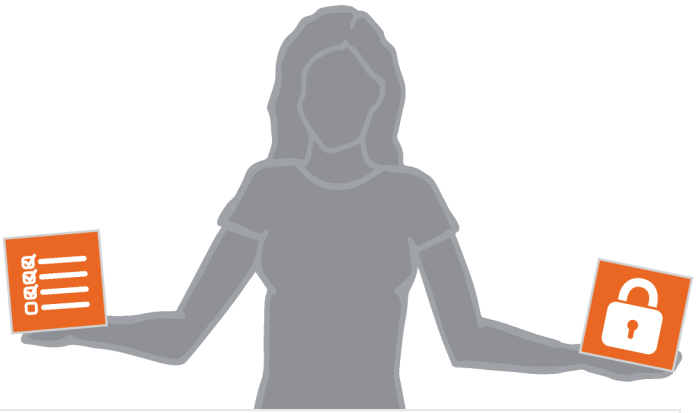
7. PRÉPARER UN PLAN DE SÉCURITÉ

> **CHAPITRE 1.7** NMP
PRÉPARER UN PLAN DE SÉCURITÉ



OBJECTIFS D'APPRENTISSAGE

> Les participants devront pouvoir identifier leurs propres objectifs de sécurité et de protection.

> Les participants devront pouvoir élaborer un plan de sécurité.

MESSAGES CLÉS

> Un plan de sécurité aide à réduire les vulnérabilités et à augmenter les capacités de manière à pouvoir faire face aux menaces ou à en diminuer la probabilité, réduisant ainsi les risques. Il est préférable d'avoir un plan de sécurité simple que les défenseurs pourront appliquer plutôt qu'un plan complexe qu'ils n'appliqueront probablement pas.

> Une bonne analyse de risques permet l'identification des principales menaces, vulnérabilités et capacités, en vue de mettre l'accent sur les choses les plus importantes dans le plan de sécurité. Dans le cas où les DDH ne disposent pas de beaucoup de temps ou de beaucoup de ressources, ceci leur permettra de faire en sorte que les ressources disponibles soient consacrées aux problèmes de sécurité prioritaires.

LA SESSION

DIFFICULTÉS POUVANT SURVENIR DURANT LA SESSION :

→ Élaborer un plan de sécurité simple et réaliste mettant l'accent sur les problèmes prioritaires.

→ Amener les participants à accepter le plan et leur indiquer comment commencer à l'appliquer à court et à moyen terme. Prendre en compte les besoins spécifiques de protection que peuvent avoir les femmes DDH ou tout autre groupe social particulier (populations indigènes, défenseurs LGBTI, défenseurs handicapés, etc.) en termes de stratégies, de normes de sécurité, etc., tant au niveau des protocoles de routine qu'au niveau des procédures d'urgence.

LA SESSION ÉTAPE PAR ÉTAPE :

Durée	Durée totale	Activité	Outil / méthode / matériel
20´		**Introduction**: • Objectifs et structure de la session. • Objectifs des mesures de sécurité.	Préparez les points à l'avance sur un paper-board ou dans une présentation PowerPoint.
90'	110'	**Élaborer un plan de sécurité.**	Résultats de l'analyse de risque réalisée au cours de la session 5.2. Feuilles de paper-board de la session 5.2. Paper-board Marqueurs Modèles de tableaux pour l'élaboration d'un plan de sécurité (à projeter via un ordinateur portable ou à préparer sur paper-board)
10'	120'	**Conclusion**	
		DURÉE : COMPTER 140 MINUTES (2 HEURES 20 MINUTES), DONT UNE PAUSE DE 20 MINUTES.	

ACTIVITÉS D'APPRENTISSAGE

OBJECTIF DES MESURES DE SÉCURITÉ

Pour introduire cette session, citez les trois objectifs généraux devant être inclus dans un plan de sécurité:

→ Faire en sorte qu'une personne cesse de faire quelque chose (p.e. qu'un agresseur cesse de menacer ou d'attaquer les DDH).

