



Revue de presse 2019

Sommaire

Silicon.fr / Janvier 2019	<u>Jacques de La Rivière : « Nous visons une certification par l'ANSSI prochainement »</u>
BFMTV / Janvier 2019	<u>Ces cyberattaques inexplicables qui préparent les conflits du futur</u>
Global Security Mag / Janvier 2019	<u>Interview : Jacques de La Rivière & Philippe Gillet, Gatewatcher : « Il est nécessaire d'anticiper les menaces »</u>
Silicon.fr / Janvier 2019	<u>Sécurité by-design : analyse des trois grands principes</u>
Silicon.fr / Janvier 2019	<u>FIC 2019 : l'ANSSI dévoile ses premiers visas de sécurité</u>
Le Mag IT / Janvier 2019	<u>FIC 2019 : l'ANSSI décerne ses labels</u>
Global Security Mag / Janvier 2019	<u>Sopra Steria se distingue parmi les premiers à recevoir la qualification Prestataire de Détection des Incidents de Sécurité</u>
ZDNet / Janvier 2019	<u>FIC 2019 : Qualifications PDIS, l'ANSSI désigne les élèves méritants</u>
Solutions Numériques / Janvier 2019	<u>FIC 2019 : l'ANSSI va pouvoir traquer les attaquants en posant des écoutes chez les hébergeurs de serveurs</u>
Ministère des Armées / Janvier 2019	<u>Dossier de presse du Ministère des Armées, Forum International de la Cybersécurité, Lille</u>
Global Security Mag / Janvier 2019	<u>HarfangLab et Gatewatcher remportent le premier prix du Défi Cyber</u>
Ministère des Armées / Janvier 2019	<u>Discours de Florence Parly, Ministre des Armées, Forum International de la Cybersécurité, Lille</u>
Global Security Mag / Janvier 2019	<u>Florence Parly, FIC: la France passe à la « cyber » offensive</u>
Global Security Mag / Janvier 2019	<u>Guillaume Poupard, FIC : « Tous connectés, tous impliqués, tous responsables ! »</u>
AFP / Janvier 2019	<u>Le groupe de technologie Altran frappé par une cyberattaque</u>

Jacques de La Rivière : « Nous visions une certification par l'ANSSI prochainement »

[LIRE](#)



Silicon Cybersecurity Awards 2018 – Lauréat de la catégorie “Solution de détection de menaces” et Grand Prix du jury, Gatewatcher propose une solution de détection des menaces qui allie analyse de signaux faibles et machine learning. 3 questions à Jacques de La Rivière, son CEO et co-fondateur.

Quelle est l'approche de votre technologie Trackwatch pour la détection des menaces ?

Jacques de La Rivière – Nous avons développé Trackwatch avec une double approche de l'innovation : la capture de l'information et l'analyse optimale. Notre technologie unique allie analyse de signaux faibles et machine learning. Présente dans nos sondes, elle utilise 4 moteurs nouvelle génération. Sur les payloads tout d'abord, un moteur analyse les données de façons protocolaire et statistique afin de détecter les anomalies et un second permet de reconnaître les APT (Advanced Persistent Threats) initiées à partir des techniques les plus élaborées (Shellcodes, encodés, ROP, JOP...).

Concernant les malwares, un moteur analyse en temps-réel de façon statique et heuristique (jusqu'à 6 millions de fichiers en 24h) et un autre permet de ré-analyser les fichiers à potentiel malicieux à posteriori, avec de nouvelles signatures.

Votre solution est en cours de qualification de premier niveau auprès de l'ANSSI (Agence Nationale de Sécurité des Systèmes d'Information), quel est l'enjeu pour Gatewatcher ?

Guillaume Poupard l'a effectivement annoncé lors du discours d'ouverture des **Assises de la Sécurité** en octobre dernier : nous visons une certification de notre sonde de détection prochainement.

Le processus de certification est certes long, mais il se justifie par la nécessité de laisser les outils de détection avoir un grand niveau de liberté sur les systèmes. Le compromis entre cette flexibilité et la robustesse est souvent délicat à trouver.

Mais ce sont tout d'abord l'expertise et le travail de notre équipe d'ingénieurs-chercheurs et notre technologie unique de détection qui sont reconnues à travers cette certification. Nous sommes toutefois conscients que cette certification n'a rien de définitif. Notre produit va continuer d'évoluer pour être toujours plus performant face aux nouvelles menaces. Nous fournirons donc des notes d'impact à l'ANSSI à chaque nouvelle mise à jour afin qu'elle puisse déterminer si le socle de sécurité et le durcissement restent conformes à ce qui est exigé.

Jacques de La Rivière : « Nous visions une certification par l'ANSSI prochainement »

LIRE

On a senti une plus grande sensibilisation aux problématiques de cybersécurité en 2018, comment l'analysez-vous ?

L'année dernière, un véritable coup de projecteur a été mis sur la notion de security et de privacy by design. Cela a fortement contribué à la prise de conscience collective sur les problématiques de cybersécurité : elles doivent être intégrées dès la conception mais pas seulement. Elles doivent être adressées tout au long du cycle de vie d'un produit, d'une application ou d'un objet connecté. Mais on constate encore aujourd'hui que de nombreuses start-ups, notamment dans l'Internet des objets, n'intègrent pas encore cette notion dès la création de leurs produits.

La sensibilisation aux problématiques de cybersécurité doit donc se poursuivre de façon intensive en 2019.

Ces cyberattaques inexplicables qui préparent les conflits du futur

[LIRE](#)

FIC 2019 - A l'occasion du Forum international de la cybersécurité, les autorités françaises se sont inquiétées d'un nouveau type de cybermenaces. Plus insidieuses et difficilement détectables, elles permettent à leurs responsables de placer leurs pions pour anticiper des conflits futurs.

C'est au fil des années devenu un classique du genre. A l'ouverture de la 10e édition du Forum International de la cybersécurité, organisée ces 22 et 23 janvier à Lille, Guillaume Poupard a dressé un bilan inquiétant de l'évolution des cybermenaces, en avançant l'expression d'"état d'urgence numérique". Le directeur général de l'ANSSI, l'agence chargée **de la sécurité informatique** des infrastructures d'État, a notamment pointé du doigt un nouveau type de menaces: des "attaques inexplicables pour l'heure" mais qui laissent augurer des conflits futurs.

Ce qui nous préoccupe le plus à l'heure actuelle a trait aux attaques dont on ne parvient pas à déterminer l'objectif", a ainsi expliqué Guillaume Poupard. "Il s'agit clairement d'un positionnement anticipé de personnes de très haut niveau qui prennent de l'avance sur les conflits de demain". Concrètement cela implique des intrusions dans les systèmes informatiques de grandes entreprises stratégiques ou d'infrastructures publiques, sans pour autant en prendre le contrôle ni rechercher d'effets immédiats.

Le but étant de préparer le terrain pour des opérations futures de sabotage ou de destruction de réseaux informatiques critiques, une fois le moment venu. Derrière ces initiatives, Guillaume Poupard ne voit pas l'oeuvre de cybercriminels attirés par l'appât du gain mais de "services dotés de moyens très importants".

Ces cyberattaques inexplicables qui préparent les conflits du futur

[LIRE](#)

L'énergie et la santé exposés

Quelles futures attaques de telles opérations de "minage numérique" laissent-elles augurer ? "Plusieurs scénarii sont possibles", anticipe Jacques de la Rivière, président de Gatewatcher, une entreprise spécialisée en sécurité et en détection d'intrusions informatiques. "On pense notamment aux attaques de réseaux critiques dans l'énergie, la santé ou les télécoms, qui nécessitent des mois voire des années de préparation. Il est également possible d'imaginer des tentatives de déstabilisation passant par le blocage de services bancaires."

L'un des clients de l'entreprise a notamment fait face à un problème de ce type. Bon nombre des coordonnées bancaires de ses fournisseurs ont été remplacées par des IBAN chinois, pour rediriger automatiquement des virements, de façon indétectable.

En avril, l'ANSSI dévoilera **une liste des cybermenaces** auxquelles l'Etat français et ses infrastructures critiques sont confrontés. Ces nouvelles attaques plus complexes à appréhender y auront une place d'honneur. L'institution a une nouvelle fois martelé l'urgente nécessité de prendre au sérieux ces considérations numériques. L'appel a déjà été entendu par l'armée. En amont du FIC, le 18 janvier, la ministre des Armées Florence Parly a indiqué que les militaires français ne devraient désormais plus seulement se défendre face aux cyberattaques mais être en mesure d'en initier.

Interview : Jacques de la Rivière & Philippe Gillet, Gatewatcher : Il est nécessaire d'anticiper les menaces

LIRE



Jacques de La Rivière (CEO) & Philippe Gillet (CTO) de Gatewatcher estiment que le FIC est un rendez-vous majeur qui leur permet de présenter l'orientation stratégique qu'ils vont donner à la nouvelle année. Ainsi pour 2019, Gatewatcher mettra en avant la GBOX, une nouvelle appliance d'analyse dynamique à travers laquelle la menace sera examinée dans le but de générer un rapport d'analyse complet et Gatewatcher Foundation : un OS serveur.

Global Security Mag : Quelle actualité allez-vous mettre en avant à l'occasion de la 11ème édition du Forum International de la Cybersécurité ?

