SÉCURITÉ DU WEB : LE RÈGNE DES PASSOIRES

LE 19 MAI 2011 ***ANTOINECHAMPAGNE***

Pendant que les médias se focalisent sur quelques petits détournements de données, les VRAIS « piratages » restent impunis. La faute à un réseau construit de manière à être impossible à protéger... et qu'aucun dirigeant ne semble vouloir colmater !

En 1994, apparaissait le Web. **L'un des premiers sites était Playboy.com**. Depuis cette époque, toutes les entreprises ont ouvert une vitrine sur cette sous-partie d'Internet. Mais avec l'explosion du nombre d'ordinateurs interconnectés, sont apparus… les piratages. En effet, le problème est que ce réseau a été bâti pour faire un nombre incroyable de choses, mais pas du commerce sécurisé. Tout est troué, mal installé, mal pensé. Les contraintes liées à la sécurité empêchent de faire du commerce en rond. Elles le compliquent. Du coup, tout le monde fait l'impasse sur la sécurité. En partie, ou en totalité.

Que vous soyez puissant ou misérable…

D'autant que généralement, le seul perdant, c'est le client. **Les hacks ultra médiatiques** sont oubliés aussi vite qu'ils apparaissent. Et dans ce domaine, **personne n'est épargné** : les plus gros, les plus riches, comme les plus anonymes. Tous se font avoir un jour ou l'autre.

Pas de souci, tout cela est si vite oublié…

Ceux qui ne l'oublieront pas sont généralement des anonymes, qui n'ont pas les moyens de faire payer ceux qui sont à l'origine de leurs ennuis. **Des clients lambda dont les données personnelles se retrouvent sur le Net**. Noms, adresses, numéros de sécurité sociale, numéros de carte bancaire, logins et mots de passe pour tel ou tel service en ligne. Factures qui s'allongent, comptes en banques qui se vident. Bienvenue sur Internet, le réseau où ceux qui transigent avec la sécurité de vos données ne seront jamais poursuivis.

Bien entendu, ces entreprises, ces ministères, blâmeront les *« pirates »* qui ont accédé à ces données. Ils sont maléfiques, viennent au choix de l'Est ou de Chine, **mettent en péril le gentil capitalisme**.

Pourtant, on semble oublier un peu vite que le défaut de protection des infrastructures est le fait desdites entreprises, desdits ministères.

Leurs économies de bouts de chandelles ont des conséquences.

Le législateur français, à une époque lointaine, lorsqu'il réagissait avec sa tête plutôt qu'en fonction de peurs infondées et sur la base d'un savant storytelling, avait compris que, s'il fallait punir le *« pirate »*, il fallait aussi punir celui qui ne prenait pas les mesures nécessaires

pour protéger les données qui lui étaient confiées.

Ainsi, la **Loi n° 78-17 du 6 janvier 1978** relative à l'informatique, aux fichiers et aux libertés (Journal Officiel du 7 janvier 1978) en son article 34 dispose que :

> ***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.***

Et l'article **226-17 du Code Pénal** dispose que :

> ***Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en oeuvre 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 Euros d'amende.***

Fuite de données personnelles : mise en garde partout, condamnation nulle part…

Maintenant, observons la jurisprudence en France dans ce domaine. Si les condamnations pour « piratage » sont légion (mais pas aussi dures que ce que la loi permet), celles qui concernent la non protection des données personnelles sont… inexistantes.

La dernière remonte à l'époque du Minitel. De mémoire, une femme avait mis en vente son appartement sur un serveur immobilier et ses données avaient malencontreusement *« basculé »* sur un serveur *« rose »*.

Les fuites de données personnelles **sans même avoir besoin d'avoir recours à un quelconque « piratage »** sont légion depuis l'arrivée d'Internet. Et pas une seule condamnation.

Le législateur (français et européen) réfléchit actuellement à un projet obligeant les entreprises à rendre public un éventuel piratage de leurs infrastructures. Voilà qui fera une belle jambe aux personnes dont les données auront fuité…

Depuis 1998, **Kitetoa.com**, vite rejoint par nombre de sites, dont l'excellent blog de **Korben**, ou le site **Zataz.com**, listent inlassablement les milliers de serveurs qui, mal paramétrés, laissent fuiter les données.

Que l'on se comprenne bien, pour ce qui est de Kitetoa.com, il ne s'agit pas d'expliquer des piratages, des moyens illégaux pour accéder à ces données. L'utilisation d'un simple navigateur, sans aucune identification sur le serveur suffit. Avec un peu d'imagination, on comprend ce que de vrais pirates pourraient faire.

Bilan des courses ? Rien.

