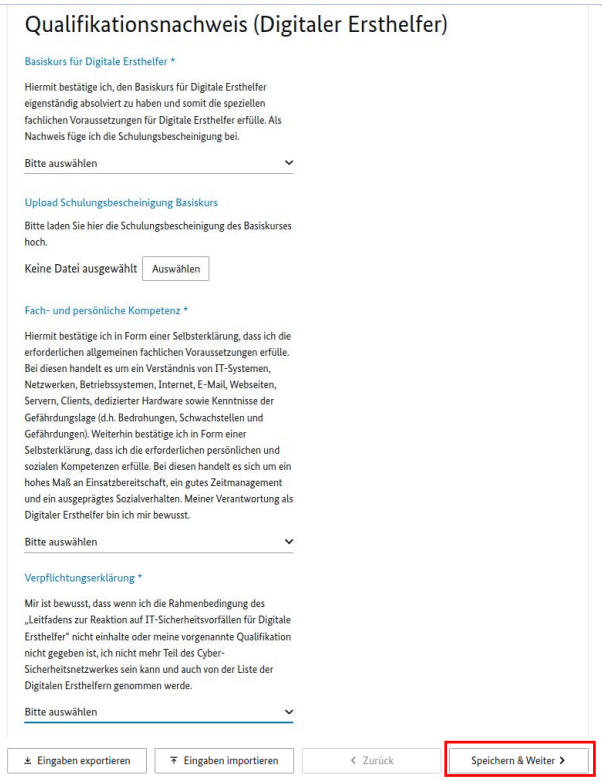
5a

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

Als Digitaler Ersthelfer[1] müssen Sie den Basiskurs[2] 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**.



5b

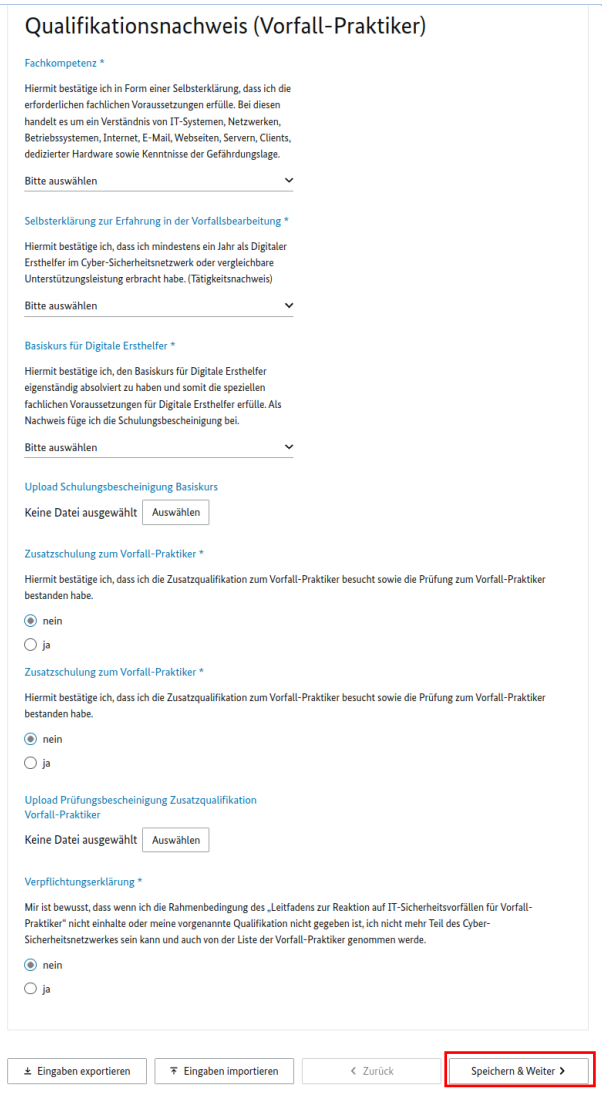
Diese Seite wird Ihnen nur angezeigt, wenn Sie zuvor folgende Rolle ausgewählt haben: Vorfall-Praktiker.

Als Vorfall-Praktiker[3] müssen Sie zum einen den Basiskurs[4] 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[5] 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**.

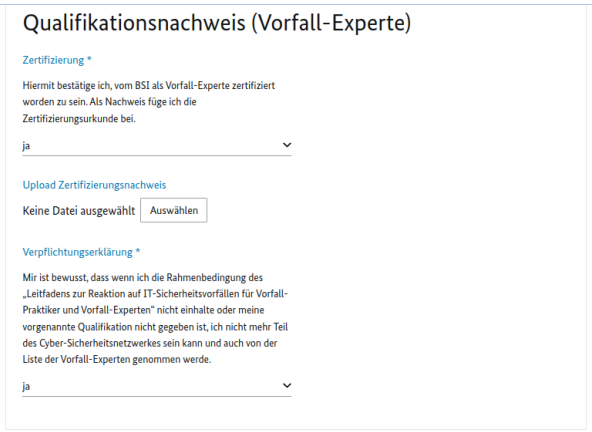


5c

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

Als Vorfall-Experte[6] müssen Sie die Aufbauschulung bei einem gelisteten Schulungsanbieter[7] besuchen und anschließend den Zertifizierungsprozess des BSI durchlaufen.

