Collectes massives et illégales par le Renseignement allemand

Collectes massives et illégales par le Renseignement allemand

Après avoir réalisé un contrôle sur place des services de renseignement, la Cnil allemande a dressé un bilan extrêmement critique des activités du Bundesnachrichtendienst (BND) en matière de collecte d'informations sur Internet.

Le site Netzpolitik a dévoilé le contenu d'un rapport jusque là confidentiel produit en juillet 2015 par Andrea Voßhoff, le commissaire à la protection des données en Allemagne, qui accable les services de renseignement allemands. Le rapport a été réalisé après la visite de l'homologue de la Cnil dans la station d'écoutes Bad Aibling, opérée conjointement en Bavière par l'agence allemande du renseignement, la Bundesnachrichtendienst (BND), et par la National Security Agency (NSA) américaine.
Malgré les difficultés à enquêter qu'il dénonce, Voßhoff dénombre dans son rapport 18 violations graves de la législation, et formule 12 réclamations formelles, qui obligent l'administration à répondre. Dans un pays encore meurtri par les souvenirs de la Stasi, le constat est violent.
L'institution reproche au BND d'avoir créé sept bases de données rassemblant des informations personnelles sur des suspects ou simples citoyens lambda, sans aucun mandat législatif pour ce faire, et de les avoir utilisées depuis plusieurs années au mépris total des principes de légalité. Le commissaire a exigé que ces bases de données soient détruites et rendues inutilisables.

Parmi elles figure une base assise sur le programme XKeyScore de la NSA, qui permet de réunir et fouiller l'ensemble des informations collectées sur le Web (visibles ou obtenues par interception du trafic), pour les rendre accessibles aux analystes qui veulent tout savoir d'un individu et de ses activités en ligne. Alors que XKeyScore est censé cibler des suspects, Voßhoff note que le programme collecte « un grand nombre de données personnelles de personnes irréprochables », et cite en exemple un cas qu'il a pu consulter, où « pour une personne ciblée, les données personnelles de quinze personnes irréprochables étaient collectées et stockées », sans aucun besoin pour l'enquête…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Le Renseignement allemand pris en flagrant délit de collectes massives illégales – Politique – Numerama

Directive sur la sécurité des réseaux et des systèmes d’information

	Directive sur la sécurité des réseaux et des systèmes d’information

Nos sociétés digitalisées reposent de plus en plus sur des réseaux électroniques qui peuvent faire l'objet de cyberattaques aux conséquences importantes. Afin de mieux faire face à ce type de menaces en ligne, le Parlement et le Conseil ont conclu en décembre dernier un accord sur les premières règles européennes en matière de cybersécurité. Celles-ci ont été soutenues par l'ensemble du Parlement réuni en session plénière ce mercredi 6 juillet.

Vols d'identité, faux sites web de banques, espionnage industriel ou inondation de données qui rendent un serveur incapable de répondre : les menaces en ligne sont nombreuses et visent tant les particuliers que les entreprises et les autorités publiques.

Les incidents et les attaques des systèmes d'information des entreprises et des citoyens pourraient représenter un coût de 260 à 340 milliards d'euros par an, selon les estimations de l'Agence européenne chargée de la sécurité des réseaux et de l'information.

Les cyberattaques menées contre certaines infrastructures clés de nos sociétés, comme les services bancaires, les réseaux d'électricité ou le secteur du contrôle aérien, peuvent avoir des conséquences particulièrement importantes sur notre quotidien.

Dans le cadre d'un Eurobaromètre publié en février 2015, les citoyens européens ont exprimé de fortes inquiétudes à propos de la cybersécurité : 89 % des internautes évitent de diffuser des informations personnelles en ligne. Selon 85 % des sondés, le risque d'être victime de cybercriminalité est de plus en plus important.

Vote en plénière

Les députés ont approuvé la directive sur la sécurité des réseaux et de l'information dans l'Union, qui définit une approche commune autour de la question de la cybersécurité.

Le texte prévoit une liste de secteurs dans lesquels les entreprises qui fournissent des services essentiels, liés par exemple à l'énergie, aux transports ou au secteur de la banque, devront être en mesure de résister aux cyberattaques.

La directive les oblige notamment à signaler les incidents de sécurité graves aux autorités nationales. Les fournisseurs de services numériques tels qu'Amazon ou Google devront également notifier les attaques majeures aux autorités nationales.

Ces nouvelles règles sur la cybersécurité visent également à renforcer la coopération entre États membres en cas d'incidents.