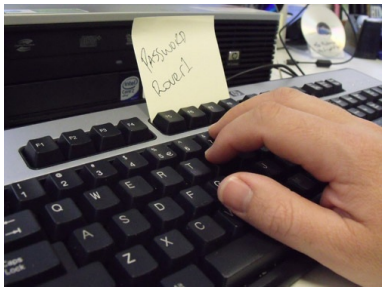
De toutes ces informations rendues publiques… qu'en est-il ressorti ?

Rien.

La **CNIL** ne s'est jamais appropriée un seul de ces dossiers. Elle n'en a jamais transmis un seul au procureur.

Et les procureurs, justement… Aucun ne s'est jamais saisi de ces affaires, pourtant

publiques. Imaginez un site listant des infractions, des actes pénalement répréhensibles. Donnant tous les détails. Il a des chances pour que des procureurs se réveillent et fassent en sorte que des vérifications soient menées. Dans le domaine de la non protection des données personnelles, rien.



Reflets.info vient de démontrer en quelques lignes que l'ensemble de la loi Hadopi est boguée et qu'il importe de tout revoir. Le problème n'est pas récent, il avait été souligné par des parlementaires pendant les débats, par exemple sous forme de questions au ministre de la culture, des questions **dont certaines sont encore sans réponse**. La Haute Autorité consciente du problème, s'est montrée très réceptive aux problématiques de protection des données personnelles qui refont aujourd'hui surface. Pour autant, très probablement, les avocats ont désormais en main de quoi faire annuler toute procédure se fondant sur ce texte (Maître Eolas ?).

Ce dernier événement dans la trop longue liste des sites troués charrie un sacré cortège de questions. Pourquoi ce texte a-t-il pu être voté par les députés et les sénateurs ? Pourquoi le sénateur, Alex Türk a-t-il voté un texte critiqué par la CNIL qu'il préside par ailleurs ? **Pourquoi personne n'a écouté ceux qui savent** et qui fournissaient leurs analyses gratuitement ? Pourquoi **tant de questions sont-elles restées sans réponses** ?

Le règne des costumes cravates

Depuis que le Net est là, depuis plusieurs postes d'observation, je contemple l'action des commerciaux en costumes cravates de mauvaise facture vendre à prix d'or des projets troués d'avance. Je les regarde vanter les mérites de leurs entreprises, qui n'en ont aucun. Les marchands de vent qui viennent crier sur tous les toits que leurs logiciels protègent contre les « hackers », contre les failles passées, présentes et futures. Je les contemple enfumer leurs clients, mais aussi les représentants du peuple.

Parmi les hommes en costumes cravates de mauvaise facture, il y en a même qui s'arrogent le droit de jouer aux cow-boys du Net. **C'était le cas de HBGary aux Etats-Unis et l'affaire a très mal fini**. Rien ne dit qu'il n'y a pas en France une ou des entreprises qui pensent engranger des millions en suivant cette voie périlleuse. L'avenir le dira sans doute. Patience.

Quoiqu'il en soit, **le réseau Internet n'a pas été conçu pour faire du commerce électronique**, bien au contraire. Il est tout sauf sécurisé. Allons plus loin, il est tout sauf sécurisable. C'est juste impossible. Alors vendre du stockage de données personnelles, du paiement d'impôts, de la e-administration publique, du commerce électronique, c'est simplement laisser, en toute conscience, un crime se dérouler.

J'ai coutume de dire dans des conférences qu'il ne faut pas craindre les piratages qui font la *Une* des journaux. Aussi incroyables soient-ils, aussi dérangeants puissent-ils paraître. Ce qu'il faut craindre, ce sont les piratages dont on n'entend jamais parler. Ils sont bien plus inquiétants. Et ils existent.

Pour ce qui est de la loi Hadopi, dire que les particuliers doivent sécuriser leur accès Internet, c'est très con. Et c'est faire preuve d'une fabuleuse mauvaise foi. Désolé de faire une comparaison avec le monde réel, mais visiblement un sénateur comme M. Türk ne doit pas comprendre autre chose.

Imaginons que l'on oblige les particuliers à prendre des mesures pour éviter que leurs voitures ne soient volées et ne servent à commettre un délit, comme une attaque à la voiture-bélier. Sans quoi ils seraient poursuivis. Stupide n'est-ce pas ? C'est pourtant à peu près la même chose que de dire que les particuliers doivent sécuriser leurs accès.

Dire que si l'adresse IP d'un particulier est repérée en train de télécharger un film cela doit aboutir à une coupure de l'accès au Net, c'est simplement méconnaître la réalité. Avec les millions de bots qui tournent pour exploiter des Windows troués, avec les milliers de logins et mots de passe qui trainent sur le Net pour se connecter à des accès Wifi de particuliers, c'est une honte de passer une telle loi.