Jacques de La Rivière & Philippe Gillet : Le FIC est pour nous un rendez-vous majeur qui nous permet de présenter l'orientation stratégique que nous allons donner à la nouvelle année. Pour 2019, nous allons mettre l'accent sur nos nouveaux produits. Tout d'abord la GBOX, une nouvelle appliance d'analyse dynamique à travers laquelle la menace sera examinée dans le but de générer un rapport d'analyse complet. La GBOX s'appuie sur une technologie unique de machine learning basée sur la connaissance générée par nos moteurs de détection. L'objectif est d'anticiper l'utilisation de fonctions malveillantes dans tous types de fichiers qui transitent sur le réseau : ransomwares, macros, cryptolockers... Nous mettrons également l'accent sur Gatewatcher Foundation : un OS serveur, à la fois durci et flexible pour s'adapter aux besoins du client en conciliant des exigences de sécurité renforcée et l'agilité.

GS Mag : Selon vous, qu'ils soient d'ordre psychologique, technique, humain ou financier, quels sont les défis liés à la sécurité et à la privacy « by-design », thème du FIC 2019 ?

Jacques de La Rivière & Philippe Gillet : Les défis liés à la sécurité et à la privacy « by-design » sont multiples. Sur l'aspect technique tout d'abord, il faut mutualiser et diversifier les expertises : un seul expert sécurité ne peut pas adresser toutes les questions générées par la mise en place d'une stratégie « by-design ». Du côté humain, la sécurité peut créer des frustrations et empêcher l'innovation : il faut donc être créatif pour contourner les obstacles. Les challenges à relever sont également d'ordre juridique car la privacy « by-design » contraint de nombreuses entreprises à repenser leur business model, les obligations légales ne permettant plus de faire « comme avant » (comme nous avons pu l'observer avec le RGPD notamment). Enfin, sur l'aspect financier, il est important de considérer la sécurité comme un investissement et non comme un coût : il est essentiel de la prévoir de manière intégrée dès le début.

GS Mag : Quels sont vos 3 conseils aux organisations pour relever ces défis ?

Jacques de La Rivière & Philippe Gillet : Nous avons utilisé les grands principes de la sécurité et de la privacy « by-design » lors de la création de Gatewatcher. Nos conseils aux organisations pour relever ces défis proviennent de notre expérience. Premièrement, l'architecture du produit doit être pensée de manière sécurisée dès le début. Chaque pièce doit comporter des notions fondamentales de sécurité et chaque choix doit être confronté à des experts sécurité.

8 janvier 2019
Par Marc Jacob

Interview : Jacques de la Rivière & Philippe Gillet, Gatewatcher : Il est nécessaire d'anticiper les menaces

[LIRE](#)

Il faut ensuite que la sécurité et la vie privée soient des facteurs d'innovation et non plus perçues comme des contraintes. Pour cela, nous intégrons des options dans nos interfaces qui permettent de se rendre réellement compte des apports de la sécurité et de la privacy « by-design » dans le produit.

Enfin, il faut que les produits possèdent de véritables guides utilisateurs permettant de comprendre comment assurer la vie privée et l'interaction des différentes options. Chez Gatewatcher, nous proposons d'ailleurs plusieurs cursus de formation sur ces sujets.

GS Mag : Qu'est-ce qui a changé pour les entreprises avec le RGPD et où en sont-elles dans leur mise en conformité ?

Jacques de La Rivière & Philippe Gillet : Une non-conformité à la RGPD peut porter atteinte à la réputation d'une entreprise et entraîner une baisse de confiance chez les clients et partenaires : bon nombre d'entre elles ont déjà bien intégré cette notion et on fait des efforts considérables pour être en conformité. Une grande majorité a mis en place une charte sur la gestion des données personnelles ou encore une politique de confidentialité. Mais leur bonne volonté semble toutefois buter sur des thématiques plus complexes, notamment en termes de consentement ou d'accès à l'information en fonction du support utilisé. Ce sont pourtant des éléments clés de la politique de protection des données personnelles qui pourraient à terme porter préjudice aux marques. Les efforts devront donc se poursuivre en 2019.

GS Mag : A quoi devons-nous, selon vous, nous attendre en 2019, que ce soit du côté de l'attaque ou de la défense ?

Jacques de La Rivière & Philippe Gillet : Nous avons publié début décembre un rapport regroupant le bilan de l'année 2018 et les tendances pour cette nouvelle année.

Parmi les perspectives auxquelles nous devons nous attendre, nous avons notamment noté l'industrialisation de la cybercriminalité (la structuration des groupes de hackers ayant déjà fortement évolué l'année dernière). Le ciblage des attaques va également se renforcer et devenir de plus en plus courant assurant un meilleur rendement et des dégâts plus importants. Les attaques sur les mobiles et l'IoT vont se généraliser, et la sécurisation de ces dispositifs nous paraît indispensable dans les mois qui viennent. Les attaques sur routeurs vont également devenir monnaie courante car ils ne sont que très peu mis à jour, laissant ainsi de nombreuses failles et vulnérabilités à la portée des hackers.

GS Mag : Quel est votre message à nos lecteurs ?

Jacques de La Rivière & Philippe Gillet : Notre équipe vous attend durant le FIC sur le stand A15, à proximité de celui de l'ANSSI et de l'espace Hexatruster, pour évoquer tous ces sujets et vous présenter Gatewatcher lors d'une démonstration ! A très vite !

Sécurité by-design : analyse des trois grands principes

LIRE

Avis d'expert

Dans chaque produit, application, système ou objet connecté la sécurité est un point clé. A l'occasion de la 11ème édition du Forum International Cybersécurité qui a pour thème la sécurité et la privacy by-design, retour sur trois des grands principes de la sécurité by-design, avec notre regard et notre expérience.

Principe n°1 : minimiser la surface d'attaque

La surface d'attaque représente tous les points d'entrée et les points de communication qu'un système d'information possède avec l'extérieur. Elle peut être logicielle (OS, librairie, accès en lecture/écriture), réseau (ports ouverts, IP actives, flux réseaux, protocoles utilisés), humaine (phishing, social engineering) ou encore physique (intrusion dans les locaux).

Un SI disposant d'une surface d'attaque étendue sera plus vulnérable aux attaques car les moyens de filtrage et de contrôle sont plus complexes à mettre en place et à organiser. Une fois que tous les points de la surface d'attaque ont été identifiés, il faut mettre en place des outils de surveillance ou de protection avancés sur ces points. Pour les systèmes très exposés, il est également conseillé de réaliser des analyses de sécurité régulières.

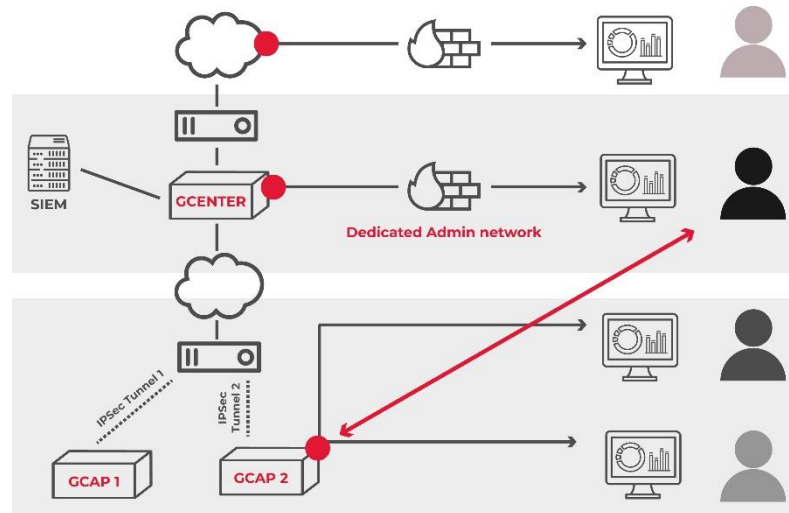
Parmi les solutions envisageables pour réduire la surface d'attaque d'un système d'exploitation, on retrouve également un principe bien connu mais peu appliqué : le durcissement. Il consiste à analyser tout ce qui n'est pas ou peu utilisé sur le système, dans le but de fermer des services et des ports pour limiter les possibilités d'interaction à distance avec ce système. C'est ce principe qui a été appliqué dans la conception de nos sondes de détection de menaces.

Principe n°2 : le moindre privilège

Selon l'ANSSI, le principe du moindre privilège stipule qu'un administrateur donné n'a accès qu'à la ou les zones d'administration dont il a le juste besoin opérationnel, sans possibilité technique d'accéder à une autre zone. Dans les cas spécifiques des droits les plus privilégiés sur l'annuaire lui-même, seuls des administrateurs du SI d'administration peuvent en disposer.

Ce principe est indissociable de la sécurité by-design. Une répartition claire des tâche, rôles et droits attribués c'est garantir le cloisonnement d'un environnement. Une fois le principe du moindre privilège mis en place, la compromission d'une sous-partie de l'environnement devient plus difficile car sa surface d'attaque est fortement réduite. Une corruption n'aura dans ce cas-là que des conséquences limitées. L'application de ce principe dès la conception va de pair avec l'idée de séparation des rôles.

Sécurité by-design : analyse des trois grands principes



Opérateur : consultation des alertes, recherche IOC, forensics.

Administrateur système : création des rôles, gestion des droits, configuration des sondes et gestion des appliances.

Administrateur local : consultation des alertes et des logs système, activation/désactivation des remontées d'informations.

Auditeur : consultation des alertes, consultation des logs des sondes.

