Ébauches de l'interface utilisateur pour l'annonce de cyberattaques

Les illustrations suivantes présentent des ébauches provisoires de l'interface utilisateur pour le système de communication prévu en cas de cyberattaques. Elles ont pour but de fournir une première orientation aux autorités et organisations soumises à l'obligation d'annonce et de visualiser les processus y relatifs pour les exploitants d'infrastructures critiques.

Veuillez noter que ces ébauches sont des concepts provisoires qui ne garantissent ni l'exactitude, ni l'exhaustivité. La configuration finale du système de communication pourrait s'écarter de manière significative de ces premières ébauches en fonction des connaissances acquises pendant la phase de développement ou des retours suite au processus de consultation.

A titre d'illustration, nous présentons le formulaire de notification dans trois états : vide, partiellement rempli avec un exemple d'incident « attaque par déni de service (DoS/DDoS) » et entièrement rempli pour une « fuite de données (Data Leak) ». Ces exemples sont purement illustratifs et inventés de toutes pièces.

Continuer vers les ébauches

Nous avons présenté les possibilités de choix pour chaque liste de sélection sur une page séparée à des fins des ébauches.

Continuer vers les listes de choix

< Retour

Annoncer une cyberattaque

Français

Pour une assistance immédiate en cas de cyberattaque, veuillez utiliser les contacts d'urgence.

Conformément à l'art. 74e de la loi sur la protection des informations LPI du 29 septembre 2023 (RS 128), les organisations et autorités soumises à l'obligation d'annoncer disposent d'un délai de 24 heures à compter de la découverte d'une cyberattaque pour la signaler à l'Office fédéral de la cybersécurité OFCS.
Conformément à l'art. 21 de l'ordonnance sur la cybersécurité (RS 120.73), un délai supplémentaire de 14 jours est accordé pour compléter l'annonce.

Tant que vous ne sélectionnez pas « Cette annonce est complète » en bas de cette page, vous pouvez compléter l'annonce aussi souvent que vous le souhaitez, la renvoyer et ainsi la sauvegarder.

Après l'envoi, vous retrouverez votre déclaration dans votre compte d'utilisateur.

Date et heure à laquelle l'attaque a été constatée

jj.mm.aaaa hh:mm

L'attaque se poursuit-elle ou est-elle terminée ?

☐ L'attaque se poursuit

Date et heure de l'attaque

jj.mm.aaaa hh:mm

☐ Cette date est inconnue

Type d'attque

Sélectionnez le type d'attaque, plusieurs choix sont possibles.

Méthodes d'attaques

Choisissez la méthode d'attaque, plusieurs choix sont possibles.

Informations sur le(s) responsa

Informations sur le(s) responsable(s)

500

Quel peut être le motif de l'attaque ?

Choisir le motif, un seul choix possible

Informations supplémentaires quant au motif

500

Une plainte a-t-elle été déposée à la suite de cette attaque ?

☐ Une plainte a été déposée

Quelles unités organisationnelles sont touchées par l'attaque ?

Listez les unités organisationnelles touchées

500

Quel est l'impact de la cyberattaque sur le **fonctionnement** des unités organisationnelles concernées ?

Décrivez l'impact sur le fonctionnement des unités organisationnelles

1000

À quel point cette attaque affecte-t-elle la **disponibilité** des informations et/ou des systèmes de **votre organisation** ?

Sélectionnez le degré de gravité

À quel point cette attaque affecte-t-elle l'**intégrité** des informations de **votre organisation** ?

Sélectionnez le degré de gravité

À quel point cette attaque affecte-t-elle la **confidentialité** des informations de **votre organisation** ?

Sélectionnez le degré de gravité

À quel point cette attaque affecte-t-elle la **disponibilité** des informations et/ou de systèmes **de tiers** ?

Sélectionnez le degré de gravité

À quel point cette attaque affecte-t-elle l' **intégrité** des informations **de tiers** ?

Sélectionnez le degré de gravité

À quel point cette attaque affecte-t-elle la **confidentialité** des informations **de tiers** ?

Sélectionnez le degré de gravité

Quelles mesures **ont été prises** par votre organisation pour lutter contre l'attaque ?

Listez les mesures que votre organisation a déjà prises pour lutter contre l'attaque

1000

Quelles mesures sont **prévues** dans votre organisation pour lutter contre l'attaque ?

Listez les mesures que votre organisation va encore mettre en œuvre pour lutter contre l'attaque.