Téléchargez la directive sur la sécurité des réseaux et des systèmes d'information – texte approuvé par le Parlement et le Conseil :
http://data.consilium.europa.eu/doc/document/ST-5581-2016-REV-1/fr/pdf
Article original du Parlement Européen

Réagissez à cet article

Original de l'article mis en page : Cybersécurité : mieux faire face aux attaques en ligne

Rançongiciels : « Désormais, plus besoin de kidnapper vos enfants, on s’en prend à vos données »

	Rançongiciels : « Désormais, plus besoin de kidnapper vos enfants, on s’en prend à vos données »

Locky, TeslaCrypt, Cryptolocker, Cryptowall… Depuis plusieurs mois, les rançongiciels (« ransomware »), ces virus informatiques qui rendent illisibles les données d'un utilisateur puis lui réclament une somme d'argent afin de les déverrouiller, sont une préoccupation croissante des autorités. Le commissaire François-Xavier Masson, chef de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, une unité de la police spécialisée dans la criminalité informatique, explique au Monde les dangers de cette menace.

Combien y a-t-il d'attaques par rançongiciel en France ?
On ne le sait pas avec précision, nous n'avons pas fait d'étude précise à ce sujet. Statistiquement, le rançongiciel ne correspond pas à une infraction pénale précise et il recoupe parfois l'intrusion dans un système automatisé de traitement de données. Il faudrait affiner le cadre car nous avons besoin de connaître l'état de la menace.
Avez-vous quand même une idée de l'évolution du phénomène ?
L'extorsion numérique est clairement à la hausse, c'est la grande tendance en termes de cybercriminalité depuis 2013. Tout le monde est ciblé : les particuliers, les entreprises, même l'Etat. Les attaques gagnent en sophistication et en intensité. Il y a aussi une industrialisation et une professionnalisation. La criminalité informatique est une criminalité de masse : d'un simple clic on peut atteindre des millions de machines. Désormais, il n'y a plus besoin de vous mettre un couteau sous la gorge ou de kidnapper vos enfants, on s'en prend à vos données.
Les victimes ont-elles le réflexe de porter plainte ?
Certaines victimes paient sans porter plainte. Ce calcul est fait par les entreprises qui estiment que c'est plus pratique de payer la rançon – dont le montant n'est pas toujours très élevé, de l'ordre de quelques bitcoins ou dizaines de bitcoins – et qu'en portant plainte, elles terniront leur image et ne récupéreront pas nécessairement leurs données. Elles pensent aussi que payer la rançon coûtera moins cher que de payer une entreprise pour nettoyer leurs réseaux informatiques et installer des protections plus solides. C'est une vision de court terme. Nous recommandons de ne pas payer la rançon afin de ne pas alimenter le système. Si l'on arrête de payer les rançons, les criminels y réfléchiront à deux fois. C'est la même doctrine qu'en matière de criminalité organisée.
Qu'est-ce qui pousse à porter plainte ?
Chaque cas est unique mais généralement, c'est parce que c'est la politique de l'entreprise ou parce que le montant de la rançon est trop élevé.
Qui sont les victimes ?
Il s'agit beaucoup de petites et moyennes entreprises, par exemple des cabinets de notaires, d'avocats, d'architectes, qui ont des failles dans leur système informatique, qui n'ont pas fait les investissements nécessaires ou ne connaissent pas forcément le sujet. Les cybercriminels vont toujours profiter des systèmes informatiques vulnérables.
Quel est votre rôle dans la lutte contre les rançongiciels ?
La première mission, c'est bien sûr l'enquête. Mais nous avons aussi un rôle de prévention : on dit que la sécurité a un coût mais celui-ci est toujours inférieur à celui d'une réparation après un piratage. Enfin, de plus en plus, nous offrons des solutions de remédiation : nous proposons des synergies avec des entreprises privées, des éditeurs antivirus. On développe des partenariats avec ceux qui sont capables de développer des solutions. Si on peut désinfecter les machines nous-mêmes, on le propose, mais une fois que c'est chiffré, cela devient très compliqué : je n'ai pas d'exemple de rançongiciel qu'on ait réussi à déverrouiller.
Quel rapport entretenez-vous avec les entreprises ?
On ne peut pas faire l'économie de partenariats avec le secteur privé. Nous pourrions développer nos propres logiciels mais ce serait trop long et coûteux. Il y a des entreprises qui ont des compétences et la volonté d'aider les services de police.
Parvenez-vous, dans vos enquêtes, à identifier les responsables ?
On se heurte très rapidement à la difficulté de remonter vers l'origine de l'attaque. Les rançongiciels sont développés par des gens dont c'est le métier, et leur activité dépasse les frontières. On a des idées pour les attaques les plus abouties, ça vient plutôt des pays de l'Est. Mais pas tous.
Parvenez-vous à collaborer avec vos homologues à l'étranger ?
Oui, c'est tout l'intérêt d'être un office central, nous sommes le point de contact avec nos confrères internationaux. Il y a beaucoup de réunions thématiques, sous l'égide de l'Office européen de police (Europol), des pays qui mettent en commun leurs éléments et décrivent l'état d'avancement de leurs enquêtes. C'est indispensable de mettre en commun, de combiner, d'échanger des informations. Il peut y avoir des équipes d'enquête communes, même si ça ne nous est pas encore arrivé sur le rançongiciel.
De plus en plus d'enquêteurs se penchent sur le bitcoin – dont l'historique des transactions est public – comme outil d'enquête. Est-ce aussi le cas chez vous ?
C'est une chose sur laquelle on travaille et qui nous intéresse beaucoup. S'il y a paiement en bitcoin, il peut y avoir la possibilité de remonter jusqu'aux auteurs. C'est aussi pour cela que l'on demande aux gens de porter plainte même lorsqu'ils ont payé.
Article original de Martin Untersinger