An dessen Ende erhalten Sie ein Zertifikat, welches Sie in dem dafür vorgesehenen Feld hochladen können.



Außerdem ist eine Verpflichtungserklärung abzugeben.

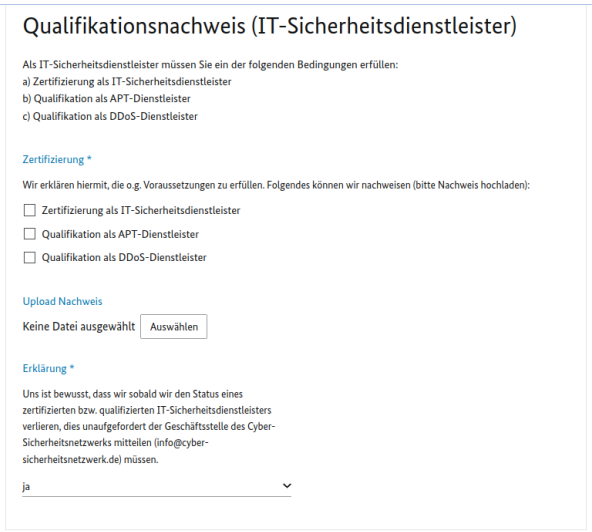
Klicken Sie auf **Speichern & Weiter**.

5d

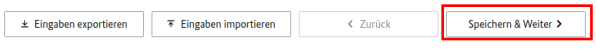
Diese Seite wird Ihnen nur angezeigt, wenn Sie zuvor folgende Rolle ausgewählt haben: IT-Sicherheitsdienstleister.

Für die Registrierung als IT-Sicherheitsdienstleister[8] geben Sie an, welche der Zulassungskriterien Ihr Unternehmen erfüllt und laden Sie anschließend den dazu passenden Nachweis hoch.

Außerdem müssen Sie eine Selbsterklärung abgeben.



Klicken Sie auf **Speichern & Weiter**.

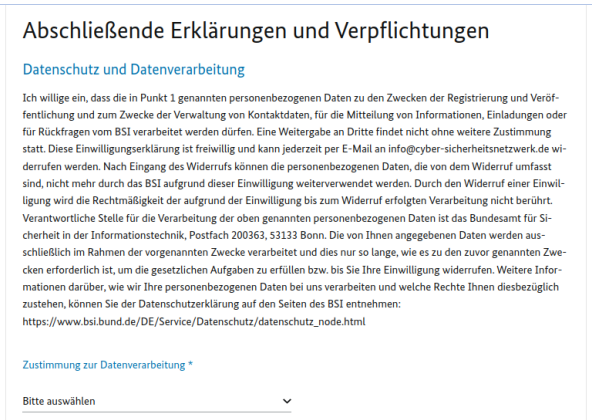


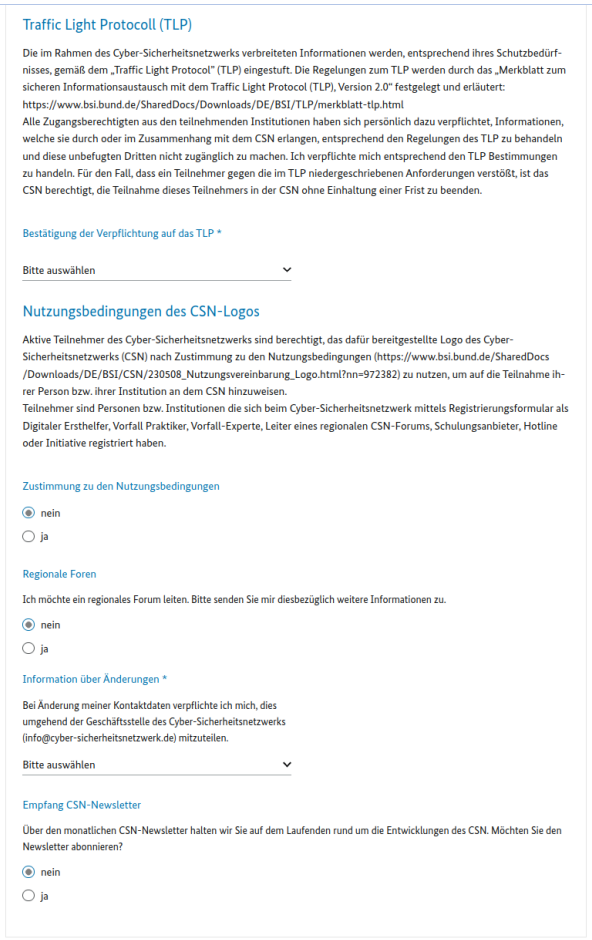
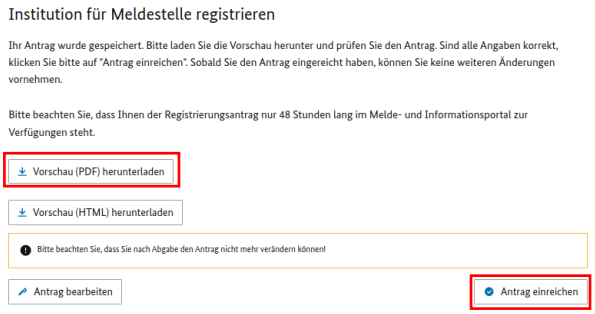
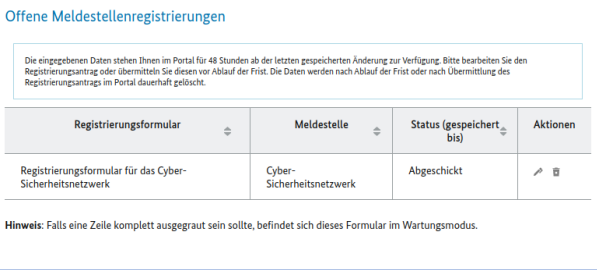
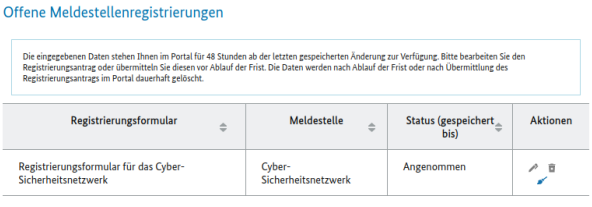
6