1000

Personne de contact pour les questions techniques

Vous pouvez nous indiquer volontairement les coordonnées d'une personne de contact pour les questions techniques. Ces indications nous aident à traiter votre message plus efficacement.

☐ Je suis votre personne de contact

Prénom: Prénom

Nom de famille: Nom de famille

E-mail: jean.dupont@domain.com

Téléphone: +41 58 123 45 67

Je demande **l'assistance technique** de l'Office fédéral de la cybersécurité pour faire face à l'attaque

Conformément à l'art. 74a de la loi sur la protection des informations LPI du 29 septembre 2023 (RS 128), les organisations et les autorités qui signalent une cyberattaque à l'OFCS ont le droit de demander une assistance pour faire face à l'attaque.

Informer le **Préposé fédéral à la protection des données et à la transparence (PFPDT)** de cette annonce

Sélectionnez cette option si l'incident concerne une violation de la sécurité des données selon l'art. 24 de la loi fédérale sur la protection des données (LPD ; RS 235.1) et qu'il entraîne par conséquent un **risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée**. Dans ce cas, veuillez remplir le formulaire de notification de violation de la sécurité des données. Si vous avez déjà rempli le formulaire, veuillez indiquer l'ID de rapport ci-dessous.

Informer l'**Autorité fédérale de surveillance des marchés financiers FINMA** de cette annonce

Sélectionnez cette option si vous êtes réglementé par la FINMA.
La transmission de la déclaration à la FINMA permet de satisfaire à l'**obligation de déclarer immédiatement une cyberattaque dans les 24h**.
Veuillez noter que l'obligation de transmettre, dans un délai de **72 heures**, un formulaire dûment rempli via la **plate-forme de saisie et de demande (EHP) directement à la FINMA** subsiste.

Cette annonce est complète

Tant que vous ne sélectionnez pas l'option « Cette déclaration est complète », vous pouvez compléter et renvoyer l'annonce aussi souvent que vous le souhaitez.
Après avoir sélectionné l'option « Cette déclaration est complète » et envoyé la déclaration, celle-ci ne peut plus être modifiée.

Après l'envoi, vous retrouvez votre annonce dans votre compte d'utilisateur.

L'OFCS est informé de toute annonce ou modification de votre annonce, qu'elle soit ou non marquée comme étant complète.

Conformément à l'art. 74e de la loi sur la protection des informations LPI du 29 septembre 2023 (RS 128) et à l'art. 21 de l'ordonnance sur la cybersécurité (RS 120.73), les organisations et autorités soumises à l'obligation d'annoncer disposent d'un délai de 24 heures à compter de la découverte d'une cyberattaque pour la signaler à l'Office fédéral de la cybersécurité BACS.
Conformément à l'art. 21 de l'ordonnance sur la cybersécurité (RS 120.73), un délai supplémentaire de 14 jours est accordé pour compléter l'annonce.

Envoyer

< Retour

Annoncer une cyberattaque

Français

Pour une assistance immédiate en cas de cyberattaque, veuillez utiliser les contacts d'urgence.

Conformément à l'art. 74e de la loi sur la protection des informations LPI du 29 septembre 2023 (RS 128), les organisations et autorités soumises à l'obligation d'annoncer disposent d'un délai de 24 heures à compter de la découverte d'une cyberattaque pour la signaler à l'Office fédéral de la cybersécurité OFCS.
Conformément à l'art. 21 de l'ordonnance sur la cybersécurité (RS 120.73), un délai supplémentaire de 14 jours est accordé pour compléter l'annonce.

Tant que vous ne sélectionnez pas « Cette annonce est complète » en bas de cette page, vous pouvez compléter l'annonce aussi souvent que vous le souhaitez, la renvoyer et ainsi la sauvegarder.

Après l'envoi, vous retrouverez votre déclaration dans votre compte d'utilisateur.

Date et heure à laquelle l'attaque a été constatée

15.04.2024 07:30

L'attaque se poursuit-elle ou est-elle terminée ?

☑ L'attaque se poursuit

Date et heure de l'attaque

jj.mm.aaaa hh:mm

☐ Cette date est inconnue

Type d'attque

Attaque par déni de service (DoS / DDoS)

Méthodes d'attaques

Erreur de configuration

Informations sur le(s) responsable(s)

Jusqu'à présent, nous avons pu identifier des adresses IP d'Europe de l'Est et d'Asie. Nous ne disposons pas encore d'informations plus précises.

500

Quel peut être le motif de l'attaque ?