Réagissez à cet article

Original de l'article mis en page : Rançongiciels : « Désormais, plus besoin de kidnapper vos enfants, on s'en prend à vos données »

Attention, le navigateur Maxhton espionne ses utilisateurs !

Attention, le navigateur Maxhton espionne ses utilisateurs !

Le navigateur Maxhton ne serait rien d'autre qu'un outil d'espionnage à la solde de la Chine ?

Des experts en sécurité informatiques de l'entreprise polonaise Exatel viennent de révéler la découverte de faits troublant visant le navigateur *Maxhton*. Ce butineur web recueille des informations sensibles appartenant à ses utilisateurs. Des informations qui sont ensuite envoyées à un serveur basé en Chine. Les chercheurs avertissent que les données récoltées pourraient être très précieuses pour des malveillants.

Les données des utilisateurs de Maxhton envoyées en Chine !
Et pour cause ! Les ingénieurs de *Fidelis Cybersecurity* et *Exatel* ont découvert que Maxthon communiquait régulièrement un fichier nommé ueipdata.zip. Le dossier compressé est envoyé en Chine, sur un serveur basé à Beijing, via HTTP. Une analyse plus poussée a révélé que ueipdata.zip contient un fichier crypté nommé dat.txt. Dat.txt stocke des données sur le système d'exploitation, le CPU, le statut ad blocker, l'URL utilisé dans la page d'accueil, les sites web visités par l'utilisateur (y compris les recherches en ligne), et les applications installées et leur numéro de version.
En 2013, après la révélation du cyber espionnage de masse de la NSA, Maxhton se vantait de mettre l'accent sur la vie privée, la sécurité, et l'utilisation d'un cryptage fort pour protéger ses utilisateurs. (Merci à I.Poireau)
Article original de Damien Bancal

Réagissez à cet article

Original de l'article mis en page : ZATAZ Le navigateur Maxhton espionne ses utilisateurs – ZATAZ

L’Internet russe prêt à ériger des frontières

L’Internet russe prêt à ériger des frontières

La Russie prévoit de contrôler davantage la partie russe du réseau Internet et son trafic, y compris l'activité des serveurs DNS et l'attribution des adresses IP.

L'an dernier, la Russie a annoncé l'entrée en vigueur d'une loi obligeant toute organisation détenant des données de citoyens russes à les stocker sur des serveurs se trouvant physiquement sur le territoire russe. Cette année, un autre projet de loi concocté par le ministère russe des communications, prévoit la création d'un système de surveillance du trafic Internet, y compris l'activité des serveurs DNS (système de noms de domaine) et l'attribution des adresses IP.

Le texte, dont le journal *Vedomosti* s'est fait l'écho, vise à réguler *« la partie russe du réseau Internet »*. Et ce officiellement pour renforcer la protection de l'Internet russe face aux cyberattaques. Le projet implique aussi la surveillance du trafic Internet transfrontalier, en s'appuyant notamment sur le système SORM (système pour activité d'enquête opératoire). Reste à savoir si la Russie a les moyens de faire appliquer de telles restrictions, dont elle devra mesurer l'impact économique.

Réseau de réseaux

Dave Allen, vice-président et avocat général de Dyn, un spécialiste de la performance réseau basé dans le New Hampshire, aux États-Unis, a publié une tribune sur le sujet dans *Venturebeat*. Allen observe qu'une grande partie du trafic Internet russe dépend actuellement beaucoup de pays avec lesquels la Russie entretient des relations compliquées, voire conflictuelles.

Les données partagées de Moscou à Saint-Pétersbourg par un abonné de l'opérateur mobile russe MegaFon, par exemple, transitent 9 fois sur 10 par Kiev, en Ukraine, selon lui. Et plus de 40 % des données qui passent par le réseau de MTS, le premier opérateur mobile russe, pour aller aussi à Saint-Pétersbourg, transiteraient par Amsterdam aux Pays-Bas et par Francfort en Allemagne.

La tendance se vérifie auprès d'entreprises publiques : ainsi, plus de 85 % des données transmises de Moscou vers Saint-Pétersbourg par TransTelekom, filiale de la Compagnie des chemins de fer russes, passeraient par Francfort. Et la plupart des données qui quittent la Russie, selon Dave Allen, passent par le backbone RETN, qui a des points de présence en Europe centrale et orientale.

