

Présentation du CERT OSIRIS

Guilhem BORGHESI

RSSI - Université de Strasbourg
14, rue René Descartes
67000 Strasbourg

Magali DAUJAT

Membre du CERT IBMP (CNRS)
12, rue du général Zimmer
67000 Strasbourg

Marc HERRMANN

RSSI - Délégation CNRS Alsace
23 rue du Loess
67000 Strasbourg

Résumé

Depuis le 1er janvier 2012, l'Université de Strasbourg et la Délégation Alsace du CNRS organisent conjointement leur action en matière de sécurité informatique. Ils proposent notamment désormais une gestion commune des incidents de sécurité informatique grâce au CERT OSIRIS. La création de cette structure transversale entre une université et une délégation CNRS régionale est une première en France.

Ses missions sont les suivantes :

- *traiter les incidents de sécurité de l'Université de Strasbourg et de la Délégation CNRS Alsace ;*
- *accompagner les correspondants de sécurité des systèmes d'information (CSSI) dans la résolution d'incident ;*
- *animer un réseau d'une centaine de CSSI pour les deux établissements ;*
- *proposer des formations et des séances de sensibilisation aux CSSI et aux utilisateurs ;*
- *relayer les informations de sécurité et de réglementation auprès des correspondants ;*
- *accompagner les composantes et laboratoires dans la mise en place de leur PSSI.*

Nous vous présenterons la démarche de création et les avantages d'une telle organisation pour la gestion au quotidien de la sécurité de l'information. Ainsi, nous aborderons les points suivants :

- *le projet et la création du CERT OSIRIS en 2012 ;*
- *le catalogue des services du CERT ;*
- *les outils du CERT pour l'accomplissement de ses missions ;*
- *les réalisations 2012/2013 ;*
- *les évolutions et les projets pour 2014 ;*
- *les problèmes rencontrés lors de la création du CERT.*

Mots-clefs

SSI, Sécurité, CERT, Incident, Université, CNRS, Correspondant, formation, sensibilisation, PSSI

1 Contexte

Dans le courant de l'année 2011, il est apparu essentiel aux acteurs de la Sécurité du Système d'Information de la délégation CNRS Alsace et de l'Université de Strasbourg de collaborer afin de mutualiser les efforts en matière de SSI. Pour mieux évaluer les raisons de ce rapprochement, nous proposons de prendre connaissance de l'état des lieux précédant la création du CERT OSIRIS.

1.1 À l'Université de Strasbourg

Deux personnes, le Responsable Sécurité du Système d'Information (RSSI) et son adjoint, étaient attachés à la résolution et prévention des incidents de sécurité de la totalité du réseau OSIRIS. Cependant, dans les faits, beaucoup de personnels étaient réellement impliqués dans ce processus comme des experts, des techniciens du support ou de l'exploitation, des développeurs logiciels, des correspondants sécurité de composante et laboratoire. Certains incidents, bien qu'étant dans le périmètre du réseau OSIRIS, étaient également signalés directement auprès de la délégation CNRS Alsace.

1.2 À la délégation CNRS Alsace

Une Coordination Régionale de la Sécurité du Système d'Information (CRSSI), sous la responsabilité du Délégué Régional, mettait en œuvre les différentes actions liées à la SSI : gestion d'un réseau de Correspondants Sécurité des Systèmes d'Information (CSSI), aide à la mise en œuvre des Politiques de Sécurité du Système d'Information (PSSI), diffusion d'informations, conduite d'actions de formation, de conseil et de soutien. Ces actions étaient réalisées indépendamment de l'Université.

1.3 Constat

La grande majorité des laboratoires de recherche de l'Université sont des unités mixtes et à ce titre s'adressaient à la fois au CNRS et à l'Université pour la résolution des incidents de sécurité. Autrement dit, les deux services SSI, à l'Université de Strasbourg comme au CNRS Alsace, travaillaient pour des publics en partie identiques avec parfois des discours totalement différents.