Sécurité by-design : analyse des trois grands principes

LIRE

Principe n°3 : la défense en profondeur

Dans cette même logique, nous retrouvons le principe de défense en profondeur ou « defense in depth ». Terme emprunté à une technique militaire destinée à retarder l'ennemi, la défense en profondeur consiste à exploiter plusieurs techniques de sécurité afin de réduire le risque lorsqu'un composant est compromis ou défaillant. L'idée est d'opposer aux menaces des lignes de défense coordonnées et indépendantes afin de faire reposer la sécurité sur un ensemble cohérent et non sur un élément. En tant que « barrière », un produit de sécurité doit être surveillé, protégé et bénéficier de plan de réaction en cas d'incident. Pour mettre en place cette défense en profondeur, les étapes recommandées sont les suivantes :

- Détermination des objectifs de sécurité pour construire la stratégie de défense en profondeur,
- Élaboration de l'organisation et de l'architecture générale du système pour définir les points de contrôle et d'évaluation,
- Élaboration de la politique de défense,
- Qualification du système au regard des critères de défense en profondeur,
- Évaluation de la défense permanente et périodique à partir des méthodes d'attaques et du retour d'expérience (contrôle et audit).

Bien sûr, l'application seule de ces trois grands principes dans la conception d'une application, d'un système, d'un objet connecté ou d'un logiciel, ne saurait garantir son imperméabilité aux attaques et aux intrusions. La démarche de la sécurité by-design doit être étendue au-delà de la phase de conception, elle doit être prise en compte tout au long du cycle de vie du produit et doit être l'affaire de tous les acteurs du développement produit.

FIC 2019 : l'ANSSI dévoile ses premiers visas de sécurité

[LIRE](#)



L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a certifié trois offres de cybersécurité, une offre de Cloud et une validation en cours pour deux sondes de détection des menaces.

Lille, envoyé spécial – Au cœur de l'écosystème français de la cybersécurité, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a annoncé ses premières certifications dans le cadre du 11ème Forum International de la Cybersécurité (FIC 2019) par la voix de son directeur général Guillaume Poupard.

Dans la catégorie "Prestataires", ils sont trois à avoir obtenu la **qualification de PDIS** (Prestataires en Détection d'Incidents de Sécurité) : Orange Cyberdefense pour son offre "Security Event Intelligence", Sopra Steria pour son **SOC PDIS** et Sogeti (Cap Gemini).

Pour les trois sociétés de service, cette certification permet d'adresser les **Opérateurs d'Importance Vitale** (OIV) qui sont obligés de faire appel à des prestataires et des offres qui répondent aux référentiels mis en place par l'ANSSI. Il s'agit de près de 200 entreprises privées et publiques, réparties dans 12 secteurs d'activité, qui exploitent ou utilisent des installations jugées indispensables pour la survie de la Nation.

Cette première vague devrait être suivie par d'autres puisque IBM France, Bull, BT Services, Cassidian Cybersecurity, Connix Technologies et Services, et Thales Services sont **en cours de qualification**.

Un label SecNumCloud

Sujet sensible et tendance forte de la cybersécurité en 2019, **la sécurisation de Cloud** est certifiée via la qualification SecNumCloud. Oodrive est le premier acteur du Cloud à obtenir le sésame basé sur les spécifications de l'ISO 27001 auxquelles s'ajoutent des exigences techniques et des engagements sur la localisation des données en Europe. " La qualification SecNumCloud est valable 3 ans, avec un audit de surveillance à mi-parcours permettant à l'ANSSI d'identifier les éventuelles évolutions de l'offre et les ajustements à prévoir" indique Oodrive.

Deux sondes de détection des menaces en attente

Enfin, les prochaines certifications sont en cours pour deux sondes de détection des menaces qui devraient être délivrées d'ici un mois, dicit Guillaume Poupard : Thales et **Gatewatcher** (lauréat d'un **Silicon Cybersecurity Award 2018**).

Orange Cyberdefense, Sogeti et SopraSteria sont désormais prestataires de services de détection d'intrusion qualifiés. Oodrive reçoit le label SecNumCloud.

Guillaume Poupard, directeur général de l'Agence nationale pour la sécurité des systèmes d'information (Anssi), l'avait glissé lors des Assises de la Sécurité, au mois d'octobre dernier, à Monaco : les premières qualifications PDIS – prestataire de services de détection d'intrusion – devaient être délivrées début 2019. Le Forum international de la cybersécurité (FIC), qui se déroule actuellement à Lille, en a été l'occasion.

A l'issue d'un processus décrit précédemment comme « douloureux, parce que les exigences sont très élevées », Orange Cyberdefense, Sogeti et SopraSteria sont donc les premiers heureux élus. Tous trois vont donc pouvoir proposer leurs services aux opérateurs d'importance vitale (OIV) pour leurs systèmes d'information d'importance vitale (SIIV), conformément à la réglementation en vigueur. Dans les travées du FIC, l'absence de Thales ou encore d'Airbus Cybersecurity, pour cette première liste de prestataires qualifiés, ne passe toutefois pas inaperçue.

Mais voilà, pour que démarre véritablement l'offre de services, encore faut-il que l'offre technique soit là. Deux sondes devaient être qualifiées par l'Anssi d'ici la fin 2018, celles de Thales et de Gatewatcher. C'était une notification faite aux Assises de la Sécurité. Elle attend encore de se concrétiser, mais cela ne devrait plus trop tarder : les annonces sont attendues pour le mois de février 2019.

Pour autant, l'Anssi continue d'avancer dans sa stratégie de qualification. Après les prestataires d'audit de sécurité (Passi) et de détection d'incidents, voire de réponse aux incidents (PRIS), l'agence prévoit de labelliser ceux d'administration et de maintenance sécurisées (infogérance, maintenance) – les PAMS. L'Anssi n'en est là qu'au tout début des travaux de définition du référentiel qui s'appliquera, à terme, à ces infogérants. Mais Guillaume Poupard évoquait déjà, à l'automne, des exigences de cloisonnement d'infrastructure ou encore de traçabilité individuelle des actions, ce qui risque de ne pas toujours passer sans grincement de dents.

FIC 2019 : l'ANSSI décerne ses labels

[LIRE](#)

Le directeur général de l'agence a également profité du FIC pour annoncer la première labélisation SecNumCloud. Dévoilée initialement fin 2016, cette qualification vise à identifier les fournisseurs de services cloud s'inscrivant dans une logique de cloud public souverain et reprend, pour ses exigences de niveau « essentiel », le référentiel Secure Cloud de 2014. Sur les rangs pour décrocher le label SecNumCloud, on trouve bien sûr Orange avec Cloudwatt, mais encore Outscale et Wordline. Mais le premier élu est Oodrive. Après beaucoup de travail, toutefois, à en croire Guillaume Poupard.

Enfin, Akerva, Sentryo, CDC Arkhinéo, Digital Security, Digitemis, Tixeo, ou encore Yes We Hack, ont reçu, à l'occasion du FIC, le label France Cybersecurity. Anoncé lors de l'édition 2015 de ce forum, par Axelle Lemaire, alors secrétaire d'Etat chargée du numérique, ce label est attribué après un examen collectif par l'Anssi, la Direction générale de l'armement, le Cesin, le Clusif, ou encore Hexatrust, notamment. A ne pas confondre avec les Visas de sécurité annoncés au mois de juin dernier.

Sopra Steria se distingue parmi les premiers à recevoir la qualification Prestataire de Détection des Incidents de Sécurité (PDIS)

[LIRE](#)

A l'occasion du Forum International de la Cybersécurité (FIC) qui s'ouvre aujourd'hui, Sopra Steria fait partie des premiers à recevoir la qualification Prestataire de Détection d'Incidents de Sécurité (PDIS) attribuée par l'Agence Nationale de Sécurité des SI (ANSSI). Partenaire cyber de confiance engagé dans la cybersécurité globale des Opérateurs d'Importance Vitale (OIV), Sopra Steria est déjà qualifié Prestataire d'Audit SSI (PASSI).

Face à l'accélération des cyber-menaces et à l'ampleur croissante de leurs impacts, les Etats prennent des dispositions depuis plusieurs années pour adresser les enjeux de résilience des infrastructures critiques et renforcer la souveraineté nationale. En France, la Loi de Programmation Militaire (LPM) impose depuis 2013 aux OIV de mettre en œuvre des mesures visant à assurer la sécurité des systèmes d'information d'importance vitale (SIIV).

Qualifications ANSSI et SOC PDIS

L'ANSSI accompagne ces OIV dans leurs démarches de mise en conformité et s'assure de la mise en application de la loi. Ainsi, les OIV ont l'obligation de recourir à des prestataires souverains et de confiance pour les phases sensibles de la cyber sécurité de leurs SIIV. Pour qualifier ces prestataires, l'ANSSI a mis en place des référentiels d'exigences, parmi lesquels PDIS dans le domaine de la détection des incidents de sécurité.

Le référentiel PDIS requiert que les moyens humains, techniques et organisationnels mobilisés pour la détection d'incidents de sécurité répondent aux meilleures pratiques dans le domaine du SOC (Security Operations Centre). La mission de ce SOC est de prévenir, détecter et traiter les incidents de sécurité, en favorisant les actions de remédiation.

Sopra Steria compte parmi les leaders dans le domaine du SOC en France

Sopra Steria accompagne de grands donneurs d'ordre issus des secteurs identifiés « d'importance vitale » notamment l'Aéronautique, l'Energie, la Banque, le Transport et la Défense. Ainsi, Sopra Steria a fait le choix d'investir dans la mise en œuvre de services respectant les exigences des référentiels de l'ANSSI. Impliqué depuis plus de 3 ans auprès de l'Anssi tout au long du processus de construction du référentiel PDIS, Sopra Steria a notamment éprouvé l'application du référentiel dans ses opérations SOC lors de la phase expérimentale.

