Lettre mensuelle – Octobre 2018 - disponible sur omc.ceis.eu

Table des matières

ANALYSES

1. FUITES DE DONNEES : CHRONIQUE D'UNE DESTANILISATION ANNONCEE ?

Les données constituent la matière première d'une entreprise ou d'une institution. L'altération, la divulgation ou l'accès non autorisé à leurs données constitue donc une menace permanente pour les organisations, publiques et privées. Les fuites de données peuvent en effet avoir des impacts considérables sur l'ensemble d'une entité, du fonctionnement des systèmes d'information aux activités « métiers » de l'organisation. Une étude datant de 2018 du *Ponemon Institute*[1] sur le coût des violations de données[2] met en évidence l'augmentation significative et le quasi doublement du nombre de violations de grande ampleur (de plus d'un million d'enregistrements). L'étude révèle également que le coût moyen d'une violation de données en France est de 3,54 millions d'euros. L'un des enjeux de la cyber résilience des organisations consiste donc aujourd'hui à limiter les risques de compromission de leurs données.

Impacts et conséquences d'une fuite de données

Les conséquences d'une fuite de données peuvent se propager au sein **d'une organisation** et porter atteinte à ses activités, son fonctionnement, son développement voire sa stratégie à long terme.

Les **conséquences peuvent d'abord** induire une **perte financière directe** pour l'entreprise (sanctions financières imposées par la CNIL et le RGPD, coût des potentielles investigations techniques permettant de déterminer l'origine et la cause de la fuite, etc).

Des **effets indirects et à long terme** peuvent être également préjudiciables pour l'organisation. Par exemple, une fuite d'informations stratégiques (commerciales, relatives à des savoir-faire ou à des nouveaux produits, etc) peut servir un concurrent commercial et entraîner ainsi un **manque à gagner** pour l'organisation victime du fait de la perte d'un **avantage concurrentiel**[3]. Dans un deuxième temps, **la compromission des données d'une organisation peut ainsi affecter sa réputation**. La médiatisation de la fuite de données peut en effet être à l'origine d'une perte de confiance de futurs partenaires commerciaux, fournisseurs ou prestataires, craignant que les conséquences de ces fuites soient dommageables pour leur propre activité. Des bases de données compromises peuvent alors être utilisées comme vecteurs dans des campagnes de dénigrement ou comme outil de chantage voire de guerre commerciale et de déstabilisation[4].

Une fuite de donnée peut également avoir un impact sur la **stratégie de l'organisation, sa gouvernance et son efficacité opérationnelle**. Par exemple, une violation similaire à celle subie par DCNS (aujourd'hui Naval Group) concernant les capacités de combat des sous-marins Scorpène et médiatisée dans la presse australienne en 2016, est susceptible de retentir sur la gouvernance industrielle et la stratégie géopolitique d'une organisation, en portant atteinte à sa réputation sur la scène internationale, et en nuisant à ses négociations précontractuelles. Le journal *The Australian* titrait d'ailleurs à l'époque « Si l'ennemi connaît les secrets [du sous-marin], la partie est perdue [5]».

Les circuits de la fuite de données

A l'origine d'une compromission : le facteur humain

Selon le premier bilan publié par la CNIL depuis l'entrée en vigueur du RGPD[6], l'origine des violations de données proviendrait à **15% d'erreurs humaines internes à l'organisation et à 65% d'actes malveillants d'origine externe**, le reste des incidents seraient d'origine indéterminée ou d'actes internes malveillants.

La négligence ou l'imprudence des collaborateurs et des partenaires de l'organisation peut être la cause de fuites de données assez graves. Plusieurs scénarios « classiques » peuvent avoir de lourdes conséquences pour l'organisation touchée.

➢ *Exemple : Achat de biens à usage personnel sur une plateforme de vente en ligne avec une adresse mail professionnelle.*

Les plateformes de vente, trop souvent mal sécurisées, sont susceptibles d'être la cible de cyberattaques qui peuvent permettent à leurs auteurs de récupérer la base de données des clients du site. Celle-ci comporte notamment leurs données d'authentification (« credentials »), dont l'adresse mail utilisée pour effectuer les achats. Il suffit alors aux attaquants d'utiliser le nom de domaine associé pour tenter de se connecter à une plateforme de messagerie professionnelle. Le mot de passe utilisé sur la plateforme de vente étant le plus souvent très similaire à celui utilisé pour leur messagerie professionnelle, les attaquants peuvent parvenir à accéder au compte de messagerie visé en essayant des variantes du mot de passe renseigné sur la plateforme. S'ils parviennent à s'y introduire, ils sont alors en mesure subtiliser des informations stratégiques pour l'entreprise.

