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 d'ouverture des Assises de la Sécurité 2013
de Patrick Pailloux, directeur général
de l'agence nationale de la sécurité des systèmes d'information,

Monaco, le mercredi 2 octobre 2013

Seul le prononcé fait foi

Bonjour à toutes et à tous,

Il y a deux ans, presque jour pour jour, le 8 octobre 2011, ici, dans cette salle, je vous interpellais. Retour aux fondamentaux de la sécurité informatique et application de règles d'hygiène. Souvenez-vous des réactions : position intenable ou règles trop complexes.

Deux ans après, j'ai surtout envie de vous dire merci. Non pas que les règles soient appliquées partout, soyons réalistes et honnêtes. Non pas non plus que ces mesures soient l'alpha et l'oméga, applicables partout. Il faudra inévitablement bien des années avant que tout cela n'entre en pratique, mais vous vous êtes appropriés le concept. Je vois les sociétés de conseil rappeler ces mesures, je vois des DSI de grands groupes mettre en place des plans d'action... J'ai même vu la presse cet été, à propos des raisons de telles fuites dans une grande agence de renseignement d'un très grand pays, recommander d'appliquer le guide d'hygiène de l'ANSSI.

À ce propos d'ailleurs, je vous annonce que nous venons de traduire le désormais célèbre guide d'hygiène en anglais. De nombreuses entreprises ici présentes sont internationales, et les services informatiques sont souvent localisés dans des pays où la langue de travail est l'anglais.

Mais soyons honnêtes entre nous, le chemin est encore long, très long et le constat que nous faisons sur le terrain c'est que dans le domaine de l'hygiène il y a encore beaucoup, beaucoup à faire. Au risque de me répéter, cela doit être votre priorité, toujours.

Il y a presque un an, jour pour jour, le 3 octobre 2012, ici, dans cette salle, je vous interpellais à nouveau. Plus largement, j'interpellais notre communauté, la communauté des informaticiens. Rappelez-vous le pouvoir de dire non et notamment au BYOD, l'utilisation de terminaux personnels à des fins professionnelles.

À l'époque que n'a-t-on pas entendu : position intenable, ridicule, passéiste... Vous noterez comme moi, sans doute, que depuis quelques mois ces critiques se font moins, voire plus du tout, entendre.

Pas sûr que nous y soyons pour grand-chose. L'actualité récente a probablement plus fait pour convaincre les récalcitrants que les discours enflammés du directeur de l'ANSSI.

Je vais d'ailleurs vous raconter une anecdote.

Il y a un certain temps, nous avons été prévenus qu'une application disponible dans tous les magasins d'application des smartphones avait un comportement étonnant. Il s'agissait d'une application gratuite d'annuaire. Simple à télécharger, simple à utiliser : vous tapiez un nom, un prénom et elle vous donnait un numéro de téléphone. Problème : on y trouvait des numéros de téléphone que l'on n'aurait pas dû trouver. En fait, elle ne faisait rien de bien intelligent : après avoir été installée sur le smartphone, elle accédait à vos contacts et les envoyait sur un serveur accessible au monde entier via ladite application. Il suffisait donc que quelqu'un disposant d'un numéro confidentiel, d'une célébrité, l'utilise pour que le monde entier, dans les secondes qui suivent, connaisse ce numéro. Fin de l'histoire. Vous aurez noté j'espère qu'il n'y a aucune attaque informatique dans cette affaire, et que les conditions d'utilisation de cette application, vous savez les 40 pages de petites lignes que personne ne lit, précisaient clairement que l'application accédait aux contacts !

Vous l'aurez compris, nous n'avons pas changé d'un iota notre position. Ce n'est pas à l'employé de définir les règles de sécurité qui doivent s'appliquer aux données informatiques de l'entreprise qu'il manipule mais bien à l'entreprise.
Question de souveraineté de l'entreprise !

* *

Mais le principal sujet dont je veux vous parler cette année n'est pas celui-là. C'est un sujet sérieux, que j'avais rapidement évoqué en fin d'intervention l'année dernière et qui va nécessiter de notre part à tous, dans les années à venir, un effort très important.