Abschließend sind noch verschiedene Erklärungen notwendig:

Verpflichtend zu bestätigen sind die Datenschutzvereinbarung und die Verpflichtung auf das Traffic Light Protocoll.

Die Zustmmung zu den Nutzungsbedingungen des CSN-Logos sind optional, allerdings dürfen Sie das Logo nur nutzen, wenn Sie die Nutzungsbedinungen akzeptieren.



	Wenn Sie Interesse haben, ein Regionales Forum zu gründen oder zu leiten, wählen Sie an der entsprechenden Frage *ja* aus. Wir kontaktieren Sie diesbezüglich gesondert. Sie müssen außerdem erklären, dass Sie uns über Änderungen zu den vorherigen Angaben umgehend informieren. 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. Klicken Sie auf **Speichern & Vorschau**.	
7	Bevor Sie den Antrag einreichen, können Sie diesen im pdf- oder html-Format für Ihre Unterlagen herunterladen. Zum Absenden klicken Sie auf **Antrag einreichen**. Sie können den Antrag anschließend nicht mehr bearbeiten!	
8	Im Bereich Institutionsverwaltung sehen Sie nun unter Offene Meldestellenregistrierungen Ihren eingereichten Antrag und den Status.	
9	Nach Annahme des Antrag sehen Sie in der Institutionsverwaltung, dass der Status auf *Angenommen* geändert wurde. Außerdem sehen Sie Ihre Nutzer-ID unter Rollenverwaltung als Institutionsverwalter und die Meldestelle unter Registrierungen.	

4 Erstellen eines Vorfallsberichts

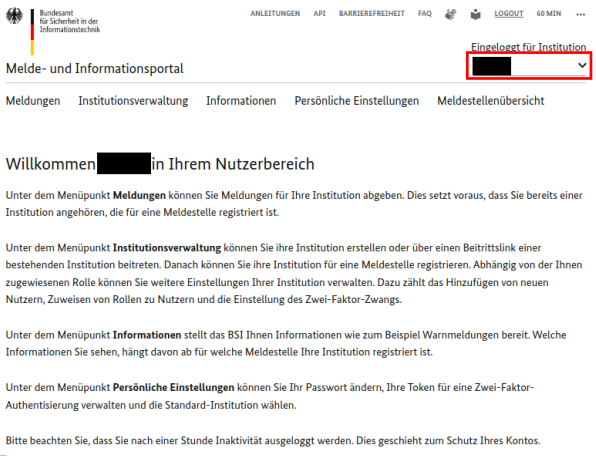
Das Modul, mit dem Sie Ihre Vorfallsberichte erstellen können, heißt im MIP „Meldungen“. Bitte füllen Sie die Meldung nach Abschluss der Vorfallsbearbeitung vollständig aus. Notieren Sie sich die Kontaktdaten des Betroffenen. Als Hilfestellung für die Vorfallsbearbeitung können Sie die Bearbeitungsvorlagen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

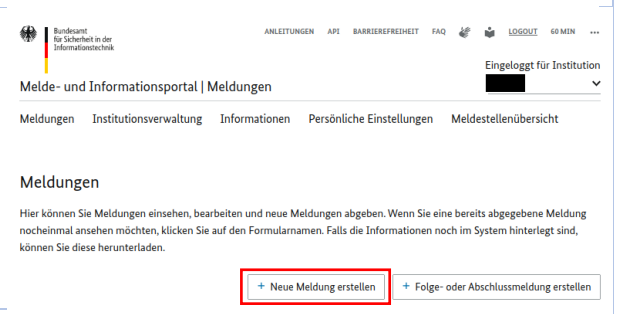
Um ein möglichst genaues Bild über die Art der Anrufe zu bekommen, bitten wir Sie, auch bei Störungen eine Meldung abzugeben.