Le motif est inconnu

Informations supplémentaires quant au motif

500

Une plainte a-t-elle été déposée à la suite de cette attaque ?

☐ Une plainte a été déposée

Quelles unités organisationnelles sont touchées par l'attaque ?

Les secteurs de la production et de la distribution sont concernés.

432

Quel est l'impact de la cyberattaque sur le **fonctionnement** des unités organisationnelles concernées ?

Suite à l'attaque, tous les systèmes de surveillance des installations de production ne sont plus opérationnels. Par conséquent, la production et donc la distribution ont été arrêtées. A défaut, la sécurité des personnes n'aurait plus été garantie.

751

À quel point cette attaque affecte-t-elle la **disponibilité** des informations et/ou des systèmes de **votre organisation** ?

Gravement affecté

À quel point cette attaque affecte-t-elle l'**intégrité** des informations de **votre organisation** ?

Pas affecté

À quel point cette attaque affecte-t-elle la **confidentialité** des informations de **votre organisation** ?

Pas affecté

À quel point cette attaque affecte-t-elle la **disponibilité** des informations et/ou de systèmes **de tiers** ?

Moyennement affecté

À quel point cette attaque affecte-t-elle l' **intégrité** des informations **de tiers** ?

Pas affecté

À quel point cette attaque affecte-t-elle la **confidentialité** des informations **de tiers** ?

Pas affecté

Quelles mesures **ont été prises** par votre organisation pour lutter contre l'attaque ?

Comme indiqué plus haut, nous avons arrêté la production et la distribution afin d'éviter tout accident. Nous avons redémarré les pare-feux, ce qui n'a eu aucun effet.

832

Quelles mesures sont **prévues** dans votre organisation pour lutter contre l'attaque ?

Comme l'attaque a commencé depuis peu, nous nous orientons vers notre plan de gestion de la continuité des activités.

1000

Personne de contact pour les questions techniques

Vous pouvez nous indiquer volontairement les coordonnées d'une personne de contact pour les questions techniques. Ces indications nous aident à traiter votre message plus efficacement.

☑ Je suis votre personne de contact

Prénom: Prénom

Nom de famille: Nom de famille

E-mail: jean.dupont@domain.com

Téléphone: +41 58 123 45 67

Je demande **l'assistance technique** de l'Office fédéral de la cybersécurité pour faire face à l'attaque

Conformément à l'art. 74a de la loi sur la protection des informations LPI du 29 septembre 2023 (RS 128), les organisations et les autorités qui signalent une cyberattaque à l'OFCS ont le droit de demander une assistance pour faire face à l'attaque.

Informer le **Préposé fédéral à la protection des données et à la transparence (PFPDT)** de cette annonce

Sélectionnez cette option si l'incident concerne une violation de la sécurité des données selon l'art. 24 de la loi fédérale sur la protection des données (LPD ; RS 235.1) et qu'il entraîne par conséquent un **risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée**. Dans ce cas, veuillez remplir le formulaire de notification de violation de la sécurité des données. Si vous avez déjà rempli le formulaire, veuillez indiquer l'ID de rapport ci-dessous.

Informer l'**Autorité fédérale de surveillance des marchés financiers FINMA** de cette annonce

Sélectionnez cette option si vous êtes réglementé par la FINMA.
La transmission de la déclaration à la FINMA permet de satisfaire à l'**obligation de déclarer immédiatement une cyberattaque dans les 24h**.
Veuillez noter que l'obligation de transmettre, dans un délai de **72 heures**, un formulaire dûment rempli via la **plate-forme de saisie et de demande (EHP) directement à la FINMA** subsiste.

Cette annonce est complète

Tant que vous ne sélectionnez pas l'option « Cette déclaration est complète », vous pouvez compléter et renvoyer l'annonce aussi souvent que vous le souhaitez.
Après avoir sélectionné l'option « Cette déclaration est complète » et envoyé la déclaration, celle-ci ne peut plus être modifiée.

Après l'envoi, vous retrouvez votre annonce dans votre compte d'utilisateur.

L'OFCS est informé de toute annonce ou modification de votre annonce, qu'elle soit ou non marquée comme étant complète.

Conformément à l'art. 74e de la loi sur la protection des informations LPI du 29 septembre 2023 (RS 128) et à l'art. 21 de l'ordonnance sur la cybersécurité (RS 120.73), les organisations et autorités soumises à l'obligation d'annoncer disposent d'un délai de 24 heures à compter de la découverte d'une cyberattaque pour la signaler à l'Office fédéral de la cybersécurité BACS.
Conformément à l'art. 21 de l'ordonnance sur la cybersécurité (RS 120.73), un délai supplémentaire de 14 jours est accordé pour compléter l'annonce.

