LE PLAT PAYS SOUS LES CYBERATTAQUES

LE 8 SEPTEMBRE 2011 ***MARCO BERTOLINI***

Piraté depuis l'Iran, le site de certification du gouvernement néerlandais suscite de grandes craintes au Benelux. La Belgique et les Pays Bas souffriraient d'un grave déficit de sécurité informatique qui en feraient des proies de choix pour les cyberattaques.

La sécurité des sites gouvernementaux est-elle garantie ? Alors que de plus en plus de données personnelles sont stockées sur les serveurs des autorités nationales, au moment où les formalités administratives en ligne sont toujours plus nombreuses, toutes les mesures pour les protéger efficacement ont-elles été prises ?

Les exemples belges et néerlandais font craindre le pire: **DigiNotar**, la société qui certifiait les sites officiels des autorités des Pays-Bas a été piratée par un hacker iranien. Et le **« Comité R »** (la commission du Sénat chargée de la surveillance des services belges de sécurité) vient de remettre un rapport dont la conclusion a fait l'effet d'une bombe: la Belgique constitue la cible idéale pour les attaques informatiques !

Les sites officiels n'auraient subi aucun dommage. Pour l'instant, les autorités travaillent à leur sécurisation avec une nouvelle entreprise. Mais pendant quelques heures, les sites publics (gouvernementaux, mais aussi municipaux) seront inutilisables. En réalité, la mise à niveau de la sécurisation prendra plusieurs jours.

Le eGov hollandais : exemplaire mais fragile

De quoi ébranler la confiance des citoyens dans la sécurité informatique. Qu'en est-il de la fiabilité des moyens de paiement en ligne ou la protection de leurs données privées quand *« DigiB »*, le certificat personnel qui atteste de l'identité des internautes, ne vaut plus rien?

Il faut dire que les Pays-Bas ont poussé l'informatisation de leurs services à un point rarement vu ailleurs: déclaration fiscale, extrait de naissance, documents officiels en tous genres peuvent s'obtenir via Internet… Dans les affaires, les factures papier tendent à disparaître. Quant au chèque bancaire, si courant dans les transactions françaises, il a tout simplement disparu des banques hollandaises depuis 15 ans. Les écoles primaires remettent certains devoirs aux écoliers sur clé USB…

Cela s'explique sans doute par le très haut degré d'équipement des foyers néerlandais : **les derniers chiffres (2009)** évoquent un taux d'équipement de 90 % des ménages tandis que 82 % d'entre eux surfent régulièrement. C'est, avec l'Islande, le taux le plus élevé d'Europe.

Par comparaison, la France, en 2009, **comptait 63 % de foyers équipés…**

Le nombre de détenteurs de tablette numériques a doublé dans les 6 premiers mois de cette année et ce sont **pas moins de 8 % des Néerlandais qui disposent de ce type d'équipement au mois d'août 2011**

L'action des pirates iraniens ne visaient pas directement les sites internet des autorités néerlandaise. Il s'agit d'une nouvelle forme de piratage qui a fait une récente apparition et qui est beaucoup plus subtile.

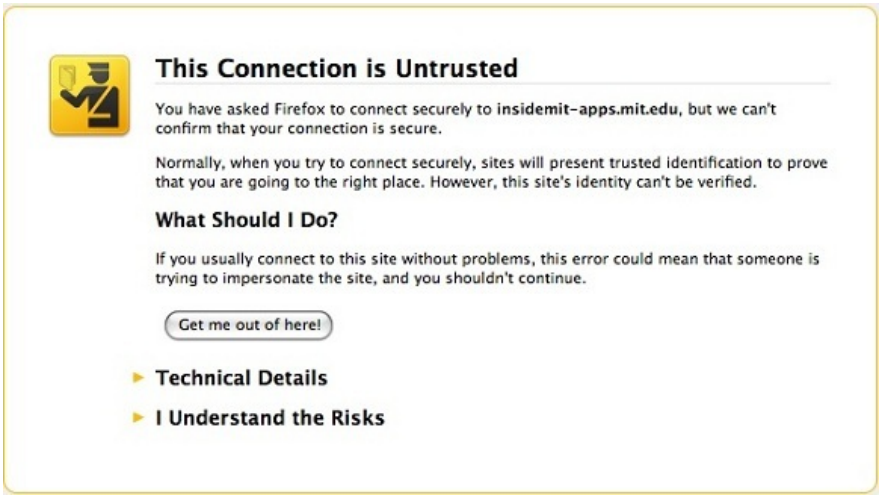
Comment savoir si le site sur lequel vous surfez actuellement est bien celui que vous croyez? Qui garantit que le site bancaire auquel vous venez de vous connecter est bien le vôtre? Que vous n'êtes pas occupé à donner vos numéros de compte, votre nom d'utilisateur et votre mot de passe à un faussaire?