Localisation de données

Les mesures de renforcement de la protection des données russes s'appliquent à toutes les entreprises ayant une activité dans le pays. L'an dernier, le régulateur russe Roskomnadzor a mené un audit auprès de 317 sociétés et administrations. Il a estimé que 2 étaient dans l'illégalité. L'audit pourrait être étendu cette année à d'autres grands groupes, dont Microsoft, HPE et Citibank.

Pour que les données puissent être transférées temporairement à l'étranger, une protection *« adéquate »* de ces données doit exister. L'Ukraine, l'Allemagne et les Pays-Bas ont signé une convention sur le traitement automatisé de données personnelles qui semble satisfaire cette condition. En revanche, le doute persiste sur le chiffrement. Le gouvernement russe, comme d'autres, envisage de l'affaiblir pour donner plus de marge de manoeuvre à ses services de renseignement.

D'autres pays ont fait des propositions en faveur de la localisation de données. En France, un amendement qui prévoyait l'interdiction de traitement de données personnelles stockées hors d'un État membre de l'Union européenne, a finalement été écarté du projet de loi République numérique.

Article original de Ariane Beky

Réagissez à cet article

Original de l’article mis en page : L’Internet russe prêt à ériger des frontières

---

Protection contre la Fuite des données, priorité pour les entreprises ?

Protection contre la Fuite des données, priorité pour les entreprises ?

Prévention des pertes de données des collaborateurs mobiles. Quand la mobilité oblige à la Data Loss Prevention.

La mobilité est à la fois un besoin et un défi pour les entreprises qui se battent pour créer une force de travail réellement fluide et entièrement digitale. Aujourd'hui, presque tous les collaborateurs travaillent avec un ou plusieurs périphériques mobiles contenant des informations d'entreprise, qu'il s'agisse d'un téléphone mobile, d'un ordinateur portable ou d'une tablette. L'un des premiers défis qui en découlent pour la direction informatique tient au fait que l'accès à distance aux données et aux e-mails se fait, par nature, « hors » du périmètre de l'entreprise, et qu'il est par conséquent très difficile de s'en protéger. La multitude des périphériques utilisés, en elle-même, complique la surveillance et le suivi des données d'entreprise consultées, partagées ou utilisées.

Data Loss Prevention : se concentrer sur les données

L'une des approches, choisie dans certaines entreprises, consiste à intégrer ces périphériques à une stratégie d'environnement de travail en BYOD. Les utilisateurs peuvent choisir le périphérique, le système d'exploitation et la version de leur choix, puisqu'il s'agit de leur propre périphérique. Malheureusement, cette approche peut en réalité créer des problèmes supplémentaires de sécurité et de DLP (prévention des pertes de données). En effet, de nombreux utilisateurs n'apprécient pas (voire interdisent) que leur employeur gère et/ou contrôle leur périphérique, pire encore, d'y installer des logiciels professionnels comme les programmes d'antivirus et de **VPN**.

Par conséquent, pour réussir, la stratégie de protection des données doit se concentrer sur la sécurisation des données uniquement, quel que soit le périphérique ou le mode d'utilisation. Dans un environnement d'entreprise, une grande majorité des données sensibles transitent dans les e-mails et leurs pièces jointes. Ainsi, une stratégie de protection des données réussie doit chercher à gérer et contrôler la passerelle par laquelle transitent les données, à savoir, ici, le compte d'e-mail d'entreprise.

Autre option : implémenter une suite d'outils de gestion de la sécurité mobile, ce qui permet de placer des mécanismes de sécurité sur la passerelle d'e-mail, et d'autoriser la création de règles de sécurité pour surveiller et contrôler la façon dont les informations d'entreprise sont traitées sur chaque périphérique.

Data Loss Prevention : Stratégie DLP tridimensionnelle

Une stratégie « DLP tridimensionnelle », surveille et contrôle le contenu transféré via un périphérique sur la base de critères précis. Par exemple, on peut limiter l'accès au contenu ou aux fichiers depuis le compte e-mail d'entreprise en fonction du pays, puisque les utilisateurs qui voyagent avec leur périphérique sont susceptibles d'accéder aux données et aux systèmes sur des réseaux Wi-Fi non sécurisés. Il est également possible de contrôler le contenu sur la base des mots clés qui figurent dans les e-mails (comme des numéros de sécurité sociale ou des numéros de contrat), afin d'interdire les pièces jointes ou le contenu incluant ce type d'information sur les périphériques mobiles. Comme les pièces jointes d'e-mail contiennent la majorité des informations sensibles transmises d'un périphérique à un autre, ce point est crucial lorsqu'il s'agit de protéger l'utilisation des périphériques dans l'environnement de travail. La troisième dimension est la surveillance du contexte, qui permet d'identifier et d'interdire le contenu pour des expéditeurs/destinataires spécifiques.