➢ *Exemple : Partage d'une publication à contenu professionnel via une plateforme de partage publique type Scribd.*

Si la publication est partagée sans évaluation préalable de la criticité des informations publiées, elle peut permettre ainsi à un public non habilité d'accéder à des informations hautement critiques.

Les fuites de données peuvent également avoir pour origine une malveillance interne, ce qui peut être le cas d'un salarié mécontent qui publie volontairement des informations préjudiciables pour l'entreprise ou d'un employé corrompu pour dérober des informations pour le compte d'un tiers.

Des individus extérieurs à l'entreprise peuvent également être à l'origine de la captation d'informations qui ne leur étaient pas destinées. Les objectifs sont divers mais l'intention est toujours malveillante :

L'espionnage à des fins économiques, concurrentielles et scientifiques peut-être mené par une organisation concurrente, voire même par un État ;

- La volonté de nuire à l'organisation ;
- Des convictions politiques, sociales, religieuses *(hacktivisme)*[7]*;*
- L'appât du gain ;
- Le challenge technique

Outils et techniques de la captation frauduleuse d'information

Il existe de nombreuses méthodes permettant capter des informations. D'abord simplement par **introduction physique dans le système d'information**, par une clef USB par exemple ou via *l'« information diving »* qui consiste à récupérer des données à partir de matériel mis au rebut ou volé.

Au-delà de ces techniques, il est possible, **à distance**, d'exploiter des failles informatiques pour accéder au contenu d'applications web hébergeant des données. Un phishing ou un typosquatting[8] convaincant sont tout autant de moyens de récupérer des données d'authentification et des données personnelles de victimes et d'infecter à distance un terminal via une pièce jointe contenant un malware. « Bruteforcer » un FTP[9], c'est-à-dire tester des combinaisons de mot de passe afin d'identifier le bon, est une technique qui a fait ses preuves. De même, pirater des objets connectés au système d'information de l'entreprise est une technique courante. Elle s'appuie sur la pratique de l'exploration réseau (*dns rebinding*), par exemple en utilisant un objet connecté comme une imprimante liée au réseau Wifi de l'organisation, dans lequel l'attaquant glisse une clef USB contenant un malware spécifique qui se propage ensuite au système d'information de l'organisation via le réseau Wifi. Précisons que le simple accès à des données d'authentification d'employés d'une organisation peut permettre une intrusion dans le système d'information de l'entreprise.

Un type d'attaque particulièrement inquiétant est **l'advanced persistent threat**. Celle-ci, quasiment indétectable et très élaborée, peut durer plusieurs années. Des attaquants utilisent des moyens très avancés pour s'infiltrer dans le système d'information cible et peuvent conserver un accès à distance à celui-ci. Il leur est possible de subtiliser toutes les informations stratégiques souhaitées.

Exploitation et détournement des données compromises

L'information compromise peut revêtir une valeur commerciale très élevée[10]. Certaines plateformes du Darkweb proposent ainsi des services d'échange, de vente et de captation d'informations stratégiques de toutes natures dont les prix peuvent s'élever à plusieurs centaines de milliers d'euros. Par exemple dans la pratique dite du « insider trading »[11], qui peut être apparentée au délit d'initié défini par le droit français, les informations compromises sont utilisées pour influencer les cours de bourse et réaliser ainsi des gains de façon illicite lors de transactions boursières.

D'autres vendeurs proposent des services de **« doxes »**, c'est-à-dire l'identification de toutes les informations privées concernant un individu ou une entreprise puis leur **publication à des fins de nuisance**.

Des services de vol d'information sont également proposés sur les marchés noirs.

