

# Comment réduire la menace ?

## Les 6 concepts de sécurisation

Ces 6 concepts, une fois la menace modélisée, permettent de la réduire. Les exemples concrets citent certaines des techniques utilisées par des membres d'Extinction Rebellion pour par exemple sécuriser les coordinations d'action.

### 1. Minimisation de la menace

**En une phrase : Réduire la surface d'attaque.**

- Réduire la surface d'attaque, c'est-à-dire diminuer le nombre d'accès (nombre d'outils, le nombre de personnes au courant) qui pourraient être des points d'entrée compromettant la sécurité.
- Collecter QUE ce qui est nécessaire, en effet ce qui n'est pas collecté ne peut pas être récupéré.
- Image pour une maison: Ne pas donner les clefs à tout le monde et avoir qu'une seule porte d'entrée. (vs. avoir une maison avec plein de baies vitrées)

**Exemples concrets :**

- Rappel "Merci de supprimer ce message après consultation" dans un mail ou message
- Utiliser les messages éphémères dans les messageries sécurisées, afin qu'ils soient automatiquement supprimés après un certain temps.
- Dans un coordination d'action, communiquer avec l'extérieur avec un seul compte (Mattermost, Protonmail) commun à l'ensemble de la coordination.
- Dans un brief d'action, partager seulement les informations utiles aux participant.es.  
Astuce: Si on souhaite cacher des éléments (exemple cible) lire le brief, messages envoyés à quelqu'un.e ne connaissant pas l'action et lui demander de deviner ces informations sensibles
- Ne pas partager d'information sur une action aux personnes qui n'en ont pas besoin (famille, ami.e, conjoint.e)
- Dans un débrief d'action, rappeler de ne pas partager les pseudos des auteurs d'acte juridiquement répréhensible.

- Juste avant et après une action, détruire les documents, données qui ne sont plus nécessaires.
- Juste avant et après une action, changer les mots de passe et une seule personne a les nouveaux
- Juste avant et après une action, stocker le matériel sensible (ordinateurs, téléphones) en dehors des lieux de résidence des membres de la coordination pour réduire l'impact d'une perquisition.
- Formulaire ne collectant que les informations nécessaires, par exemple le prénom / pseudo mais pas la Civilité / Prénom / Nom de famille.
- Restreindre les accès aux documents/échanges de la coordination aux membres actifs.ves
- Utiliser les messages éphémères dans les messageries sécurisées, afin qu'ils soient automatiquement supprimés après un certain temps. Sur Signal pensez à mettre ce paramètre par défaut !
- Stocker les documents sensibles uniquement sur le cryptpad de l'équipe.
- Supprimer et copier à l'identique les documents du cryptpad pour supprimer l'historique et les noms des personnes ayant fait les modifications
- Quand on contacte des groupes de supports (GST), faire en sorte d'inclure le moins de gens possibles.
- Se passer du numérique pour les sujets plus sensibles.

## 2. Compartimentation (sectorisation) de la menace

### En une phrase : Répartir le secret.

- Ne pas donner toutes les informations à tout le monde afin de diminuer les impacts d'une compromission.
- Cloisonner la détention d'une information cloisonne le risque de sa compromission  
→ Ex : Avoir un mot de passe différent par compte. La compromission d'un mdp ne compromet pas les autres comptes.
- Tracer des frontières et définir les différents périmètres de chaque groupe (cercles de confiance, groupe de travail).  
→ établir un schéma organisationnel  
→ si grand groupe avec beaucoup d'infos : DANGER
- Concept du "droit à connaître": si je n'ai pas besoin d'une information sensible, je ne devrais pas la connaître, ni chercher à la connaître.
- Image pour une maison: une clé différente pour chaque chambre.

### Exemples concrets :

- Toute les membres de la coordination d'une action n'ont pas forcément besoin de connaître la cible, le mode d'action ou d'avoir accès à la liste des participantes.

- La coordination qui a une vue d'ensemble, les référent.e.s de groupe qui ont des informations nécessaires pour gérer leur groupe mais parcellaires, les simples participantes qui ont seulement les informations nécessaires à leur rôle.
- Mettre les militant.e.s les plus sûr.e.s sur les rôles clés.
- Utiliser des mots de passe différents.