Envoyer

< Retour

Annoncer une cyberattaque

Français

Pour une assistance immédiate en cas de cyberattaque, veuillez utiliser les contacts d'urgence.

Conformément à l'art. 74e de la loi sur la protection des informations LPI du 29 septembre 2023 (RS 128), les organisations et autorités soumises à l'obligation d'annoncer disposent d'un délai de 24 heures à compter de la découverte d'une cyberattaque pour la signaler à l'Office fédéral de la cybersécurité OFCS.
Conformément à l'art. 21 de l'ordonnance sur la cybersécurité (RS 120.73), un délai supplémentaire de 14 jours est accordé pour compléter l'annonce.

Tant que vous ne sélectionnez pas « Cette annonce est complète » en bas de cette page, vous pouvez compléter l'annonce aussi souvent que vous le souhaitez, la renvoyer et ainsi la sauvegarder.

Après l'envoi, vous retrouverez votre déclaration dans votre compte d'utilisateur.

Date et heure à laquelle l'attaque a été constatée

15.04.2024 08h10

L'attaque se poursuit-elle ou est-elle terminée ?

☐ L'attaque se poursuit

Date et heure de l'attaque

14.04.2024 17:34

☐ Cette date est inconnue

Type d'attque

Fuite de données (data leak)

Méthodes d'attaques

Délit d'initié

Informations sur le(s) responsable(s)

Nous soupçonnons un ancien collaborateur d'être à l'origine du vol de données.

421

Quel peut être le motif de l'attaque ?

Intérêt financier ou économique

Les données détournées peuvent être vendues sur le Dark Web.

439

Une plainte a-t-elle été déposée à la suite de cette attaque ?

☑ Une plainte a été déposée

Quelles unités organisationnelles sont touchées par l'attaque ?

Notre service commercial s'occupe d'informer les clients concernés, ce qui génère beaucoup de travail. Notre communication travaille avec des médias sélectionnés afin d'informer le public de l'attaque de manière contrôlée.
Le reste des activités fonctionne normalement.

229

Quel est l'impact de la cyberattaque sur le **fonctionnement** des unités organisationnelles concernées ?

Il en résulte un surplus de travail et du stress lié à la situation pour toutes les personnes concernées. Pour le reste, l'exploitation fonctionne normalement.

839

À quel point cette attaque affecte-t-elle la **disponibilité** des informations et/ou des systèmes de **votre organisation** ?

Pas affecté

À quel point cette attaque affecte-t-elle l'**intégrité** des informations de **votre organisation** ?

Pas affecté

À quel point cette attaque affecte-t-elle la **confidentialité** des informations de **votre organisation** ?

Gravement affecté

À quel point cette attaque affecte-t-elle la **disponibilité** des informations et/ou de systèmes **de tiers** ?

Pas affecté

À quel point cette attaque affecte-t-elle l' **intégrité** des informations **de tiers** ?

Pas affecté

À quel point cette attaque affecte-t-elle la **confidentialité** des informations **de tiers** ?

Gravement affecté

Quelles mesures **ont été prises** par votre organisation pour lutter contre l'attaque ?

On ne peut plus lutter contre l'attaque. Les données sont irrémédiablement perdues. Nous ne pouvons plus qu'essayer d'empêcher leur publication ou leur vente. Une plainte pénale a été déposée à cet effet.

795

Quelles mesures sont **prévues** dans votre organisation pour lutter contre l'attaque ?

Nous allons revoir et renforcer le processus de suppression des comptes et des accès des employés afin que tous les accès puissent être immédiatement bloqués à la fin d'une relation de travail.

806

Personne de contact pour les questions techniques

Vous pouvez nous indiquer volontairement les coordonnées d'une personne de contact pour les questions techniques. Ces indications nous aident à traiter votre message plus efficacement.

☐ Je suis votre personne de contact

Prénom: John
Nom de famille: Doe
E-mail: j.doe@domain.com
Téléphone: +41 58 123 45 67

Je demande l'**assistance technique** de l'Office fédéral de la cybersécurité pour faire face à l'attaque

Conformément à l'art. 74a de la loi sur la protection des informations LPI du 29 septembre 2023 (RS 128), les organisations et les autorités qui signalent une cyberattaque à l'OFCS ont le droit de demander une assistance pour faire face à l'attaque.