Le SOC PDIS Sopra Steria est un service de détection des incidents de sécurité, 100% externalisé sur son centre de cybersécurité de Toulouse. Il répond aux exigences PDIS en matière de réalisation des activités du SOC, de sécurité du service, de gouvernance et de compétence des analystes. Sopra Steria a retenu les sondes GCAP de Gatewatcher, spécialiste de la détection des menaces cyber, qui équipent déjà de nombreux OIV.

Sopra Steria associe à ce service toute son expertise dans la définition et l'implémentation d'une stratégie de détection adaptée au profil de risque cyber des organisations et au traitement de leurs incidents de sécurité en 24/7.

FIC 2019 : Qualifications PDIS, l'Anssi désigne les élèves méritants

Business : Le directeur de l'Anssi Guillaume Poupard annonce les premiers prestataires labellisés PDIS, le label de l'Anssi qualifiant les prestataires de service de détection d'incidents de sécurité. Une distinction qui se mérite.

L'Anssi aimerait y voir un peu plus clair, et elle entend trouver les partenaires qui vont l'y aider. Le directeur de l'agence nationale de sécurité des systèmes d'information a profité du FIC pour détailler les grands chantiers de l'Anssi pour l'année 2019 et a mis l'accent sur un sujet essentiel dès lors qu'il est question de sécurité informatique : la détection des attaques.

Ce n'est pas la première fois que l'Anssi évoque cette question. En réalité, le sujet est sur la table depuis plusieurs années : la LPM 2014-2019 a en effet mis en place une liste d'opérateurs d'importance vitale, qui doivent se soumettre à toute une série d'exigences réglementaires en matière de sécurité informatique. Pour accompagner ces exigences, c'est à l'Anssi de designer quels acteurs sont aujourd'hui en mesure de proposer des services disposant d'un niveau de qualité suffisant. « Pour nous, l'enjeu est de permettre aux offreurs de solutions et aux demandeurs de monter en gamme de manière parallèle. C'est un équilibre à trouver, on ne peut pas exiger des OIV qu'ils se dotent de prestataires de services certifiés puis leur présenter une liste vide », résumait Guillaume Poupard lors de sa conférence de presse.

Au royaume des aveugles, les borgnes sont rois

L'Anssi entend en effet se doter d'un écosystème de prestataires qualifiés et a révélé les premiers bénéficiaires de ses qualifications PDIS, pour Prestataire de Détection des Incidents de Sécurité. Un terme qui désigne notamment des sociétés proposant des services de type SOC (Security Operation Center) sur le marché. Parmi les heureux élus, on retrouve donc Orange Cyberdefense, Sopra Steria et Sogeti. Une première vague, mais d'autres attendent leur tour : le site de l'Anssi liste ainsi huit sociétés ayant officiellement entrepris le processus de qualification pour se voir labellisé PDIS et précise que la liste recense uniquement les entreprises ayant choisi de rendre publique leur candidature.

Si le terme peut paraître un peu barbare au premier abord, il désigne les entreprises qui sont capables de proposer des prestations conformes au « référentiel d'exigences applicables aux prestataires de détection des incidents de sécurité. » Un document publié initialement en 2015 par l'Anssi à titre expérimental puis remanié courant 2017 et qui regroupe toutes les exigences de l'agence pour les entreprises qui entendent proposer un service de détection qualifié par l'état. Et ça n'est pas une simple affaire de case à cocher, comme l'explique Jean Philippe Cassard, responsable de la conformité réglementaire chez Sopra Steria : « Le référentiel, cela représente plus de 400 exigences à prendre en compte pour notre activité. Concrètement, nous avons été obligés de mettre en place un SOC PDIS séparé de notre SOC « traditionnel » pour pouvoir répondre au niveau d'exigence requise pour obtenir la qualification. »

FIC 2019 : Qualifications PDIS, l'Anssi désigne les élèves méritants

Ce n'est donc pas vraiment une simple lubie d'entreprise qui voudrait pouvoir afficher fièrement une qualification de plus à son CV, Jean Philippe Cassard rappelle que les investissements nécessaires pour atteindre le niveau de sécurité exigé sont considérables, tant sur l'infrastructure qu'en termes de moyens humains mis en œuvre pour suivre le dossier. Pour prétendre toucher le marché des OIV et assurer le rôle de SOC auprès de ces clients d'un genre un peu particulier, c'est toute l'architecture qui doit être repensée avec la sécurité en ligne de mire. « Autant sur des qualifications PASSI, qui visaient plutôt les prestataires d'audit, l'essentiel des contrôles portait sur les personnes. Mais avec cette qualification, ce sont des questions liées à l'infrastructure et à l'architecture du système qui se posent » rappelle Arnaud Hess, directeur du développement cybersécurité chez Sopra Steria.

Un coût non négligeable et un travail de fourmi sont nécessaires, mais c'est à ce prix que les sociétés s'ouvrent une voie royale pour toucher les clients faisant partie de la catégorie des « opérateurs d'importance vitale. » Et si on pense évidemment à eux, ce ne sont pas les seuls en ligne de mire comme l'explique Jean Philippe Cassard : « C'est vrai que c'est un investissement important. Mais il faut voir que ça va structurer le marché : les entreprises qui vont vouloir prendre un SOC vont naturellement se tourner vers les prestataires qualifiés, même s'ils n'en ont pas forcément l'obligation. »

Certifier et choisir

Outre cette qualification PDIS, l'Anssi a aussi profité du FIC pour annoncer avoir remis la qualification de prestataire cloud (SecNumCloud) à la société Oodrive, et que Thalès et Gatewatcher devraient bientôt se voir labelliser de la même manière pour leurs sondes de détection. En favorisant l'écosystème et en labellisant les acteurs, l'Anssi tente donc de donner des ressources aux acteurs de la sécurité et de désigner l'excellence.

On pourrait s'étonner que l'ensemble des solutions aujourd'hui approuvées par l'Anssi soient françaises. Interrogé, Guillaume Poupard se défend de faire du favoritisme, mais rappelle certaines réalités : « ces certifications sont tout à fait ouvertes aux acteurs étrangers, mais ils se heurtent souvent à des limites évidentes, par exemple sur les questions liées à la territorialisation des données. » Comme à son habitude, l'Anssi ne veut pas faire de géopolitique et préfère le concret.



FIC 2019 – L'ANSSI va pouvoir traquer les attaquants en posant des écoutes chez les hébergeurs de serveurs



Dix ans après la création de l'ANSSI, la mission de l'autorité française de la cybersécurité évolue. Désormais, l'ANSSI va pouvoir traquer les attaquants en posant des écoutes chez les hébergeurs de serveurs. Une évolution sous le contrôle de l'Arcep, l'Autorité de régulation des communications électroniques et des postes.

Comme chaque année, le discours d'ouverture de Guillaume Poupard était très attendu sur le Forum International de la Cybersécurité (FIC) qui se déroule les 22 et 23 janvier à Lille. Appelant chacun, et non plus seulement les RSSI, à assurer la cybersécurité, le directeur de l'ANSSI est revenu sur l'année 2018. Dans le cadre de la transposition de la directive européenne NIS (Network and Information Security), elle a vu la nomination des 120 premiers OSE français, les Opérateurs de Services Essentiels. On a d'ailleurs appris qu'il s'agissait en fait des 120 OIV (Opérateurs d'Importance Citale) déjà listés. Néanmoins, plusieurs autres vagues de désignations vont survenir dans les mois et années à venir pour élargir le nombre d'entreprises françaises concernées par cette réglementation.

De nouveaux fournisseurs décrochent leur certification ANSSI

Guillaume Poupard a aussi révélé les noms des trois premiers prestataires de détection à avoir décroché leur certification PDIS (Prestataires de détection d'incidents de sécurité) : Orange Cyberdéfense, Sopra Steria et Sogeti. D'autres nominations devant suivre très prochainement. Côté outillage, les sondes Gatewatcher et Thales sont sur le point d'être finalisées, tandis qu'Oodrive est le premier prestataire Cloud à recevoir le coup de tampon de l'ANSSI. « D'autres acteurs Cloud vont arriver. Cette certification est ouverte à des acteurs pas nécessairement franco-français, néanmoins, les réglementations extraterritoriales de certains posent question et sont clairement contradictoires avec nos règles. »

L'ANSSI passe en mode détection d'attaques, sous le contrôle de l'Arcep

Outre son travail de contrôle, de certification des offres de cybersécurité et d'assistance aux administrations et entreprises françaises sous le feu d'une attaque, l'ANSSI va jouer un rôle plus actif sur le plan de la détection des attaques. « Si nous savons aujourd'hui traiter le volet réponse à incident, nous étions souvent frustrés lorsque nous savions que les serveurs d'une entreprise française étaient infiltrés mais nous ne pouvions mettre ces serveurs sous surveillance et observer les attaquants. Le décret a été publié et il permet aux opérateurs de faire de la détection d'attaque sur les flux de leurs clients de même que nous allons pouvoir positionner des systèmes de détection d'attaque sur les serveurs des opérateurs et des hébergeurs sous le contrôle de l'Arcep. »

FIC 2019 – L'ANSSI va pouvoir traquer les attaquants en posant des écoutes chez les hébergeurs de serveurs