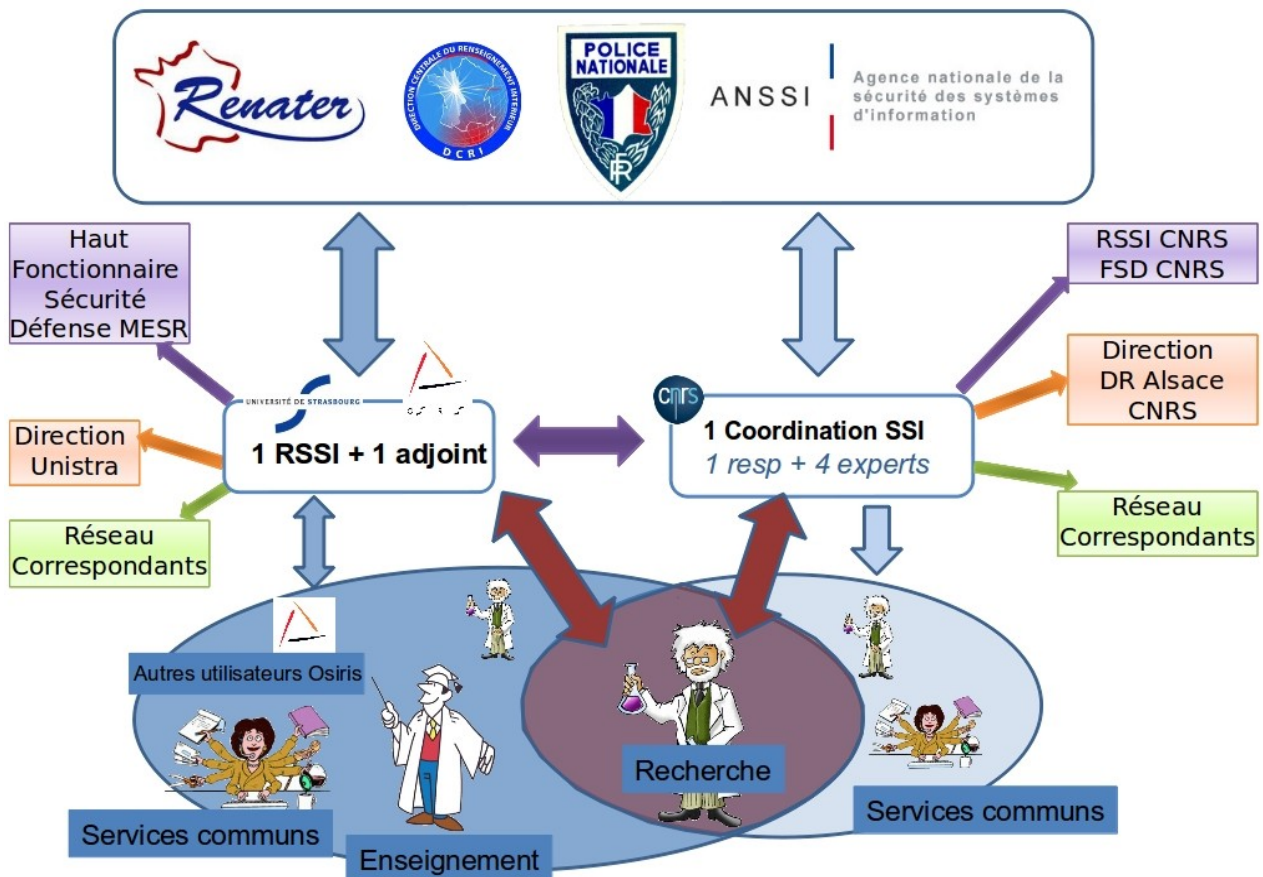


Figure 1 - La situation avant le CERT

Fort de cette constatation, dans une volonté d'améliorer la sécurité de nos SI, la mutualisation de nos actions nous a paru devenir indispensable. La structure opérationnelle qui nous a semblé la plus pertinente pour mettre en œuvre cette

coordination est celle d'un CERT.

1.3.1 Qu'est-ce qu'un CERT ?

Un CERT (Computer Emergency Response Team) est une équipe d'experts en sécurité informatique. Son but est la protection du patrimoine numérique par la réduction du nombre d'incidents majeurs, la diminution de leur impact et des conséquences préjudiciables sur les activités stratégiques de l'établissement pour lequel il travaille.

Généralement, les types de service rendus sont de deux ordres :

- réactifs : signalement, traitement, analyse et appui à la réponse d'incidents ;
- préventifs : veille, détection, diffusion d'information, audit, formation et sensibilisation.

Il nous a fallu nous interroger sur la manière dont cette nouvelle structure allait s'intégrer dans le paysage de la sécurité des SI de nos deux établissements.

