Sensibiliser à la sécurité numérique au plus près des acteurs sur les territoires : un enjeu majeur

Jérôme NOTIN

Directeur général de cybermalveillance.gouv.fr

Le dispositif Cybermalveillance.gouv.fr a été partenaire du Tour de France de la Cybersécurité pour la 2ème année en 2019.

Chaque étape du TDFCyber a été une occasion de présenter aux participants en plénière le dispositif et ses missions de sensibilisation aux risques numériques, d'assistance aux victimes d'actes de cybermalveillance, et d'observation de la menace cyber, ainsi que la plateforme et les typologies de victimes et de modes opératoires de cyberattaques traités sur Cybermalveillance.gouv.fr.

Lors de plusieurs étapes du Tour de France de la Cybersécurité, un atelier a été organisé pour aider les participants à comprendre les étapes méthodologiques d'une démarche de sensibilisation interne, en entreprise ou dans une collectivité. Cet atelier a été construit comme une mise en situation concrète des participants et a été l'objet de réflexions et retours très constructifs et encourageants.

Globalement, la participation de Cybermalveillance.gouv.fr au TDFCyber est l'occasion pour le dispositif d'aller à la rencontre de ses publics sur les territoires, de faire connaître ses missions et les contenus de sensibilisation, mais aussi d'apprendre, de la part des participants du TDFCyber, de nombreuses remontées de terrain et enseignements sur les pratiques de sensibilisation et d'assistance.

La richesse des interventions et des publics, ainsi que la qualité des conditions d'accueil et des intervenants, fait du TDFCyber un événement auquel le dispositif Cybermalveillance.gouv.fr est fier de contribuer.

Article atelier de sensibilisation

Lors du Tour de France de la Cybersécurité 2019, le dispositif Cybermalveillance.gouv.fr a organisé sur plusieurs étapes un atelier de sensibilisation appelé « Construire une démarche interne de sensibilisation aux enjeux de cybersécurité, un enjeu majeur pour les entreprises et les collectivités ».

Cet atelier a été imaginé pour répondre à un besoin de méthodologie et de réflexion sur la manière dont on peut élaborer des stratégies de sensibilisation, et pas uniquement utiliser des contenus de sensibilisation déjà préparés.

Pour Cybermalveillance.gouv.fr, cet atelier a été également une manière de recueillir, auprès des participants, leurs retours d'expériences permettant de nourrir les contenus et stratégies de sensibilisation et de recommandations de bonnes pratiques du dispositif.

L'atelier a été proposé pour 12 à 15 participants maximum à chaque fois.

Ceux-ci ont été partagés en deux groupes qui ont reçu chacun une situation concrète à mettre en place :

- un groupe recevant la simulation d'une stratégie de sensibilisation pour les agents d'une collectivité territoriale de 5 000 habitants ;

- l'autre groupe recevant la simulation d'une stratégie de sensibilisation pour une PME de 35 salariés travaillant comme sous-traitante dans le secteur automobile.

Ces deux scénarii font alors l'objet d'une réflexion, par petits groupes, cadrée par une trame écrite qui permet aux participants de balayer petit à petit les différentes phases de construction d'une méthode de sensibilisation.

Au bout de 45 minutes environ, les deux groupes se réunissent et vont présenter chacun le fruit de leur réflexion. L'animateur-trice de l'atelier va alors enrichir cette restitution, si besoin, avec des bonnes pratiques déjà éprouvées, mais aussi noter et recueillir des pratiques qui seraient intéressantes à faire remonter.

Les participants sont tout d'abord invités à une première phase d'identification et d'analyse des informations et données qui sont à protéger dans l'entité : cela permet, avant d'entamer la démarche de sensibilisation proprement dite, de prendre conscience de l'application concrète et du périmètre qu'elle va devoir prendre. Il faut identifier les informations sensibles, qui y a accès, et comment.