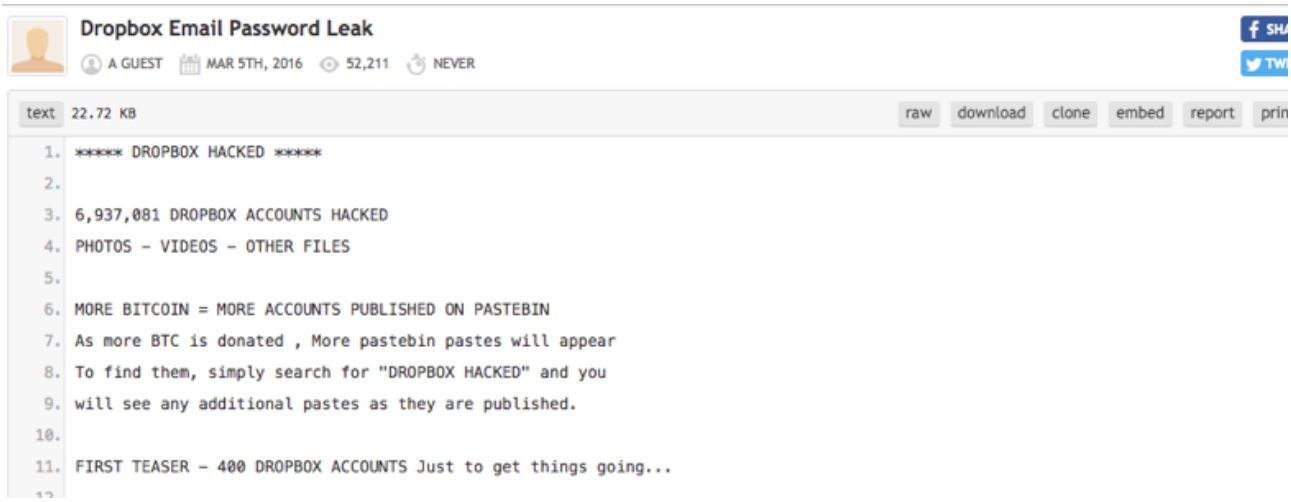
- *Exemple : Sites du Darkweb spécialisés dans la vente de service de hacking : mise sous surveillance d'un ordinateur, d'un téléphone, recherches d'informations sur une personne, introduction de malware dans des systèmes d'information, etc.*

De même, des **informations « prêtes à l'emploi »** sont proposées sur l'ensemble des marchés noir du

Darkweb. Elles sont parfois accessibles sur des plateformes publiques de type Pastebin lorsqu'elles ont perdu de leur valeur (données trop anciennes, ou déjà vendues plusieurs fois).

Les « credentials » (données d'authentification) sont des produits très couramment proposés à la vente à des prix très bas (l'unité pour quelques centimes). [13] Ils servent pourtant de porte d'entrée à de nombreuses intrusion frauduleuses et, lorsqu'il s'agit d'adresses mail professionnelles, représentent un risque élevé pour les organisations.

➢ *Exemple : Vente de données sur Pastebin*



Comment faire face à une fuite de données ?

S'il est inutile d'imaginer un système d'information totalement exempt de vulnérabilité, il reste cependant possible de limiter les risques de fuites de données et de mettre en place des solutions de prévention (data loss prevention, DLP[14]) voire de détection. Il faut garder à l'esprit que le coût d'un vol de données est grandement lié au temps de détection et de remédiation aux cas d'intrusions.

Il convient tout d'abord de répertorier les données sensibles puis les référencer, afin de contrôler leur diffusion et leur stockage. **L'objectif est d'assurer la disponibilité, la traçabilité, l'intégrité et la confidentialité des données.**

Un stockage sécurisé suppose d'une part le chiffrement des matériels et des terminaux (disques, fichiers, dossiers, supports amovibles) mais également des messageries en ligne ; et d'autre part l'utilisation de plateformes d'archivage sécurisées et à vocation probatoire – « coffres-forts numériques ». Il est également judicieux d'interdire la copie, la diffusion, l'impression de certaines données vers certaines destinations.

Le contrôle de la diffusion des données peut être facilité par des solutions permettant la **traçabilité numérique** des données. L'utilisation de la signature numérique permet de garantir l'intégrité du document et l'authentification de l'auteur. L'organisation peut par exemple mettre en place des codes d'accès personnels à chaque utilisateur conditionnant le cycle d'utilisation des documents, permettant d'attribuer à un collaborateur tout accès, tout envoi et toute modification des documents.

Des solutions de cybersécurité plus générales permettent de limiter les risques de compromission et de créer un environnement mieux sécurisé (filtres anti-spams, anti-virus, pare-feu, anti-malware, proxies, segmentation du réseau, gestion des privilèges, des identités et des droits d'accès, surveillance du traffic du réseau au niveau applicatif et système de détection d'intrusion, etc).