J'ai l'habitude de dire que nos sociétés dépendent de l'informatique et des communications électroniques pour vivre. Que ces technologies sont désormais les systèmes nerveux de nos Nations. Que notre survie, au sens étroit du terme, dépend parfois du bon fonctionnement des systèmes d'information : équipements médicaux, transport aérien et ferroviaire, production et distribution d'énergie, transport de l'eau, etc.

Les systèmes industriels, les systèmes de contrôle-commande, les SCADA, puisque c'est de cela dont il s'agit, sont en train de migrer à grande vitesse vers l'IP, de s'intégrer dans les systèmes d'information de l'entreprise, voire d'être connectés à Internet, sans que l'on se soit véritablement préoccupé de leur sécurité. Je dis bien de leur sécurité.

Si j'insiste c'est que je connais le discours des spécialistes de ces systèmes : peut-être que l'on a des problèmes de sécurité mais ce n'est pas grave parce que les dispositifs de sûreté de fonctionnement mis en place nous protègent. Donc tout va bien.

D'abord un petit commentaire sémantique : j'entends par « sécurité » la défense contre les actions malveillantes et par « sûreté » la défense contre les défaillances. Tout ceci n'est pas très simple car dans certains domaines c'est l'inverse et en anglais aussi. Mais peu importe.

Ne nous y trompons pas : ce n'est pas parce que le dispositif est sûr au plan de la sûreté qu'il l'est au plan de la sécurité. Pourquoi ?C'est la façon d'appréhender les choses.

Vous tous ici êtes plus ou moins des scientifiques. Pourtant, si je fais venir un magicien sur cette scène, qu'il me met dans une boîte, me transperce d'épées et me coupe en morceaux, je vais survivre, enfin j'espère. Vous avez beau avoir un esprit scientifique, vous n'aurez rien compris.

Soyons plus concrets et revenons à l'informatique. Dans les dispositifs de sûreté, il y a des capteurs de mesures. Si un capteur déraille ou tombe en panne, le dispositif se considère en danger et peut s'arrêter. Oui, mais si un attaquant est présent sur le réseau (IP la plupart du temps, quand ce n'est pas Internet tout simplement), qu'il intercepte le paquet, remplace la valeur numérique du capteur par une autre, hé bien le dispositif de sûreté va le croire !

On sait bien ici, entre experts de la sécurité, comment résoudre cette question : chiffrement des échanges, authentification forte...

Faites donc le tour de vos installations industrielles et regardez combien de communications entre des capteurs et des automates sont chiffrées et fortement authentifiées...
Tout cela pour vous dire que la séparation entre sécurité et sûreté n'est pas aussi simple qu'il y parait au premier abord.

Il est donc essentiel - vraiment important - que dans ce domaine, on se retrousse les manches et on agisse.

Il faut que les équipementiers qui fournissent des systèmes industriels introduisent des dispositifs de sécurité et, croyez-moi, c'est encore trop rarement le cas.

À ce titre, l'ANSSI a constitué un groupe de travail avec les représentants des industriels du domaine afin de définir, d'ici la fin de cette année, un ensemble de règles de sécurité qui devra être mis en place au sein des systèmes de contrôle-commande industriels.

Il faut que les industriels qui utilisent des machines et autres robots recensent leurs systèmes critiques, analysent leur sécurité, prennent les mesures conservatoires indispensables (par exemple déconnecter d'Internet une installation - on en trouve encore beaucoup trop dans cette situation) et mettent en place un plan de sécurisation. Nous avons fait un guide pour les aider. Il y a ici de nombreuses entreprises qui peuvent les aider à faire ce bilan. Il faut agir et agir vite.

L'État n'est pas en reste.

Le Livre blanc sur la défense et la sécurité nationale publié le 29 avril de cette année en parle abondamment. Je rappelle que ce Livre blanc n'est pas un document marketing d'un groupe de penseurs mais bien la doctrine de défense et de sécurité nationale approuvée par le Président de la République.