Informer le **Préposé fédéral à la protection des données et à la transparence (PFPDT)** de cette annonce

ID du rapport violation de la sécurité des données: ABCD-1234-ABCD

Sélectionnez cette option si l'incident concerne une violation de la sécurité des données selon l'art. 24 de la loi fédérale sur la protection des données (LPD ; RS 235.1) et qu'il entraîne par conséquent un **risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée**. Dans ce cas, veuillez remplir le formulaire de notification de violation de la sécurité des données. Si vous avez déjà rempli le formulaire, veuillez indiquer l'ID de rapport ci-dessus.

Informer l'**Autorité fédérale de surveillance des marchés financiers FINMA** de cette annonce

Adresse e-mail du "Gestionnaire superviseur d'acompte clé (KAM)": c.asch@domain.com

Sélectionnez cette option si vous êtes réglementé par la FINMA.
La transmission de la déclaration à la FINMA permet de satisfaire à l'**obligation de déclarer immédiatement une cyberattaque dans les 24h**.
Veuillez noter que l'obligation de transmettre, dans un délai de **72 heures**, un formulaire dûment rempli via la **plate-forme de saisie et de demande (EHP) directement à la FINMA** subsiste.

Cette annonce est complète

Tant que vous ne sélectionnez pas l'option « Cette déclaration est complète », vous pouvez compléter et renvoyer l'annonce aussi souvent que vous le souhaitez.
Après avoir sélec… 'e-ci ne peut plus être mo…

Après l'envoi, vou…

L'OFCS est inform… …uée comme étant con…

Vous êtes sur le point de clôturer votre annonce. Si vous indiquez votre annonce comme étant complète, vous ne pourrez plus la compléter ultérieurement. Si vous souhaitez compléter votre annonce dans le délai de 14 jours, décochez la case « Cette annonce est complète ».

Souhaitez-vous clôturer votre annonce et l'envoyer de manière définitive ?

Envoyer | Annuler

Conformément à l'… …(RS 128) et à l'art. 21 de l'ordonnance sur la cybersécurité (RS 120.73), les organisations et autorités soumises à l'obligation d'annoncer disposent d'un délai de 24 heures à … découverte d'une cyberattaque pour la signaler à l'Office fédéral de la cybersécurité BACS.
Conformément à l'art. 21 de l'ordonnance sur la cybersécurité (RS 120.73), un délai supplémentaire de 14 jours est accordé pour compléter l'annonce.

Envoyer

Choix possibles par champ de sélection

Type d'attque

Sélectionnez le type d'attaque, plusieurs choix sont possibles.

- Attaque par déni de service (DoS / DDoS)
- Accès non autorisé à un système de traitement de données (hacking)
- Logiciel malveillant (malware)
- Logiciel de cryptage ou d'extorsion (ransomware).
- Fuite de données (data leak)
- Vol d'identifiants (credential theft)
- Autres

Méthodes d'attaques

Choisissez la méthode d'attaque, plusieurs choix sont possibles.

- Exploitation d'une vulnérabilité (vulnerability exploit)
- Vol d'identifiants (par force brute ou sprayed)
- Erreur de configuration
- Délit d'initié
- Ingénierie sociale
- Publicité mensongère (rogue advertising)
- Inconnues (jusqu'à ce moment)
- Autres

Quel peut être le motif de l'attaque ?

Choisir le motif, un seul choix possible

- Menace
- Chantage
- Contrainte
- Intérêt financier ou économique
- L'agression est motivée par des raisons politiques
- Le motif est inconnu

Les 6 questions suivantes comportent toutes les mêmes choix :

À quel point cette attaque affecte-t-elle la **disponibilité** des informations et/ou des systèmes de **votre organisation** ?

À quel point cette attaque affecte-t-elle l'**intégrité** des informations de **votre organisation** ?

À quel point cette attaque affecte-t-elle la **confidentialité** des informations de **votre organisation** ?

À quel point cette attaque affecte-t-elle la **disponibilité** des informations et/ou de systèmes **de tiers** ?

À quel point cette attaque affecte-t-elle l' **intégrité** des informations **de tiers** ?

À quel point cette attaque affecte-t-elle la **confidentialité** des informations **de tiers** ?

Sélectionnez le degré de gravité

- Pas affecté
- Légèrement affecté
- Moyennement affecté
- Gravement affecté

Retour vers vers les ébauches