Enfin, former et sensibiliser les collaborateurs aux cybermenaces est crucial, car l'humain reste l'une des premières vulnérabilités (notamment via le phishing et l'ingénierie sociale). La diffusion des bonnes pratiques d'hygiène informatique (surtout l'imposition d'une politique de mots de passe sécurisés et l'interdiction de l'utilisation des adresses mail professionnelles à des fins personnelles). L'organisation doit toutefois savoir adapter sa politique de sécurité aux besoins métiers afin de ne pas rendre la cybersécurité trop contraignante et de faciliter son appropriation par les employés.

En complément de solutions permettant de prévenir les fuites de données, il est fortement recommandé de se doter **de solutions de Cyber Threat Intelligence.** Ceux-ci offrent des services clef en mains de veille et de détection des menaces sur toutes les couches du Web et permettant d'anticiper les attaques en détectant les signaux faibles.

[1] https://www-03.ibm.com/press/fr/fr/pressrelease/54150.wss

[2] https://www-03.ibm.com/security/fr/fr/data-breach/

[3] https://www.lesechos.fr/idees-debats/cercle/cercle-167557-fuite-de-donnees-un-impact-financier-non-negligeable-2072567.php

[4] https://www.meta-media.fr/2018/03/16/les-fuites-de-donnees-armes-de-destabilisation-massive.html

[5] https://www.agoravox.fr/actualites/international/article/branle-bas-de-combat-a-la-dcns-184008

[6] https://www.cnil.fr/fr/violations-de-donnees-personnelles-1er-bilan-apres-lentree-en-application-du-rgpd

[7] *https://www.zataz.com/data-gouv-fr-pirate-informatique-dxb/*

https://www.zataz.com/site-internet-signalement-gouv-fr-attaque/

[8] Technique d'usurpation de sites web légitimes consistant en le fait de changer des caractères dans l'URL afin de duper les internautes, utilisés pour faire du phishing

[9] Un FTP est un protocole simple qui permet de manipuler des répertoires et des fichiers sur un ordinateur distant

[10] http://www.economiematin.fr/news-internet-vol-donnees-vente-marche-noir

[11] https://www.zdnet.com/article/insider-trading-takes-the-dark-web-by-storm/

[12] https://www.lebigdata.fr/dark-web-donnees-dgsi

[13] https://www.zataz.com/des-bases-de-donnees-didentifiants-de-connexion-de-700-000-francais-en-vente-dans-le-black-market/

[14] Sans atteindre l'exhaustivité, les quelques recommandations ci-dessous permettent de lister quelques axes importants en matière de protection des données.

2. CYBERSECURITE DES SYSTEMES D'ARMES AUX ETATS-UNIS : LE CONSTAT INQUIETANT DU *GOVERNMENT ACCOUNTABILITY OFFICE* (GAO)

Le 9 octobre 2018, le Government Accountability Office (GAO), l'équivalent américain de la Cour des Comptes, a publié un rapport sur la cybersécurité des systèmes d'armes des forces armées américaines[1]. C'est la première fois que cette institution rédige un rapport sur ce sujet. Les conclusions alarmistes n'ont pas manqué de susciter de nombreuses réactions au sein de la communauté de défense américaine.

La digitalisation des systèmes d'armes et l'interconnexion progressive des réseaux ont accru la surface d'attaque et les vulnérabilités auxquelles ces systèmes sont exposés. Toute connexion est aujourd'hui un point d'entrée, une faille potentielle au sein d'un système et plus largement d'un système de système. Et ce en raison des nombreuses interfaces que possèdent désormais les systèmes d'armes (port USB utilisé pour la maintenance, port permettant l'accès au système de diagnostic embarqué, récepteur radar, récepteur de communications radio, équipements électroniques personnels des opérateurs, etc.).

L'étude du GAO repose sur des travaux du Department of Defence (DoD) et de diverses organisations gouvernementales[2] d'une part, et sur des entretiens menés auprès de responsables de ces entités d'autre part. Elle couvre neuf grands programmes d'armement en cours de développement, non rendus publics, qui se veulent représentatifs de chaque armée, de la majorité des domaines de lutte, et des différents degrés d'interconnexion des systèmes d'armes. Le GAO n'a pas directement réalisé de tests de cybersécurité car il ne dispose pas des moyens nécessaires, mais il a analysé les résultats des évaluations de cybersécurité réalisés entre 2012 et 2017 par le DoD, notamment via le DOT&E[3], qui est en charge de la conduite des essais de développement et opérationnel.

