Entwürfe der Benutzeroberfläche zur Meldung von Cyberangriffen

Die folgenden Abbildungen präsentieren vorläufige Entwürfe der Benutzeroberfläche für das geplante Kommunikationssystem im Falle von Cyberangriffen. Sie sollen den meldepflichtigen Behörden und Organisationen eine erste Orientierung bieten und die geplanten Meldeprozesse für Betreiber kritischer Infrastrukturen visualisieren.

Bitte beachten Sie, dass es sich bei diesen Entwürfen um vorläufige Konzepte handelt, die weder Gewähr für Genauigkeit noch für Vollständigkeit bieten. Die endgültige Ausgestaltung des Kommunikationssystems könnte basierend auf den Erkenntnissen während der Entwicklungsphase oder Rückmeldungen aus dem Konsultationsprozess signifikant von diesen ersten Entwürfen abweichen.

Zur Veranschaulichung zeigen wir das Meldeformular in drei Zuständen: leer, teilweise ausgefüllt mit einem Beispielvorfall „Angriff auf die Verfügbarkeit (DoS/DDoS)“ und vollständig ausgefüllt für einen „Datenabfluss (Data Leak)“. Diese Beispiele sind rein illustrativ und frei erfunden.

Weiter zu den Entwürfen

Die Auswahlmöglichkeiten der jeweiligen Auswahllisten haben wir zur Veranschaulichung auf einer separaten Seite dargestellt.

Weiter zu den Auswahllisten

Zurück

Cyberangriff melden

Deutsch

Für sofortige Unterstützung zu einem Cyberangriff, nutzen Sie bitte die Notfallkontakte

Gemäss Art. 74e des Informationsschutzgesetzes ISG vom 29. September 2023 (SR 128) haben meldepflichtige Organisationen und Behörden, ab der Entdeckung eines Cyberangriffs, eine Frist von 24 Stunden, um den Angriff dem Bundesamt für Cybersicherheit BACS zu melden.
Gemäss Art. 21 der Verordnung über die Cybersicherheit (SR 120.73) besteht eine weitere Frist von 14 Tagen, um die Meldung zu vervollständigen.

So lange Sie die Auswahl "Diese Meldung ist vollständig" am Ende dieser Seite nicht auswählen, können Sie die Meldung beliebig oft ergänzen und erneut absenden und damit speichern.
Nach dem Absenden, finden Sie Ihre Meldung in Ihrem Benutzerkonto wieder.

Datum und Uhrzeit der Feststellung des Angriffs

dd.mm .jjjj hh:mm

Dauert der Angriff noch an oder ist er abgeschlossen?

☐ Der Angriff dauert an

Datum und Uhrzeit des Angriffszeitpunkts

dd.mm .jjjj hh:mm

☐ Dieser Zeitpunkt ist unbekannt

Art des Angriffs

Art des Angriffs auswählen, mehrere Auswahlen sind möglich

Angriffsmethoden

Angriffsmethode auswählen, mehrere Auswahlen sind möglich

Angaben zum Verursacher

Angaben zum Verursacher

500

Welches Motiv kann dem Angriff zu Grunde liegen?

Motiv auswählen, eine Auswahl ist möglich

Zusätzliche Informationen zum Motiv

500

Wurde auf Grund dieses Angriffs Strafanzeige erstattet?

☐ Strafanzeige wurde erstattet

Welche Organisationseinheiten sind von dem Angriff betroffen?

Listen Sie hier die betroffenen Organisationseinheiten auf

500

Wie wirkt sich der Cyberangriff auf die **Funktionsfähigkeit** der betroffenen Organisationseinheiten aus?

Beschreiben Sie die Auswirkungen auf die Funktionsfähigkeit der Organisationseinheiten

1000

Wie schwer ist die **Verfügbarkeit** der Informationen und/oder Systeme **Ihrer Organisation** durch den Angriff beeinträchtigt?

Schweregrad auswählen

Wie schwer ist die **Integrität** der Informationen **Ihrer Organisation** durch den Angriff beeinträchtigt?

Schweregrad auswählen

Wie schwer ist die **Vertraulichkeit** der Informationen **Ihrer Organisation** durch den Angriff beeinträchtigt?

