CONCOURS INTERNE DE TECHNICIEN TERRITORIAL
SESSION 2018

SPÉCIALITÉ « INGÉNIERIE, INFORMATIQUE ET SYSTÈMES D'INFORMATION »

ÉPREUVE DE RAPPORT

NOTE OBTENUE : 13,75 / 20

Techniville le 12 avril 2018

Direction des Systèmes d'Information

RAPPORT TECHNIQUE
A l'attention du Directeur des Systèmes d'Information

Objet : les attaques virales de type "Ronsomware"

L'arrivée d'internet dans le fonctionnement des citoyens, des entreprises et des administrations a entrainé une multiplication des échanges de données et d'information, ceci liés aux bouleversements dans les démarches et les procédures quotidiennes. En parallèle, cela a entraîné une multiplication des dangers liés aux virus informatiques. Les auteurs de ces virus ont ainsi la possibilité de toucher plusieurs milliers d'ordinateurs dans de nombreux pays en quelques jours, comme l'a montré la cyberattaque mondiale du 12 mai 2017. Celle-ci a été particulièrement marquante par son ampleur et sa spécificité, avec l'utilisation massive de virus de type "Ronsomware".

Etant concernées par ce phénomène, on peut se demander comment les collectivités territoriales peuvent lutter contre ce fléau de plus en plus menaçant.

Ainsi, après avoir expliqué le fonctionnement d'un ronsomware et ses enjeux associés (I), la seconde partie démontrera qu'une politique globale et transversale doit être nécessaire pour lutter efficacement contre ces attaques (II).

I – Les enjeux associés à la lutte contre une attaque de type ronsomware

Les enjeux de la lutte contre une attaque virale de type ronsomware étant importants (2), il est important d'en comprendre précisément la nature (1).

1) Un ronsomware, c'est quoi ?

Leronsomware est un virus informatique. Il s'agit d'un logiciel malveillant cryptant les données qui ont été infectées, et demandant ensuite une rançon en échange du code permettant de les décrypter. Si le code n'est pas renseigné, alors il n'est plus possible de consulter ou récupérer les données. Certains ronsomware peuvent avoir une nature un peu différente, comme une demande de régularisation d'une amende policière, ou la nécessité de devoir cliquer sur de nombreuses publicités, action rémunératrice pour l'auteur du virus.

Ces logiciels ne sont pas nouveaux. En effet, le premier date de 1989, mais aujourd'hui, leur nombre ne cesse d'exploser avec 120 000 nouveaux ronsomware au second trimestre 2012, soit quatre fois plus que l'année précédente. Ces rançongiciels se propagent de deux façons. Soit ils pénètrent l'ordinateur via un document ou un lien dans un mail (par exemple Locky), soit ils se propagent via des failles dans la sécurité des systèmes informatiques permettant le partage de fichiers (Warnacry ou Notletya par exemple).

Aujourd'hui, leur utilisation est en pleine expansion. En 2016, il y avait une attaque de type ronsomware toutes les deux minutes ; à la fin de l'année,il y en avait toutes les 40 secondes dans le monde. Aux Etats-Unis, il aurait été extorqué environ 209 millions de dollars de cette façon au premier trimestre 2016.

2) Enjeux et objectifs de la lutte contre les ronsomwares

Comme l'a montré la cyberattaque mondiale du mai 2017, tout le monde peut être touché : l'Etat, les entreprises, les collectivités, tout le monde est concerné. Certaines usines ont été mises à l'arrêt en Allemagne, des banques ukrainiennes ont du arrêter certains services : chacun doit prendre conscience du phénomène. Ça peut également toucher les collectivités, comme une commune restée anonyme, en février 2017. L'enquête suppose que ça pourrait venir d'une personne hostile à certaines décisions locales.

La lutte contre les ronsomwares répond à deux enjeux principaux. Il faut tout d'abord pouvoir récupérer le contrôle sur son propre système et ses propres donnés afin de relancer un fonctionnement normal. Il s'agit d'une problématique évidente pour les services de santé par exemple. Egalement, il faut lutter contre la fuite des donnés à caractère personnel que toutes les entreprises ou administrations conservent. La capacité à réagir en cas d'attaque est donc très importante.

Dans ce contexte, l'entrée en vigueur du RGPD rédigé par l'Union Européenne, fournit un cadre aux entreprises et administrations pour éviter les intrusions et pour pouvoir intervenir au cas où. Elles doivent ainsi se mettre en conformité avec ce document juridique afin de ne pas être mises en demeure pour une violation de données à caractère personnel, qu'elle soit accidentelle ou illicite par un tiers.

Une fois cernés les enjeux de la lutte contre une attaque virale de type ronsomware, il convient de voir concrètement comment une collectivité peut lutter contre ce phénomène.

II – <u>Une politique globale et transversale doit être nécessaire pour une lutte efficace</u>

Une politique globale d'établissement ne peut être efficace (1) que si elle obéit à un dicton : "Mieux vaut prévenir que guérir" (2).

1) Une démarche globale et transversale

Pour une prise en compte optimale des enjeux par tous les agents, il doit y avoir la mise en place d'un véritable projet d'établissement, soutenu par les élus, la direction et les représentants des salariés. Le problème peut arriver dans tous les services, à tous les niveaux hiérarchiques : le projet doit donc être transversal.

Une fois un diagnostic réalisé, une charte informatique peut être mise en place afin que les agents aient à disposition un résumé de la politique générale de sécurité de l'établissement. En parallèle, des référents "Sécurité des Systèmes d'Information" peuvent être définis par direction afin de faire le relais entre le personnel et le Responsable SSI.

La définition de postes sensibles (Ressources Humaines, direction Mobilités, Etat Civil par exemple) peut être importante afin que ces services là puissent bénéficier dune prévention accrue.

En parallèle de toutes ces démarches, il y a une véritable politique de sécurisation informatique à mener, avec l'équipement de personnels et de matériels dédiés à cette fonction ;

Au bout de quelques temps de mise en place, cette politique de sécurisation informatique devra être évaluée et testée, afin d'anticiper le nouvelles attaques plus évoluées.

2) Mieux vaut prévenir que guérir

Concrètement, les services de sécurité informatique doivent faire en sorte de prévenir toute attaque virale de type "ronsomware", plutôt que de devoir difficilement essayer de récupérer leurs données.

Ainsi, la première étape est de réaliser des sauvegardes des données sur des supports non connectés à internet : une récupération de données sera moins pénalisante si elle doit se faire sur des données datant de la veille.

Ensuite, il s'agit de protéger au maximum le système informatique de toute intrusion de virus via les documents ou le réseau. Des logiciels antivirus performants sont à préconiser, ainsi que des protections type proxy ou firewalls sur l'accès internet. Il peut être également intéressant de distinguer des serveurs relais des serveurs de données, créant une protection supplémentaire. Les identifiants de chaque utilisateur doivent enfin être robustes et difficilement trouvables.

La troisième étape est de mettre à jour, autant que faire se peut, tous les logiciels afin d'éviter de laisser des failles informatiques exploitables par les virus.

Enfin, l'action sûrement la plus importante est de faire de la prévention envers les utilisateurs afin qu'ils aient sans cesse les risques en tête lorsqu'ils naviguent sur internet ou manipulent leur boîte mail. La messagerie professionnelle étant la première porte d'entrée pour les attaques virales, ils doivent être prévenus sur son utilisation. Sensibiliser par des jeux ou en faisant un parallèle avec les bonnes pratiques à adopter dans leur vie personnelle peut être une bonne méthode.