2 Articulation avec les Politiques de Sécurité des établissements

2.1 A l'Université de Strasbourg

En 2012, l'Université de Strasbourg, dans le cadre d'un Schéma Directeur du Numérique, a lancé un « Système de Management de la Sécurité Informatique » (SMSI). Il a permis de mettre en place les fondations de la sécurité pour tout le système d'information de l'Université. Dans ce cadre là, il a été nécessaire de produire des fonctionnements normalisés (procédures et audits) pour tout ce qui concerne l'exploitation de la sécurité et la sensibilisation auprès des utilisateurs. Une organisation telle qu'un CERT pouvait naturellement prendre en charge cette activité au sein même du SMSI.

2.2 Au CNRS

Le CNRS dispose d'une PSSI nationale signée en novembre 2006 ; chaque unité déclinant localement cette PSSI suite à un diagnostic et une analyse de son système d'information.

Les PSSI abordent la sécurité des systèmes d'information de manière globale. Certains chapitres (gestion d'incidents, sensibilisation, information et formation des utilisateurs par exemple) sont naturellement mutualisables avec des structures locales tout en intégrant les consignes nationales spécifiques. La création d'un CERT commun avec l'Université de Strasbourg était donc tout à fait envisageable dans ce contexte.

3 Objectifs

Les objectifs avancés lors de la création du CERT au 1er janvier 2012 étaient les suivants :

1. Augmenter uniformément les niveaux de sécurité de nos établissements ;
2. Donner plus de visibilité à la sécurité auprès de nos utilisateurs et partenaires externes ;
3. Mettre en place un tableau de bord commun de la SSI.

4 Le projet CERT OSIRIS

Nous avons commencé à travailler au début de l'année 2011 sur le lancement de cette structure unique en France. Au préalable, nous nous sommes assurés que la démarche serait bien perçue par nos partenaires et instances.

Ainsi, le CERT-Renater, premier de nos partenaires externes, nous a fortement encouragé dans le lancement d'une telle structure décentralisée. Ils nous a notamment été répondu qu'une telle organisation renforcerait localement l'efficacité de leur action.

Nous avons également reçu le plus vif soutien dans cette démarche de la part de nos interlocuteurs fonctionnels SSI au sein du Ministère de l'Enseignement Supérieur et de la Recherche par l'entremise de Mme Isabelle MOREL (FSD MESR) et de M. François MORRIS (RSSI Adjoint CNRS).

La démarche validée et les objectifs définis, nous avons pu travailler à la définition de la structure cible.

4.1 Organisation du CERT

Le CERT OSIRIS est une structure informelle composée de :

- pour la partie CNRS Alsace : les 4 membres de la Cellule Régionale SSI ;
- pour la partie Université de Strasbourg : le RSSI et son adjoint, un membre du support utilisateur, un membre des informaticiens de composante.

L'animation de cette structure transversale aux deux établissements est confiée aux RSSI des deux établissements, de manière collégiale.

Le pilotage en est assuré par le Comité de Pilotage du réseau OSIRIS/RAREST. Ce comité rassemble tous les établissements d'enseignement et de recherche raccordés au réseau métropolitain de Strasbourg.

