Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Discours de Patrick Pailloux, directeur général de l'Agence nationale de la sécurité des systèmes d'information lors des Assises de la sécurité 2012

Monaco, le mercredi 3 octobre 2012

Seul le prononcé fait foi

Bonjour à tous,

La dernière fois que l'on s'est vu, c'était quasiment il y a un an, jour pour jour, pour la clôture des Assises 2011. On se retrouve pour l'ouverture des Assises 2012.

Permettez-moi de profiter de l'occasion pour une nouvelle fois remercier et féliciter Gérard Rio et son équipe, notamment Sophie Guérin.

Ces mots de remerciement ne sont pas qu'une formule, mais avoir l'occasion de voir comme cela, une fois par an, réunis quasiment tous les acteurs français de la cybersécurité, c'est une chance unique et mon premier message, à l'occasion de cette introduction, c'est : **profitez-en !** Les enjeux que nous avons à relever sont extraordinaires, donc échangez, partagez, rencontrez, étudiez,...

Si j'en reviens à l'année dernière, j'étais intervenu sur le thème de l'hygiène informatique, du retour aux bases.

Je voudrais bien vous dire que tout le monde s'y est mis.

Mais évidemment vous ne me croiriez pas, et vous auriez raison. Pour autant, nous avons rencontré plusieurs entreprises, dont de très grandes qui ont, suite à cette proposition d'actions que je faisais l'année dernière, mis en place un plan concret de progrès. C'est déjà le début d'un succès.

Mais évidemment, c'est sans doute l'arbre qui cache la forêt.

Je rencontre de nombreux chefs d'entreprises et la bonne nouvelle, c'est que la plupart d'entre eux sont désormais conscients du problème et de la nécessité d'agir dans le domaine de la cybersécurité, notamment pour protéger le patrimoine de leur entreprise.

Par contre, la plupart du temps, ils sont assez désarmés, ne savent pas quoi faire concrètement.

Je voudrais partager avec vous le conseil que je donne généralement :

En matière de sécurité informatique, la priorité c'est l'hygiène. Concrètement, il y a un certain nombre de vérifications à faire et de mesures à prendre qui sont proposées par l'ANSSI. Demandez à votre directeur des systèmes d'information de faire ces vérifications, de vous rendre compte point par point, de faire un bilan de situation sur les mesures proposées et de proposer un plan d'actions pour répondre aux difficultés éventuellement rencontrées.

Pour aider à ce travail, l'ANSSI publie aujourd'hui un précis d'hygiène informatique. Nous vous proposons en treize étapes, soit 40 règles concrètes et pratiques, d'assainir votre système d'information. **Ces 40 règles doivent toutes être appliquées** systématiquement, partout. Appliquer ces 40 règles garantira à vos systèmes d'information une meilleure résilience face aux cyberattaques, et donc protégera l'entreprise qui vous fait confiance pour sa sécurité informatique.

Avec ce document plus personne n'a désormais d'excuse pour ne pas appliquer ces mesures.

Je connais d'avance ce que l'on va me rétorquer : votre document est trop compliqué, n'est pas en relation avec la réalité terrain. Je ne crois pas. Nous avons maintenant, croyez-moi, une bonne expérience terrain. Mais admettons. Nous publions aujourd'hui une version 0 que l'on va appeler « version de travail ».

Je fais appel à vous tous aujourd'hui : faites-nous, dans le mois qui vient, tous les commentaires que vous estimerez utiles, si possible constructifs, et sur cette base, nous publierons une première version officielle.

Mon objectif dans cette affaire est simple. Je ne veux plus qu'il soit possible de me dire: « *on ne savait pas quoi faire, c'est compliqué, mon pauvre monsieur si vous saviez, on n'a pas la compétence* ».

Il va désormais y avoir une liste publique de vérifications à faire, de mesures simples à prendre, compréhensibles par presque tout le monde et, c'est une certitude, par tous les informaticiens.

Ceux qui n'auront pas appliqué ces mesures ne pourront s'en prendre qu'à eux-mêmes.

* *

Cela m'amène au deuxième sujet que je voulais évoquer devant vous, qui lui aussi fait souvent l'objet de « *mon pauvre monsieur si vous saviez* » et qui résonne avec le titre de mon intervention sur le pouvoir de dire non.

Sur les raisons de l'absence de sécurité informatique, je crois que j'ai entendu tous les arguments possibles et imaginables. Le plus souvent, ils se résument à deux sujets :

- c'est trop difficile, on n'a pas la compétence, on ne sait pas quoi faire... Le document que nous avons publié répond à cette question ;
- ce n'est pas accepté par les utilisateurs, c'est trop de contraintes.

A force d'entendre, comme vous, ces arguments, je me suis forgé la conviction que l'on a, dans le monde immatériel, des modes de raisonnement que l'on n'a pas dans le monde matériel.