Alors que Florence Parly, ministre des Armées dévoilait la doctrine offensive de la France en matière de cyberguerre, Guillaume Poupard a apporté quelques précisions. Si le directeur de l'ANSSI considère des opérations de représailles menées par des entreprises privées en cas d'attaque comme une « *abomination* », il a souligné que le discours de Florence Parly n'était pas véritablement un changement de doctrine pour la France : « *Dès le texte de la loi de 2008 qui a donné naissance à l'ANSSI, il était évoqué des capacités de cyberdéfense offensive. Il ne faut pas opposer offensif et défensif et il ne faut pas rester les mains dans les poches en cas d'attaque, c'est dans l'évolution des conflits. L'important, c'est de disposer d'un encadrement légal, c'est la voie qu'a choisie la France et je me félicite que la France ait eu le courage de le faire.* »

Guillaume Poupard écarte la polémique sur l'interdiction de Huawei

L'arrivée de la 5G, qui devrait marquer une nouvelle étape vers l'omniprésence des réseaux dans l'économie de demain, donne encore plus d'importance à la défense des intérêts français dans cette cyberguerre mondiale. Face aux annonces de plusieurs pays de vouloir barrer l'accès de leurs infrastructures 5G aux fournisseurs chinois, et en particulier à Huawei, Guillaume Poupard a adopté une position plus mesurée. Il s'est notamment félicité du rôle de la commission R226 qui accorde, ou pas, le droit de commercialisation en France d'un équipement qui entre en jeu dans le secret des correspondances. « *Cette approche témoigne d'une volonté étatique de garder la main sur ces infrastructures. C'est une approche dépassionnée, basée sur des éléments techniques et qui évite de pointer un pays ou un fournisseur.* » Cette commission, qui peut réclamer un accès au code source des équipements, analyse et teste les équipements sur des critères techniques avant de délivrer son verdict. Guillaume Poupard a ainsi révélé que celle-ci a déjà retoqué plusieurs solutions pour leur marque de sécurité par le passé.

Reste à boucler le « Cyber-Act » de l'Europe, un texte sur lequel les européens travaillent depuis plus d'un an. Guillaume Poupard confie entrevoir « *un bon point de sortie* ». Le texte devrait notamment promouvoir la certification des produits de sécurité au niveau du continent, et le rôle de l'Enisa, l'Agence européenne chargée de la sécurité des réseaux et de l'information, semble désormais pérenne.



Dossier de presse du Ministère des Armées Forum International de la Cybersécurité, Lille

LIRE

22 janvier 2019

DGA – DEFI CYBER

Porté par la DGA en relation avec l'AID, le Défi cyber lancé en septembre 2018 vise à faire émerger une solution innovante, expérimentable par les forces armées, pour l'investigation à distance à des fins de défense, des cyberattaques sur les réseaux du ministère des Armées. Les deux lauréats du Défi cyber seront présents sur le stand du ministère pour présenter leurs solutions, et l'un d'entre eux sera déclaré vainqueur du challenge. Il verra son prototype testé au sein du ministère des Armées.

FOCUS : LE DÉFI CYBER DE LA DGA

Dans un marché dominé par de grands acteurs internationaux, la Direction générale de l'armement (DGA) veut favoriser l'émergence d'une solution innovante portée par une startup ou une PME/ETI française, permettant de mener des investigations à distance sur des cyberattaques visant les réseaux informatiques du ministère des Armées.

L'objectif est de prototyper des solutions présentant des fonctionnalités pour effectuer plus rapidement certaines opérations de prélèvement ou d'analyse sur différents équipements des réseaux, de manière automatisée et à distance, en prenant en compte les différentes contraintes liées aux réseaux du ministère des Armées.

Les deux lauréats retenus seront présents sur le stand de la DGA pour présenter les démonstrateurs qu'ils ont conçus :

Hurukai, proposée par les sociétés Harfanglab et Gatewatcher, est une solution d'investigation numérique adaptée aux contraintes opérationnelles des armées pour accélérer la détection des attaques, investiguer sans impact sur les métiers, et détruire la menace avec précision. Cet agent logiciel léger et intelligent permet de rechercher des compromissions sur des parcs informatiques, propose une boîte à outils pour la réponse à des incidents et remplit la fonction d'agent d'alerte pour les réseaux sensibles.

Myrmex, de la société Amossys, permet une recherche pointue, rapide et discrète de compromission système. Composé d'une suite de cinq outils complémentaires, il permet de mener des opérations de prélèvement ou d'analyse sur des équipements réseaux, de manière automatisée et à distance, ainsi qu'un travail collaboratif entre analystes. La solution du vainqueur du Défi cyber de l'édition 2019 du FIC sera testée au sein du ministère des Armées.

HarfangLab et Gatewatcher remportent le premier prix du Défi Cyber

[LIRE](#)

La Ministre des Armées, Florence Parly a remis hier le premier prix du Défi Cyber à deux PME, Harfanglab et Gatewatcher, pour leur projet Hurukai.

Organisé par le Ministère des Armées et la DGA, le Défi Cyber devait faire émerger une solution d'investigation à distance des cyberattaques sur les réseaux militaires.

Gatewatcher et Harfanglab se sont associées pour proposer Hurukai, un outil d'investigation numérique adapté aux théâtres d'opération. Cette nouvelle solution de cybersécurité allie sonde réseau et agents sur les terminaux informatiques. Elle permet une qualification des menaces plus rapide, plus fiable et plus précise. Le logiciel se distingue par sa flexibilité : sur les terrains difficiles, il peut fonctionner hors ligne et à distance.

Parmi les 12 projets déposés, le jury et la Ministre des Armées ont distingué Hurukai comme la solution innovante la plus à même d'assurer la cybersécurité des réseaux militaires. Grégoire Germain, Président Fondateur d'Harfanglab, et Jacques de La Rivière, CEO de Gatewatcher ont donc reçu hier le premier prix du défi cyber des mains de la Ministre.

22 janvier 2019

Discours de Florence Parly, Ministre des Armées Forum International de la Cybersécurité, Lille

LIRE

Monsieur le préfet,
Mesdames et messieurs les élus,
Mesdames et messieurs,
Chers amis,

La cybersécurité, c'est un sport collectif.

La faille peut venir de partout. Les hackers sont plein d'inventivité. Aussi puissants que peuvent être nos pare-feu, une simple inattention peut ouvrir une brèche dans laquelle bien des personnes, des groupes et des États voudront s'engouffrer.

Alors, oui, nous devons agir ensemble pour la cybersécurité de nos réseaux. Nous devons, ensemble, concevoir et échanger les bonnes méthodes et les bonnes pratiques. Nous devons bâtir pour chaque entreprise, chaque ministère, chaque personnel, une culture et une hygiène cyber irréprochable.

Nous parlons aujourd'hui de cybersécurité « by design », par essence presque. C'est précisément ce qu'il nous faut construire. Chaque système doit être conçu en pensant à sa cybersécurité. Chaque réseau doit être pensé dès l'origine en se demandant comment le protéger.

Le ministère des Armées le sait bien car les chiffres sont là. En 2017, les réseaux de la défense ont subi 700 événements de sécurité dont 100 cyberattaques. En 2018, les chiffres ont encore augmenté et dès septembre, nous dépassons ce chiffre de 700. Mon petit doigt me dit que cela ne va pas baisser en 2019.

Et non seulement le nombre d'attaques augmente mais les attaquants ont toujours des profils aussi variés. Un adolescent peut pirater les mails de la chancellerie allemande pour s'amuser, presque par hasard. Un groupe anonyme peut s'en prendre à nos industries, nos transports, nos hôpitaux sans raison apparente. Un État, enfin, peut chercher à affirmer sa puissance en nous espionnant, nous manipulant ou même en sabotant nos capacités. Et derrière chaque ordinateur, comment identifier avec certitude l'agresseur ? Tout le monde peut se cacher derrière son ordinateur et l'impunité est presque totale.

Voilà la réalité du cyberspace. Ce sont des opportunités inouïes pour nos quotidiens comme pour notre défense. Ce sont aussi des risques, des risques majeurs qui peuvent mettre en péril notre sécurité.

22 janvier 2019

Discours de Florence Parly, Ministre des Armées Forum International de la Cybersécurité, Lille

LIRE

Et non seulement le nombre d'attaques augmente mais les attaquants ont toujours des profils aussi variés. Un adolescent peut pirater les mails de la chancellerie allemande pour s'amuser, presque par hasard. Un groupe anonyme peut s'en prendre à nos industries, nos transports, nos hôpitaux sans raison apparente. Un Etat, enfin, peut chercher à affirmer sa puissance en nous espionnant, nous manipulant ou même en sabotant nos capacités.

Et derrière chaque ordinateur, comment identifier avec certitude l'agresseur ? Tout le monde peut se cacher derrière son ordinateur et l'impunité est presque totale.

Voilà la réalité du cyberspace. Ce sont des opportunités inouïes pour nos quotidiens comme pour notre défense. Ce sont aussi des risques, des risques majeurs qui peuvent mettre en péril notre sécurité.

Mesdames et messieurs, la guerre cyber a bel et bien commencé.

Nous ne serons ni naïfs ni aveugles, et nous allons nous y préparer.

L'année dernière sur cette même estrade, je vous annonçais que la France se dotait d'une cyberdéfense renforcée avec 1000 recrutements de cybercombattants supplémentaires d'ici 2025 et 1,6 milliard d'euros pour la lutte dans le cyberspace.

Depuis ces investissements sont entrés dans le marbre de la loi puisque la loi de programmation militaire a été votée puis promulguée par le Président de la République le 13 juillet.