Tout cela a été dit lors des débats précédant le vote de la loi par ceux qui savent comment fonctionne le réseau. Personne ne les a écoutés. Depuis des années et des années, nous sommes nombreux à dire que si l'on n'attaque pas les entreprises au portefeuille, les données personnelles continueront de fuiter. En vain.

Laisser le secteur s'auto-réguler, prendre des dispositions comme **PCI-DSS**, c'est le laisser faire n'importe quoi (voir **Sony** et **Hartland** par exemple). C'est à peu près aussi stupide que d'attendre des financiers qu'ils arrêtent, sans aucune pression extérieure, de créer des crises monumentales.

Les seuls qui pourraient faire quelque chose, les procureurs, la CNIL, le législateur, les politiques, sont silencieux et inactifs. Il y a bien quelques écrans de fumée déclenchés de temps à autre. **Sept minutes d'amende pour Google** par exemple. Mais pour TMG, combien ? Pour ceux qui ont monté l'usine à gaz qu'est la loi Hadopi, combien de minutes d'amende ?

Article initialement publié sur **Reflets.info**

Photos flickr **CyberHades**; **Le Bourg Heïdi** ; **AngusKingston** ; **Reza Vaziri**.

NORMAL.
le 20 mai 2011 - 0:30 • SIGNALER UN ABUS - PERMALINK

Perso, j'ai une lpi 201-202, + a l'époque certif w2ksrv, j'ai jamais trouvé de boulot (refus de faire des stages a 30 ans en 2002, et que des propositions de stagiaire…), maintenant je bosse dans autre chose et bidouille les ordis pour particulier…

Sur 20 de ma formation, seulement 12 ont travaillé par la suite MAIS 10 etaient deja en entreprise (fongecif). J'ai dépensé 6000€ de ma poche, mangé des nouilles pendant 3 ans pour remboursé mon emprunt…

*Pays de cons ! ^^*

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

CLÉMENT
le 21 mai 2011 - 19:26 • SIGNALER UN ABUS - PERMALINK

"Quoiqu'il en soit, le réseau Internet n'a pas été conçu pour faire du commerce électronique, bien au contraire. Il est tout sauf sécurisé. Allons plus loin, il est tout sauf sécurisable. C'est juste impossible. Alors vendre du stockage de données personnelles, du paiement d'impôts, de la e-administration publique, du commerce électronique, c'est simplement laisser, en toute conscience, un crime se dérouler."

Sans remettre en question l'ensemble de l'article , je trouve ce paragraphe bien rétrograde et péremptoire. Internet n'a pas été conçu pour transporter la voix, internet

n'a pas été conçu pour les jeux massivement multijoueurs, internet n'a pas… A vous lire il faudrait tout arrêter sur le simple prétexte que la toile n'est pas sécurisée, ni sécurisable. C'est bien restons-en au HTML dans ce cas. Tout cela me paraît très alarmiste. Il faut quand même rappeler que des milliards d'échanges (mails, paiements, votes, chat, tweets, etc.) se déroulent sans problème chaque minute sur internet.
D'après vous il faudrait faire quoi pour rendre le réseau sûr?

Oui, comme pour toute autre structure lucrative en cas de détournement, il y aura toujours des malfaiteurs qui tenteront de trouver la faille pour en tirer profit. Ces gens là auront toujours l'avantage sur les responsables de la sécurité, car ils passent leur journée à chercher "l'exploit" (en anglais) et le font de manière très ciblée et organisée.
La sécurité totale est bien évidemment impossible comme pour tout autre système (surtout quand il y a une composante humaine). Mais aujourd'hui, pour ce qui est d'internet, il est quand même aisé d'atteindre un niveau de sécurité très élevé, que ce soit à l'échelle de l'entreprise ou privée. C'est uniquement une question de volonté, d'éducation et aussi de moyens. Les cas d'attaques massives avec vols de donnée sont souvent le résultat d'un laxisme de la part des responsables de la sécurité, généralement provoqué par un manque de ressources car la hiérarchie n'est pas consciente des enjeux.
Il faut aussi noter que bon nombre d'attaques utilisent le "social engineering" qui repose uniquement sur la naïveté/ignorance/faiblesse d'esprit des utilisateurs finaux. Dans ce type d'attaques, on aura beau mettre tous les moyens technologiques en oeuvre, elle seront toujours possible si l'utilisateur n'est pas sensibilisé/formé/éduqué.

Je pense que la toile est un environnement suffisamment sécurisé, mais il est en perpétuelle lutte contre des menaces, tout comme un système immunitaire est en constante adaptation et recherche de réponses face à des éléments perturbateurs.

