



Fuite de données – que faire?

Mesures techniques

Du point de vue technique, **déterminez si les assaillants ont pu pénétrer dans vos systèmes** et, le cas échéant, comment ils y sont parvenus et ce qu'ils ont fait dans ceux-ci.

Il faut non seulement remédier aux failles et fermer les accès ouverts mais aussi **empêcher que les assaillants ne puissent procéder à d'autres attaques** en se servant d'une porte dérobée qu'ils ont installée.

Si les connaissances à ce sujet ne sont pas disponibles dans votre entreprise, l'OFCS vous recommande de mandater une **entreprise de sécurité informatique**.

Mesures organisationnelles

Vous devriez prendre quelques mesures avant même d'être victime d'une attaque. Elles pourront vous aider à maîtriser efficacement un tel incident le cas échéant.

- Établissez un **plan de communication**. Celui-ci détermine si et comment communiquer en cas d'attaque.
- Établissez un **plan de continuité d'activité**. Celui-ci décrit la façon dont vos collaborateurs pourront continuer à travailler si l'infrastructure informatique est indisponible pour une période plus ou moins longue.
- Si la fuite des données crainte se concrétise, l'OFCS recommande d'**informer les clients de façon proactive**. Vous leur donnerez ainsi la possibilité de prendre des mesures appropriées. Disposez d'une vue d'ensemble des données qui peuvent potentiellement être dérobées et du risque en lien avec la fuite de ces données (dommages de réputation par ex.). Ces informations devraient servir à prendre d'autres mesures proactives.
- Conformément à l'art. 24 de la nouvelle loi sur la protection des données qui a été en vigueur le 1er septembre 2023, les violations de la sécurité des données devront désormais être annoncées au Préposé fédéral à la protection des données et à la

transparence (PFPDT) si elles entraînent un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées par la fuite de données. Cette obligation d'annoncer est valable pour les particuliers, les entreprises et les organes fédéraux et doit être satisfaite dans les meilleurs délais. Vous trouverez le formulaire d'annonce ici:

<https://databreach.edoeb.admin.ch/report>

(<https://databreach.edoeb.admin.ch/report>)

(1)

- Déposez une **dénonciation pénale à la police cantonale** de votre siège. Celle-ci procédera aux investigations nécessaires. Vous trouverez sur le site <https://www.suisse-epolice.ch/#/search-station>

(<https://www.suisse-epolice.ch/#/search-station>)

(2) les postes de police proches de chez vous et leurs données de contact.

Informations sur le paiement des rançons

L'OFCS déconseille de payer une rançon. Il n'y a aucune garantie que les criminels ne publieront pas les données ou n'en tireront pas un autre profit après le paiement de la rançon. En outre, tout chantage qui réussit incite les assaillants à continuer, finance le développement des attaques et favorise leur propagation.

Si vous envisagez tout de même de payer une rançon, l'OFCS vous recommande instamment de discuter de ces opérations avec la police cantonale.

Dernière modification 01.01.2024

<https://www.ncsc.admin.ch/content/ncsc/fr/home/infos-fuer/infos-behoerden/vorfall-was-nun/datenabfluss.html>

Page Links

-
1. <https://databreach.edoeb.admin.ch/report>
 2. <https://www.suisse-epolice.ch/#/search-station>