J'avais l'année dernière parlé d'innover, de dénicher et d'attirer tous les talents et toutes les bonnes volontés. Le premier défi cyber du ministère des Armées était lancé. Son objectif était de répondre à une urgence opérationnelle du Commandement cyber en développant rapidement un outil de confiance avec un accès distant pour rechercher les traces d'attaques cyber sur un parc informatique.

Discours de Florence Parly, Ministre des Armées Forum International de la Cybersécurité, Lille

LIRE

22 janvier 2019

12 candidats ont relevé ce défi et j'ai le plaisir d'annoncer les deux lauréats : **les PME Harfanglab et Gatewatcher** d'un côté et AMOSSYS, de l'autre. Ils ont mis au point des projets novateurs, protecteurs et d'une remarquable efficacité. Nous allons poursuivre le travail avec eux pour s'assurer que leurs solutions soient très vite expérimentées, challengées et intégrées sur nos réseaux. Je veux remercier tous ceux qui ont permis ce défi et qui y ont participé.

Vous avez prouvé qu'on pouvait agir vite et bien. Prouvé qu'on pouvait acquérir des technologies utiles différemment. Je veux tous vous en remercier.

Et ce défi est une méthode nouvelle qui vient de prouver son efficacité, c'est bien qu'il faut continuer ! D'autres arrivent et je pense, en particulier au défi sur l'intelligence artificielle lancé tout récemment par l'Agence Innovation Défense et auquel je le sais, vous êtes très nombreux à avoir répondu.

Nous avons montré notre volonté. Notre capacité à nous mettre en ordre de marche, vite. Et vendredi, à Paris, avec le chef d'état-major des Armées, nous avons encore franchi une étape supplémentaire. J'ai annoncé devant le Commandement cyber, notamment, que la France revendiquait d'utiliser l'arme cyber au même titre que toutes les armes conventionnelles. J'ai pu énoncer les grands principes de notre nouvelle doctrine cyber offensive et le renforcement de notre défense cyber.

L'arme cyber n'est pas seulement pour nos ennemis ou nos fictions. Non. Nous aussi, en France, pouvons défendre, répliquer et attaquer.

Alors, vendredi nous avons révélé une partie de notre doctrine offensive. En opération, nous employons déjà l'arme cyber. Nous avons publié les grandes lignes de cette doctrine pour le faire savoir et nous donner un cadre d'emploi.

Il faut maintenant intégrer l'arme cyber à tous nos programmes, et je compte sur la DGA. Il faut aussi plus de coopérations, de partenariats, de convergences avec nos alliés européens. S'il y a bien une menace qui nous touche tous et se moque éperdument des frontières, c'est bien la menace cyber. Alors nous devons créer une culture commune, des remparts plus forts et agir ensemble, y compris avec de la lutte informatique offensive en opérations.

22 janvier 2019

Discours de Florence Parly, Ministre des Armées Forum International de la Cybersécurité, Lille

LIRE

S'agissant de notre doctrine défensive, mon message est clair : ne pas tendre la joue.

Le ministère des Armées a entamé sa révolution numérique. Il en est même à la pointe et c'est un mouvement qui me tient à coeur. Aujourd'hui, grâce au numérique, le ministère des Armées devient plus simple, plus rapide, plus efficace.

C'est une opportunité extraordinaire. Une opportunité que tout l'État saisit. Mais une opportunité qui n'est pas sans dangers.

Alors, le ministère des Armées se prépare, renforce sa défense. Le Commandement cyber a été conforté, son organisation renforcée. Nous redoublons de vigilance et nous dotons des meilleurs outils. Mais une chose est sûre, plus les Armées se protègent, plus les industriels, les sous-traitants sont susceptibles d'être des proies toutes désignées pour pénétrer dans nos systèmes d'information. Alors, c'est toute une chaîne de défense qui doit être protégée de bout en bout.

J'ai donné une instruction en la matière fin décembre. Toute notre communauté de défense doit se protéger et toute notre chaîne de défense se responsabiliser. Le COMCYBER, avec la DGA, sera la tour de contrôle de cet effort et j'appelle tous nos industriels à s'engager pour consolider encore notre cybersécurité.

C'est pourquoi je veux aujourd'hui faire une proposition à nos industriels de défense. Unissons nos forces pour protéger notre chaîne d'approvisionnement de la menace cyber. A l'été, je souhaite que nous puissions formaliser, en étroite liaison avec l'ANSSI, les engagements mutuels sur la cybersécurité. Il nous faudra mieux définir les rôles et les responsabilités de chacun pour protéger nos systèmes et réagir en cas d'attaque. Cette démarche collective est une absolue nécessité. Elle seule permettra de protéger le développement, la fabrication et la maintenance de nos équipements de défense.

22 janvier 2019

Discours de Florence Parly, Ministre des Armées Forum International de la Cybersécurité, Lille

LIRE

Elle nous permettra de répondre ensemble à plusieurs grands défis.

D'abord, la mise en place d'une coordination : c'est une évidence. Nous devons dialoguer en permanence et joindre à cet échange nos services de renseignement. Nous allons identifier un cadre et une démarche claires pour faire avancer nos travaux de concert. Nous devons échanger nos informations sur telle ou telle menace, tel ou tel incident. Nous pourrions partager nos outils, aussi, les mutualiser.

Nous établirons une stratégie ambitieuse de sécurisation de nos systèmes. C'est la finalité même de notre démarche, alors il nous faudra cartographier, identifier les priorités.

Nous devons enfin réfléchir à comment aider et protéger efficacement notre chaîne de sous-traitance. Nous ne pouvons pas les laisser devenir les chevaux de Troie de nos adversaires. Il faudra donc les soutenir, à la fois en méthode et en technique. Il nous faudra aussi être extrêmement exigeant et imposer dans les critères d'achat des clauses sur la cybersécurité.

Je parle de cette chaîne de confiance cyber. Elle passe également par les PME, les start-up. Par leurs idées et leur inventivité. J'ai eu le plaisir de voir quelques démonstrations à l'instant, d'échanger avec nos entrepreneurs. Alors, je veux aussi vous dire une chose : nous avons besoin de vous. Nous avons besoin de vous pour concevoir et produire des produits de sécurité utilisables en toute confiance par nos Armées. Nous avons besoin de vous pour préserver notre autonomie stratégique.

Discours de Florence Parly, Ministre des Armées Forum International de la Cybersécurité, Lille

LIRE

22 janvier 2019

Car les outils de confiance que nos entreprises développent, tous en Europe pourront en profiter. Je veux saluer ici les responsables internationaux présents aujourd'hui. Ils sont nombreux. Et c'est bien au FIC, forum international s'il en est, que nous devons en profiter pour nous inspirer et laisser sa chance à la vitalité des PME européennes.

Et au ministère des Armées, la confiance donnée aux PME et aux entrepreneurs, ce ne sont pas que des mots, c'est du concret.

Il y a quelques mois, cinq PME issues du cluster Hexatrust ont ainsi remporté face à des grands groupes, un marché de prestations cyber pour aider nos opérationnels à sécuriser les systèmes d'information et les réseaux du ministère.

Nous protégeons les PME, nous leur donnons leur chance. Aussi, j'ai lancé cette année un Plan Action PME qui comprend 40 mesures concrètes pour mieux prendre en compte les PME dans notre stratégie d'achat, pour renforcer le soutien à l'innovation et le dispositif RAPID, en particulier. Pour établir également une relation équilibrée entre les PME et les grands groupes.

Je sais que notre souveraineté numérique passe par les PME et j'ai bien l'intention de les choyer. Et quand je parle de confiance, cela va loin. Un partenariat a été noué entre le COMCYBER et une start-up, « YesWeHack ». Alors, oui, je l'annonce, nous allons lancer fin février le premier « bugbounty » du ministère des armées. Des hackers éthiques, recrutés au sein de la réserve opérationnelle cyber, pourront se lancer à la recherche des failles dans nos systèmes et s'ils en découvrent en être comme il se doit, récompensés.

Mesdames et messieurs,

Nous avons devant nous des défis et des opportunités.

Nous devons créer des liens entre le ministère des Armées et nos industriels de défense, entre le ministère et les PME, œuvrer pour une Europe de la cyberdéfense. Nous devons agir de concert pour une irréprochable cybersécurité.



22 janvier 2019

Discours de Florence Parly, Ministre des Armées Forum International de la Cybersécurité, Lille

LIRE

Et pour y parvenir, il existe un dernier défi que nous devons collectivement relever. Le défi des talents, le défi du recrutement.

Le ministère des Armées doit faire savoir, partout, qu'il cherche des personnes prêtes à coder pour la France. Les industriels mettre en avant les compétences fines qu'ils cherchent. Nous devons tendre la main aux entrepreneurs, aux innovateurs, leur dire que la défense leur ouvre ses portes et qu'elle est prête les soutenir et les pousser vers des parcours, des missions, des vies passionnantes.

L'année 2018 a été riche pour notre cybersécurité. L'année 2019 commence sur les chapeaux de roue. Alors, réfléchissons ensemble. Agissons ensemble. Assurons ensemble notre cyberdéfense. Cette 11^e édition du FIC en est une nouvelle opportunité. Saisissons-la pleinement. Je vous souhaite un excellent FIC 2019.

Vive la République ! Vive la France !

25 janvier 2019
Par Emmanuelle Lamandé



La ministre des Armées, Florence Parly, est venue présenter la toute nouvelle doctrine cyber offensive de la France à l'occasion de la 11ème édition du Forum International de la Cybersécurité à Lille. L'arme cyber est aujourd'hui une arme comme les autres, et la France le revendique dorénavant. La ministre a également annoncé un renforcement de la défense cyber, ainsi que le recrutement massif de cybercombattants.