## 3. Confiance

**En une phrase : S'assurer de fiabilité d'un outil, entité ou personne. La confiance est contextuelle.**

- S'assurer de la fiabilité des outils et des militant.e.s.
  - Pour les outils ça peut se traduire par la réputation de l'outil ou le fait qu'il soit open-source par exemple.
  - Pour un.e militant.e, souvent c'est le passé et les relations avec qu'il faut prendre en compte.
- Fiabilité des outils, des machines, hébergeurs/entités qu'on utilise. Est-ce que j'accorde la confiance à tel ou telle camarade ?
- La confiance est contextuelle, pour un moment précis ou un usage précis.
- Transitivité de la confiance, chaîne de confiance => Si A fait confiance à B, que B fait confiance à C alors B peut faire confiance à C.
- Confiance, confiance qui vient du passé. Les échos du passé font que j'ai une certaine confiance.
- La confiance n'exclut pas le contrôle. Boucle de rétroaction pour contrôler que tout se passe bien.
- Image pour une maison: Laisser rentrer une amie mais pas un.e inconnu.e

**Exemples concrets :**

- Recrutement de participant.e.s par le système de cooptation.
- Prendre en compte l'historique d'un.e militant.e pour juger son niveau de confiance: est-ce que cette personne est active dans le mouvement ? A-t-elle participé à des actions dans le passé ? etc...
- Se poser la question, ai-je assez confiance en mon ami.e pour parler des mes actions de DNCV ?
- Utiliser des logiciels libres réputés dans lesquels on a confiance.

## 4. Confidentialité

**En une phrase : S'assurer que l'information n'est accessible qu'aux personnes que l'on souhaite.**

- Ne donner certaines informations seulement à des personnes souhaitées.
- Obfuscation (cacher des infos dans d'autres infos)

- Chiffrement, cryptographie
- Image pour une maison: avoir une haie qui cache des regards indiscrets des voisin.es, passant.es.

## Exemples concrets :

- Noms de code pour parler des éléments principaux (lieux) de l'action.
- Filtres de confidentialité sur ordinateur/téléphone pour se protéger des regards indiscrets
- Utilisation des protocoles numériques sécurisées: HTTPS, VPN, Tor.
- Porter un masque, combinaison pour cacher son identité.
- Avoir une validation par l'admin pour l'ajout à une boucle Signal par le lien d'invitation.
- Avoir ses téléphones et ordinateurs cryptés + mot de passe long et fort + éteints lors moments sensibles
- Pseudo temporaire (exemple le jour de l'action) pour réduire l'impact d'une arrestation avec téléphone pas propre.
- Utiliser une adresse email protonmail pour communiquer avec rebelles car entre les adresses emails protonmail les emails sont cryptés.
- Faire le brief des rôles risqués à de manière discrète.
- Ne pas donner les rôles de chacun.e à voix haute à l'ensemble du groupe.

## 5. Intégrité

**En une phrase : S'assurer que l'information reçue correspond à l'information envoyée. Vérifier la véracité de l'information.**

- Vérifier la véracité des informations, que celles-ci ne soient pas altérées.
- Faire une double / triple vérification.
- Avoir des sources multiples.
- S'assurer que l'information reçue soit bien l'information envoyée. Information interceptée ? Information dégradée lors de la transmission ?
- Image pour une maison: vérifier qu'une lettre de sa banque vient bien de sa banque en l'appelant.

## Exemples concrets :

- Est-ce que quelqu'un.e a modifié le CR depuis la réunion ?
- Vérifier qu'un repérage via maps soit conforme à la réalité en allant sur place.

## 6. Authentification

**En une phrase : Garantir l'origine des informations dans nos échanges.**

- S'assurer que la personne est bien celle qu'elle prétend être.
- Garantir l'origine des informations (identité, etc.) dans nos échanges / interactions.

- Mot de passe (qqch que je sais).
- 2FA (qqch que je sais + qqch que j'ai)
- 3FA (qqch que je sais + qqch que j'ai + qqch que je suis).
- Image pour une maison: être sûr de la personne qu'on a en face.

## Exemples concrets :

- Lors d'un brief d'action physique, vérifier les "identités" des personnes entrant dans la zone de brief grâce à une personne les connaissant.
- Lors d'un brief d'action digital, vérifier les "identités" des personnes entrant dans la zone de brief en demandant d'allumer leurs caméras au début.
- Authentification à deux facteurs sur les sites sensibles (email)
- Lors d'un premier échange par Signal, demander confirmation par Mattermost que la personne est bien celle qu'on croit.

---

Révision #1

Créé 8 septembre 2023 18:14:56 par mollusque

Mis à jour 23 février 2025 11:53:23 par mollusque