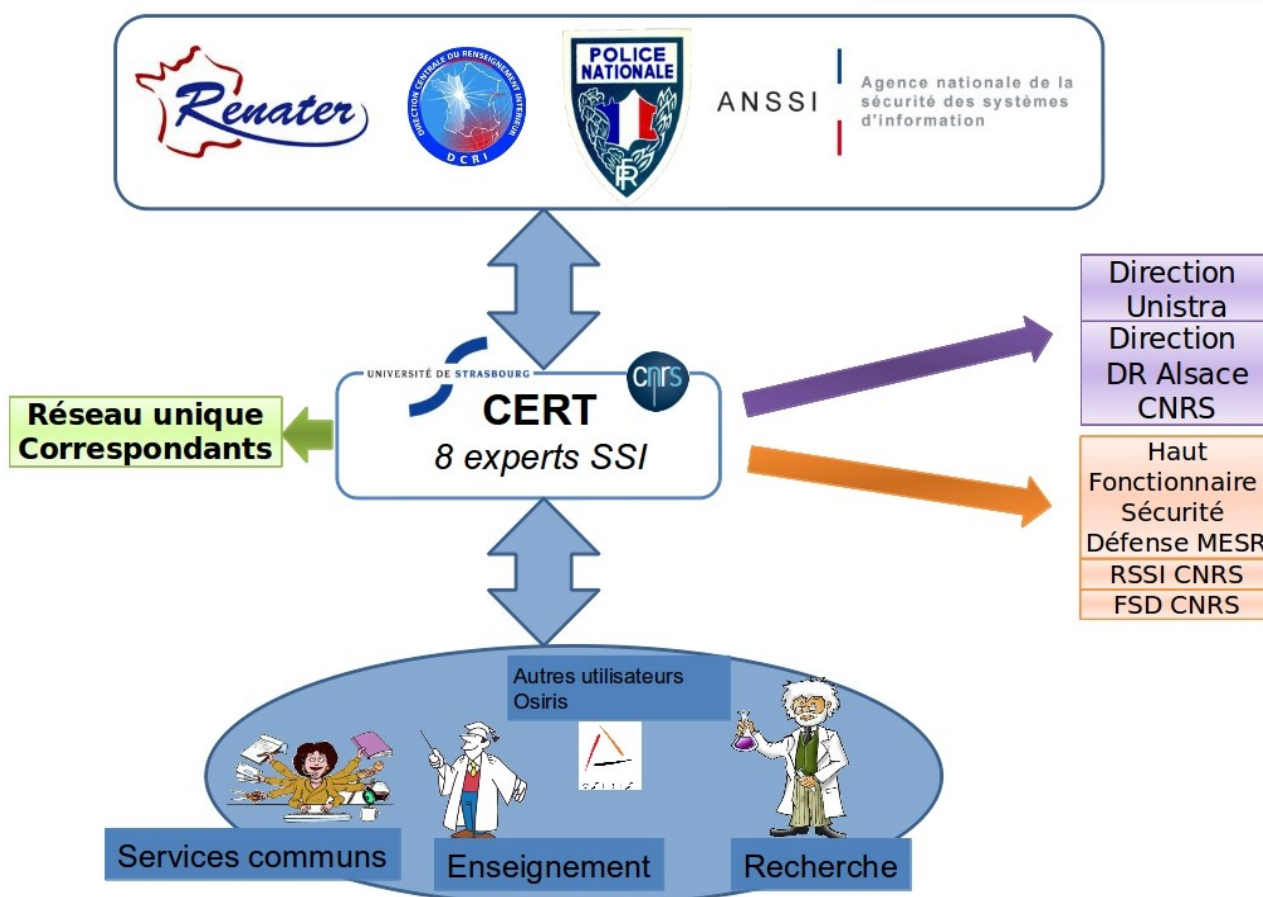


Figure 2 - La situation avec le CERT

4.2 Les services

Pour faciliter la compréhension de l'action de cette nouvelle structure, il nous a paru essentiel de l'adosser à une offre de service lisible. Nous avons donc conçu un catalogue des services spécifique à l'activité du CERT. Nous proposons :

- Traitement des incidents de sécurité :
 - Surveillance des réseaux et détection des intrusions

- Signalement d'incidents au CSSI
- Suivi d'incidents et accompagnement sur le terrain
- Coordination des services impliqués dans le traitement (chaînes fonctionnelles et hiérarchiques, juridique, police / gendarmerie, ...)
- Formations et sensibilisations
 - Formations des utilisateurs et des correspondants
 - Séances de sensibilisation
- Diffusion d'informations
 - Diffusion des bulletins SSI (Avis, alertes CERTA et CERT-RENATER, ...)
 - Veille juridique
- Accompagnement à la mise en œuvre de PSSI
 - Mise en place de la Protection du Potentiel Scientifique et Technique (PPST)
 - Composantes et laboratoires en demande
- Analyse technique d'incidents
 - Collecte de preuves
 - Analyse des traces

4.3 Les outils

Les outils indispensables dont dispose le CERT OSIRIS pour accomplir ses missions sont les suivants :

4.3.1 Réseau unique des correspondants SSI

Le réseau comporte aujourd'hui une centaine de personnes, majoritairement des personnels techniques. Il doit être étendu aux services centraux de l'Université vers des profils de correspondant moins technique et plus fonctionnel. Le rôle des correspondants est principalement d'être un relais d'information au sein des laboratoires et composantes.