« La cybersécurité est un sport collectif », souligne Florence Parly. « La faille peut venir de partout. Les cybercriminels sont pleins d'inventivité. Aussi puissants que peuvent être nos pare-feux, une simple inattention peut ouvrir une brèche dans laquelle bien des personnes, des groupes et des États voudront s'engouffrer. »

En 2017, les réseaux de la défense ont subi 700 événements de sécurité, dont 100 cyberattaques. En 2018, les chiffres ont encore augmenté et, dès septembre, ce chiffre dépassait les 700. Et cela ne devrait pas aller à la baisse en 2019. Les profils des attaquants sont, quant à eux, toujours aussi variés. « Un adolescent peut pirater les mails de la chancelière allemande pour s'amuser, presque par hasard. Un groupe anonyme peut s'en prendre à nos industries, nos transports, nos hôpitaux sans raison apparente. Un État, enfin, peut chercher à affirmer sa puissance en nous espionnant, nous manipulant ou même en sabotant nos capacités. » La menace peut donc venir de partout, et la difficulté d'identifier avec certitude un attaquant complexifie encore davantage la tâche pour la défense.

« Voilà la réalité du cyberspace. Ce sont des opportunités inouïes pour nos quotidiens comme pour notre défense. Ce sont aussi des risques, des risques majeurs qui peuvent mettre en péril notre sécurité. La guerre cyber a bel et bien commencé. Nous ne serons ni naïfs ni aveugles, et nous allons nous y préparer. »

Face à ce constat, c'est tout l'écosystème qui doit agir ensemble pour la cybersécurité de nos réseaux. Cela passe à la fois par l'échange des bonnes méthodes et des bonnes pratiques, le développement d'une culture commune et une hygiène cyber irréprochable. La cybersécurité doit, de plus, être pensée et intégrée « by design » dans tous nos systèmes et réseaux. Sans compter bien sûr sur le défi des talents et du recrutement.

Le recrutement au cœur de tous les enjeux

La ministre des Armées avait d'ailleurs annoncé l'an passé le recrutement de 1 000 cybercombattants supplémentaires d'ici 2025, ainsi qu'un budget de 1,6 milliard d'euros alloué à la lutte dans le cyberspace. Ces investissements ont depuis été actés dans la Loi de programmation militaire (LPM) 2019-2025, promulguée par le Président de la République le 13 juillet dernier. En 2025, les effectifs du ministère des Armées s'élèveront à plus de 4 400 cybercombattants pour renforcer les capacités des Armées en matière de prévention, de détection et d'attribution des cyberattaques.

Depuis plus d'un an, le COMCYBER a en ce sens multiplié ses actions de recrutement, via notamment sa présence sur des salons, une campagne digitale, mais aussi son intervention dans les écoles.

Florence Parly, FIC: la France passe à la « cyber » offensive

[LIRE](#)

25 janvier 2019

Par Emmanuelle Lamandé

Le ministère des Armées avait également annoncé l'an passé son intention d'innover et d'attirer tous les talents, à travers le lancement de son premier défi cyber. L'objectif de ce défi était de répondre à une urgence opérationnelle du Commandement cyber en développant rapidement un outil de confiance avec un accès distant, permettant de rechercher les traces d'attaques cyber sur un parc informatique. 12 candidats ont relevé ce défi et les deux lauréats sont, d'un côté, les PME Harfanglab et **Gatewatcher** pour leur projet Hurukai, et de l'autre la société Amossys pour son projet Myrmex. « Leurs solutions seront très vite expérimentées, challengées et intégrées sur nos réseaux. »

D'autres défis sont à venir, comme celui lancé récemment en matière d'intelligence artificielle par l'Agence Innovation Défense.

La France se dote d'une doctrine cyber offensive

Autre avancée significative pour le ministère, Florence Parly annonçait il y a une semaine que la France revendiquait d'utiliser l'arme cyber au même titre que toutes les armes conventionnelles. Elle a d'ailleurs énoncé à cette occasion les grands principes de la nouvelle doctrine cyber offensive française, ainsi que le renforcement de sa défense cyber, autour d'un objectif clair : « ne pas tendre la joue ».

La Lutte informatique offensive (LIO) devient ainsi une composante à part entière de la palette opérationnelle des armées, une arme d'emploi dans ses opérations. Son intégration est désormais assumée par l'État au sein des composantes tactiques et dans les processus de développement capacitaire à venir.

« L'arme cyber n'est pas seulement pour nos ennemis ou nos fictions. Non. Nous aussi, en France, pouvons défendre, répliquer et attaquer. Alors, vendredi nous avons révélé une partie de notre doctrine offensive. En opération, nous employons déjà l'arme cyber. Nous avons publié les grandes lignes de cette doctrine pour le faire savoir et nous donner un cadre d'emploi. », explique Florence Parly.

Cette doctrine est désormais actée, reste à la mettre en œuvre, et à intégrer l'arme cyber dans l'ensemble des différents programmes. La DGA sera en charge du développement des capacités de LIO au profit des armées. La LIO nécessite, en outre, une expertise opérationnelle et technique nouvelle. Le personnel devra y être formé. Elle suppose enfin une coopération étroite entre acteurs, et une convergence opérationnelle avec certains partenaires européens, comme internationaux.

Plus les Armées se protègent, plus les industriels et les sous-traitants sont susceptibles d'être des proies

Le ministère des Armées a entamé sa révolution numérique et est à la pointe. Cependant, cette opportunité que l'État saisit n'est pas sans dangers. C'est pourquoi, le ministère des Armées se prépare et renforce sa défense. « Le Commandement cyber a été conforté, son organisation renforcée. Nous redoublons de vigilance et nous dotons des meilleurs outils.

Mais une chose est sûre, plus les Armées se protègent, plus les industriels, les sous-traitants sont susceptibles d'être des proies toutes désignées pour pénétrer dans nos systèmes d'information. Alors, c'est toute une chaîne de défense qui doit être protégée de bout en bout. J'ai donné une instruction en la matière fin décembre. Toute notre communauté de défense doit se protéger et toute notre chaîne de défense se responsabiliser. Le COMCYBER, avec la DGA, sera la tour de contrôle de cet effort et j'appelle tous nos industriels à s'engager pour consolider encore notre cybersécurité. »

Florence Parly, FIC: la France passe à la « cyber » offensive

25 janvier 2019

Par Emmanuelle Lamandé

[LIRE](#)

Les industriels de défense ont en effet un rôle clé à jouer. « Unissons nos forces pour protéger notre chaîne d'approvisionnement de la menace cyber. A l'été, je souhaite que nous puissions formaliser, en étroite liaison avec l'ANSSI, les engagements mutuels sur la cybersécurité. Il nous faudra mieux définir les rôles et les responsabilités de chacun pour protéger nos systèmes et réagir en cas d'attaque. »

Cette démarche collective est essentielle et permettra de répondre à plusieurs grands défis :

- La mise en place d'une coordination : cela passera notamment par un dialogue permanent entre les différents services, y compris de renseignement, l'identification d'un cadre et d'une démarche clairs, l'échange d'informations sur telle ou telle menace, tel ou tel incident, ou encore le partage ou la mutualisation des outils.
- L'établissement d'une stratégie de sécurisation des systèmes. Il faudra pour cela cartographier et identifier les priorités.
- La protection de la chaîne de sous-traitance du ministère : « Nous ne pouvons pas les laisser devenir les chevaux de Troie de nos adversaires. Il faudra donc les soutenir, à la fois en méthode et en technique. Il nous faudra aussi être extrêmement exigeant et imposer dans les critères d'achat des clauses sur la cybersécurité. »

Notre souveraineté numérique passe aussi par les PME

La chaîne de confiance cyber passe également par les PME et les start-ups. L'État a en effet aussi besoin de ces acteurs pour concevoir des produits de sécurité de confiance et préserver son autonomie stratégique. Le ministère des Armées souhaite d'ailleurs donner sa chance à toute entreprise innovante présente en France ou en Europe, y compris aux plus petites structures. « Il y a quelques mois, cinq PME issues du cluster Hexatruster ont ainsi remporté face à des grands groupes, un marché de prestations cyber pour aider nos opérationnels à sécuriser les systèmes d'information et les réseaux du ministère. Nous protégeons les PME, nous leur donnons leur chance.

Aussi, j'ai lancé cette année un Plan Action PME qui comprend 40 mesures concrètes pour mieux prendre en compte les PME dans notre stratégie d'achat, pour renforcer le soutien à l'innovation et le dispositif RAPID, en particulier. Pour établir également une relation équilibrée entre les PME et les grands groupes. Je sais que notre souveraineté numérique passe par les PME et j'ai bien l'intention de les choyer. »

Le ministère des Armées lancera son premier Bug Bounty fin février, en partenariat avec YesWeHack

Autre nouveauté cette année pour le ministère des Armées : le lancement fin février d'un programme de Bug Bounty, en partenariat avec la société YesWeHack. « Des hackers éthiques, recrutés au sein de la réserve opérationnelle cyber, pourront se lancer à la recherche des failles dans nos systèmes et s'ils en découvrent en être, comme il se doit, récompensés. »

Des liens étroits doivent donc être noués entre le ministère des Armées, les industriels de défense et les PME, afin de renforcer de concert notre cyberdéfense et notre cybersécurité. Pour cela, il faudra également répondre collectivement, comme évoqué précédemment, au défi du recrutement. « Le ministère des Armées doit faire savoir, partout, qu'il cherche des personnes prêtes à coder pour la France. »

« L'année 2018 a été riche pour notre cybersécurité. L'année 2019 commence sur les chapeaux de roue. Alors, réfléchissons ensemble. Agissons ensemble. Assurons ensemble notre cyberdéfense. », conclut-elle.