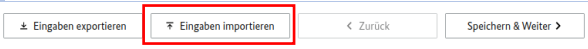
Die gemeldeten IT-Sicherheitsvorfälle fließen in das Lagebild Wirtschaft und Gesellschaft ein und werden durch das BSI regelmäßig ausgewertet. Gemeldete Störungen ermöglichen uns die Erstellung von FAQs, welche wiederrum für eine Vorfilterung der Anrufe sorgen kann.

Bitte geben Sie auf keinen Fall personenbezogene Daten ein!

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

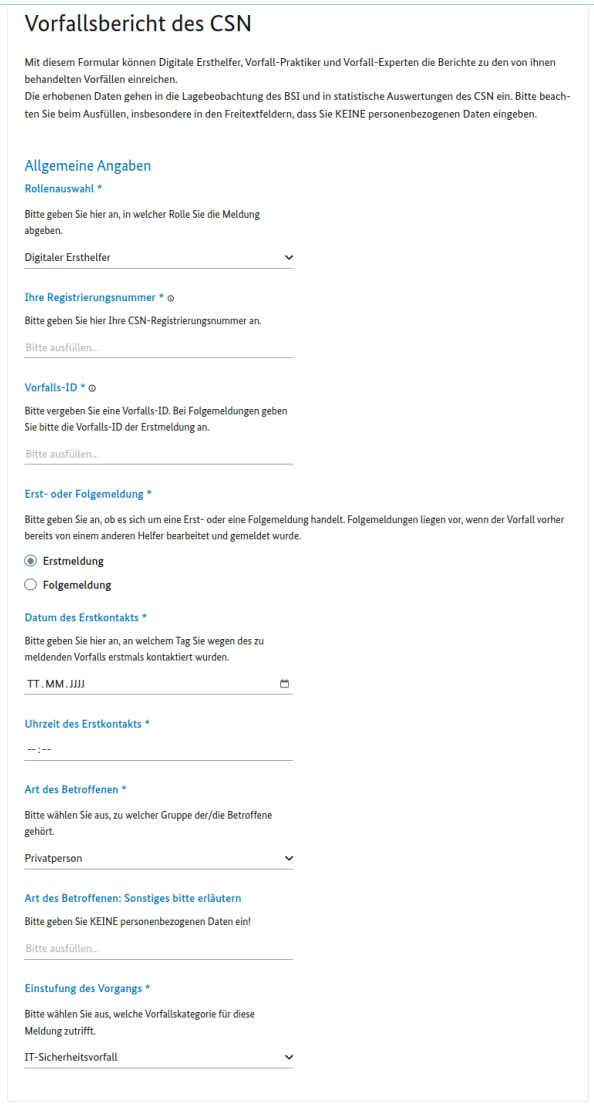






5

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



<u>Rollenauswahl:</u> Wählen Sie die Rolle aus, in der Sie den Vorfall bearbeitet haben.

<u>Ihre Registrierungsnummer:</u> Geben Sie Ihre für die Rolle zutreffende CSN-Registrierunsnummer an.

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

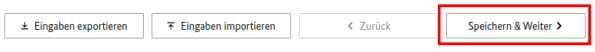
<u>Erst- oder Folgemeldung:</u> Bitte geben Sie Folgemeldung an, wenn der Vorfall bereits von einem anderen Glied der Digitalen Rettungskette vorher bearbeitet wurde. Lassen Sie sich in diesem Fall den vorherigen Vorfallsbericht vom Betroffenen geben – idealerweise die json-Datei.

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

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

<u>Einstufung des Vorgangs:</u> Dies ist eine Vorwegnahme des Bearbeitungsergebnisses und dient zur Auswahl der folgenden Seiten.

Klicken Sie auf **Speichern & Weiter**.

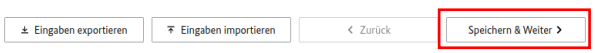


6a

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**.