@Normal : Je ne vois pas trop le rapport avec l'article… La prochaine fois pensez à faire vos formations là (si vous parlez anglais): http://www.koenig-solutions.com . Ca coûte 5 fois moins cher (billet d'avion compris) et la formation est vraiment de qualité (j'y suis actuellement et pour 3 mois). Ceci dit, sans expérience sur le terrain, tout ces papiers ne servent à rien. Il ne faut pas croire qu'on va être catapulté Sysadmin directement sans passer par la case stage. Personnellement, je serai ultra heureux qu'on m'en propose un quand je rentre.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

KITETOA
le 21 mai 2011 - 19:36 • SIGNALER UN ABUS - PERMALINK

@Clément : vous ne dites pas autre chose que ce que je dis dans l'article.
Globalement : vous dites que la majorité des échanges se passent sans souci sur Internet. Oui. Ce que vous ne pouvez pas prendre en compte, ce sont les milliers de hacks de haut vol qui ne sont pas publics et qui ne le seront jamais. Ceux-là, ils font peur.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

CLÉMENT
le 22 mai 2011 - 9:39 • SIGNALER UN ABUS - PERMALINK

Vous faites référence à quoi en parlant de "hack de haut vol" ? Puisqu'ils sont cachés, avez-vous des statistiques pour en prouver l'ampleur? Il suffit de se rendre aux conférences de White/Black Hats (pas si inaccessibles) pour se rendre compte de ce qui est possible de réaliser. Après c'est sûr qu'on peut en faire ce qu'on veut, mais c'est aussi aussi un moyen de se prémunir.

Je ne suis pas persuadé qu'il y ait tant de hacking caché. Les crackers capables de complètement couvrir leurs traces ne courent pas vraiment les rues et partir du moment où ils se servent de leur "butin", ils se mettent à découvert d'une manière où d'une autre. En fin de compte, le préjudice est souvent uniquement financier, ce n'est pas anodin mais ça ne va pas provoquer la fin du monde.
Le plus grave des vols selon moi, c'est celui de l'identité, pour ça il n'y a pas besoin d'être un génie pour en abuser vu la tendance actuelle qu'on les internautes à se déshabiller sur la toile. Ce n'est pas une question de sécurité, mais de bon sens.

Je veux bien que la toile ne soit pas un monde de bisounours, mais il ne faut pas non plus sombrer dans le catastrophisme et affirmer que " vendre du stockage de données personnelles, du paiement d'impôts, de la e-administration publique, du commerce électronique, c'est simplement laisser, en toute conscience, un crime se dérouler". C'est surtout cette phrase qui m'a fait tiquer.

Ce qui m'inquièterait le plus c'est la tendance des Etats/grosses entreprises (pas vraiment de différence) à capter les échanges sur internet pour essayer d'en prendre le contrôle et de manipuler l'information (cf. Lybie, Egypte et consorts). Ceci ne correspond pas à un "hack" ni à la sécurité à proprement parler, mais à un abus de pouvoir puisqu'ils peuvent avoir accès aux infrastructures de bas niveau. Il n'y a qu'à prendre conscience du genre d'outils qui existent pour avoir des sueurs froides : http://www.amesys.fr/index.php?g=2&pid=62

Bref, en fin de compte nous sommes d'accord, je crois que le "différend" ce situe juste au niveau de la formulation et de la mesure.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

KITETOA
le 22 mai 2011 - 10:21 • SIGNALER UN ABUS - PERMALINK

@clement: on est visiblement tout à fait sur la même longueur d'ondes. C'est amusant le lien que vous avez donné… Suivez-nous sur Reflets.info, vous allez vous régaler dans pas très longtemps.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

CLÉMENT
le 22 mai 2011 - 13:41 • SIGNALER UN ABUS - PERMALINK

@Kitetoa : reflets.info est déja dans mes favoris et je me régale depuis un moment avec le fail de TMG… Continuez comme ça, c'est du bon boulot. Peut-être que vous serez la torpille qui a fini de couler Hadopire.

Oui amusant… Si jamais on peut trouver le PDF avec un peu plus de détails sur les fonctions de la bête là: http://www.amesys.fr/PRODUITS/DTSHEET/Glint_EN.pdf
J'avais fait une demande d'envoi de doc par e-mail, mais ils ne m'avaient pas répondu. Fallait juste fouiller un peu.

Bonne continuation !

dEXtErn1ty

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

2 pings

Arnaques sur Internet | le café clic le 22 mai 2011 - 12:59

[...] aller plus loin sur le sujet de la sécurité et Internet, un article très bien fait sur Owni Cette entrée a été publiée dans Arnaque, Cybercriminalité, Internet, avec comme [...]

Sécurité du web : le règne des passoires « sw1ngc le 9 juin 2011 - 20:38

[...] Source: Owni [...]