Cybercriminalité : nous devons prendre la mesure du défi !

Par ***mogirard***
Créé le ***16/06/2017 - 00:00***

Edito : Cybercriminalité : nous devons prendre la mesure du défi !

Jeudi, 15/06/2017 - 23:00 0 commentaire

- Diminuer la police
- Augmenter la police
- Imprimer
- Version PDF

-
- Tweeter
-
-

4 avis :

zoom

La cyberattaque qui a déferlé sur le Net le 12 mai dernier restera certainement dans les annales à cause de la rapidité de sa propagation et des dégâts très concrets qu?elle a provoqués, tant au niveau des institutions publiques que des entreprises. Cette attaque a utilisé un « rançongiciel » (ransomware) c?est-à-dire un malware, baptisé WannaCry, qui chiffre les fichiers d'un ordinateur. Il rend ceux-ci inaccessibles et exige une rançon pour les déchiffrer. S'agissant de cette attaque, la rançon exigée était de 300 dollars, payable en Bitcoin (monnaie numérique). En cas de non-paiement, la rançon était doublée sous trois jours et si la rançon n'était toujours pas payée au bout d'une semaine, les fichiers étaient purement et simplement effacés, avec toutes les conséquences qu'on imagine pour les institutions, services public et entreprises concernées.

Près de 200 000 ordinateurs ont été touchés dans 150 pays, principalement en Europe et en Asie. Cette attaque, sans précédent, a entraîné un véritable chaos dans le service national de santé britannique qui s?est retrouvé sans accès à ses données et a été contraint d?annuler de nombreux rendez-vous. En France, de grandes entreprises comme Renault ont subi de plein fouet cette attaque et ont dû fermer des

sites de production, ce qui a entraîné des pertes d'exploitation considérables et la mise au chômage technique de 5000 employés.

La spécificité de cette attaque réside dans le fait qu'elle a exploité une vulnérabilité de Windows en utilisant des outils de la NSA, l'agence de renseignement électronique des Etats-Unis. Au lieu d'avoir recours à des emails frauduleux, cette attaque a ciblé, pour contaminer ses victimes, le protocole SMB (Server Message Block), utilisé jusqu'à Windows 8. Dans les attaques "classiques", la victime installe à son insu un "rançongiciel" en ouvrant une pièce jointe corrompue, comme un document Word ou PDF. Mais WannaCry est plus vicieux, car même si l?utilisateur prend la précaution de ne pas ouvrir des pièces jointes corrompues, il peut néanmoins ,une fois installé sur un premier ordinateur, contaminer en chaîne d'autres machines connectées, via un réseau local.

De manière étonnante, la vulnérabilité du protocole SMB utilisé par WannaCry pour se propager a initialement été découverte par la NSA, l?Agence de Sécurité américaine. Fait encore plus surprenant, la NSA n?a pas révélé cette faille, baptisée "EternalBlue", à Microsoft, préférant l?utiliser pour son propre compte. Mais, dans des circonstances pour le moins troubles et qui devront être élucidées, la NSA s?est fait pirater et EternalBlue s?est alors retrouvé en avril dernier dans les mains d?un groupe de pirate, les Shadowbrokers. Entretemps, Microsoft avait comblé cette faille mais cette parade arrivait trop tard car de nombreux logiciels malveillants intégrant EternalBlue étaient déjà en circulation sur le Net, infectant des centaines de milliers de machines tournant sous d?anciennes versions de Windows non mises à jour, soit par négligence, soit parce que Microsoft avait tout simplement cessé de proposer ces mises à jour pour inciter ses clients à acheter des versions plus récentes de Windows?.

On ne le répétera jamais assez, si de telles attaques sont si dévastatrices, c'est d'abord parce que la plupart des utilisateurs, qu'il s'agisse de particuliers ou d'entreprises, considèrent la question de la sécurité informatique comme mineure et voient dans la mise à jour de leur système une perte de temps. Face à cette réalité, Microsoft a décidé d'employer les grands moyens et, depuis Windows 10, la firme ne laisse plus le choix aux utilisateurs de repousser sans cesse une mise à jour. Dans le monde de l'entreprise, la situation n'est pas meilleure car celles-ci sont souvent liées par des contrats qui les empêchent de changer de système ou de logiciels pour des équipements spécialisés, comme des outils d'imagerie médicale par exemple.