6b

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

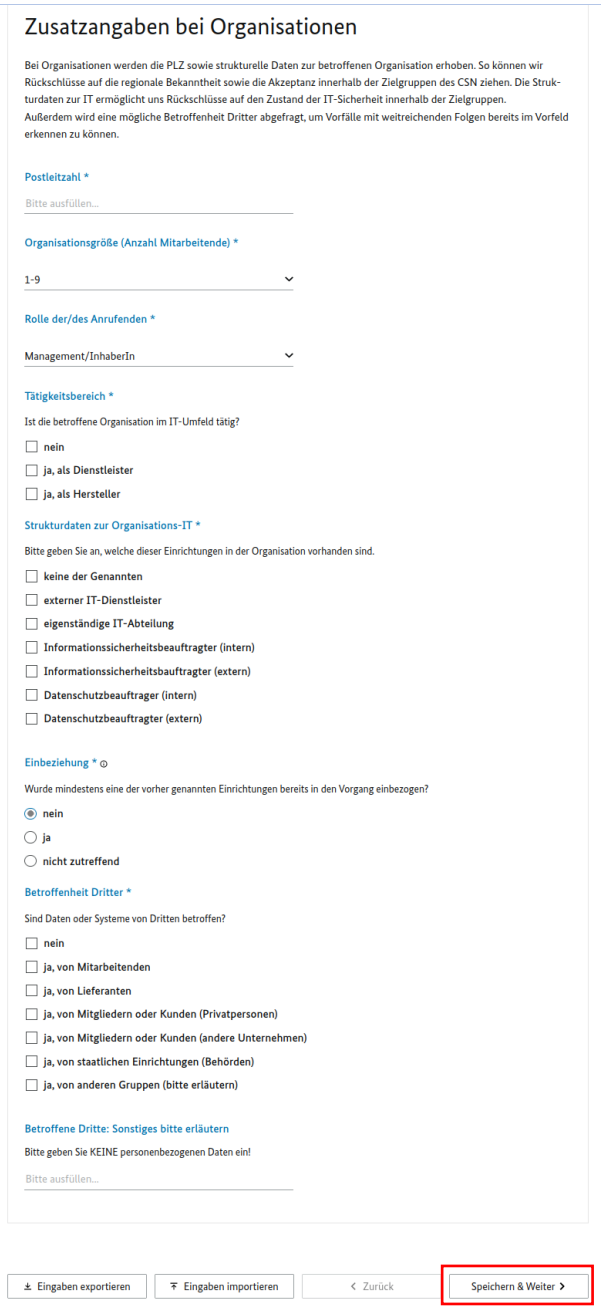
Bitte geben Sie die Postleitzahl des Betroffenen an. Diese hilft dabei, lokale Häufungen von Vorfällen zu detektieren.

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!

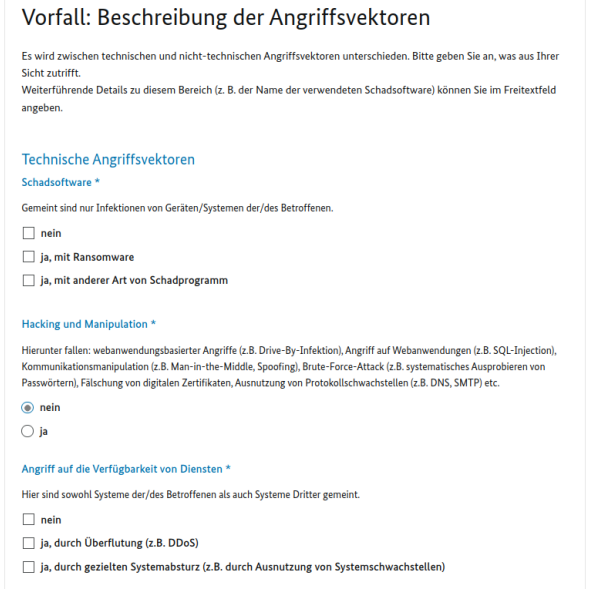
Klicken Sie auf **Speichern & Weiter**.



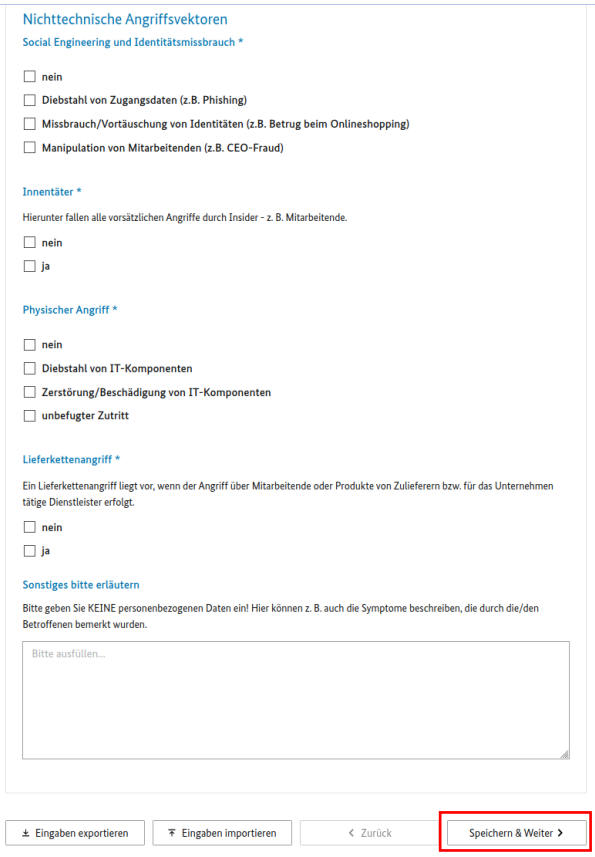
7a

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.