Prenons ensemble quelques exemples :
- la vitesse : dans le monde immatériel il faut être connecté à tout, en permanence pour aller vite. Sur la route, pour faire Paris-Lyon, vous êtes limités à 130 km/h. Pourtant, si vous pouviez aller plus vite, vous pourriez gagner du temps, travailler plus, voir plus de monde. Oui, mais en moyenne, vous ne le faites pas parce qu'il y a une règle, et que, globalement, vous la respectez. En plus, les gendarmes vous aident à la respecter si jamais vous aviez quelques tentations.

- les mots de passe, les cartes d'authentification c'est pénible, c'est long, on perd du temps et puis verrouiller son ordinateur quand on part c'est inutile...
Pourtant, quand vous sortez de chez vous, vous fermez bien les fenêtres, les volets peut-être, les serrures évidemment, vous activez l'alarme, vous fermez le portail... vous ne laissez pas tout ouvert ?

- vos affaires de valeur, vous les mettez peut-être dans un coffre à la banque ? Pourtant, pour y aller, il faut s'organiser, se déplacer aux horaires d'ouverture. Vos affaires de valeur, vous ne les laissez pas traîner n'importe où ?

- en plus, vos affaires de valeur sont triées. Je n'imagine pas que, chez vous par exemple, vos feuilles de salaires ou vos feuilles d'impôts traînent au milieu de piles d'anciens prospectus.

Pourtant, c'est bien ce que l'on fait dans le monde immatériel : on mélange les données sensibles et avec le tout-venant. Celles-ci sont stockées n'importe où. Et le nec plus ultra, les données sont accessibles depuis partout, depuis n'importe quel terminal, de façon immédiate et sans contrainte avec le Cloud, votre smartphone...

J'arrête les exemples.

La question c'est pourquoi dans l'immatériel on n'accepte pas les contraintes et que l'on se croit en sécurité.

Je ne suis pas sociologue, psychologue ou philosophe... je suis ingénieur. Mais ce dont je suis sûr, c'est que si on ne change pas ces comportements, on n'arrivera à pas grand-chose, comme avec l'hygiène.

Le message à faire passer c'est que, dans le monde immatériel, comme ailleurs, il y a des règles, il y a des contraintes, ce n'est pas la jungle, et ceux qui ne respectent pas les règles, d'une manière ou d'une autre, sont sanctionnés.

Alors je sais, les systèmes de sécurité sont parfois lourds. Alors je sais, les tablettes, c'est formidable.

Tenez, restons un instant sur les tablettes. C'est un sujet que j'entends souvent. Je n'ai rien contre cette technologie. Je suis convaincu qu'elle va remplacer à terme, au moins pour partie, les ordinateurs portables. La technologie elle est ce qu'elle est. Mais dès qu'on la connecte, doit-on accepter, pour pouvoir l'utiliser de façon nominale, qu'il faille passer notamment par les fourches caudines de la gestion d'identité d'Apple ou de Google ? Je dis clairement non. En tout cas, dès que l'on manipule des données sensibles. Et franchement, qui dans le milieu professionnel ne manipule pas des données sensibles : les contrats, le fichier clients, les résultats de l'entreprise, l'organisation de la production sont des données sensibles.

Il y a des solutions, ou du moins elles commencent à pointer leur nez, qui permettent de répondre au besoin de mobilité et qui s'adaptent tant bien que mal aux nouvelles technologies. Mais évidemment, elles sont moins conviviales, plus difficiles à gérer pour les équipes informatiques, et elles coûtent de l'argent. Toutes les bonnes raisons de ne pas les utiliser.

Je vais vous dire ma vision des choses : **il faut entrer en résistance contre la liberté totale dans l'usage des technologies de l'information**. Dans une entreprise : **non** on ne travaille pas avec son terminal privé, **non** on ne connecte pas un terminal contrôlé par un tiers, **non** on n'installe pas le dernier joujou à la mode, **non** je ne mets pas les données de mon entreprise dans le Cloud gratuit, **non** je ne mets pas au même endroit mes données sensibles et les autres, **non** je ne laisse pas mon ordinateur connecté si je ne suis pas là. A l'étranger : **non** je ne peux pas, depuis ma chambre d'hôtel, accéder à mes données sans un dispositif de sécurité, **non** je ne vais pas au restaurant en laissant mon portable avec des données sensibles dans ma chambre d'hôtel, **non** je n'envoie pas par mail des informations très sensibles,...

La sécurité c'est aussi avoir le courage de dire non.

Évidemment, c'est au patron de l'entreprise d'assumer ces règles et croyez-moi, c'est comme l'hygiène, c'est possible.

En matière de sécurité, pardonnez-moi cette référence détournée : il est autorisé d'interdire.

Attention, et ce point est évidemment critique : face à l'interdiction, il faut d'une part, expliquer les raisons de ces contraintes, et d'autre part, lorsque la demande correspond à un réel besoin (et non à une envie), trouver et expliquer la façon, certes sans doute moins conviviale, d'arriver au même résultat.

Donc en fait, la bonne réponse n'est pas non, c'est **non mais**.