Ensuite, les participants vont relever quelles sont les menaces qui peuvent viser l'entité qu'ils ont mission de protéger, quelles sont les mesures de sécurité déjà existantes, et faire un état des lieux de la maturité et de la formation des personnels.

À partir de là, ils vont pouvoir donner des objectifs précis à leur démarche de sensibilisation : définir les sujets à traiter, établir un calendrier, prioriser les actions et les publics.

Enfin, ils commencent une réflexion sur la mise en œuvre concrète, à court et moyen terme, de la démarche de sensibilisation aux risques cyber adaptée à leur entité.

Cette démarche partant de la situation de l'organisation est l'occasion de faire un état des lieux et une première réflexion d'analyse des risques en prenant en compte la réalité de la vie d'une entreprise ou d'une collectivité. Les participants à l'atelier doivent se mettre dans la peau du responsable de cette mission de sensibilisation (DSI ou autre) et aller chercher dans l'ensemble des activités et des personnels de l'entité le périmètre et les ressources qui vont ensuite être au cœur de l'activité de sensibilisation.

En mettant l'accent sur les besoins et la démarche à long terme de sensibilisation, cet atelier permet aux participants de s'identifier et donc de pouvoir réfléchir aux propres démarches mises en œuvre dans leur organisation d'origine. Cela permet également, par la suite, de choisir ou de créer des contenus de sensibilisation qui vont être particulièrement adaptés à la démarche choisie, plutôt que de construire une démarche a posteriori en fonction des ressources disponibles.

Les retours des participants, et l'enthousiasme qu'ils ont mis durant les différents ateliers, montrent que cet exercice est utile et intéressant à mettre en œuvre. Après une phase de démarrage qui prend quelques minutes d'explication, le temps que chacun comprenne bien le cadre de réflexion et ce qui est attendu, les groupes se prennent au jeu et vont permettre une mise en commun d'avis et de retours d'expériences qui alimentent la construction de la démarche de sensibilisation.

La restriction de l'atelier à deux petits groupes de 5 à 6 personnes, si possible en situation de management dans leur entité (publique ou privée), permet un réel échange d'idées et d'informations, en laissant à chacun la place de s'exprimer.

L'animateur-trice de l'atelier doit avoir à cœur de ne pas laisser un groupe s'enliser dans une réflexion stérile ou un monopole de parole par un intervenant, afin de s'assurer que chaque groupe ait pu avancer au maximum pendant le temps imparti.

La phase de restitution finale est très importante et il faut y consacrer un temps significatif, d'abord pour que chaque groupe puisse restituer sa réflexion, mais aussi pour permettre l'échange entre chaque groupe (pourquoi tel choix, qu'est-ce qu'il y a derrière comme réflexion), et l'enrichissement par l'animateur-trice avec des idées, des pratiques, des suggestions qui n'auraient pas été identifiées par les groupes. Lors des ateliers organisés avec le Tour de France de la Cybersécurité en 2019, cette phase de restitution durait entre 30 et 45 minutes.

L'intérêt de ce type d'atelier de sensibilisation réside non pas dans la somme de connaissances qui va être apportée de façon descendante vers les participants, mais bien dans la discussion collective qui a lieu et qui invite chaque participant à la réflexion. Cette réflexion est ancrée dans des situations réelles et guidée par une fiche de progression qui permet aux groupes d'avancer concrètement de l'analyse d'une situation initiale aux solutions pratiques.

À l'heure où les contenus et solutions clés en main de sensibilisation foisonnent, cette démarche de réflexion collective et d'adaptation à son environnement de terrain est proposée pour aider les personnes en situation de responsabilité à exercer leur faculté de choix et de décision avec une méthodologie progressive.

Il serait bien entendu intéressant de pratiquer en situation réelle, et sur un temps plus complet, cette démarche auprès d'une entité publique ou privée de taille moyenne comme il est question dans cet atelier, afin de pouvoir faire un retour d'expérience plus complet et précis sur ce type de méthodologie.