Guillaume Poupard, FIC : « Tous connectés, tous impliqués, tous responsables ! »

[LIRE](#)

A l'occasion de la 11ème édition du Forum International de la Cybersécurité (FIC), Guillaume Poupard, Directeur général de l'ANSSI, a appelé à un engagement collectif pour stabiliser le cyberspace autour du leitmotiv : « Soyons tous connectés, tous impliqués, tous responsables ! ». Afin de renforcer et de garantir la stabilité et la confiance dans le cyberspace, tous les acteurs doivent en effet identifier et assumer aussi leur part de responsabilité au plus tôt.

Le constat de cette année 2018 est relativement inquiétant, souligne Guillaume Poupard. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a pu observer ces derniers mois une menace toujours plus forte, ainsi que la prolifération d'attaques sophistiquées, élaborées, et encore plus destructrices, touchant désormais toute la société. Le numérique ayant envahi nos vies personnelles et professionnelles, la surface d'attaque ne fait quant à elle qu'augmenter, et le développement massif de l'Internet des objets ne fait qu'étendre le phénomène. L'absence de frontières dans le monde cyber complexifie, de son côté, la lutte contre ces cybermenaces et l'attribution de ces attaques.

Autre tendance majeure : l'attaque des sous-traitants, prestataires, partenaires... C'est toute la supply chain qui est désormais mise à rude épreuve, et le moindre maillon faible est dorénavant exploité. Les risques et objectifs de toutes ces attaques sont nombreux : espionnage, vol d'information, détournement de données à caractère personnel, sabotage... Mais l'ANSSI a également pu remarquer en 2018 le développement d'une menace marquée par la préparation d'attaques futures, ce qui ne laisse rien présager de bon...

Nous sommes tous responsables !

Face à ce constat et à cet état d'urgence numérique, il est plus que jamais nécessaire de s'organiser collectivement pour assurer le développement d'un cyberspace stable et de confiance. Afin de renforcer la stabilité de l'espace numérique mondial en 2019 et au-delà, l'ANSSI appelle ainsi l'ensemble des acteurs à être « tous connectés, tous impliqués, tous responsables ». Nous sommes tous concernés, il faut donc faire face à la menace collectivement. Tous les acteurs de l'écosystème numérique doivent, de plus, assumer leur part de responsabilité dans la prise en compte de la sécurité au juste niveau. « Ces dernières années ont montré l'importance capitale du rôle que doivent jouer les acteurs privés, publics et la société civile. C'est en travaillant collectivement que nous pourrons stabiliser le cyberspace et éviter la structuration d'un farwest numérique », souligne Guillaume Poupard.

Au niveau national, la réglementation continue à évoluer. C'est un outil essentiel majeur et efficace qui nous permet d'accélérer les processus. « Nous sommes actuellement dans le RUN et l'exécution de la LPM. Quant à l'application de la directive NIS au niveau national et le renforcement de nos Opérateurs de services essentiels, nous avons dans un premier temps désigné 120 OSE. »

Guillaume Poupard, FIC : « Tous connectés, tous impliqués, tous responsables ! »

[LIRE](#)

2019 : l'effort portera sur un renforcement des capacités de détection

Le défi consiste aussi à concevoir et déployer ensemble les outils les plus pertinents pour organiser cette défense collective des systèmes d'information contre les menaces croissantes. Cela passe entre autres par la qualité des solutions de sécurité développées par les prestataires et leur certification. Trois prestataires viennent d'ailleurs d'obtenir la qualification PDIS (Prestataire de Détection d'Incidents de Sécurité) attribuée par l'ANSSI : Sopra Steria, Orange Cyberdefense et Sogeti. En appui de ces solutions de détection, les deux sondes de Thales et Gatewatcher arriveront bientôt. La société Oodrive a, quant à elle, obtenue la qualification SecNumCloud.

L'effort portera notamment en 2019 sur le renforcement de nos capacités de détection, qui peuvent encore être améliorées, afin de réduire le gap entre les flux et les menaces que nous voyons aujourd'hui et ceux que nous pourrions voir. L'ANSSI a la volonté de réduire cet angle mort.

Pour faire face à l'ensemble de ces défis, nous devons également nous appuyons sur l'humain, le partage, la formation et la collaboration.

Appel de Paris : le cyberspace doit être et rester un espace de paix

Cette approche nationale est complémentaire de l'approche européenne et internationale. La certification européenne des produits et services de sécurité numériques, prévue dans le cadre du Cyber Act, s'inscrit d'ailleurs dans la même logique que celle déjà établie en France. Cette certification européenne va devenir une réalité et permettre à tous les États membres d'élever conjointement leurs niveaux de sécurité.

Autre initiative lancée en 2018, ayant quant à elle une visée internationale : l'Appel de Paris, d'ores et déjà signé par plusieurs centaines d'acteurs. « L'objectif, à travers cette démarche, est d'appeler toutes les bonnes volontés à nous rejoindre sur le fait que le cyberspace est un espace de biens communs, qui doit être un espace de paix, et par ce biais éviter l'escalade. Il est essentiel de se mettre d'accord à l'échelle internationale sur ce qu'il est permis ou non de faire dans le cyberspace, de fixer des règles, des limites et des normes de comportement. » Chacun ayant une culture et des valeurs qui lui sont propres, cette tâche ne sera pas aisée, mais indispensable si l'on veut maintenir la paix dans le cyberspace et plus globalement à travers le monde dans les années à venir.



29 janvier 2018

Le groupe de technologies Altran frappé par une cyber-attaque

Le géant français du conseil en technologie **Altran**, qui emploie près de 45.000 personnes dans plus de 30 pays, a été victime la semaine dernière d'une cyber-attaque dans certains pays qui l'a conduit à déconnecter temporairement son réseau informatique, a-t-il révélé lundi.

Dans un communiqué diffusé lundi matin avant l'ouverture de la Bourse, **Altran** a assuré que l'attaque n'avait donné lieu à "aucun vol de données" ni "aucun cas de propagation de l'incident à des clients".

Altran est particulièrement surveillé par le marché boursier, après avoir augmenté son endettement pour investir fortement ces dernières années, notamment avec l'achat fin 2017 de l'américain Aricent.

De fait, l'action du groupe français a clôturé lundi sur une perte d'environ 3% à 8,18 euros, dans un marché globalement en baisse de 0,64%.

Les communiqués d'annonce de cyber-attaque sont encore rares, mais beaucoup d'experts estiment qu'ils risquent de se multiplier dans les prochaines années du fait de la numérisation croissante de l'économie et du recours de plus en plus important à l'informatique, dans tous les secteurs de la société.

Selon une porte-parole **d'Altran** interrogée par l'AFP, l'attaque a touché l'entreprise le 24 janvier dans "une grande partie des pays européens, y compris la France".

"Il est encore trop tôt pour avoir une vision précise" sur le préjudice économique subi, a prévenu la porte-parole. Mais l'attaque est restée limitée géographiquement et "n'a touché qu'une partie des opérations européennes", dont les opérations en France, a-t-elle souligné.

Selon elle, les "fonctions critiques" des systèmes informatiques **d'Altran** devaient toutes être rétablies lundi soir, notamment les messageries de courriels. D'autres applications pourraient devoir attendre un peu, comme la téléphonie.

Altran, qui a porté plainte, est couvert par des assurances pour ce type de dommage, a-t-elle précisé.

- Un logiciel "extrêmement virulent" -

Pendant la journée, la communauté des experts en cybersécurité a cherché à reconstituer ce qui s'était passé.

Selon **Altran**, les ordinateurs visés ont été pris pour cible par un logiciel de cryptoverrouillage, qui crypte les fichiers et les rend inutilisables.

Selon plusieurs experts interrogés par l'AFP, il semble que le code malveillant ait été signalé à au moins à deux reprises deux jours avant l'attaque sur virustotal, un analyseur gratuit de fichiers en ligne.



29 janvier 2018

Le groupe de technologies Altran frappé par une cyber-attaque

"Soit l'attaquant essayait de tester son virus pour voir s'il était connu des grands antivirus, soit ce sont des victimes qui essayaient de se renseigner", a expliqué Ivan Fontarensky, qui dirige le service de renseignement d'intérêt cyber de Thales.

Le virus qui a touché Altran chiffre les fichiers des ordinateurs sur lesquels il est présent "un par un", comme un rançongiciel, a détaillé M. Fontarensky. Mais du fait des pratiques de partage de réseaux très courantes dans les grandes entreprises, "il peut vite en arriver à chiffrer tous les fichiers des serveurs centraux".

C'est un logiciel malveillant "extrêmement virulent, il faut être très prudent", a estimé pour sa part Jacques de la Rivière, le patron de **Gatewatcher**, une start-up française qui commercialise une sonde permettant de détecter les menaces sur les réseaux.

Pour un expert du Clusif (club de la sécurité de l'information français), cette première communication d'Altran était en tout cas "bonne et bien dans les clous" de ce qui est attendu d'une entreprise frappée par une cyber-attaque.

"Toutefois, il va falloir attendre encore quelques jours, quelques semaines pour connaître un peu mieux le dessous des cartes", c'est-à-dire les détails de l'attaque, et une évaluation plus précise des dégâts subis, a-t-il estimé.