Détournement de certificats

Très tôt lors de la naissance du réseau des réseaux, la question s'est posée. Et l'une des solutions trouvées est celles des « certificats »: ceux-ci, émis par quelques société hautement spécialisées, garantissent à l'internaute la validité d'un site. Ils sont en quelque sorte la « carte d'identité » d'un site Internet. C'est une opération dite « transparente ».

C'est votre navigateur – Explorer, Chrome, Firefox, Safari, Opera, etc. – qui vérifie le certificat avant de vous donner accès à un site. S'il n'y a pas de certificat ou si les données du certificats ne sont pas fiables, votre navigateur vous avertit par un message : cette connexion n'est pas fiable. *« This connection is untrusted »*, dans la langue de Shakespeare.

Si le certificat est un faux, vous n'avez plus aucune garantie de sécurité. Comme une fausse carte d'identité. Ce monsieur qui vous montre une carte d'inspecteur des finances est en fait un fraudeur qui veut avoir accès à vos données bancaires. Ce site qui ressemble trait pour trait à celui de votre banque est l'œuvre d'un hacker…



Dans un premier temps, l'identification de la provenance du pirate, l'Iran, a fait croire à une attaque du gouvernement. Ce dernier est devenu un acteur actif autant que la cible d'attaques du type « cyberguerre » : les Américains et les Israéliens ont tenté de saboter le programme de développement nucléaire iranien **à l'aide d'un virus particulièrement sophistiqué, le Stuxnet**.

L'Iran a également attaqué diverses cibles européennes ou américaines. Et notamment, une société américaine émettrice de certificats : Comodo. Cette entreprise a perdu tout crédit en étant attaquée deux fois cette année. **Une première fois en mars** et une seconde, à la fin du mois d'août. Les spécialistes sont formels : **l'attaque est d'origine iranienne**.

Dans le cas de l'attaque du mois d'août, ce sont des certificats de services Google qui ont été attaqués. Les opposants iraniens craignent le pire. Le gouvernement a donc pu avoir accès à leurs courriels et ils peuvent s'attendre à des représailles. On sait que l'Iran est particulièrement dur à l'égard des blogueurs, comme Hossein Derakshan, dit Hoder, **condamné à 19 ans et demi de prison** pour *« entente avec des gouvernement hostiles à la République Islamique, diffusion de propagande anti-islamique et anti-révolutionnaire, blasphème et exploitation et gestion de sites pornographiques »*.

L'attaque de DigiNotar a été signée. Le hacker a laissé des messages en anglais. Il se présente comme le ComodoHacker. Autrement dit, celui qui a piraté l'entreprise Comodo…

Vengeance contre les bataillons hollandais de Srebreanica

Il se décrit comme un *« jeune homme de 21 ans »* avec les *« compétences de 1 000 pirates, l'expérience de 1 000 programmeurs »*.