Ce type de considération permet de limiter les risques liés aux pertes de données et aux problèmes de sécurité pour cette partie des activités professionnelles Bien que cette approche ne suffise pas à contrôler et à sécuriser entièrement les banques de données d'une entreprise, la sécurité mobile va jouer un rôle de plus en plus vital pour la réussite des stratégies complètes de protection des données, au fur et à mesure que davantage de périphériques s'intègrent à nos habitudes de travail.

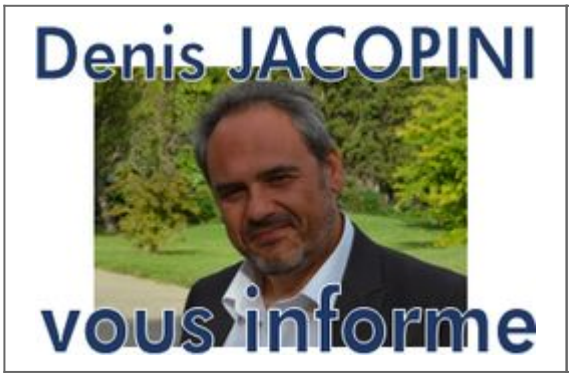
(Par Eran Livne, Product Manager LANDESK)

Article original de Damien Bancal

Réagissez à cet article

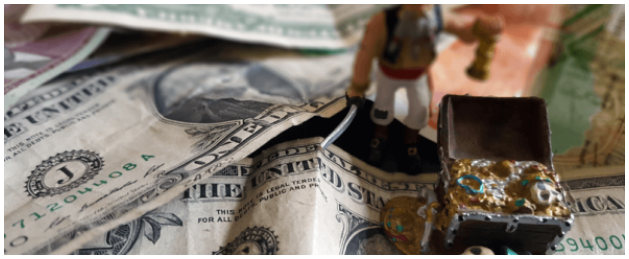
Original de l’article mis en page : Data Loss Prevention – Data Security BreachData Security Breach

Paypal ne protégera plus les transactions crowdfunding

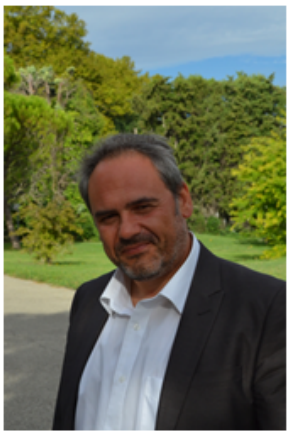


Paypal ne protégera plus les transactions crowdfunding

Trop d'arnaques au financement participatif ? Trop de remboursements pour des produits jamais livrés ? Paypal ne protégera plus les transactions crowdfunding à partir de la fin juin 2016.



Paypal semble ne plus apprécier les transactions bancaires entre ses utilisateurs et les projets lancés sur les portails de crowdfunding. Trop d'arnaques au Crowdfunding ? Á partir du 26 juin 2016, le géant de la finance, ne protégera plus les transactions effectuées sur les sites de financement participatif.
Trop d'arnaques au transactions crowdfunding ? Trop d'argent envolé sans le moindre produit/projet finalisé ? Bref, des problèmes se posent des deux côtés – vendeurs et acheteurs. Paypal ne veut tout simplement plus faire partie d'une équation qui le place au milieu des conflits. Par conséquent, vous pourrez toujours payer via Paypal, mais la structure financière n'assurera plus cette transaction. Elle sera à vos risques et périls.



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

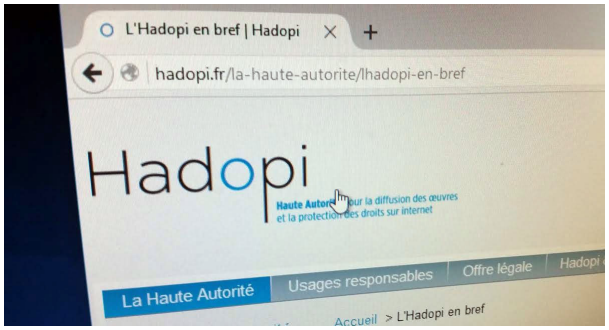
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *ZATAZ Paypal ne protégera plus les transactions crowdfunding – ZATAZ*

Peut-on s’attendre à la fin de la loi Hadopi ?



Peut-on s’attendre à la fin de la loi Hadopi ?

Les députés ont adopté un amendement qui supprimera l'institution Hadopi en 2022, mais même s'il est promulgué en l'état, le texte ne fait pas disparaître la riposte graduée, qui pourra être reprise par une autre administration.

Il ne faut pas confondre l'Hadopi et la loi Hadopi

Victimes d'un excès d'optimisme, certains imaginent que la riposte graduée elle-même disparaîtra en 2022. Mais il n'en est rien. Si les quatre députés qui ont fait majorité ont bien voté une mise à mort de l'institution Hadopi, il n'en va pas de même pour la riposte graduée.