Des résultats inquiétants

Les résultats de l'audit conduit par le GAO entre juillet 2017 et octobre 2018 sont alarmants. Des vulnérabilités qualifiées de « critiques » ont été découvertes dans quasiment tous les systèmes d'armes alors qu'ils étaient encore en développement. Dans l'ensemble, les faiblesses identifiées touchaient aussi bien les capacités de protection, de détection, de réponse que de résilience (recover). Les red teams du DoD ont même été capables de prendre le contrôle, partiel ou total, de certains systèmes, en peu de temps. Parfois, ces intrusions n'ont même pas été détectées par les opérateurs. Pourtant, les testeurs eu recours à des outils et techniques relativement basiques et ne disposaient que d'un temps limité. A ce propos, le manque de rigueur dans la politique de gestion des mots de passe s'est avéré être un problème récurrent facilitant les intrusions. Dans plusieurs cas, les mots de passe par défauts des logiciels commerciaux ou open-source installés n'avaient même pas été modifiés. Le GAO a également découvert que les vulnérabilités précédemment identifiées n'avaient pas toutes été corrigées. En matière de capacités de détection, il ressort que les analyses de logs ne sont pas réalisées de manière systématique et régulière.

Autre élément d'inquiétude du GAO : les tests de sécurité réalisés n'étant pas exhaustifs, le DoD ne connaît pas à ce jour l'étendue exact de ses vulnérabilités. Et ce d'autant plus que les évaluations de cybersécurité sont conduites sur de courtes périodes de temps et que leur périmètre est parfois limité à certains réseaux pour des raisons de sécurité.

Une prise en compte tardive de la nécessité de la cybersécurité « by design »

Jusqu'en 2014, le DoD se concentrait surtout sur la cybersécurité périmétrique des réseaux et non sur la cybersécurité des systèmes d'armes. La formulation d'exigences en matière de cyber-résilience dans les spécifications des futurs systèmes d'armes n'était alors pas systématique. En conséquence, le DoD possède aujourd'hui en inventaire de nombreux systèmes d'armes pour lesquels la cybersécurité n'a pas été prise en compte nativement (« by design »). Par exemple les contraintes de cybersécurité ont été complètement négligées dans les spécifications du programme GPS OCX (Operational Control Segment) de l'US Air Force. C'est l'une des raisons de la procédure de révision « Nunn-McCurdy » dont il a fait l'objet en 2016. De même, la cybersécurité n'était pas prise en compte dans la dimension AoA (Analysis of Alternative), étape pourtant importante dans un programme d'armement pour évaluer l'efficacité, les coûts et les risques potentiels. Enfin, jusqu'à cette date, le DOT&E ne réalisait pas systématiquement d'évaluation de cybersécurité avant la mise en œuvre en service d'un nouveau système d'armes.

Des mesures correctives …

Depuis, le DoD a pris un certain nombre de mesures pour remédier à cette situation et faire en sorte que la cybersécurité s'applique jusqu'aux systèmes d'armes. Aussi, une quinzaine de directives, documents d'orientation et mémo destinés à favoriser la prise ne compte de la cybersécurité dans les systèmes d'armes ont été publiés ou actualisés depuis 2014. Citons ici :

- L'Instruction ministérielle DODI n° 8500.01 de 2014 qui identifie les responsabilité et procédures relatives à la gestion des risques cyber tout au long du cycle de vie des systèmes d'armes[4];
- Le mémorandum *Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs* de 2014, [5];
- La *Cyber Strategy* du DoD de 2015 qui plaide pour l'amélioration de la cybersécurité des systèmes d'armes, la définition de standards pour ses futurs systèmes et une réforme des politiques et pratiques d'acquisition pour favoriser la cybersécurité tout au long du cycle de vie des systèmes[6].
- Le *DoD Cybersecurity test and Evaluation Guidebook*[7]de 2015;
- La directive DODI n° 5000.02 de 2017 faisant de la cybersécurité une exigence devant être prise en compte dans chaque aspect d'un programme[8].

Par ailleurs, les armées américaines se sont dotées en interne de structures devant favoriser une meilleure prise en compte de la cyber sécurité dans les systèmes d'armes :

- US Navy : le programme Cybersecurity Safety (CYBERSAFE) institué en 2015 ;
- US Air Force : le Cyber resilience Office for Weapons Systems créé en 2017 ;
- US Army : la Task Force Cyber Strong établie en 2017.