Une telle posture a également un autre avantage : plutôt que d'enrichir encore un peu plus les fournisseurs de solutions non sécurisées, on favorisera les industriels, qui tant bien que mal, et ils sont nombreux ici, essayent de fournir des solutions sécurisées.

* *

Il y a un dernier point que je voudrais exposer devant vous. Ce sujet est plus grave, d'une certaine façon, que les deux autres. Il ne vous aura pas échappé, je l'espère, que l'ANSSI a publié un guide (un guide et un cas pédagogique) sur la cybersécurité des systèmes industriels.

J'en profite d'ailleurs : on n'a pas publié que cela. Nous avons publié :

- des recommandations de sécurité relatives à un système GNU/Linux ;
- des recommandations de sécurité relatives à Ipsec pour la protection des flux réseau ;
- des recommandations de sécurité relatives à la téléassistance ;
- une méthodologie et des outils d'audit des permissions d'un Active Directory ;
- un guide sur les problématiques de sécurité associées à la virtualisation des systèmes d'information ;
- un guide pour la définition d'une architecture de passerelles d'interconnexion sécurisée ;
- les bons réflexes en cas d'intrusion sur un système d'information ;
- des conseils de prévention et de réaction en cas de dénis de service.

Bref, pas mal de recommandations techniques que l'on voudrait bien voir mises en œuvre. Ces éléments, vous pouvez en user et en abuser.

Pour en revenir à la sécurité des systèmes industriels, je dois vous dire que ce sujet m'inquiète énormément. L'exemple d'Aramco en Arabie Saoudite n'est d'ailleurs pas pour me rassurer.

D'une part, on observe de plus en plus de systèmes industriels informatisés, de plus en plus de systèmes industriels interconnectés avec le réseau de l'entreprise, voire avec Internet, et d'autre part, on voit de plus en plus de personnes s'intéresser à l'attaque de ces dispositifs, on commence même à avoir quelques exemples d'attaques à l'étranger.

Il est absolument impératif que les entreprises qui disposent de systèmes industriels vérifient bien l'isolation de ces derniers de l'Internet et, si ce n'est pas le cas, je n'ai pas d'autre recommandation à faire que de les déconnecter, et je suis extrêmement sérieux.

Si jamais, pour des raisons de fonctionnement, il est impossible de les déconnecter d'Internet, je ne saurais trop recommander de rapidement chercher une solution alternative.

De la même façon, je voudrais attirer l'attention des industriels qui développent et installent des systèmes industriels. J'ai dit précédemment qu'il fallait respecter les règles d'hygiène informatique. Dans le cas des systèmes industriels, c'est presque criminel – et je pèse mes mots - de ne pas les respecter.

Je vous rassure, dans la très grande majorité des cas que nous avons observés, dans la totalité des affaires les plus critiques, ces règles sont bien appliquées, mais il y a de très très nombreux systèmes industriels…

Plus largement, même si ce n'est pas l'objet de la conférence d'aujourd'hui, plongez-vous dans l'étude de cas publiée par l'ANSSI, vous y trouverez matière à réflexion.

Sachez en tout cas que ce sujet est une priorité pour l'ANSSI et que nous sommes à la disposition de ceux d'entre vous qui voudraient échanger sur ce sujet.

On aura sûrement l'occasion d'y revenir dans les années à venir.

* *

Au moment de clore mon intervention, je mesure bien une nouvelle fois le côté un peu agressif et professoral de mon discours. Sincèrement, je préfèrerais être parmi vous et vous dire que cette année les attaques ont baissé, que nos clignotants sont au vert, que mes équipes d'audit n'arrivent plus à pénétrer les systèmes qu'ils testent, que le monde cyber s'apaise…

Malheureusement, ce n'est pas ce que je constate. Et si l'on ne fait pas changer les choses, je ne sais pas où l'on va. Ou plutôt si je sais. Et personne n'aurait envie de ce monde là. L'ANSSI, plus que n'importe qui, doit agir et je veux rendre ici hommage à mes collaborateurs dont les nuits sont souvent courtes.

Je n'ai pas beaucoup parlé de l'ANSSI dans mon intervention mais pour ceux que cela intéresse trois petites brèves :

- Les divisions techniques de l'ANSSI vont déménager au cours du second semestre 2013. Les locaux actuels sont devenus bien trop petits pour absorber notre montée en puissance. Nous allons nous installer dans des locaux de haute qualité environnementale dans le XVème arrondissement de Paris.
- Le challenge glissé dans notre logo sur le site n'est toujours pas résolu…
- Mais surtout, l'ANSSI continue de recruter, sans doute autour de 80 personnes l'année prochaine, en tenant compte du turnover. Donc, si vous connaissez des candidats de valeur qui n'ont pas trop besoin de sommeil... La liste des fiches de poste est d'ailleurs consultable sur Internet et sur notre stand.

Voilà, j'en ai terminé. Il me reste à vous souhaiter de bonnes assises de la sécurité. L'ANSSI est, comme l'année dernière, présente avec un stand. Cela nous donnera l'occasion de multiplier les échanges.