Schweregrad auswählen

Wie schwer ist die **Verfügbarkeit** der Informationen und/oder Systeme **Dritter** durch den Angriff beeinträchtigt?

Schweregrad auswählen

Wie schwer ist die **Integrität** der Informationen **Dritter** durch den Angriff beeinträchtigt?

Schweregrad auswählen

Wie schwer ist die **Vertraulichkeit** der Informationen **Dritter** durch den Angriff beeinträchtigt?

Schweregrad auswählen

Welche Massnahmen hat Ihre Organisation **getroffen**, um dem Angriff entgegen zu wirken?

Listen Sie die Massnahmen auf, welche Ihre Organisation bereits getroffen hat, um dem Angriff entgegen zu wirken

1000

Welche Massnahmen sind in Ihrer Organisation **geplant**, um dem Angriff entgegen zu wirken?

Listen Sie die Massnahmen auf, welche Ihre Organisation noch umsetzten wird, um dem Angriff entgegen zu wirken

1000

Kontaktperson für technische Rückfragen

Sie können uns freiwillige Angaben zu einer Kontaktperson für technische Rückfragen geben. Diese Angaben helfen uns, Ihre Meldung effizienter zu bearbeiten.

☐ Ich bin Ihre Kontaktperson

Vorname Vorname

Nachname Nachname

E-Mail max.mustermann@domain.com

Telefon +41 58 123 45 67

Ich beantrage **technische Unterstützung** des Bundesamts für Cybersicherheit für die Bewältigung des Angriffs

Gemäss Art. 74a des Informationsschutzgesetzes ISG vom 29. September 2023 (SR 128) haben Organisationen und Behörden, welche dem BACS einen Cyberangriff melden, Anspruch auf Unterstützung bei der Bewältigung des Angriffs.

Den **Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB)** über diese Meldung informieren

Wählen sie diese Option an, wenn der Vorfall eine Verletzungen der Datensicherheit nach Art. 24 des Bundesgesetzes über den Datenschutz (DSG; SR 235.1) betrifft und dementsprechend ein **hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt**. In diesem Fall füllen Sie bitte das Formular zu Meldung von Datensicherheitsverletzungen aus. Sollten Sie das Formular bereits ausgefüllt haben, tragen Sie bitte nachfolgend die Report-ID ein.

Die **Eidgenössische Finanzmarktaufsicht FINMA** über diese Meldung informieren

Wählen sie diese Option an, sofern Sie durch die FINMA reguliert sind.
Mit der Übermittlung der Meldung an die FINMA kann die **Pflicht zur unverzüglichen Meldung eines Cyberangriffs innerhalb von 24h** erfüllt werden.
Bitte beachten Sie, dass Sie weiterhin innerhalb von **72 Stunden** ein vollständig ausgefülltes Formular auf der webbasierten **Erhebungs- und Antragsplattform (EHP) direkt an die FINMA** übermitteln müssen.

Diese Meldung ist vollständig

So lange Sie die Auswahl "Diese Meldung ist vollständig" nicht auswählen, können Sie die Meldung beliebig oft ergänzen und erneut absenden.
Nachdem Sie die Option "Diese Meldung ist vollständig" auswählen und die Meldung absenden, kann die Meldung nicht mehr angepasst werden.

Nach dem Absenden, finden Sie Ihre Meldung in Ihrem Benutzerkonto wieder.

Das BACS wird über jede Meldung oder Änderung Ihrer Meldung informiert, unabhängig davon, ob die Meldung als vollständig bezeichnet ist.

Gemäss Art. 74e des Informationsschutzgesetzes ISG vom 29. September 2023 (SR 128) und Art. 21 der Verordnung über die Cybersicherheit (SR 120.73) haben meldepflichtige Organisationen und Behörden, ab der Entdeckung eines Cyberangriffs, eine Frist von 24 Stunden um den Angriff dem Bundesamt für Cybersicherheit BACS zu melden.
Gemäss Art. 21 der Verordnung über die Cybersicherheit (SR 120.73) besteht eine weitere Frist von 14 Tagen um die Meldung zu vervollständigen.