… confrontées à des limites rédhibitoires

Si ces diverses initiatives d'ordre normatives et organisationnelles sont encourageantes, leur efficacité demeure limitée par certains freins devenus structurels et rédhibitoires. Le premier est lié aux difficultés du DoD à recruter et retenir ses experts en cybersécurité en raison, d'une part du manque de main d'œuvre qualifiée sur le marché, et d'autre part de la concurrence avec le secteur privé qui offre des conditions de travail et de rémunération plus avantageuses. Cette difficulté n'est pas cependant pas propre au DoD et est partagée par l'ensemble des structures gouvernementales. Le DoD éprouve tout particulièrement des difficultés pour disposer d'experts disposant à la fois de connaissances sur les procédures d'acquisition, les systèmes d'armes, et la cybersécurité. Le manque d'opérateurs au sein des Red Team est particulièrement criant, ce qui n'est pas sans poser problème car les besoins en la matière ont doublé depuis 2009. Ce déficit de personnels qualifiés provoque ainsi des retards dans les essais opérationnels et réduit les capacités de ces équipes à conduire les évaluations. En outre, cela accroît leur rythme opérationnel et réduit le temps dédié à leur formation, alors même qu'elles ont constamment besoin de se tenir à jour sur les outils et techniques utilisés par leurs adversaires.

Dans son rapport, le GAO évoque par ailleurs des difficultés dans le partage de l'information et des connaissances sur les vulnérabilités et menaces au sein du DoD, qui par exemple ne possède pas encore de politique de classification des informations relatives à la cybersécurité. Quant aux informations concernant les vulnérabilités des systèmes d'armes et les menaces, leur niveau de classification élevé permet certes de les protéger mais empêche leur diffusion au sein du DoD. Concrètement, cette incapacité à partager l'information se traduit à plusieurs niveaux. Par exemple :

- Les responsables de systèmes ne disposent d'informations sur les systèmes auxquels leur système est connecté,
- Les responsables de programmes ne reçoivent pas d'informations sur les attaques touchant les autres systèmes d'armes,
- Les organismes réalisant les audits de sécurité et développant des stratégies de remédiation ne sont pas habilités à partager les informations dont ils disposent sur les vulnérabilités observées,
- Les opérateurs de systèmes ne disposent pas tous du même niveau d'accès à l'information,
- Dans le cas de l'US Navy, certains bâtiments ne disposent pas des équipements et systèmes adéquats pour recevoir et stocker des informations hautement classifiées une fois qu'ils ont déployés en mer.

Un rapport partiel et à vocation politique

Ce travail du GAO demeure incomplet, le périmètre de l'audit excluant les vulnérabilités liées à chaîne d'approvisionnement, à la microélectronique, ou aux automates industriels (ICS/SCADA). La question de la cybersécurité de la chaîne d'approvisionnement est pourtant majeur. Les exemples en la matière ne manquent pas[10]. Preuve qu'il s'agit d'un enjeu majeur, le DoD souhaiterait à l'avenir pouvoir tester le niveau de sécurité des réseaux classifiés et non classifiées de ses fournisseurs au moyen de Red Teams. Des discussions entre le département et les industriels sur les modalités et le périmètre de cette pratique ont déjà été engagées[11].

Dans l'ensemble, ce rapport n'apportera que très peu d'informations nouvelles aux fins connaisseurs du sujet. Cependant, ce document constitue une bonne synthèse de l'état de l'art et porter le problème au niveau politique –le GAO étant rattaché au Congrès qui est le premier destinataire de ses audits. Le rapport ne contient ainsi aucune conclusion et se veut davantage descriptif que prescriptif. Le paysage alarmiste qui dessiné devrait alerter le pouvoir législatif sur les difficultés récurrentes constatées pour limiter les vulnérabilités dans les systèmes d'armes et pourrait favoriser la prise de mesures, budgétaires et/ou normatives, destinées à les atténuer.

[1] « DOD Juste beginning to Grapple with Scale of Vulnerabilities », Government Accountability Office (GAO), 09/10/2018 https://www.gao.gov/products/GAO-19-128

[2] National Research Council (NRC), Defense Science Board (DSB), GAO, etc.

[3] Crée en 1983 à l'initiative du Congrès, le DOT&E (US Office of the Director Operational Test & Evaluation, l'équivalent local de la Direction Technique (DT) de la DGA,) est responsable de l'approbation des programmes d'essais des grands programmes d'armement.

