Points clé présentation prévention cyber

par Sébastien Leroy
Référent Cybersécurité Région de Gendarmerie IDF

Dans un premier temps, outre le constat numérique, j'attire votre attention sur la lutte contre le cyber harcèlement. En parler, c'est commencer à agir. Pour cela, voici quelques réflexes à avoir :

- Ne pas répondre aux provocations
- Bloquer les auteurs des messages indésirables
- Signaler les comptes concernés aux plateformes où les faits ont lieu
- Conserver les preuves des messages reçus (captures d'écran, e-mails)
- Solliciter l'aide et le soutien de proches ou d'une association
- Déposer une plainte si nécessaire
- Protéger ses informations personnelles

Dans le même esprit, les mineurs sont de plus en plus victime d'atteinte numérique. Les spécialistes s'accordent à dire que les écrans sont nocifs au développement de l'enfant. Raison pour laquelle, ils conseillent les éléments suivants :

Avant 3 ans	pas d'écran
Avant 6 ans	usage limité avec un adulte
Avant 13 ans	pas de téléphone connecté à Internet
À partir de 15 ans	Usage autorisé des réseaux sociaux

En ce qui concerne les risques liés à Internet, il est important d'en parler avec son enfant. De la même façon que vous lui apprenez à évoluer dans l'espaces publics et dans la vie (traverser la rue, respecter les autres, ne pas faire confiance à n'importe qui, ...), vous devez informer et sensibiliser votre enfant aux différents risques de l'internet. Oui, Internet est également un espace public. Pour protéger votre enfant, utilisez un contrôle parental sur les appareils qu'il utilise. Ce n'est par pour le surveiller ou pour lui interdire de faire des choses, c'est pour le protéger. Surveillez son usage des messageries ou autres applications telles que les jeux (achats in-app, messagerie interne,…). Si vous ou votre enfant avez besoin d'aide, vous pouvez consulter le site internet de e-enfance (3018) https://e-enfance.org/. Celui-ci accompagne les jeunes, les parents et les professionnels sur toutes les problématiques liées au numérique, ses usages, ses dangers potentiels et ses conséquences sur la santé. Enfin, voici quelques conseils à destination de votre enfant :

- Réfléchir avant d'envoyer un message ou de publier une photo

- Garder sa vie privée, privée. Internet espace public
- Bien choisir ses amis sur les réseaux sociaux
- Ne pas partager ses identifiants MDP
- Ne communiquer qu'avec des personnes que l'on connait vraiment

Prévention cyber au profit des professionnels :

En qualité de dirigeant, vous êtes responsable de votre système d'information et vous êtes tenus de connaître les exigences légales et réglementaires applicables à votre organisation et être capable d'apprécier son niveau de conformité. Cette responsabilité est accentuée par les réglementations actuelles (RGPD, NIS2, LPM, etc…).

Pour vous aider à mieux comprendre et appréhender ce risque et plus particulièrement en cas d'utilisation d'un traitement de données à caractère personnelle, vous pouvez consulter l'ensemble des documentations disponibles sur le site de la CNIL à l'adresse suivante : https://www.cnil.fr/.

Bien s'entourer, c'est avoir un DSI, un RSSI et un DPO à ses côtés ou vous pouvez également confier cette activité à une entreprise extérieure.

Aujourd'hui, la réponse des organisations face au risque numérique figure parmi les enjeux les plus stratégiques. Il est donc primordial de bien identifier les valeurs métiers et les biens les plus critiques de votre écosystème.

Le facteur humain est l'un des leviers d'action privilégiés par les attaquants. Il est donc essentiel de l'inclure dans sa stratégie de sécurité numérique. Pour y parvenir, sensibilisez vos collaborateurs et fixez les règles d'utilisation du système d'information et les responsabilités de chacun par la mise en place d'une charte.

Aussi, l'élaboration d'un plan de continuité d'activité (PCA) a pour objet de décliner la stratégie et l'ensemble des dispositions qui sont prévues pour garantir la continuité de ses activités à la suite d'un sinistre ou d'un évènement perturbant gravement son fonctionnement normal. Pour être pertinent, le PCA prend appui sur l'étude des pires scénarios. Il constitue un chapitre essentiel de la politique de sécurité de votre entreprise.

Face à une attaque cyber, pour redémarrer les applications et les processus métiers le plus rapidement possible, la mise en place d'un plan de reprise d'activité (PRA) peut s'avérer très utile. Pour cela, il doit être revu, challengé et enrichi à intervalles réguliers pour rester efficace.

Enfin, des conseils qui serviront à tous, Il faut :

- Adopter une politique de mot de passe rigoureuse
- Sauvegarder ses données régulièrement
- Faire ses mises à jour régulièrement

- Se protéger des virus et autres logiciels malveillants
- Évitez les réseaux Wifi publics ou inconnus
- Bien séparer ses usages professionnels et personnels
- Éviter de naviguer sur des sites douteux ou illicites et être vigilant lors du téléchargement d'un fichier
- Contrôler les permissions des comptes utilisateurs
- Être vigilant sur les liens ou les pièces jointes contenus dans des messages électroniques
- Faire attention aux informations personnelles ou professionnelles que l'on diffuse sur Internet

Comment réagir dans le cas où un acteur malveillant souhaite faire de vous sa victime ? Dans un premier temps, ne communiquez jamais d'information sensible. Au moindre doute, contactez directement l'organisme concerné pour confirmer que c'est bien lui qui vous a contacté. Si vous subissez une attaque par rançongiciel, déconnectez du réseau les ordinateurs ou autres matériels infectés. Ne les éteignez pas afin de conserver les traces pour l'enquête. Alertez immédiatement votre support technique. Ne payez jamais la rançon. Déclenchez votre plan de gestion de crise. Et déposez plainte.

Transition toute trouvée, abordons maintenant le dépôt de plainte. Tout d'abord, il existe une idée reçue qui demeure dans la pensée collective : déposer plainte pour des actes de cybermalveillance ne sert à rien. C'est faux ! En effet, pour la victime d'une cyberattaque ou d'une atteinte cyber, le fait de déposer plainte lui permet d'être reconnue comme victime et faire valoir ses droits. Elle est accompagnée à la suite d'une cyberattaque. Cet acte permet de fournir des informations sur les faits dont elle est victime. Si elle est couverte par une police d'assurance, le dépôt de plainte permet d'activer le processus d'indemnisation. Dans le cas où les auteurs des faits sont identifiés, la victime pourra être indemnisée et récupérera ses données chiffrées. Pour les services de police et de Gendarmerie, le dépôt de plainte, oriente l'action des enquêteurs et favorise les recoupements. Ce qui permet de disposer d'une vision plus précise de l'état de la menace et d'augmenter le taux d'élucidation. Par la suite nous pouvons sensibiliser la population aux cybermenaces. Pour le dépôt de plainte et le signalement, rendez-vous sur www.masecurite.interieur.gouv.fr.

Pour terminer, n'oubliez pas que la cybersécurité est l'affaire de tous. La présentation de la conférence sur la cybersécurité de sucy-en-Brie se base sur le Rapport Annuel sur la Cybercriminalité (RACY) du commandement du ministère de l'Intérieur dans le cyberespace (COMCYBER-MI) que vous trouverez à l'adresse suivante : https://www.gendarmerie.interieur.gouv.fr/gendinfo/actualites/2024/premier-rapport-annuel-sur-la-cybercriminalite-racy.

Restez vigilant !