Senden

Zurück

Cyberangriff melden

Deutsch

Für sofortige Unterstützung zu einem Cyberangriff, nutzen Sie bitte die Notfallkontakte

Gemäss Art. 74e des Informationsschutzgesetzes ISG vom 29. September 2023 (SR 128) haben meldepflichtige Organisationen und Behörden, ab der Entdeckung eines Cyberangriffs, eine Frist von 24 Stunden, um den Angriff dem Bundesamt für Cybersicherheit BACS zu melden.
Gemäss Art. 21 der Verordnung über die Cybersicherheit (SR 120.73) besteht eine weitere Frist von 14 Tagen, um die Meldung zu vervollständigen.

So lange Sie die Auswahl "Diese Meldung ist vollständig" am Ende dieser Seite nicht auswählen, können Sie die Meldung beliebig oft ergänzen und erneut absenden und damit speichern.
Nach dem Absenden, finden Sie Ihre Meldung in Ihrem Benutzerkonto wieder.

Datum und Uhrzeit der Feststellung des Angriffs

15.04.2024 07:30

Dauert der Angriff noch an oder ist er abgeschlossen?

☑ Der Angriff dauert an

Datum und Uhrzeit des Angriffszeitpunkts

dd.mm .jjjj hh:mm

☐ Dieser Zeitpunkt ist unbekannt

Art des Angriffs

Angriff auf die Verfügbarkeit (DoS / DDoS)

Angriffsmethoden

Konfigurationsfehler

Angaben zum Verursacher

Bisher konnten wir IP-Adressen aus Osteuropa und Asien identifizieren. Genauere Informationen liegen noch nicht vor.

383

Welches Motiv kann dem Angriff zu Grunde liegen?

Das Motiv ist unbekannt

Zusätzliche Informationen zum Motiv

500

Wurde auf Grund dieses Angriffs Strafanzeige erstattet?

☐ Strafanzeige wurde erstattet

Welche Organisationseinheiten sind von dem Angriff betroffen?

Die Bereiche Produktion und Vertrieb sind betroffen.

448

Wie wirkt sich der Cyberangriff auf die **Funktionsfähigkeit** der betroffenen Organisationseinheiten aus?

Durch den Angriff sind alle Systeme für die Überwachung der Produktionsanlagen nicht mehr funktionsfähig. Dementsprechend wurde die Produktion und somit auch der Vertrieb eingestellt. Anderenfalls wäre die Personensicherheit nicht mehr gewährleistet.

753

Wie schwer ist die **Verfügbarkeit** der Informationen und/oder Systeme **Ihrer Organisation** durch den Angriff beeinträchtigt?

schwer beeinträchtigt

Wie schwer ist die **Integrität** der Informationen **Ihrer Organisation** durch den Angriff beeinträchtigt?

nicht beeinträchtigt

Wie schwer ist die **Vertraulichkeit** der Informationen **Ihrer Organisation** durch den Angriff beeinträchtigt?

nicht beeinträchtigt

Wie schwer ist die **Verfügbarkeit** der Informationen **Dritter** durch den Angriff beeinträchtigt?

mittelschwer beeinträchtigt

Wie schwer ist die **Verfügbarkeit** der Informationen und/oder Systeme **Dritter** durch den Angriff beeinträchtigt?

nicht beeinträchtigt

Wie schwer ist die **Vertraulichkeit** der Informationen **Dritter** durch den Angriff beeinträchtigt?

nicht beeinträchtigt

Welche Massnahmen hat Ihre Organisation **bereits getroffen**, um dem Angriff entgegen zu wirken?

Wie oben bereits erwähnt, haben wir die Produktion und den Vertreib stillgelegt, um Unfälle zu vermeiden. Wir haben die Firewalls neu gestartet, was keine Wirkung zeigte.

723

Welche Massnahmen sind in Ihrer Organisation **geplant**, um dem Angriff entgegen zu wirken?

Da der Angriff erst vor Kurzem begonnen hat, orientieren wir uns an unserem Business Continuity Management Plan.

887

Kontaktperson für technische Rückfragen

Sie können uns freiwillige Angaben zu einer Kontaktperson für technische Rückfragen geben. Diese Angaben helfen uns, Ihre Meldung effizienter zu bearbeiten.