Plusieurs raisons invitent donc à ne pas sauter trop vite aux conclusions :

Sur l'ensemble des quatre sous-sections du code de la propriété intellectuelle dédiées à la riposte graduée, seule la première intitulée « Compétences, composition et organisation » sera supprimée le 4 février 2022. Les autres, notamment la troisième relative à la riposte graduée, est conservée.

Il sera donc facile pour le législateur de pérenniser la riposte graduée en confiant simplement la riposte graduée à une autre autorité administrative. Comme nous l'expliquions hier, c'est ce qui est proposé dans le rapport Warsmann qui accompagne la proposition de loi examiné par les députés, sur les autorités publiques ou administratives indépendantes : « les compétences (de l'Hadopi) pourraient être transférées soit au CSA, soit à l'ARCEP, soit à une nouvelle AAI ayant une compétence élargie en ces matières ».

Avant cela, le Sénat pourra faire sauter la disposition lorsqu'il examinera lui-même la proposition de loi. Lui qui et traditionnellement attaché à la protection des droits d'auteur devrait y être sensible, même s'il ne sera sans doute pas fâché de se débarrasser d'une patate chaude à quelques mois de la campagne présidentielle.

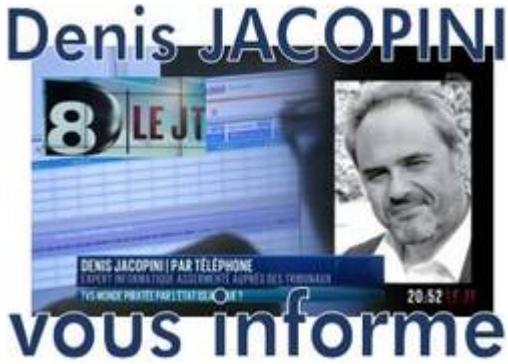
Enfin, quand bien même le texte serait-il adopté et promulgué, il restera cinq ans à la prochaine majorité, pour glisser dans un projet de loi un amendement qui supprimera l'article qui supprime l'Hadopi. Une seule ligne suffira.

Pour toutes ces raisons, aucun cri d'orfraie n'a été entendu ce vendredi du côté des ayants droit, d'habitude très prompts à publier des communiqués rageurs dès que leurs intérêts sont bousculés. Ils savent que l'affaire est plus anecdotique qu'autre chose, et que le bug législatif sera vite réparé. Voire, que l'amendement adopté leur rend service, puisqu'il précipitera un éventuel transfert des compétences de l'Hadopi vers le CSA, qu'ils appellent de leurs vœux depuis plusieurs années… [Lire la suite]

Réagissez à cet article

Source : *Non, la loi Hadopi ne va pas mourir – Tech – Numerama*

Vos données personnelles en otage, puis chantage



Vos données personnelles en otage, puis chantage

Chantage aux données personnelles et « rançongiciels » : de nouvelles formes de cybercriminalité

Quel mode opératoire ?

Le mode opératoire est toujours sensiblement le même :
Un individu parvient à s'introduire dans le système informatique d'une entreprise ou d'un particulier. en extrayant les données y étant stockées.
Dans un second temps, l'internaute ou l'entreprise victime se voit réclamer le versement d'une rançon.
A défaut de paiement, ces informations personnelles seront diffusées sur la toile.
L'exemple le plus significatif en la matière est le cas du site de rencontres extraconjugales canadien ASHLEY-MADISON.COM, victime d'une cyberattaque le 15 juillet 2015.
Un groupe de « hackers » se faisant appel « The Impact Team » a réussi à pénétrer sur les serveurs du site et à en récupérer les données relatives à ses 37 millions d'abonnés de par le monde.
La fermeture du site a alors été exigée, son éditeur se voyant menacé d'une publication en ligne de l'intégralité de ses données. Précisons que cette menace a été mise à exécution au cours du mois d'août 2015.
Une fois ces informations rendues publiques, certains (anciens) clients du site se sont vus demander la remise de fonds, à défaut de quoi leurs informations personnelles seraient adressées directement à leurs proches ou à leurs relations professionnelles.
Autant dire que l'image de l'entreprise victime est ternie, la sécurité de son système informatique étant clairement remise en cause.
Les abonnés voient également des informations (très) personnelles dévoilées publiquement, telles que leur lieu de résidence, leurs coordonnées bancaires, leurs loisirs et habitudes de consommation, leurs fantasmes et désirs sexuels.

Dans une moindre mesure, les particuliers peuvent être individuellement les cibles de phénomènes de ce type.

