Soutien aux enquêtes sur les cyberincidents – Questions des forces de l'ordre aux victimes

Les questions suivantes doivent être posées aux entreprises ou aux plaignants qui ont été victimes d'une atteinte à la protection des données, lorsqu'un paiement est demandé en échange de la restauration des données chiffrées ou d'une promesse de ne pas divulguer les données volées.

Chaque incident est unique, mais les réponses à ces questions aideront les forces de l'ordre à mener leur enquête criminelle.

La personne qui répond aux questions doit avoir une connaissance directe de l'incident et des mesures prises face à celui-ci.

Plus les réponses seront fournies rapidement, plus les forces de l'ordre seront en mesure de déterminer le ou les auteur(s) de l'incident.

Remarque importante : le contexte et la justification des renseignements demandés dans les questions qui suivent sont présentés en ANNEXE, à la fin du présent document. Ce document vise à fournir à l'agent d'application de la loi qui pose les questions et à l'organisation qui y répond une compréhension commune des raisons pour lesquelles ces questions sont posées et de la façon dont les renseignements recueillis appuieront les mesures d'application de la loi visant à réduire la cybercriminalité.

RENSEIGNEMENTS SUR LE SIGNALEMENT, PREMIÈRE ÉTAPE (des sections peuvent être laissées vides au besoin)

A. Renseignements sur le plaignant ou la personne qui signale l'incident

1. En tant que personne ayant signalé l'incident, êtes-vous la personne-ressource principale des forces de l'ordre pour les discussions futures concernant cet incident?

i. Si non, qui est la personne-ressource principale avec qui les forces de l'ordre pourront faire un suivi concernant cet incident?

2. Coordonnées de la personne-ressource principale :

i. Nom

ii. Rôle ou titre professionnel (si elle a un lien avec l'organisation touchée par l'incident)

iii. Numéro de téléphone et adresse de courriel

3. Y a-t-il des préoccupations en matière de confidentialité que vous aimeriez soulever en lien avec le signalement de cet incident (c.-à-d. des préoccupations qui vous touchent personnellement ou professionnellement ou qui sont susceptibles de compromettre votre sécurité)?

4. Quel est votre lien avec l'incident signalé?

B. Renseignements sur la victime de l'incident

1. Quel est le nom officiel de l'organisation victime de l'incident signalé?

2. Quelle est l'adresse de l'organisation victime?

3. Quel est le lieu physique où s'est produit l'incident (par exemple, l'endroit où se trouvent les serveurs touchés)?

4. L'organisation victime est-elle présente physiquement ailleurs au Canada et/ou dans le monde?

C. Renseignements clés décrivant l'incident

1. Veuillez fournir, au meilleur de vos connaissances à ce stade, une description générale des répercussions de l'incident sur les activités de votre organisation.

2. Veuillez décrire la chronologie de l'incident, depuis le moment où vous (ou l'organisation) avez eu connaissance de l'incident jusqu'à aujourd'hui, en mentionnant tout élément que vous jugez pertinent pour expliquer le contexte.

3. Y a-t-il des conséquences importantes liées à cet incident qui devraient être prises en compte immédiatement (p. ex. menaces pour la sécurité publique, conséquences financières, conséquences sur la chaîne d'approvisionnement en aval et/ou conséquences sur les infrastructures et les services essentiels)?

D. Renseignements sur l'auteur de la menace (peut être laissé vide si ces renseignements ne sont pas encore connus)

1. À votre connaissance, y a-t-il eu une communication entre l'auteur de la menace associé à cet incident et un ou des représentant(s) de l'organisation, y compris vous-même?

2. **S'il n'y a pas de communication connue avec l'auteur de la menace :** compte tenu de la nature de l'incident, et en supposant qu'il n'y a pas de communication connue à ce jour, si une personne ou une division de l'organisation est susceptible d'avoir rencontré l'auteur de la menace ou d'avoir communiqué avec lui, pourriez-vous fournir le nom et les coordonnées de dette personne?

3. **S'il y a eu une communication avec l'auteur de menace :**
   i. Quand et comment cette communication s'est-elle produite pour la première fois?

ii. Y a-t-il eu plusieurs communications?

iii. Avec qui ces communications ont-elles eu lieu?

iv. Savez-vous s'il y aura d'autres communications dans le futur?

E. Autres renseignements sur l'incident qui n'ont pas encore été fournis

1. Y a-t-il des renseignements relatifs à l'incident qui n'ont pas encore été mentionnés et qui seraient, selon vous, importants pour les forces de l'ordre à ce stade?

F. Renseignements sur les personnes-ressources principales d'autres parties concernées

1. Savez-vous si d'autres parties externes de votre organisation ont été jointes en lien avec cet incident (p. ex. un cabinet d'avocats, un conseiller en matière d'atteinte à la vie privée, un fournisseur tiers de services de réponse aux incidents cybernétiques, le Centre canadien pour la cybersécurité, une compagnie d'assurance, une banque, etc.)?