☑ Ich bin Ihre Kontaktperson

Vorname: Vorname

Nachname: Nachname

E-Mail: max.mustermann@domain.com

Telefon: +41 58 123 45 67

Ich beantrage **technische Unterstützung** des Bundesamts für Cybersicherheit für die Bewältigung des Angriffs

Gemäss Art. 74a des Informationsschutzgesetzes ISG vom 29. September 2023 (SR 128) haben Organisationen und Behörden, welche dem BACS einen Cyberangriff melden, Anspruch auf Unterstützung bei der Bewältigung des Angriffs.

Den **Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB)** über diese Meldung informieren

Wählen sie diese Option an, wenn der Vorfall eine Verletzungen der Datensicherheit nach Art. 24 des Bundesgesetzes über den Datenschutz (DSG; SR 235.1) betrifft und dementsprechend ein **hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt**. In diesem Fall füllen Sie bitte das Formular zu Meldung von Datensicherheitsverletzungen aus. Sollten Sie das Formular bereits ausgefüllt haben, tragen Sie bitte nachfolgend die Report-ID ein.

Die **Eidgenössische Finanzmarktaufsicht FINMA** über diese Meldung informieren

Wählen sie diese Option an, sofern Sie durch die FINMA reguliert sind.
Mit der Übermittlung der Meldung an die FINMA kann die **Pflicht zur unverzüglichen Meldung eines Cyberangriffs innerhalb von 24h** erfüllt werden.
Bitte beachten Sie, dass Sie weiterhin innerhalb von **72 Stunden** ein vollständig ausgefülltes Formular auf der webbasierten **Erhebungs- und Antragsplattform (EHP) direkt an die FINMA** übermitteln müssen.

Diese Meldung ist vollständig

So lange Sie die Auswahl "Diese Meldung ist vollständig" nicht auswählen, können Sie die Meldung beliebig oft ergänzen und erneut absenden.
Nachdem Sie die Option "Diese Meldung ist vollständig" auswählen und die Meldung absenden, kann die Meldung nicht mehr angepasst werden.

Nach dem Absenden, finden Sie Ihre Meldung in Ihrem Benutzerkonto wieder.

Das BACS wird über jede Meldung oder Änderung Ihrer Meldung informiert, unabhängig davon, ob die Meldung als vollständig bezeichnet ist.

Gemäss Art. 74e des Informationsschutzgesetzes ISG vom 29. September 2023 (SR 128) und Art. 21 der Verordnung über die Cybersicherheit (SR 120.73) haben meldepflichtige Organisationen und Behörden, ab der Entdeckung eines Cyberangriffs, eine Frist von 24 Stunden um den Angriff dem Bundesamt für Cybersicherheit BACS zu melden.
Gemäss Art. 21 der Verordnung über die Cybersicherheit (SR 120.73) besteht eine weitere Frist von 14 Tagen um die Meldung zu vervollständigen.

Senden

‹ Zurück

Cyberangriff melden

Deutsch

Für sofortige Unterstützung zu einem Cyberangriff, nutzen Sie bitte die Notfallkontakte

Gemäss Art. 74e des Informationsschutzgesetzes ISG vom 29. September 2023 (SR 128) haben meldepflichtige Organisationen und Behörden, ab der Entdeckung eines Cyberangriffs, eine Frist von 24 Stunden, um den Angriff dem Bundesamt für Cybersicherheit BACS zu melden.
Gemäss Art. 21 der Verordnung über die Cybersicherheit (SR 120.73) besteht eine weitere Frist von 14 Tagen, um die Meldung zu vervollständigen.

So lange Sie die Auswahl "Diese Meldung ist vollständig" am Ende dieser Seite nicht auswählen, können Sie die Meldung beliebig oft ergänzen und erneut absenden und damit speichern.
Nach dem Absenden, finden Sie Ihre Meldung in Ihrem Benutzerkonto wieder.

Datum und Uhrzeit der Feststellung des Angriffs

15.04.2024 08h10

Dauert der Angriff noch an oder ist er abgeschlossen?

☐ Der Angriff dauert an

Datum und Uhrzeit des Angriffszeitpunkts

14.04.2024 17:34

☐ Dieser Zeitpunkt ist unbekannt

Art des Angriffs

Datenabfluss (Data leak)

Angriffsmethoden

Insiderwissen

Angaben zum Verursacher

Wir vermuten einen ehemaligen Mitarbeitenden hinter dem Datenklau.

