De l'action
A la Negociation.

Le lundi de la Cybersécurité du mois d'octobre a été marqué par l'intervention **d'Olivier HERISSON**, ancien Officier de Police, aujourd'hui Manager en sécurité numérique chez EY. Il a choisi de s'exprimer sur le vol des données et le ransomware, en répondant, en particulier, aux deux questions qui suivent : ***« pourquoi et comment négocier avec un hacker ? »***

Crédit photographique : © Gérard Peliks.

Propos liminaire

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) définit le ransomware ou le rançongiciel comme : « *une technique d'attaque courante de la cybercriminalité* » qui « *consiste en l'envoi à la victime d'un logiciel malveillant qui chiffre l'ensemble des données et lui demande une rançon en échange d'une clé de déchiffrement* »[1].

Outre la question des données à caractère personnel, il s'agit donc d'une atteinte à **la disponibilité** (garantir l'accès à un service ou à des ressources dans un temps acceptable), à **la confidentialité** (s'assurer que seules les personnes autorisées à en prendre connaissance le peuvent) ainsi qu'à **l'intégrité** (garantir que les données n'ont pas été modifiées par quelqu'un qui n'en avait pas le droit).

Il est, d'ores et déjà, rappelé que, s'acquitter de la rançon ne saurait constituer la garantie de récupérer tout ou partie des données.

In fine, céder au principe du chantage pourrait avoir pour conséquence d'encourager le développement de ces actes particulièrement malveillants à l'endroit de nos entreprises et/ou de toute autre forme d'organisation.

---

[1] https://www.ssi.gouv.fr/entreprise/principalesmenaces/cybercriminalite/rancongiciel/

Du droit pénal général au droit pénal spécial : une pluralité de qualifications pour ester en justice.

L'extorsion

Elle est définie à l'**article 312-1 du Code pénal** comme : « *le fait d'obtenir par violence, menace de violences ou contrainte soit une signature, un engagement, une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeur ou d'un bien quelconque. L'extorsion est punie de sept ans d'emprisonnement et de 100 000 euros d'amende* ».

En l'espèce, le ransomware s'apparente à une extorsion de fonds en ce que les données du système d'information sont monnayées par ceux qui les ont chiffrées contre le versement d'une somme d'argent.

Le chantage

Le procédé du rançongiciel pourrait s'apparenter à du chantage en ce qu'il cherche à « *obtenir, en menaçant de révéler ou d'imputer des faits de nature à porter atteinte à l'honneur ou à la considération* » d'une entreprise ou d'une personne, « *la remise de fonds, de valeur, ou de bien quelconque. Le chantage est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende* » (**article 312-10 du Code pénal**).

La demande de fonds sous contrainte

La qualification de demande de fonds sous contrainte pourrait être envisagée en ce qu'elle suppose de solliciter, en réunion (c'est-à-dire au moins deux personnes) et de manière agressive la remise de fonds (**article 312-12-1 du Code pénal**). « *Elle est punie de six mois d'emprisonnement et de 3 750 euros d'amende* ».

Le vol & le recel

Du fait de « « *la soustraction* » *frauduleuse de la chose d'autrui* » (de tout ou partie des données, même temporairement), le rançongiciel constitue un vol au sens de **l'article 311-1 du Code pénal.** Quant au recel, il pourrait trouver à s'appliquer dès lors que la personne aurait eu connaissance que la chose remise provenait d'un crime ou d'un délit (**article 321-1 du Code pénal**).

Les atteintes aux systèmes de traitement automatisé des données

La loi du 5 janvier 1988 dite loi « **Godfrain** » a instauré un dispositif répressif pour lutter contre la cybercriminalité, assurer la sécurité des systèmes d'information, et enfin, réprimer la fraude informatique.

Désormais sont sanctionnées **aux article 323-1 à 323-7 du Code pénal** certains comportements constitutifs de délits et liés à l'utilisation d'un outil informatique.

Précisons que sont prohibés :

- l'accès, le maintien dans un système de traitement automatisé de données ;
- l'entrave ou le faussement du fonctionnement d'un tel système ;
- l'extraction, la reproduction, la transmission, la suppression ou la modification frauduleuse des données qu'il contient.

A noter, enfin : la peine d'emprisonnement est de trois ans ; la peine d'amende est de **100 000** euros.