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

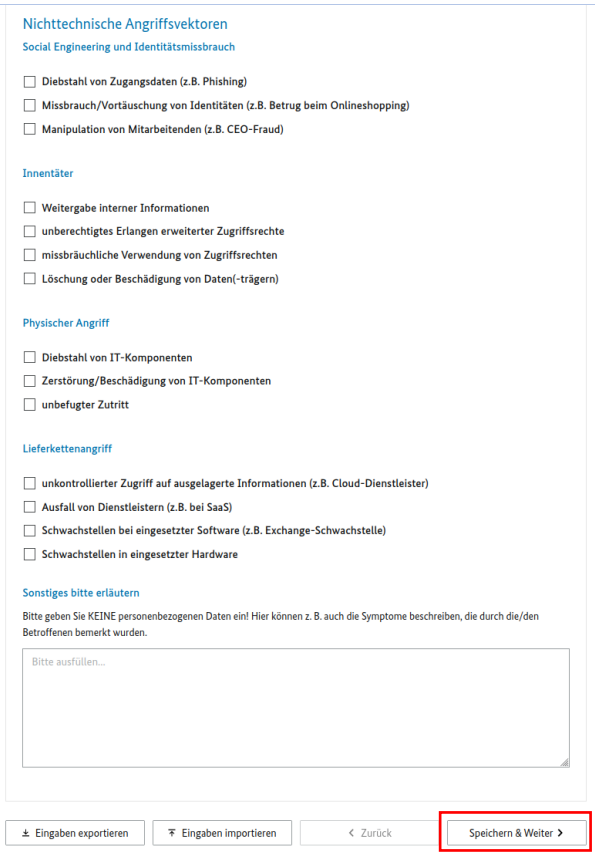
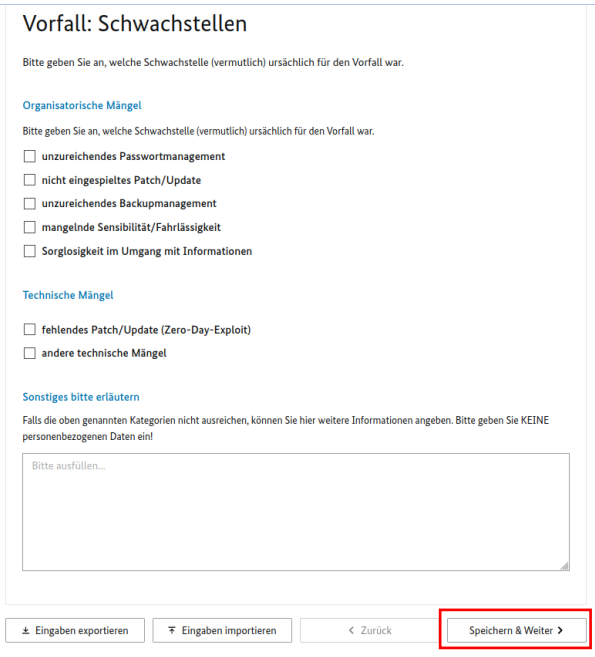


Klicken Sie auf **Speichern & Weiter**.

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.

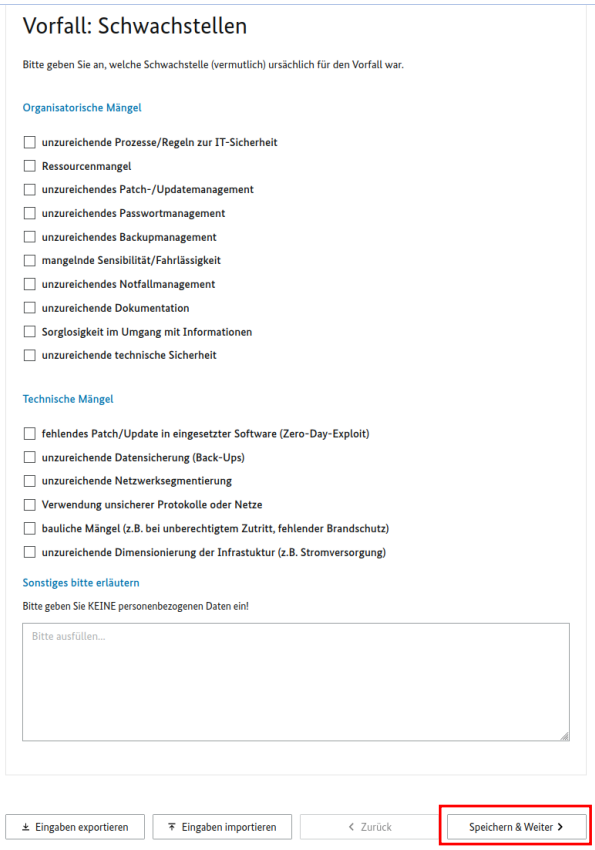
	Falls Sie darüberhinaus weitere Angaben machen möchten, nutzen Sie das Freitextfeld. Geben Sie KEINE personenbezogenen Daten an! Klicken Sie auf **Speichern & Weiter**.	
8a	*Diese Seite wird Ihnen nur angezeigt, wenn Sie auf der Startseite als Rolle Digitaler Ersthelfer und als Einstufung des Vorfalls 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! 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!