[4] https://fas.org/irp/doddir/dod/i8500_01.pdf

[5] http://www.dote.osd.mil/pub/policies/2014/8-1-14_Procs_for_OTE_of_Cybersec_in_Acq_Progs(7994).pdf

[6] http://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf

[7] http://www.dote.osd.mil/docs/tempguide3/cybersecurity_te_guidebook_july1_2015_v1_0.pdf

[8] https://www.dau.mil/guidebooks/Shared%20Documents%20HTML/DoDI%205000.02.aspx#toc311

[9] http://www.dote.osd.mil/pub/reports/FY2016/pdf/other/2016DOTEAnnualReport.pdf

FOCUS INNOVATION : QUOSCIENT, COMBINER LE MEILLEUR DE L'INTELLIGENCE HUMAINE ET DES TECHNOLOGIES DE CYBERDEFENSE

Entretien avec Constantin Schüßler, Communications Manager, et Fabien Dombard, CEO

Présentation

Fondée en avril 2016 par Fabien Dombard et Ioanis Bizimis, cette PME basée à Francfort s/ Main (Allemagne) mais également installée à Boston (Etats-Unis), compte aujourd'hui 42 spécialistes de la cyberdéfense avec des profils variés tels qu'analystes en géopolitique mais aussi ingénieurs logiciels, passant par des spécialistes de la réponse a incident.

La société s'est développée très rapidement, bénéficiant d'abord du soutien d'un fonds d'amorçage, puis, très prochainement, d'une première levée de fonds.

La cyberdéfense « as a service »

QuoScient propose une solution de cyberdéfense active « as a service » de lutte contre la cybercriminalité, à des clients issus de tous secteurs d'activités : des services financiers aux télécommunications en passant par l'industrie pharmaceutique ou agroalimentaire, les infrastructures critiques (transports, énergie) mais aussi le secteur public et les agences étatiques.

Une conception globale mais modulaire de la cyberdéfense

Les solutions de cyberdéfense active proposées par QuoScient sont basées sur approche globale mais modulaire de la cyberdéfense, et reposent sur l'interaction de trois de ses composantes essentielles :

- Le RENSEIGNEMENT sur la menace à destination des décideurs, réalisé par le biais d'une veille de sources combinant OSINT, sources de confiance et plateformes de partage d'information type MISP ou STIX/TAXII, et qui ont pour objectif d'identifier et anticiper les menaces tout en les communiquant autant à un niveau stratégique (prévisions, tendances), opérationnel (rapports d'analyse et bulletins d'information) et tactique (indicateurs).
- Les opérations de CYBERSÉCURITÉ, qui permettent aux équipes de sécurité d'une organisation de détecter les menaces mais aussi de collaborer lors d'investigations touchant plusieurs entités.
- Les TECHNOLOGIES DE CYBERDÉFENSE qui font de plus en plus appel à l'automatisation et orchestration, ainsi que le *machine learning* pour faciliter la réponse à incident et la rendre plus efficace et plus rapide grâce à l'enrichissement et la caractérisation automatisée de l'information.

La cyberdéfense collaborative et décentralisée

Focus : QuoLab, plateforme décentralisée, agile et automatisée de cyberdéfense

QuoLab intègre des sources de données opérationnelles (rapports d'analyse, gestion de l'information) et tactiques (indicateurs et information enrichie), à des outils analytiques pour permettre une gestion plus efficace et plus rapide des menaces et des incidents.

Elle constitue ainsi une interface unique fournissant aux équipes de sécurité les outils d'analyse et de réaction permettant une réponse rapide en cas d'attaque.

Cette plateforme innovante repose sur la combinaison originale de plusieurs fonctionnalités :

- LA COLLECTE ET LA GESTION D'INFORMATIONS issues de sources et protocoles variés, internes et externes pour une collecte automatisée de données structurées et non-structurées.
- LE PARTAGE D'INFORMATIONS au sein de communautés de professionnels de la sécurité dont les échanges sont régis par des règles assurant granularité et anonymat ;
- LE CONTRÔLE sur l'information partagée, qui reste hébergée par chaque organisation ;
- DES COLLABORATIONS avancées entre communautés, permettant de suivre et commenter en temps réel tout type d'information, de participant, de source technique ;
- L'ANALYSE DE DONNÉES de données à grande échelle à travers un répertoire d'outils variés alliant statistiques et techniques de visualisation, facilitant la détection des menaces ;
- UNE LOGIQUE POUSSEE D'INTEGRATION avec les contrôles de sécurités (SIEM, NIDS, EDR, etc..), plateformes de gestion IT et outils d'analyse (désassembleurs, collecte post mortem), afin d'enrichir, collecter et mettre à jour les défenses de l'organisation.