→ Faire en sorte qu'une personne fasse ce qu'elle doit faire (p.e. qu'une autorité légitime empêche des agresseurs de nuire aux DDH).

→ Faire en sorte que les DDH soient moins vulnérables et augmentent leurs capacités de protection.

Utilisez des exemples tirés des expériences personnelles des participants pour illustrer ces trois objectifs. Rappelez ensuite aux participants l'équation du risque (voir NMP et Chapitre 5.2. de ce Guide). Indiquez que les deux premiers objectifs concernent les menaces et que le dernier concerne les vulnérabilités et les capacités. Soulignez également le fait que les deux premiers objectifs sont liés à leurs capacités. Les mesures qu'ils prennent augmenteront en effet leur capacité à dissuader les agresseurs potentiels.

ÉLABORER UN PLAN DE SÉCURITÉ

L'élaboration d'un plan de sécurité complet est une tâche complexe qui requiert un temps considérable. Dans cet exercice, vous vous concentrerez uniquement sur la manière de concevoir un plan de sécurité simple basé sur les priorités établies par l'analyse de risques d'une organisation.

COMMENT TRAVAILLER:

Ce travail se base sur l'analyse de risques réalisée précédemment. Si vous travaillez avec un groupe homogène, référez-vous aux résultats de l'exercice d'évaluation de risques figurant dans le Chapitre 5.2. (Si vous travaillez avec un groupe hétérogène, voyez les Conseils aux facilitateurs.) Ayez à votre disposition les feuilles de paper-board de cet exercice, afin de faciliter le processus.

1. **Sélectionner les menaces les plus spécifiques:** Les participants devront choisir les menaces les plus sérieuses ou celles qui se rapportent le plus à leurs principales vulnérabilités, car ce sont ces menaces-là qui leur font encourir les plus grands risques (voir **NMP, chapitre 1.2.** fpour trouver des conseils et des indications). (10 minutes)
2. **Réévaluer les vulnérabilités :** Donnez aux participants quelques minutes pour réévaluer les vulnérabilités qu'ils ont associées précédemment aux menaces sélectionnées. Faites des ajustements là où vous pensez que c'est nécessaire. Focalisez-vous plus particulièrement sur ces vulnérabilités-là quand vous planifierez des actions visant à réduire les risques engendrés par les menaces sélectionnées. Souvenez-vous : toutes les vulnérabilités ne sont pas associées à toutes les menaces. (10 minutes)
3. **Réévaluer les capacités :** Demandez aux participants de réaliser le même exercice pour la liste des capacités qu'ils ont associées aux menaces sélectionnées. (10 minutes)
4. **Transformer les vulnérabilités en «objectifs» dans le plan de sécurité :** Aidez-vous du tableau ci-dessous (l'exemple n'est pas exhaustif). (30 minutes)

Menace	Objectif	Vulnérabilité (associée à la menace)	Objectif
«Effraction - Des effractions ont eu lieu dans d'autres bureaux.»	«Réduire la possibilité d'une effraction dans notre bureau.» «Réduire l'impact négatif d'une effraction dans nos bureaux si elle devait se produire.»	«Nous possédons des informations sensibles stockées dans les ordinateurs du bureau.»	«Même si une effraction a lieu, nous prévenons : • la perte d'informations stockées dans nos ordinateurs ; • l'accès à ces informations pour des personnes non-autorisées.»

5. **Développer chaque objectif :** Écrivez les actions pouvant être réalisées pour atteindre l'objectif. Attirez l'attention des participants sur le fait que des mesures de sécurité doivent inclure des actions préventives et des mesures réactives. Ces objectifs et ces actions constitueront la trame du plan de sécurité (30 minutes). Exemple :