Que dit le Livre blanc dans ce domaine ?

Il ne dit pas : il est important de sécuriser nos systèmes critiques et l'État va travailler avec les industriels pour qu'un effort important soit fait. Il est beaucoup plus précis :

Je cite : *S'agissant des activités d'importance vitale pour le fonctionnement normal de la Nation, l'État fixera, par un dispositif législatif et réglementaire approprié, les standards de sécurité à respecter à l'égard de la menace informatique et veillera à ce que les opérateurs prennent les mesures nécessaires pour détecter et traiter tout incident informatique touchant leurs systèmes*

sensibles. Ce dispositif précisera les droits et devoirs des acteurs publics et privés, notamment en matière d'audit, de cartographie de leurs systèmes d'information, de notification des incidents...

C'est fort et clair !

Le Livre blanc a été publié le 29 avril de cette année. Le 2 août 2013, le gouvernement a déposé sur le bureau du Sénat le projet de loi de programmation militaire dont l'article 15 est l'exacte traduction législative de ce que je viens de vous lire. Entre ces deux dates, il s'est écoulé 95 jours pour consulter des industriels, rédiger et soumettre au conseil d'État le projet de texte.

Vous l'aurez compris, il s'agit bien d'une priorité gouvernementale.

Que dit le texte ? Je vous engage à aller sur le site du Sénat, vous y trouverez le texte.

En substance, l'État va réguler la sécurité des systèmes d'information critiques des opérateurs d'importance vitale. La cible est précise :

- les opérateurs d'importance vitale, un peu plus d'une centaine pour ceux qui sont privés, dans 12 secteurs d'activité ;
- les systèmes critiques de ces opérateurs. Donc pas les Intranets ni la paye mais essentiellement les contrôle-commandes de leurs systèmes industriels.

Pour ces systèmes uniquement et si le Parlement en décide ainsi :

- l'État aura la possibilité de fixer des règles de sécurité à appliquer impérativement. Par exemple, tel système critique ne devra pas être connecté à Internet. Dans certains cas, l'État pourra imposer d'installer des sondes de détection fournies et opérées par des opérateurs de confiance labellisés ;
- l'État pourra auditer, ou faire auditer par des prestataires qu'il aura labellisés, ces systèmes afin de vérifier la bonne application des règles édictées et plus largement le niveau de sécurité de ces dispositifs ;
- les opérateurs, toujours pour ces systèmes uniquement, devront signaler à l'ANSSI tout incident informatique affectant leur fonctionnement.

Il s'agit là de mesures préventives. En cas d'attaque importante en cours contre ces systèmes, l'État aura la possibilité d'imposer des mesures aux opérateurs.

Je signale enfin que l'État devra préserver la confidentialité des informations qu'il recueille dans ce cadre. C'est tout à la fois une demande naturelle des opérateurs et un impératif de sécurité pour ne pas dévoiler à des acteurs mal intentionnés des vulnérabilités sur nos systèmes critiques.

Tout ceci, notamment les règles contraignantes, sera discuté, secteur par secteur, pour identifier avec les industriels compétents les mesures à prendre. On imagine assez bien que l'on n'appliquera pas les mêmes règles à une centrale nucléaire qu'à un opérateur de communications électroniques : l'un peut être isolé d'Internet, l'autre c'est "plus difficile". Ce travail a déjà commencé comme je l'indiquais tout à l'heure en mentionnant le groupe de travail que nous avons monté avec les représentants des entreprises de la filière "informatique industrielle".

Vous conviendrez avec moi que le raisonnement est finalement assez simple : l'État ne peut, et ne doit, se désintéresser de la sécurité de ce qui est consubstantiel à la survie de la Nation et à la vie de nos concitoyens. C'est fait en matière de sûreté industrielle, d'environnement, d'incendie, de sûreté médicale. Il n'y a aucune raison de ne pas le faire dans le domaine de la cybersécurité.

* *

Mais l'État ne fait pas que réguler.