ACTUALITE

Second Forum cybersécurité le 6/11 à Paris et le 18/11 à Rennes

La 2nd édition du Forum cybersécurité aura lieu le 6 novembre à Paris, et le 18 novembre à Rennes

Organisé par Edens Forum dans le cadre de la European Cyber Week, cet événement est le premier forum de recrutement en France dédié à la cybersécurité et à la cyberdéfense.

L'objectif de cette manifestation qui doit permettre de mettre en contact recruteurs et « talents cybers » part d'un constat simple : en 2017, on comptait 1 seul candidat pour 5 postes à pourvoir dans les métiers de la cybersécurité. En 2018, on estime que près de 400 entreprises ont recruté ou recruteront dans ce secteur. Cinq à dix années de tension sont ainsi à prévoir dans le recrutement des profils requis.

Le Forum cybersécurité rassemblera donc d'une part les professionnels du secteur tels que les services de l'État, les grands comptes mais aussi les PME et les Startups, et d'autre part les étudiants de toutes disciplines liées à la cybersécurité. Il référencera l'ensemble des entreprises qui recrutent en cybersécurité ainsi que les postes ouverts, devenant ainsi une plateforme et une interface unique de rencontre et de prise de contact entre employeurs et spécialistes qui contribuera à répondre au manque de compétences et de personnels qualifiés dans le secteur de la cybersécurité.

Plus de 1000 candidats, 450 professionnels et 50 entreprises sont attendus cette année ainsi que plusieurs institutions telles l'ANSSI, le PEC, la Marine Nationale ou la DGA pour le ministère des Armées, ou la DSIC pour le ministère de l'Intérieur.

CALENDRIER

Seconde édition des Rencontres Cyberdéfense & Entreprise : Défis et technologies clés : anticipation, hypervision, résilience

Le Commandement de la cyberdéfense organise le 7 décembre 2018 la seconde édition des Rencontres Cyberdéfense & Entreprise sur le thème “Défis et technologies clés : anticipation, hypervision, résilience”. Cette journée aura pour objectif de renforcer le lien armée/nation en matière de défense cyber et sera l’occasion d’échanger sur les besoins capacitaires de la communauté de défense.

La journée sera introduite par une allocation du Général Olivier de Paillerets, Commandant de la Cyberdéfense, suivi d’une intervention de Frédéric Valette, Chargé de mission cyber auprès du DGA.

Programme provisoire :

09h00-9h45 Introduction
• GDI Olivier de Paillerets, Commandant de la Cyberdéfense
• IGA Frédéric Valette, Chargé de mission cyber auprès du DGA

9h45-12h00 **Session 1 : L’hypervision au service de la cyberdéfense**

• Présentation des solutions :
Hypervision Technology : Xavier Laszcz, CEO
Egidium : Laurent Denizot, CEO
• Table ronde :
Parmi les intervenants, Philippe Netzer-Joly, Head of Global Security Operations Center

12h00-12h30 : Cocktail déjeunatoire

13h30-15h15 **Session 2 : Comment améliorer nos capacités de détection et d’anticipation grâce à l’Intelligence Artificielle ?**

• Présentation de solutions :
Cyber-Detect : Stéphane Gégout, Président du Conseil de Surveillance et Guillaume Bonfante Mondobrain : Augustin Huret, Fondateur et CEO
• Table ronde :
Parmi les intervenants : Pascal Bourra, Expert Sécurité, SOC Crédit Agricole

15h15-15h45 : Pause

15h45-17h30 **Session 3 : Comment renforcer la résilience des systèmes d’arme ?**

• Présentation des solutions :
Algodone : Jérôme Rampon, CEO
Yagaan : Hervé Le Goff, CEO
• Table ronde

17h30-18h00 Clôture

Pour toute question ou demande d'inscription merci de contacter : arives@ceis.eu

Inscriptions dans la limite des places disponibles, soumises à validation du ministère des Armées.

La **Direction Générale des Relations Internationales et de la Stratégie (DGRIS)** propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation. Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique**, sous le numéro de marché 1502492543. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère des Armées
Direction Générale des Relations Internationales et de la Stratégie
60 Boulevard du Général Martial Valin – CS21623 – 75 509 Paris Cedex 15

CEIS
Tour Montparnasse – 33, avenue du Maine – BP 36 – 75 755 - Paris Cedex 15
Téléphone : 01 45 55 00 20
E-mail : omc@ceis-strat.com