Est-ce vrai ? Ou s'agit-il d'une *« personna »* – une fausse personnalité Internet – empruntée par le gouvernement iranien ? En tout cas, l'égo surdimensionné, l'envie de publicité tout en gardant l'anonymat, le besoin de prouver ses compétences hors-pair, tout cela cadre avec la personnalité du hacker de base…

Vrai ou pas, le pirate insiste lourdement sur le fait qu'il a agi seul et qu'il n'a rien à voir avec les autorités de Téhéran:

> ***Je suis une personne seule, n'essayez pas ENCORE de me faire passer pour une ARMEE iranienne. Si quelqu'un a utilisé les certificats que j'ai créés, je ne suis pas celui qui doit fournir une explication.***

Il se vante également d'avoir piraté d'autres entreprises de certification – GlobalSign, StartCom – ainsi que WinVerifyTrust de Microsoft…
Quelles sont donc les motivations de ce pirate ? En-dehors de l'énorme besoin de reconnaissance qui éclate à chaque phrase de ses messages ou presque, **le hacker déclare** :

> ***Le gouvernement néerlandais paie pour ce qu'il a fait à Srebrenica, il y a 16 ans. Vous n'avez plus de e-government, hein ? Vous êtes retourné à l'âge du papier et des photocopieuses et des signatures manuelles et des sceaux ? Oh, excusez-moi ! Mais avez-vous jamais pensé à Srebrenica ? 8.000 morts [d'un côté, contre] 30 ? Impardonnable ! Jamais ! J'entends que le gouvernement néerlandais est en train de rassembler des documents et se prépare à déposer plainte contre l'Iran, vraiment ? Honte sur vous, les gars ! Avez-vous été jugé pour Srebrenica ? Qui devrait déposer plainte pour Srebrénica ? Vous deviez payer: voilà les conséquences de Srebrenica, sachez le ! Ceci est la conséquence du combat de votre parlement contre l'Islam et les Musulmans.***

Pourquoi Srebrenica ? **Srebrenica** est la ville où 8 000 musulmans bosniaques ont été massacrés en juillet 1995, en pleine guerre yougoslave. La population musulmane de Bosnie était alors sous la protection des forces de l'ONU. En l'occurrence, les Dutchbats ou bataillons néerlandais, accusés depuis par les familles des victimes d'être responsables du massacre. Ou en tout cas, d'avoir laissé l'armée serbe d'avoir massacré des civils – hommes, femmes et enfants – sans avoir réagi.

Voilà qui déplace le débat néerlandais à propos de l'islam sur un nouveau champ de bataille, celui de la cyber-guerre…

Le ministre Donner a annoncé qu'une enquête était en cours et que les certificats sont restaurés par d'autres entreprises. Getronics, une filiale de la société de Télécoms néerlandaise, engrange des dizaines de clients depuis trois jours, parait-il: Le malheur des uns…

La Belgique « cible idéale » selon un rapport sénatorial

Et en Belgique, qu'en est-il de la sécurité informatique ? La situation n'est guère plus enviable. Le Comité R (Comité Permanent de Contrôle des Services de Renseignement et de Sécurité) est une commission spéciale du Sénat belge. Comme son nom l'indique, sa première mission et de contrôler le travail des services de renseignement et de sécurité, mais aussi de se livrer à un travail d'analyse et de prospective en la matière.

C'est dans ce cadre, que le Sénat lui avait confié, en 2007, une *« enquête sur la manière dont les services belges de renseignement envisagent la nécessité de protéger les systèmes d'information contre des interceptions et cyberattaques d'origine étrangère »*.

Malgré son titre interminable, le rapport consiste en 5 pages claires, concises et lisibles pour le commun des mortels. Mais ses conclusions sont alarmantes:

> ***La Belgique constitue une cible idéale pour les attaques informatiques.***

Ce qui est mis en cause, ce n'est pas l'absence de services consacrés à la protection informatique. Ce qui pose problème, c'est au contraire la multiplicité des services en charge de cette matière et leur manque de coordination. Pas moins de 6 institutions ont dans leur missions la protection de données ou de systèmes informatiques :

l'Autorité Nationale de Sécurité (**ANS**) ;
la Sûreté de l'Etat (**service de renseignement civil**) ;
le SGRS (**service de renseignement militaire**) ;
le FEDICT (**Service public fédéral de l'Information et de la Communication**) ;
BELNET (**le fournisseur de services Internet des autorités belges**) ;
l'IBPT (**Institut Belge des Services Postaux et des Télécommunications**)
Le résultat de cette dispersion est évident: plus personne n'a donc une vue d'ensemble de la situation ! Et les auteurs du rapport précisent:

> ***L'absence d'une politique fédérale globale en matière de sécurité de l'information (et de réelle autorité en la matière) entraîne une très grande vulnérabilité du pays en cas d'agression sur ses systèmes et réseaux vitaux d'information.***

Ils ne laissent planer aucun doute sur la gravité de la menace:

> ***Les menaces qui pèsent sur ces systèmes d'information sont susceptibles de porter atteinte à la sécurité et aux intérêts fondamentaux de l'Etat.***

Mise en garde globale

Mais le pire est à venir: l'Autorité Nationale de Sécurité est l'organisme qui serait le mieux placé pour assurer cette coordination. Or, le rapport précise que *« les moyens techniques mis à [sa] disposition sont nettement insuffisants »*.

Le rapport pointe aussi du doigt l'importance des certificats et recommande la création d'une instance nationale de certification afin de ne plus dépendre de l'étranger. Mais le cas hollandais démontre malheureusement, que cela ne constitue pas une garantie de sécurité …

Les auteurs recommandent *« la plus grande prudence dans le choix des équipements techniques sécurisés »* ainsi que dans celui *« des fournisseurs de ce matériel »*.

Enfin, le rapport insiste sur la nécessité de protéger les sites des ministères autres que celui de la Défense ou *« ceux d'infrastructures critiques pour le fonctionnement du pays »* . Autrement dit, ils sont pour l'instant exposés aux menaces les plus diverses. Et il recommande de confier cette mission à la Sûreté de l'Etat (VSSE).

Le mot de la fin appartient sans doute à l'association Bits of Freedom, une organisation de défense des données privées des citoyens qui considère que l'attaque de DigiNotar, devrait

constituer *« un 'wake-up call [un coup de smeonce] pour les autorités du monde entier »* .

Alors que la sécurité informatique reste une prérogative nationale jalousement gardée, l'attaque des certificats publics néerlandais tout comme le rapport belge incitent à se demander si les Etats sont vraiment prêts à faire face à une des dimensions les plus subtiles et pourtant les plus dangereuses de la guerre post-moderne : la cyberguerre ? La réponse, pour ces deux pays au moins, est clairement: Non !

—

Article initialement publié sur **MyEurop** sous le titre **Belgique et Pays-Bas : la cyberguerre a commencé !**

FlickR ; **Christopher Schirner** ; **Gianni Dominici** ; **FaceMePLS**; **romainguy** ;

MICHAËL
le 9 septembre 2011 - 9:44 • SIGNALER UN ABUS - PERMALINK

Une petite erreur est présente dans cet article : le Comité R n'est pas une « commission spéciale du Sénat » mais une organisation à part entière (mais dont le président et les deux conseillers sont nommés par le Sénat).

Par contre, il existe au Sénat une commission permanente chargée du suivi parlementaire du Comité R. Autrement dit, un organe de suivi d'un organe de contrôle des services de renseignements. C'est un peu confus, je vous l'accorde :)

La composition et les dossiers étudiés par la commission du Sénat chargée du suivi du Comité R sont visibles ici : http://senate.be/www/?MIval=/index_senate&MENUID=25200&LANG=fr (cinquième commission de la liste).

Et, tant que j'y suis, voici l'URL du rapport du Comité R mentionné dans l'article : http://www.comiteri.be/images/pdf/eigen_publicaties/rapport_181_%20fr.pdf

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

MARCO BERTOLINI
le 12 septembre 2011 - 10:46 • SIGNALER UN ABUS - PERMALINK

Merci pour ces précisions, Michael. Amicalement, Marco

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

1 ping

La Belgique mauvaise eleve en securite informatique ? I mart-e le 10 septembre 2011 - 20:04

[...] Le plat pays sous les cyberattaques [...]