Pour ces derniers, il prendra la forme d'un programme informatique malveillant appelé « rançongiciel », dérivé de l'anglicisme «ransomware » et, précisons-le, contraction des termes « rançon » et « logiciel ».
Ce programme chiffre ou crypte les données de l'internaute, présentes sur le disque dur de son ordinateur.
Si il souhaite les récupérer ou éviter leur divulgation, il devra là encore payer la rançon exigée.
Une variante consiste à arborer le logo d'une unité de police de type INTERPOL, en accusant l'internaute de détenir illicitement des œuvres protégées par le droit d'auteur ou bien des vidéos ou photographies pédopornographiques.

Quelles Infractions pénales ?

Le chantage et l'extorsion

« Le chantage est le fait d'obtenir, en menaçant de révéler ou d'imputer des faits de nature à porter atteinte à l'honneur ou à la considération, soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque. » (article 312-10 du Code pénal)
Ce délit est puni de 5 ans d'emprisonnement et de 75.000,00 Euros d'amende.
« Lorsque l'auteur du chantage a mis sa menace à exécution, la peine est portée à sept ans d'emprisonnement et à 100.000 euros d'amende. » (article 312-11 du Code pénal)
La menace sera mise à exécution, à partir du moment où les données sensibles seront publiées en ligne ou communiquées à des tierces personnes.
« L'extorsion est le fait d'obtenir par violence, menace de violences ou contrainte soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque. »
« L'extorsion est punie de sept ans d'emprisonnement et de 100 000 euros d'amende. » (article 312-1 du Code pénal)
En la matière, la contrainte ne reposera pas sur la force physique, mais sera purement morale ou psychologique.

L'intrusion dans un système informatique

L'accès et le maintien frauduleux dans un système

« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende.
Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende. » (article 323-1 du Code pénal)

L'entrave au fonctionnement d'un système

« Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende. » (article 323-2 du Code pénal)
Le chiffrement ou le cryptage de données entrave nécessairement le bon fonctionnement d'un sytème informatique.

La suppression ou la modification frauduleuse de données

« Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende. » (article 323-3 du Code pénal)

Les atteintes à la vie privée

« Est puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :
1° En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;
2° En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé.» (article 226-1 du Code pénal)
« Est puni des mêmes peines le fait de conserver, porter ou laisser porter à la connaissance du public ou d'un tiers ou d'utiliser de quelque manière que ce soit tout enregistrement ou document obtenu à l'aide de l'un des actes prévus par l' article 226-1.» (article 226-2 du Code pénal)
L'atteinte à l'intimité de la vie privée sera ainsi caractérisée, lorsque l'objet du chantage consistera en des photographies ou des vidéos représentant des personnes dans un lieu privé.

La violation du secret des correspondances (électroniques)

« Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45000 euros d'amende.
Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions. » (article 226-15 du Code pénal)
Le délit de violation du secret des correspondances est pleinement constitué, dès lors que la menace porte sur la teneur de courriers électroniques, d'emails ou de messages privés échangés entre abonnés ou utilisateurs d'un site.

Les infractions à la législation sur les données personnelles

Le traitement illicite de données personnelles
« Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. »(article 226-16 du Code pénal)
La collecte frauduleuse de données personnelles
« Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 € d'amende. » (article 226–18 du Code pénal)
Le défaut de sécurité des données
La particularité de cette dernière infraction est qu'elle vise, non pas l'auteur de l'attaque, mais bel et bien sa victime directe, le responsable du traitement des données.

En effet, les personnes, entreprises, organismes et collectivités, en charge du traitement des données de leurs utilisateurs ou de leurs usagers, sont tenus de mettre en œuvre toutes les mesures nécessaires, afin d'assurer la sécurité et la confidentialité desdites données.
A défaut, ils engageront leur responsabilité civile et pénale sur le fondement des articles 34 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et 226–15 du Code pénal:
« Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. » (article 34 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)
« Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 € d'amende. » (article 226-15 du Code pénal)

Au cas par cas, d'autres infractions peuvent également être constituées, telles que les délits d'escroquerie, d'usurpation d'identité (numérique), voire même d'usurpation de fonctions, dans la situation où le cyber-délinquant se fait passer pour une unité de police, afin de se faire remettre des fonds.

Quelles solutions ?

La plainte pénale

Que l'on soit une entreprise, une collectivité ou un particulier victime de ce type d'agissements, le premier réflexe est de déposer plainte auprès des services de police ou de gendarmerie ou bien directement auprès du Procureur de la République.
Ce dernier se réservera le droit d'engager des poursuites ou bien de procéder à un classement sans suite de la plainte, faute notamment de disposer d'éléments suffisants afin d'identifier et de localiser précisément le ou les auteur(s) des faits.
En cas de classement sans suite, la victime disposera alors de la faculté de se constituer partie civile auprès du doyen des juges d'instruction, ce qui déclenchera automatiquement des poursuites pénales.