Objectifs	Actions
«Réduire la possibilité d'une effraction dans notre bureau.»	• Conjointement avec d'autres organisations, faire une déclaration publique dénonçant le nombre d'effractions commises dans des organisations, et exigeant que des mesures soient mises en place par le gouvernement pour arrêter le phénomène. • - Exercer une pression sur les autorités concernées (la police et le pouvoir législatif) pour qu'elles enquêtent sur les intentions qui se cachent derrière la vague d'effractions et qu'elles traduisent les auteurs en justice.
«Même si une effraction se produit, nous ne perdrons pas les informations stockées sur les ordinateurs et des personnes non-autorisées ne pourront pas y avoir accès.» Note : cet objectif suppose que l'organisation possède dans son réseau de soutien des équipes de spécialistes en technologies de l'information.	• - Mettre en place un réseau informatique doté d'un serveur central. • - Effectuer des back-ups réguliers du disque dur du serveur central et conserver les copies dans un coffre ou dans un endroit protégé en dehors du bureau. • - Installer un programme de cryptage simple et sécurisé pour le serveur central, de manière à empêcher l'utilisation des informations en cas de vol du matériel.

6. **Faire la liste de toutes les actions à entreprendre, sous la forme d'un plan:** Pour cela, projetez sur un écran le tableau ci-dessous. Utilisez soit l'exemple fourni, soit un exemple tiré de l'expérience personnelle du groupe. Vous pouvez également choisir d'écrire les éléments-clés sur votre paper-board pour guider les participants dans leur travail de groupe, plus tard. Demandez aux participants de former des groupes de 4 à 5 personnes et attribuez un nombre égal de menaces à chaque groupe. Chaque groupe devra élaborer des mesures de sécurité pour chaque menace qui lui aura été attribuée. Pour rendre ce plan réaliste/opérationnel, soulignez qu'il est important d'attribuer un délai à chaque action et d'assigner des responsabilités. Chaque groupe devra ensuite présenter les résultats à l'ensemble de l'assemblée, et les actions proposées devront être débattues entre tous les participants. A la fin de l'exercice, ils auront la trame générale de leur plan de sécurité. Plus vous avez de temps à consacrer à cet exercice, plus le plan sera concret. L'organisation pourra commencer à travailler sur le plan immédiatement après la formation.

   Le tableau suivant illustre plus en détail l'élaboration du plan en utilisant les mêmes exemples :

Objectifs		Mesures de sécurité	Responsabilités	Coûts	Délai
Généraux (liés aux menaces)	**Spécifiques (liés aux vulnérabilités)**				
«Réduire les possibilités d'une effraction dans notre bureau».	«Même si une effraction a lieu, nous prévenons : • la perte d'informations stockées dans nos ordinateurs ; • l'accès à ces informations pour des personnes non-autorisées.»	Déterminer quelles informations sont sensibles afin de prendre des mesures complémentaires pour empêcher l'accès non-autorisé	**Chargés de programmes et membres de la direction**	**$0**	**Dans les trois mois**
		Mettre en place un réseau informatique avec un serveur central au bureau. Le serveur ne doit pas être facilement accessible aux personnes extérieures	**Chargé des technologies de l'information / Consultant externe en technologies de l'information**	**$0**	**Dans les trois mois**
		Acheter un disque dur externe	**Chargé des finances**	**$200**	**Dans les deux semaines**
		Faire un back-up (une copie) du disque dur du serveur central chaque semaine	**Chargé de l'information et de la communication**	**$0**	**Tous les mois**
		Conserver une copie du back-up dans un coffre ou dans un endroit sûr (à l'extérieur du bureau)	**Chargé de programmes**	**$0** (si on utilise un logiciel libre)	**Tous les six mois**
		Trouver, apprendre à utiliser, et utiliser un programme de cryptage	**Chargé de l'information et de la communication**	**$0** (si on utilise un logiciel libre)	**Dans les deux mois**