433

Welches Motiv kann dem Angriff zu Grunde liegen?

Wirtschaftliches Interesse

Die abgezogenen Daten können im Dark Web verkauft werden.

442

Wurde auf Grund dieses Angriffs Strafanzeige erstattet?

☑ Strafanzeige wurde erstattet

Welche Organisationseinheiten sind von dem Angriff betroffen?

Unser Vertrieb kümmert sich darum, die betroffenen Kunden zu informieren, was viel Aufwand generiert. Unsere Kommunikation arbeitet mit ausgewählten Medien, um über den Angriff die Öffentlichkeit kontrolliert zu informieren.
Der Rest des Betriebs funktioniert normal.

232

Wie wirkt sich der Cyberangriff auf die **Funktionsfähigkeit** der betroffenen Organisationseinheiten aus?

Es entsteht Mehraufwand und situationsbedingter Stress für alle beteiligten. Ansonsten funktioniert der Betrieb normal.

880

Wie schwer ist die **Verfügbarkeit** der Informationen und/oder Systeme **Ihrer Organisation** durch den Angriff beeinträchtigt?

nicht beeinträchtigt

Wie schwer ist die **Integrität** der Informationen **Ihrer Organisation** durch den Angriff beeinträchtigt?

nicht beeinträchtigt

Wie schwer ist die **Vertraulichkeit** der Informationen **Ihrer Organisation** durch den Angriff beeinträchtigt?

schwer beeinträchtigt

Wie schwer ist die **Verfügbarkeit** der Informationen und/oder Systeme **Dritter** durch den Angriff beeinträchtigt?

nicht beeinträchtigt

Wie schwer ist die **Integrität** der Informationen **Dritter** durch den Angriff beeinträchtigt?

nicht beeinträchtigt

Wie schwer ist die **Vertraulichkeit** der Informationen **Dritter** durch den Angriff beeinträchtigt?

schwer beeinträchtigt

Welche Massnahmen hat Ihre Organisation **bereits getroffen**, um dem Angriff entgegen zu wirken?

Dem Angriff kann nicht mehr entgegen gewirkt werden. Die Daten sind unwiderruflich abgeflossen. Wir können nur noch versuchen zu verhindern, dass diese veröffentlich bzw. verkauft werden. Dafür wurde Strafanzeige erstattet.

776

Welche Massnahmen sind in Ihrer Organisation **geplant**, um dem Angriff entgegen zu wirken?

Wir werden den Prozess zur Löschung von Mitarbeiterkonten und -zugängen überprüfen und härten, sodass bei Beendigung eines Arbeitsverhältnisses unverzüglich alle Zugänge gesperrt werden können.

751

Kontaktperson für technische Rückfragen

Sie können uns freiwillige Angaben zu einer Kontaktperson für technische Rückfragen geben. Diese Angaben helfen uns, Ihre Meldung effizienter zu bearbeiten.

☐ Ich bin Ihre Kontaktperson

Vorname John

Nachname Doe

E-Mail j.doe@domain.com

Telefon +41 58 123 45 67

Ich beantrage **technische Unterstützung** des Bundesamts für Cybersicherheit für die Bewältigung des Angriffs

Gemäss Art. 74a des Informationsschutzgesetzes ISG vom 29. September 2023 (SR 128) haben Organisationen und Behörden, welche dem BACS einen Cyberangriff melden, Anspruch auf Unterstützung bei der Bewältigung des Angriffs.

Den **Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB)** über diese Meldung informieren

Report ID der Meldung einer Datenschutzverletzung: ABCD-1234-ABCD

Wählen sie diese Option an, wenn der Vorfall eine Verletzungen der Datensicherheit nach Art. 24 des Bundesgesetzes über den Datenschutz (DSG; SR 235.1) betrifft und dementsprechend ein **hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt**. In diesem Fall füllen Sie bitte das Formular zu Meldung von Datensicherheitsverletzungen aus. Sollten Sie das Formular bereits ausgefüllt haben, tragen Sie bitte nachfolgend die Report-ID ein.