Cette cyberattaque du 12 mai dernier aurait pu avoir des conséquences bien plus dévastatrices si un jeune Britannique n?avait pas, presque par hasard, ralenti sérieusement la propagation de ce virus en achetant « par réflexe » un simple nom de domaine. En outre, trois spécialistes français, Adrien Guinet, Matthieu Suiches et Benjamin Delpy - ?directeur de Projets Sécurité à la Banque de France, ont réussi à développer deux programmes, WannaKey et WannaKiwi, permettant aux victimes de déverrouiller l?accès à leurs données, sans payer la rançon. Disponible librement, ce logiciel peut être téléchargé et installé facilement et fonctionnerait dans 60 % des cas pour les machines tournant sous Windows XP. En revanche, sous Windows 7, le taux de réussite ne serait que de 10 %. Au final, même si des chiffres contradictoires circulent, il semblerait que peu d'utilisateurs touchés aient payé la rançon exigée, ce qui est une bonne nouvelle car céder immédiatement aux exigences des pirates ne peut que les encourager à réitérer ce type d'attaque. Il n'en demeure pas moins vrai que cette cyberattaque a causé des dégâts humains et économiques, directs et "collatéraux", très importants, bien que difficilement évaluables.

Rappelons que, selon une enquête internationale du cabinet PWC, la cybercriminalité aurait coûté 3,36 milliards d'€ aux entreprises en 2015 et toucherait les deux tiers des entreprises. Ce coût, qui était estimé à 1,7 milliard d?euros en 2011 aurait donc doublé en seulement quatre ans?Au niveau mondial, ce coût serait de 327 milliards d?euros (environ 0,6 point du Produit Brut Mondial), selon le Center for Strategic

and International Studies (CSIS). Face à un tel fléau, le directeur des affaires juridiques de Microsoft appelle donc tous les gouvernements à se réveiller après cette attaque et à "adhérer dans le cyberespace aux mêmes règles qui sont appliquées pour les armes dans le monde réel".

Réunis à Bari, en Italie, le 13 mai dernier, les ministres des Finances de l?Union européenne ont publié un communiqué commun dans lequel on peut notamment lire "Nous reconnaissons que les cyber incidents représentent une menace croissante pour nos économies et qu'une politique de réponses appropriées pour l'ensemble de l'économie est nécessaire". Mais ces bonnes intentions et ces déclarations de principe ne suffisent plus et il faut à présent, si nous voulons éviter une catastrophe numérique planétaire de grande ampleur dont les dommages pour l?économie mondiale seraient autrement plus graves que celle de « WannaCry », prendre ce problème à bras le corps.

La première mesure qui doit être prise concerne la mise en ?uvre plus vigoureuse et plus complète de la Convention de Budapest sur la cybercriminalité, signée en 2001. Cette Convention qui rassemble 67 états (dont 55 ont ratifié le texte) s?est donnée comme objectif de poursuivre une politique pénale commune destinée à protéger la société contre le cybercrime, notamment par l'adoption d'une législation appropriée et la stimulation de la coopération internationale. Cette convention prévoit également des procédures spécifiques de lutte contre le piratage informatique concernant la perquisition de réseaux informatiques et l'interception de données numériques. La France et l'Union européenne doivent intensifier leurs efforts politiques et diplomatiques pour qu'elle soit signée et ratifiée par le plus grand nombre de pays possibles.

La deuxième mesure concerne la responsabilité des entreprises qui doivent absolument cesser de sous-estimer cette menace et engager des moyens de prévention et de lutte à la hauteur des dommages qu?elles risquent. Cette lutte contre la cybercriminalité exige, il est vrai, des moyens importants qui ne sont pas toujours à la portée des petites et moyennes entreprises. C?est d?ailleurs pourquoi, bien que neuf Pme sur dix soient conscientes des risques de piratage et de fraude informatique, plus de la moitié ne prennent aucune mesure de protection contre la cybercriminalité. Autre indicateur révélateur : on estime que seule une entreprise sur six dispose d?un Centre Opérationnel de Sécurité (SOC) leur permettant de détecter les cyber-attaques et a souscrit une assurance couvrant les cyber-risques, ce type d?assurance étant généralement jugée trop complexe.