Il nous faut impérativement, pour sécuriser les systèmes critiques (et les autres), disposer d'outils de sécurité adaptés et de confiance. J'ai déjà eu plusieurs fois l'occasion de le dire ici, chaque année, nous avons la chance d'avoir des industriels capables de fournir des solutions de sécurité. La plupart sont présents ici, aux Assises de la sécurité. Il faut vous adresser à eux.

Ces industriels sont une chance pour la France. C'est la raison pour laquelle le Président de la République a annoncé le 12 septembre dernier que, parmi les 34 plans de reconquête pour dessiner la France industrielle de demain, un plan était consacré à la cybersécurité.

Il s'agit de fédérer et mobiliser l'ensemble des acteurs de la filière, publics et privés, pour identifier et mettre en œuvre tous les moyens à notre disposition permettant de faire de la France un champion de demain dans la cybersécurité.

Sans attendre le résultat de ces travaux, et dans le cadre des investissements d'avenir, un appel à projet de R&D a été lancé. Il vise notamment à couvrir les domaines suivants :
- les terminaux mobiles sécurisés,
- la visiophonie et la voix sur IP sécurisées,
- les systèmes de détection,
- les dispositifs de protection pour les SCADA,
- les systèmes de supervision de la sécurité (SIEM).

Je signale aux industriels intéressés qu'ils ont jusqu'au 29 novembre pour soumettre leurs projets.

Vous pouvez vous adresser à l'ANSSI pour toute question.

* *

Je ne voudrais pas que l'on se quitte sans vous donner quelques nouvelles de l'ANSSI.

D'abord nous recrutons toujours, donc les candidats sont bienvenus. N'hésitez pas, si vous connaissez des personnes intéressées, à nous les envoyer. Je signale que nous ne recrutons pas que des experts en sécurité mais aussi des informaticiens ou des spécialistes de l'informatique industrielle par exemple. Vous trouverez sur notre site Internet les différentes fiches de poste.

Vous savez que nous avons comme stratégie de non seulement labelliser des produits mais aussi des prestataires de service. Nous avons plusieurs projets dans ce domaine notamment dans le domaine de la cyberdéfense.

Il y en a un dont vous avez du entendre parler, c'est la labellisation des prestataires d'audit de la sécurité des systèmes d'information (PASSI dans notre jargon). Trois sociétés ont déjà réussi leur examen de passage dans le cadre de la procédure expérimentale. Une quatrième est en cours et 20 sociétés vont probablement dans les semaines à venir se lancer. Vous n'aurez plus aucune excuse pour ne plus faire d'audit dans vos entreprises !

Je veux aussi ici vous rappeler que nous publions régulièrement des guides, des recommandations... Ce n'est pas seulement pour emporter ou pour offrir, c'est pour consommer et appliquer.

Le dernier exemple, c'est sur la mise en œuvre correcte du protocole BGP. Le guide sera mis en ligne aujourd'hui sur le site de l'ANSSI.

Je peux également vous conseiller le rapport de l'observatoire de la résilience de l'Internet français, réalisé en collaboration avec l'Afnic.

Je tiens enfin à signaler des recommandations pour la mise en œuvre de dispositifs de vidéoprotection. Dans ce domaine aussi il y a beaucoup à faire. Les nouvelles caméras de surveillance sont de petits PC facilement piratables.

Bref, nous essayons de vous aider, utilisez nos outils !

L'ANSSI est présente sur le salon. N'hésitez pas à venir nous voir.

* *

Enfin puisqu'il me revient l'honneur et le plaisir d'introduire les Assises 2013, je veux souhaiter à tous les exposants beaucoup de réussite - soyez convaincants ; dire à tous les visiteurs : profitez-en ! Il y a ici une concentration d'experts en cybersécurité comme rarement, donc posez vos questions, partagez vos expériences.

Enfin je veux remercier les organisateurs, Gérard Rio et toute son équipe dirigée de main de maître par Sophie Guérin, pour leur énergie, leur savoir-faire et aussi leur sens de l'intérêt général. Si l'on progresse en France dans ce domaine c'est aussi un peu grâce à eux.

Merci à tous et bonnes Assises 2013 !