Les précieuses recommandations d'Olivier Herisson ...

... Et ce, à partir d'un exemple concret :

« Lundi matin, l'ensemble du réseau de votre entreprise est paralysé par un ransomware[2]. Vos bases de données (notamment celles des comptes clients), votre messagerie ainsi que l'ensemble de vos sauvegardes sont chiffrées.

Le hacker affiche sur les écrans son adresse email permettant de le contacter. Ainsi, vous avez 24h00 pour payer 100 bitcoins[3] ; passé ce délai, les données seront détruites ! ».

Un process en 5 étapes :

1 - Enquêter

2 - Alerter

3 - S'organiser

4 - Négocier

5 - Faire le bilan

[2] A noter : le malware est inconnu sur « *Nomoramsom* ».
[3] Soit environ **843 823 euros**.

1- **Analysez les logs** et vérifiez que l'attaquant n'est plus dans le système.

2- **Prévenez Cyber malveillance** [4], la Police/la Gendarmerie, l'ANSSI et la CNIL dans les 72h00.

3- **Mettez en place une cellule de crise** (la résilience) et identifiez clairement le rôle des différents acteurs :

- *« **le coordinateur** (centralise et communique les informations) ;*
- ***le négociateur** (est en général un informaticien ou un commercial qu'il conviendra de protéger) ;*
- ***le décideur** (il définit la stratégie, autrement dit l'intérêt à négocier, mais il ne négocie pas !) ;*
- ***le délégué à la protection des données** (DPO) (si l'incident constitue une violation des données à caractère personnel une analyse d'impact devra être réalisée)*[5] *;*
- ***les autres services** seront sollicités suivant la taille de la société (direction de la communication, direction financière, RSSI, DSI) »* et la direction juridique, serions-nous tentés d'ajouter.

4-

4.1 *« Pourquoi négocier ? »*

Nonobstant les réserves indiquées dans notre propos liminaire, divers arguments plaident en faveur de la négociation :

- *« contrôler les impacts sur le business ;*
- *gagner du temps* [6]*;*

---

[4] https://www.cybermalveillance.gouv.fr,

[5] Elle vise à déterminer les traitements de données personnelles qui sont susceptibles d'engendrer **un risque élevé** pour les droits et les libertés des personnes concernées. Dans l'hypothèse où le risque serait important, le DPO devra prévenir les personnes concernées par cette violation.

[6] Compter environ une dizaine de jours pour finaliser la négociation et récupérer l'ensemble des données.

- diminuer le montant de la rançon [7];
- récupérer les données ;
- minorer les impacts sur la vie privée ».

4.2 *« Comment négocier ? »*

Olivier Herisson a insisté sur le fait qu'il ne fallait ***« jamais sous-estimer le hacker ».***

Par ailleurs, il est préconisé d'adopter ***« une position basse »*** (*« ne pas s'arrêter aux mots »,* se méfier de l'effet narcissique qui pourrait faire monter les enchères), ***« de créer du lien avec le hacker »*** (lui poser des questions tout en évitant de lui donner des informations sur vous), et ce, afin de protéger le plus longtemps possible l'« intérêt » de l'organisation.

En outre, il est impératif de définir une stratégie, autrement dit, de « ***donner un mandat clair au négociateur*** ».

Aussi, et en substance, après avoir « *différencié* ***la position, l'objectif et l'intérêt »,*** vous devrez :

- *« coordonner ;*
- *décider ;*
- *gérer l'incident ;*
- *piloter la réponse (à incident) ;*
- *communiquer efficacement* »...

... Sans omettre de garder **les pièces** (notamment la main courante) qui sont essentielles à l'action policière et judiciaire.

5- Pour finir, ***« débriefez »*** (échangez sur le déroulement de l'incident, améliorer vos procédures afin de préserver votre structure, etc.) ***« en vue de capitaliser » !***

---

[7] Une demande de plus d'un million d'euros s'est terminée par une remise de 30 k €.

A titre de propos conclusifs :

En toute hypothèse, il conviendra de prévenir les autorités compétentes et, le cas échéant, (s'agissant en particulier de l'action pénale), de se faire accompagner /conseiller par un professionnel du droit.

alice.louis@netcourrier.com
MBA - Cybersécurité - Institut Léonard de Vinci