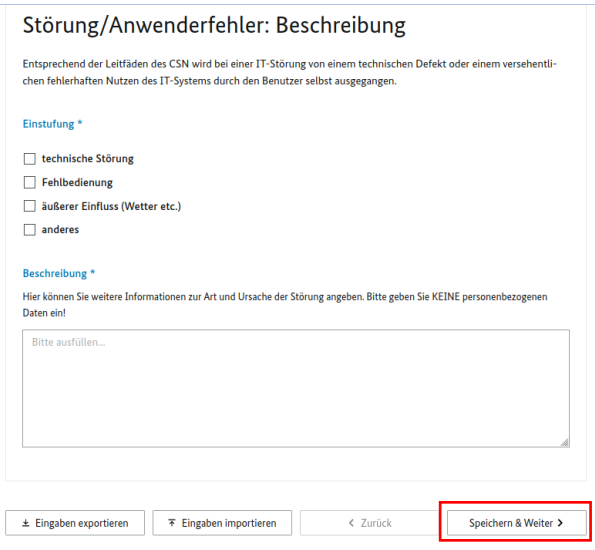
Klicken Sie auf **Speichern & Weiter**.

8c

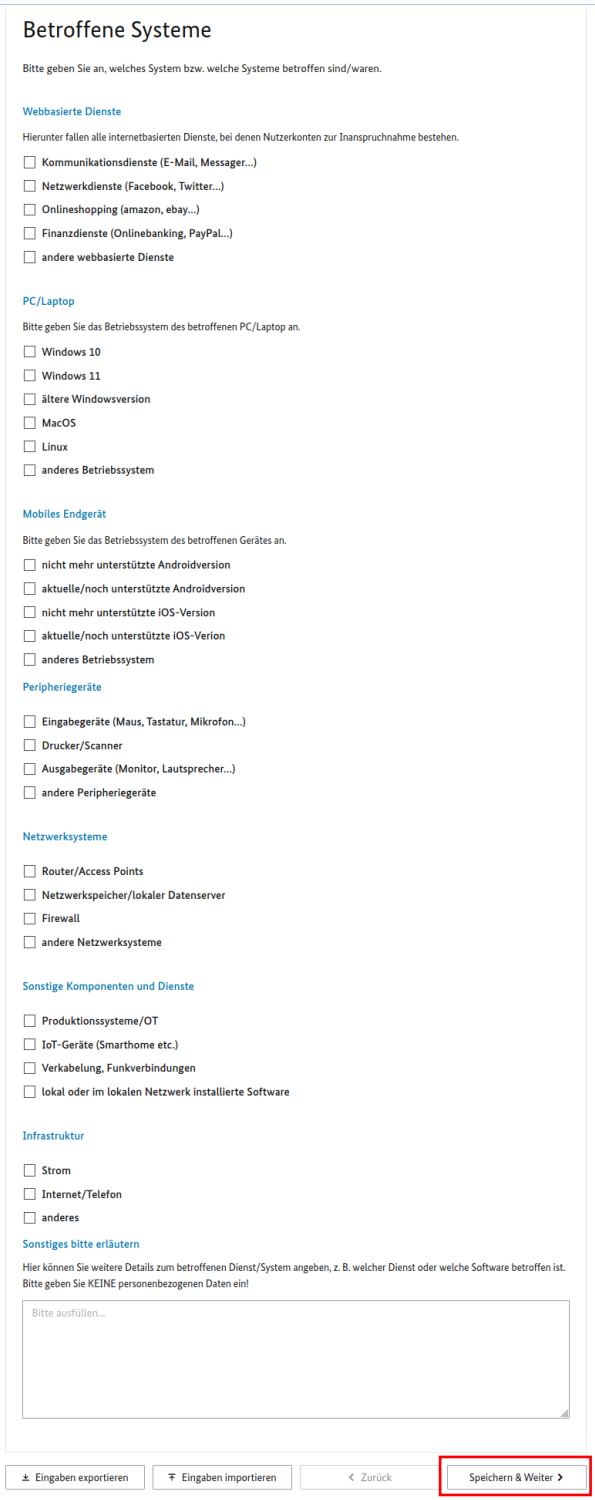
Diese Seite wird Ihnen nur angezeigt, wenn Sie auf der Startseite als Einstufung des Vorfalls Störung oder Fehlbedienung ausgewählt haben.

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**.