Le retrait de contenus illicites

Si les informations personnelles sont publiées sur un site internet en particulier, leur retrait peut être demandé directement auprès de son éditeur.
A défaut de réponse de sa part ou si il n'existe aucun moyen de le contacter, la suppression des contenus illégaux devra être alors demandée à l'hébergeur du site, en application de l'article 6-I-5 de la loi n°2004-575 pour la confiance dans l'économie numérique.

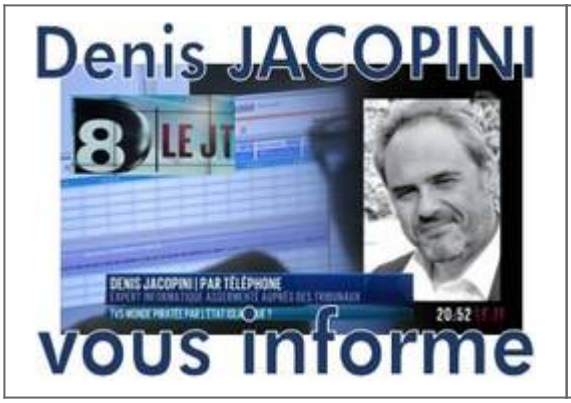
Le déréférencement et la désindexation des moteurs de recherche

Lorsque le nom et le prénom d'une personne sont tapés sur un moteur de recherche, la liste des résultats de recherche peut faire apparaître des liens renvoyant vers les informations frauduleusement obtenues et divulguées.
Dans ce cas, il est envisageable de demander la désindexation de ces liens directement auprès du moteur de recherche et, le cas échéant, par voie judiciaire.

Réagissez à cet article

Source : *Chantage aux données personnelles et « rançongiciels » : de nouvelles formes de cybercriminalité – Maître thibault prin*
Thibault PRIN AVOCAT
Avocat inscrit au Barreau de PARIS

Les entreprises doivent prendre au sérieux la protection des données



Les entreprises doivent prendre au sérieux la protection des données

---

L'intelligence économique est devenue un mode de gestion (Le management est la mise en ?uvre des moyens humains et matériels d'une entreprise pour (…)) et de gouvernance de l'entreprise. Cet ouvrage réfléchit sur la démarche que le chef d'entreprise peut entreprendre pour éclairer ses décisions, garder sa marge de manoeuvre de compétitivité et toutes ses possibilités de développement afin de sécuriser sa pérennité.
Traitement de l'information et renseignements
Un renseignement utile peut être obtenu de façon proactive, active, ou réactive.
Le cycle de renseignement pour l'entreprise doit s'intégrer au processus de veille stratégique sur les différents volets de l'intelligence économique : veille technologique, veille d'image, veille concurrentielle, etc.
L'intelligence économique distingue trois niveaux d'information utile au renseignement :
image: http://www.atlantico.fr/sites/atlantico.fr/files/u65387/2015/12/capture_2_0.jpg
L'intelligence économique ne cherche pas à obtenir l'information noire. Elle se limite à l'information que l'on peut obtenir par des moyens légaux (ex : pour se protéger des problèmes de réputation, d'escroquerie, de fraude, de cybercriminalité, de propriété intellectuelle, de savoir-faire, de brevets, etc.).
Il s'agit surtout de formaliser de façon pragmatique, ou de rendre systématique, une démarche proactive de veille dans ce domaine, notamment pour l'obtention de l'information « grise ».
Les PME sont souvent très en retrait sur la construction du savoir (ex : suivi des avancées des concurrents, organisation de la veille juridique, réglementaire, lobbying, etc.).
Sécurité et protection de l'information
Trop peu d'entreprises prennent au sérieux la protection des données. Il devient impératif de disposer d'un solide processus de sauvegarde, de prévention, d'action, et de réaction aux pannes et aux attaques informatiques. Notons ici que certaines entreprises sensibles aux problématiques de reprise après incident commencent à considérer les prestations d'externalisation applicatives (Cloud computing ou autres solutions) pour optimiser le niveau de sécurité des données.
Quantité et gouvernance des données
Les données sont la base de l'information, et comme le disent souvent les anglo-saxons: « data is the oil of the 21st century ». Savoir chercher et collecter l'information, la traiter et la diffuser (tout en protégeant la part de données sensibles qui doivent être protégées), constitue une tâche prioritaire de tous les acteurs économiques, et la définition même de l'intelligence économique.
image: http://www.atlantico.fr/sites/atlantico.fr/files/u65387/2015/12/capture_3_0.jpg
Le pouvoir c'est l'information, mais à condition qu'elle soit de qualité …
La direction et les organes sociaux doivent s'appuyer sur des informations de qualité (fiables, précises, actualisées)
Read more at http://www.atlantico.fr/decryptage/entreprises-doivent-prendre-au-serieux-protection-donnees-gouvernance-et-intelligence-economique-en-pme-georges-nurdin-daniel-2494228.html##Vrl3qqLdiB14upbK.99

Réagissez à cet article

Source : *Marketing/ Les entreprises doivent prendre au sérieux*

la protection des données