4.3.2 Outil de suivi d'incident unifié

Afin de réaliser des statistiques consolidées, nous avons mis en place un processus de traitement des incidents sécurité s'appuyant sur un outil de suivi unique. Le logiciel retenu a été Request Tracker (RT) car il était déjà en fonction à l'Université pour tous les incidents et demandes de service. Il a été adapté pour que nous disposions d'un espace sécurisé pour le CERT. Il est doté de fonctionnalités spécifiques pour la remontée de statistiques et l'espace CERT reste inaccessible aux autres utilisateurs de RT pour des raisons évidentes de confidentialité des incidents de sécurité.

4.3.3 Outils de communication

Dans le but de rendre plus facile l'accès aux informations fournies par le CERT OSIRIS (supports de formation, de séminaire, de sensibilisation, procédures, ...), nous avons mis en place un site web <http://cert-osiris.unistra.fr>. Il sera bientôt complété par un intranet plus spécifiquement destiné aux CSSI. Ils pourront y trouver une information plus technique et surtout pourront également y déposer des informations à destination des autres membres du réseau.

Par ailleurs, la création d'une adresse unique de contact a été indispensable. C'est l'adresse par laquelle tout usager ou correspondant peut faire appel à nos services ou déclarer un incident de sécurité.

4.3.4 Tableau de bord SSI

Le CERT, pour améliorer ses actions de fond, doit disposer d'une série d'indicateurs fiables. Ils sont rassemblés dans un document de synthèse, véritable tableau de bord SSI. Il comprend, entre autres, des données annualisées sur :

- le nombre d'incidents de sécurité, triés par catégorie ;
- les vols de matériels ;
- les pannes d'infrastructure ;

- les sensibilisations et formations des utilisateurs et correspondants.

5 Difficultés rencontrées

Il va sans dire que la mise en place d'un tel projet a rencontré des difficultés. Assez étonnamment, elles ne sont pas survenues de la disparité de vue entre les deux établissements. Elles sont en revanche plutôt dues à une culture différente des publics bénéficiaires du CERT.

5.1 Hétérogénéité des utilisateurs

Les catégories de public qui utilisent les SI du CNRS et de l'Université de Strasbourg sont disparates : chercheurs, étudiants, enseignants, personnels administratifs, ...

Chacun de ces profils d'utilisateurs a une sensibilité particulière dans son usage des moyens informatiques mis à sa disposition. Le discours de sensibilisation ne peut donc pas être le même, monolithique, pour tous les utilisateurs. Cette adaptation à la culture de nos usagers est l'un des défis que doit relever quotidiennement le CERT dans l'accomplissement de ses missions. Cela prend tout son sens notamment lors de la conception des supports de sensibilisation à destination du plus grand nombre.

5.2 Déclinaisons locales divergentes des PSSI

Dans certains laboratoires de recherche mixtes, l'imbrication est telle que, par exemple, des personnels CNRS utilisent au quotidien des matériels informatiques achetés sur des crédits universitaires. On peut aisément imaginer la facilité à contourner les règles basiques de sécurité si les discours ne sont pas cohérents.

5.3 Cadre institutionnel inexistant

Le dernier contrat quadriennal entre le CNRS et l'Université est échu depuis plusieurs années. Il ne comportait d'ailleurs que peu d'éléments sur la collaboration en matière de système d'information. Nous ne disposons donc pas d'un document de référence cadrant les relations inter-établissements. Nous avons donc dû « inventer » un cadre de fonctionnement efficace entre personnels de deux établissements.

6 Réalisations

Nous présentons ici une liste non exhaustive des réalisations du CERT OSIRIS depuis sa création en janvier 2012.

6.1 Harmonisation de la procédure de traitement des incidents de sécurité

Le premier travail structurant a été de définir ensemble la façon que nous aurions de collaborer sur les incidents de sécurité. Nous avons donc formalisé un processus prenant en compte la majorité des incidents pour clarifier les rôles de chacun et optimiser les ressources de traitement de ces incidents.

6.2 Le réseau des correspondants sécurité

C'est l'une des premières réalisations du CERT. Nous avons créé un réseau de CSSI dans la plupart des laboratoires et composantes de l'Université. Pour ce faire, nous avons établi une fiche de référence du CSSI comportant ses missions, ses moyens et les compétences requises pour la fonction. Cette fiche a été transmise à tous les responsables de structure pour une nomination d'un CSSI. C'est la pierre angulaire de la communication en matière de SSI avec les sous-structures de nos établissements.