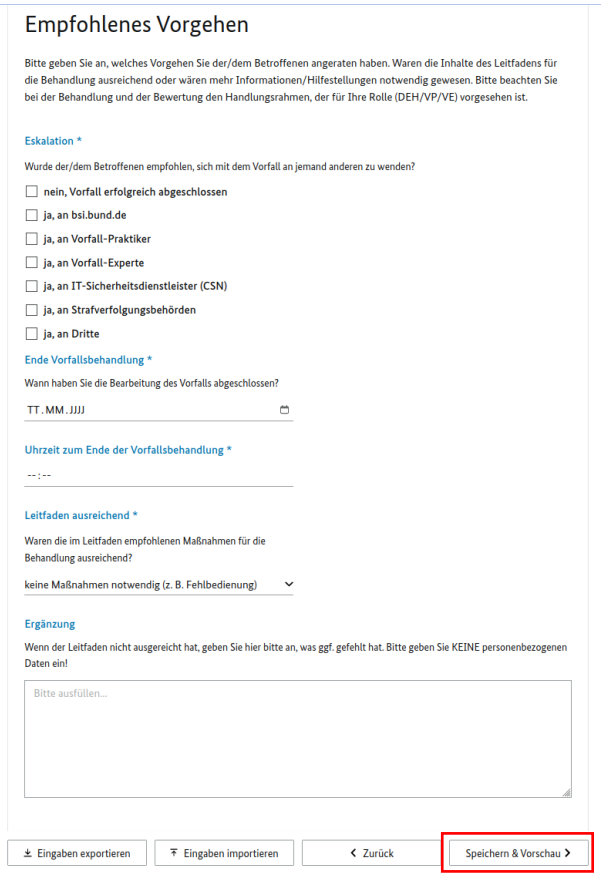
9	Bitte wählen Sie aus, welche Systeme/Dienste von dem Vorfall bzw. der Störung betroffen sind. Insbesondere bei Störungen können Sie im Freitextfeld weitere Details angeben, z. B. welche Art Kabel defekt war. Bitte geben Sie KEINE personenbezogenen Daten an! Klicken Sie auf **Speichern & Weiter**.	

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.

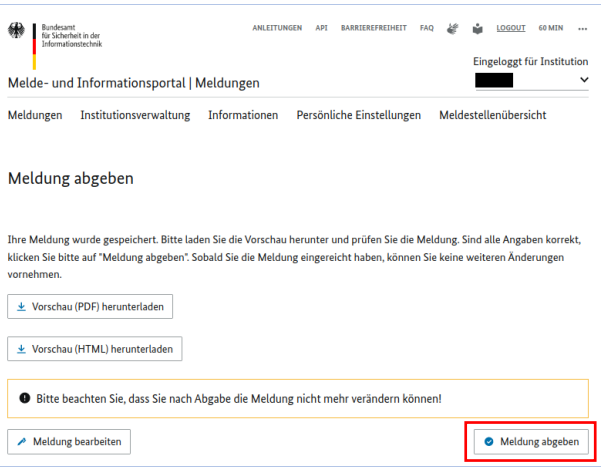
Anschließend geben Sie an, ob der Ihnen vorliegende Leitfaden für die Behandlung des Vorfalls im Rahmen Ihrer Rollen ausreichend war. Sollten Sie Ergänzungen haben, geben Sie diese bitte im Freitextfeld an. Bitte geben Sie KEINE personenbezogenen Daten ein!

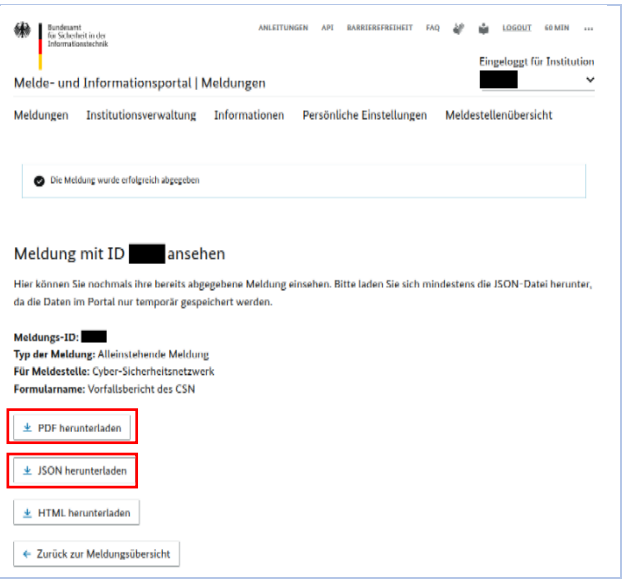
Klicken Sie auf **Speichern & Vorschau**.



11

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



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.	

Links und Verweise

[1] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Qualifizierung/Digitaler_Ersthelfer/Digitaler_Ersthelfer_node.html

[2] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Onlinekurs/Module/Onlinekurs_node.html

[3] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Qualifizierung/Vorfall_Praktiker/Vorfall_Praktiker_node.html

[4] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Onlinekurs/Module/Onlinekurs_node.html

[5] 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

[6] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Qualifizierung/Vorfall_Experten/Vorfall_Experte_node.html

[7] 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

[8] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Qualifizierung/Sicherheitsdienstleister/Sicherheitsdienstleister_node.html