Die **Eidgenössische Finanzmarktaufsicht FINMA** über diese Meldung informieren

E-Mailadresse des "Aufsichts-Key Account Manager (KAM)" c.asch@domain.com

Wählen sie diese Option an, sofern Sie durch die FINMA reguliert sind.
Mit der Übermittlung der Meldung an die FINMA kann die **Pflicht zur unverzüglichen Meldung eines Cyberangriffs innerhalb von 24h** erfüllt werden.
Bitte beachten Sie, dass Sie weiterhin innerhalb von **72 Stunden** ein vollständig ausgefülltes Formular auf der webbasierten **Erhebungs- und Antragsplattform (EHP) direkt an die FINMA** übermitteln müssen.

Diese Meldung ist vollständig

So lange Sie die Auswahl "Diese Meldung ist vollständig" nicht auswählen, können Sie die Meldung beliebig oft ergänzen und erneut absenden.
Nachdem Sie die Option "Diese Meldung ist vollständig" auswählen und die Meldung absenden, kann die Meldung nicht

Nach dem Abs

Das BACS wird

Meldung als vo

Gemäss Art. 74
Verordnung über
ab der Entdeckung eines Cy
Cybersicherheit BACS zu me
Gemäss Art. 21 der Verordnu
Tagen um die Meldung zu vervollständigen.

Sie sind dabei Ihre Meldung abzuschliessen. Wenn Sie die Meldung nun als vollständig abschliessen, können Sie diese später nicht mehr ergänzen. Wenn Sie Ihre Meldung später in der Frist von 14 Tagen ergänzen möchten, deaktivieren Sie bitte die Auswahl "Diese Meldung ist vollständig".

Wollen Sie Ihre Meldung abschliessend und endgültig einreichen?

Senden

Abbrechen

Senden

Auswahlmöglichkeiten pro Auswahlfeld

Art des Angriffs

Art des Angriffs auswählen, mehrfach Auswahlen sind möglich

- Angriff auf die Verfügbarkeit (DoS / DDoS)
- Unerlaubtes Eindringen in eine Datenverarbeitungsanlage (Hacking)
- Schadsoftware allgemein (Malware)
- Im spezifischen Verschlüsselungs- oder Erpressungssoftware (Ransomware)
- Datenabfluss (Data leak)
- Abfluss von Zugangsdaten (Credential theft)
- Andere

Angriffsmethoden

Angriffsmethode auswählen, mehrfach Auswahlen sind möglich

- Ausnutzung einer Schwachstelle (Vulnerability Exploit)
- Abgeflossene Zugangsdaten (durch Brute force oder Spayed)
- Konfigurationsfehler
- Insiderwissen
- Social Engineering
- Abtrünnige Werbung (Rogue advertising)
- Unbekannt (bis zu diesem Zeitpunkt)
- Andere

Welches Motiv kann dem Angriff zu Grunde liegen?

Motiv auswählen, eine Auswahl ist möglich

- Drohung
- Erpressung
- Nötigung
- Der Angriff ist politisch motiviert
- Wirtschaftliches Interesse
- Das Motiv ist unbekannt

Die folgenden 6 Fragen haben alle dieselben Auswahlmöglichkeiten:

Wie schwer ist die **Verfügbarkeit** der Informationen und/oder Systeme **Ihrer Organisation** durch den Angriff beeinträchtigt?

Wie schwer ist die **Integrität** der Informationen **Ihrer Organisation** durch den Angriff beeinträchtigt?

Wie schwer ist die **Vertraulichkeit** der Informationen **Ihrer Organisation** durch den Angriff beeinträchtigt?

Wie schwer ist die **Verfügbarkeit** der Informationen und/oder Systeme **Dritter** durch den Angriff beeinträchtigt?

Wie schwer ist die **Integrität** der Informationen **Dritter** durch den Angriff beeinträchtigt?

Wie schwer ist die **Vertraulichkeit** der Informationen **Dritter** durch den Angriff beeinträchtigt?

Schweregrad auswählen

- nicht beeinträchtigt
- leicht beeinträchtigt
- mittelschwer beeinträchtigt
- schwer beeinträchtigt

Zurück zu den Entwürfen