6.3 Production d'indicateurs SSI

L'utilisation d'un outil unique pour le suivi des incidents de sécurité associé à une définition précise des différentes catégories d'incident nous a permis de produire des éléments statistiques fiables. Chaque incident étant désormais

catégorisé, nous allons pouvoir mettre en œuvre des actions correctives en regard de ces indicateurs.

6.4 Opérations « mots de passe faibles », niveau 1 et 2

Dans le cadre d'une recherche d'amélioration de la robustesse des mots de passe « utilisateurs », deux actions ciblées ont été entreprises. Elles ont eu pour but d'identifier les mots de passe très faibles (vides, courts, ...). Cette première série d'opérations a permis l'identification de plusieurs centaines de comptes qui ont été rendu inopérants ou dont le mot de passe a été changé par l'utilisateur.

6.5 Campagne de sensibilisation des utilisateurs

Une vaste campagne de sensibilisation à la sécurité a été réalisée en septembre 2013. Elle a eu pour objet la formation et la distribution de supports de sensibilisation à la sécurité pour les CSSI du CERT OSIRIS. C'est un des moyens que nous avons identifié pour atteindre plus efficacement les personnels de nos structures. Aujourd'hui, plusieurs sensibilisations, s'appuyant sur les documents fournis par le CERT, ont d'ores et déjà eu lieu dans les laboratoires et composantes de notre réseau.

6.6 Formations aux utilisateurs et CSSI

Parallèlement à cette campagne générale de sensibilisation, le CERT continue de proposer des formations à la sécurité informatique pour les utilisateurs de nos établissements. Ces formations sur une journée, permettent d'aborder dans les détails les menaces et les manières d'y remédier, dans un contexte professionnel ou privé.

7 Perspectives

7.1 Extension du CERT

Dès la lancement du CERT, nous avons la volonté de pouvoir l'élargir aux établissements qui le souhaitent. En effet, nous parions sur le fait que l'harmonisation des pratiques en matière de sécurité et de sensibilisation sera profitable pour tous. La mutualisation des ressources est un gain évident de ressources qui permettra à de petites organisations de pouvoir bénéficier de ces services.

7.2 Perfectionnement des outils de supervision et de détection

Un des enjeux de l'avenir du CERT OSIRIS est de mettre en place dès 2014 des outils de détection et de surveillance internes. Pour l'instant, nous sommes encore grandement dépendants des alertes externes. La recherche proactive de vulnérabilités du SI nous ferait gagner grandement en efficacité dans le traitement des incidents de sécurité.

7.3 Opération « mots de passe faibles », niveau 3

Au printemps 2014, la dernière phase de recherche des mots de passe faibles sera lancée. Elle mettra en évidence les mots de passe issus du « dictionnaire ». Elle nécessite au préalable l'adaptation de l'application de gestion de compte des utilisateurs de l'Université.

7.4 Chiffrement des matériels portables

Pour répondre à un des axes de la PPST, nous allons suivre les recommandations de chiffrement des matériels informatiques. Une vaste campagne est en cours au sein du CNRS s'appuyant notamment sur le logiciel TrueCrypt pour les postes utilisant Microsoft Windows. Parallèlement, une expérimentation a été validée à l'Université qui a donné lieu à un chiffrement similaire des matériels nomades de la Direction Générale et de tous les directeurs. Une telle réalisation n'a pu avoir lieu que grâce à la mutualisation des compétences au sein du CERT, le CNRS étant bien plus mature sur ces questions que l'Université.

8 Conclusion

Il est désormais clairement établi que la création d'un interlocuteur unique nous a permis de tenir un discours autour de la sécurité qui soit cohérent et commun entre les deux établissements. Cela a contribué en une meilleure acceptation de la sensibilisation aux enjeux. La création de cette structure unique a eu un effet positif incontestable sur la visibilité de la SSI auprès des utilisateurs, des correspondants sécurité, de la gouvernance de nos établissements, des chaînes fonctionnelles SSI et de nos partenaires externes. C'est un gain indéniable pour accomplir la mission qui est la nôtre. Et ceci a été réalisé grâce à une organisation transversale et informelle, qui n'a pas nécessité de ressources humaines et financières supplémentaires.