	Formation interne sur le programme de cryptage et sur les mots de passe sécurisés	**Tout le monde**	**$0**	**Dans le mois**
	Installer un programme de cryptage pour le serveur central et les back-ups, de manière à empêcher l'accès aux informations en cas de vol	**Chargé de l'information et de la communication**	**$0** (si on utilise un logiciel libre)	**Dans les deux semaines**
	Conjointement avec d'autres organisations, faire une déclaration publique dénonçant le nombre d'effractions commises dans des organisations, et exigeant que des mesures soient mises en place par le gouvernement pour arrêter le phénomène	**Chargé de l'information et de la communication**	**$0**	**Dans le mois**
	Exercer une pression sur les autorités concernées (la police et le pouvoir législatif) pour qu'elles enquêtent sur les intentions qui se cachent derrière la vague d'effractions et qu'elles traduisent les auteurs en justice	**Chargé de plaidoyer**	**$0**	**Immédiat**

→ **Communiquez aux participants les informations suivantes sur le lancement d'un processus de préparation d'un plan de sécurité:**

- **Un plan de sécurité n'est utile que s'il est mis en application :** disposer d'un plan de sécurité ne réduit pas automatiquement les risques. Les plans doivent être partagés, expliqués et appliqués pour avoir un impact sur la sécurité des DDH.
- **La gestion de la sécurité est un processus dynamique qui évolue avec le temps et qui requiert une réévaluation régulière:** Le risque est en effet un concept dynamique, car il dépend d'un environnement en perpétuel changement. Un plan qui est bon aujourd'hui sera peut-être inapproprié dans six mois. Si la situation évolue, les défenseurs doivent revoir leur analyse et leur plan en conséquence. Il faut penser la gestion de la sécurité comme un processus permanent, basé sur l'analyse de menaces, de vulnérabilités et de capacités changeantes, ainsi que sur le contexte sociopolitique.
- **Pour être efficaces, les plans de sécurité doivent être réalistes :** An effective security plan must take into account a realistic timeframe and the organisation's capacities. If the plan is too ambitious or demanding, it runs the risk of being shelved. Your role as facilitator is to ask questions that help defenders to assess whether their planned actions are realistic and achievable.
- **Les plans de sécurité doivent comprendre une dimension réactive et une dimension préventive.**

→ **Difficultés pouvant survenir lors de l'activité d'élaboration d'un plan de sécurité :**

- Vous travaillerez peut-être avec une longue liste de menaces et de vulnérabilités, ce qui pourra engendrer des difficultés. Une fois que vous aurez sélectionné les menaces, il ne faudra sélectionner

que les vulnérabilités qui y sont liées. Cela rendra l'exercice plus facile, et cela permettra au plan de cibler les problèmes de sécurité prioritaires. Voir **NMP, chapitre 1.7.** pour des exemples concrets

- Si vous travaillez avec un groupe hétérogène, vous devrez inventer un exemple ou diviser les participants en plusieurs groupes (chacun correspondant à une organisation). Une manière simple de procéder serait de se servir de l'activité réalisée dans le **chapitre 5.2** de ce Guide. Gardez à l'esprit que s'il y a un manque de confiance entre les participants, il sera peut-être difficile d'échanger des détails ayant trait à des analyses de risques et à des plans de sécurité réels (d'où l'intérêt de travailler sur des exemples fictifs). Chaque organisation devra cependant réaliser les exercices, de manière à pouvoir définir son propre plan de sécurité au terme de l'atelier.
- Les participants confondront peut-être objectifs et actions. Cela ne devrait pas poser de problème tant qu'ils parviennent à définir des mesures de sécurité pertinentes et concrètes. Ne perdez donc pas trop de temps à des éclaircissements purement conceptuels. Consacrer plutôt vos efforts à obtenir des résultats concrets.

CONCLUSION

> Demandez aux participants de rappeler les enseignements-clés.

> Rappelez-leur l'importance d'intégrer dans la conception du plan de sécurité les analyses effectuées dans les sessions précédentes en matière de gestion de la sécurité (analyse du contexte, évaluation des risques, analyse des menaces et des incidents de sécurité).

> Indiquez aux participants que pour le travail à suivre il leur sera utile de lire le chapitre du NMP consacré à ce thème.

RESSOURCES COMPLÉMENTAIRES

> Van Brabant. Op. Cit. Chapitre 5. (pp. 56-72) et chapitre 21. (pp. 310-322).

> FLD. Op. Cit. Chapitre 5