CONSEIL SUPÉRIEUR DU NOTARIAT

Cyber-attaques

Les 15 points réflexes en cas de cyber-attaques

Fiche réflexes

Voici une conduite à tenir en 15 points, qui suppose une parfaite coordination entre les notaires et les collaborateurs de l'office.
Ces éléments complètent le Plan de Continuité d'Activité que vous avez peut-être déjà établi.

Dans le premier quart d'heure

1. **Isolez l'ordinateur** en débranchant les connectiques électriques et réseaux, filaire ou Wifi, de l'ordinateur identifié pour l'extraire du système informatique et éviter toute propagation.
2. **Alertez immédiatement par oral, en interne à l'étude,** les autres notaires et collaborateurs, et isoler de la même manière les postes menacés.

Dans la première demi-heure

3. **Alertez votre Centre de services bancaires de la CDC**, assurez-vous de la coupure de tous les flux bancaires au débit de vos comptes, assurez-vous de l'état des soldes de comptes, et demandez le cas échéant le retour des fonds. Le dépôt de plainte pourra être exigé de la CDC pour récupérer les sommes. Il est probable que le gestionnaire bancaire, compte tenu du contexte, effectuera un contre-appel.
4. **Demandez à votre gestionnaire d'annuler tous les virements en instance jusqu'à nouvel ordre**, y compris ceux programmés à l'avance et demander l'inventaire afin d'identifier les virements frauduleux dans la période suspecte.
5. **Prévenez FIDELIA,** assistance MMA associée au contrat CYBER et en lien avec LSN.
6. **Fermez momentanément l'office** pour apprécier de manière optimale la situation et adopter la conduite qui s'impose.

Dans la première heure

7. **Recensez les événements inhabituels survenus avant et lors de l'intrusion** afin d'informer les autres utilisateurs de la faille et stopper la diffusion.
8. **Prévenez votre service ou prestataire informatique,** votre opérateur réseau et support assistance de l'ADSN en fonction des services ou matériels impactés.

Dans les trois premières heures

9. **Changez vos mots de passe** : session, messagerie, clef Real (à partir d'un ordinateur non infecté)
10. **Assurez-vous que votre sauvegarde** ne peut être touchée par l'intrusion.

Fiche réflexes

Dans la première journée

11. **Conservez les preuves de l'intrusion** : logiciel de prise en main, mail de sollicitation…
12. **Prévenez le Procureur** de la République.
13. **Déposez plainte** en vous appuyant sur le registre des interventions (essentiel à mettre en place au sein de l'office).
14. **Gérez la communication** interne et externe (clients et partenaires).

Dans les 48 heures

15. **Notifiez votre correspondant informatique et liberté ou la CNIL** si l'incident affecte des données personnelles.

CONTACTS

- **Mes contacts CSB – gestionnaire bancaire** *(à compléter par l'office)* :
  - Numéro de téléphone :
  - Mail du pôle de CSB :
- **ADSN assistance technique** : du lundi au vendredi de 8h30 à 21h sans interruption et le samedi de 8h30 à 13h par mail : hotline@adsn.fr ou au 0 800 306 212 Service & appel gratuits
- **FIDELIA Assistance** au **01 47 11 70 29** (joignable 24H/24 et 7J/7) en indiquant le numéro de contrat : 145 154 406 et le code protocole : 100 381
- **CNIL :** https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

POUR EN SAVOIR PLUS @

- Le site CYBERMALVEILLANCE du Gouvernement :
  https://www.cybermalveillance.gouv.fr/
  https://www.cybermalveillance.gouv.fr/diagnostic/accueil
- Le site de l'ANSSI : https://www.ssi.gouv.fr

Cette fiche est à présenter à tous dans l'office et à conserver à portée de mains, dans un endroit inaccessible au public mais connu de tous en interne