Pourtant, dans la plupart des cas, il suffit de prendre quelques précautions de bon sens pour prévenir la grande majorité des cyberattaques, comme vient de le rappeler la CGPME (Confédération générale des petites et moyennes entreprises) et l?Anssi (Agence nationale de la sécurité des systèmes d'informations), qui ont publié en ligne un petit guide contenant 12 règles anti-piratage (www.ssi.gouv.fr). Mais, face à l?extension de cette forme de criminalité, les entreprises doivent également accepter le principe d?une mutualisation de leur sécurité informatique, ce qui passe par l?externalisation qui seule permet d?accéder aux meilleures capacités et compétences face aux nouvelles cyber-menaces.

On pourrait également imaginer que l?Etat, par le biais de ses différents services centraux et décentralisés, puisse proposer gratuitement aux entreprises, sans que celles-ci aient besoin d?en faire la demande, des « kits de protection » informatique et que des déductions fiscales spécifiques soient prévues pour les entreprises qui dépassent un certain niveau de dépenses (par rapport à leur chiffre d?affaires) pour renforcer leur sécurité informatique.

La troisième mesure qui me semble indispensable pour éviter que la cybercriminalité ne devienne incontrôlable est la création d?une agence européenne de lutte contre la criminalité numérique, dont le financement serait assuré conjointement par les états-membres, les grandes entreprises du secteur informatique et électronique et une taxe sur les échanges de certaines données informatisées. Cette

agence, qui travaillerait en étroite collaboration avec les meilleurs laboratoires de recherche publics de privés d?informatique et de mathématiques, aurait pour mission le mise aux points d?outils et de solutions innovantes, recourant notamment à l'intelligence artificielle, pour permettre une détection précoce des différents types de cyberattaque et la mise en ?uvre immédiate de parades et contre-mesures efficaces en cas d'attaque.

Enfin, la dernière mesure qui s?impose concerne la refonte et l?adaptation de notre cadre juridique et pénal, tant sur le plan national et européen. Il faut bien comprendre que le calcul des pirates informatiques est assez simple : comparée à la criminalité « classique », concernant les biens et les personnes, la cybercriminalité est bien moins risquée et rapporte beaucoup plus. Face à cette équation, il faut changer de raisonnement et instaurer une échelle des peines qui soit aussi dissuasive et répressive que celle en vigueur pour les crimes physiques et les atteintes aux personnes et aux biens. Si un cybercriminel en puissance sait qu?il risque, non pas un an de prison avec sursis, mais 5 ou 10 ans de prison ferme et la saisie immédiate de tous ses biens, y compris ceux acquis à travers des "prête-noms" (comme cela est à présent le cas en France pour les chefs d'organisations criminelles ou les trafiquants de drogue), on peut parier qu?il y réfléchira à deux fois avant de passer à l?acte?

La cybercriminalité est devenue un fléau économique et financier pour nos sociétés mais elle pourrait demain, si nous ne réagissons pas avec assez de vigueur, provoquer des milliers de morts, si une organisation criminelle parvenait à prendre le contrôle informatique d?installations sensibles, comme certaines usines chimiques, des centrales nucléaires ou encore des systèmes de transports. Ne rêvons pas : quels que soient nos efforts et notre détermination, nous n'éliminerons jamais complétement le piratage informatique qui a trouvé, avec le fulgurant développement d'Internet un extraordinaire vecteur de développement. Mais face à cette menace majeure, qui ne relève plus du tout de la science-fiction, notre Pays doit mobiliser l?ensemble de ses forces vives et de ses responsables politiques, économiques, scientifiques pour mettre un coup d?arrêt à cette criminalité numérique et apprendre à mieux prévenir à la source ces cyberattaques de plus en plus sophistiquées, de manière à en limiter les effets dévastateurs et à empêcher qu'un jour ne survienne une catastrophe numérique majeure au niveau planétaire.

René TRÉGOUËT

Sénateur honoraire

Fondateur du Groupe de Prospective du Sénat

Noter cet article :

Recommander cet article :

-
- Tweeter
-

- **Nombre de consultations :** 1229
- **Publié dans :** Internet
- **Partager :**
  - Facebook
  - Viadeo

- Twitter
- Wikio

Internet administrations attaques Bitcoin convention crimes cybercriminalité entreprises EternalBlue exploitation hôpitaux intelligence internet logiciel loi machines malwares mémoire Microsoft NSA numérique peines piratage porte programme protocole rançon rançongiciel réseau résolution Shadowbrokers système usines virus WannaCry WannaKey Windows

---

URL source: https://www.rtflash.fr/cybercriminalite-nous-devons-prendre-mesure-defi/article