Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'intérieur DFI
Office fédéral des assurances sociales OFAS

Liste de contrôle : comment réagir en cas de cyberincident

Date :	28.3.2025 / Mma
Domaine(s) :	Sécurité de l'information et protection des données dans le 1er pilier

Remarque : Il est impossible de définir de manière générale la marche à suivre concrète en cas de cyberattaque. Les mesures présentées ci-après ont pour but d'aider les organes d'exécution à accroître leur réactivité ; cette liste n'est toutefois pas exhaustive. La priorité à donner à ces mesures (ou à d'autres mesures éventuelles) doit être définie individuellement par chaque organe d'exécution.

1. **Garder son calme**
2. **Isoler les systèmes touchés** (les déconnecter du réseau, mais ne pas les arrêter)
3. **Interrompre la sauvegarde (backup)**
4. **Documenter l'incident**
   → Noter la date et l'heure, les systèmes touchés, les premières observations
5. **Informer les préposés à la sécurité de l'information et à la protection des données**
6. **Faire appel à des experts en sécurité informatique**
7. **Conserver des preuves** (procès-verbaux, captures d'écran, fichiers suspects)
8. **Informer l'OFAS et, le cas échéant, le PFPDT** au moyen du formulaire de communication de l'OFCS
   → dans un délai de 24 heures (https://security-hub.ncsc.admin.ch/)
9. **Informer les autres autorités compétentes** (police, autorité de surveillance cantonale)
10. **Informer les personnes concernées via des canaux appropriés** (collaborateurs, assurés)
11. **Si nécessaire, activer les plans d'urgence et s'assurer que le système a bien été restauré**
12. **Analyser les causes de l'incident**
    → Identifier les points faibles, améliorer les mesures de protection
13. **Établir un rapport de clôture**

Vous trouverez ce document sur
https://sozialversicherungen.admin.ch/fr/f/20762

Contact
Office fédéral des assurances sociales OFAS
IT Management
isms@bsv.admin.ch