Observatoire du Monde Cybernétique

Lettre n°33 – Septembre 2014

Cette note est disponible sur le portail OMC. Pour y accéder, rendez-vous sur : https://omc.ceis.eu/

[Assemblée nationale] Point sur les nouvelles dispositions relatives à la lutte contre le terrorisme.

Le projet de loi « lutte contre le terrorisme » est actuellement à l'étude par les parlementaires. Il propose de renforcer les sanctions à l'encontre de l'apologie du terrorisme et des actes terroristes, en prévoyant une procédure de blocage administratif des sites concernés. L'originalité de ce projet est de remettre en cause la notion de responsabilité en cascade protégeant notamment l'hébergeur. Le texte accorde également plus de pouvoir aux enquêteurs. Le projet a été adopté par les députés le jeudi 18 septembre.

[Conseil d'Etat] Numérique et droits fondamentaux : le Conseil d'Etat dévoile 50 propositions.

Le Conseil d'Etat dévoile 50 propositions pour « mettre le numérique au service des droits individuels et de l'intérêt général ». Le conseil souhaite repenser les principes fondant la protection des droits fondamentaux en consacrant le principe de la neutralité du net, mais aussi en créant une nouvelle catégorie juridique propre aux « plateformes », distincte de l'éditeur ou de l'hébergeur. Le Conseil souhaite également renforcer les pouvoirs de la CNIL, réformer le « Safe Harbor » ou encore promouvoir la démocratisation de l'ICANN. Suite à cette étude, le projet de loi sur le numérique devrait être soumis au Parlement en 2015.

[ANSSI] L'Observatoire de la Résilience de l'Internet français publie son Rapport 2013

Réalisé par l'ANSSI en collaboration avec l'AFNIC, ce rapport a pour objectif d'analyser en détails l'état et, plus précisément, la résilience de l'Internet français. Cette édition 2013 souligne que l'Internet français est dans un état « satisfaisant », notamment grâce à la résilience des Autonomous Systems en cas de panne. Le rapport propose également une liste de bonnes pratiques pour BGP et DNS.

[INHESJ] Nouveau rapport de l'INHESJ et du CIGREF sur l'ingérence et les politiques de SSI.

Si les notions de PSSI ou de SMSI sont claires et bien définies à l'échelle nationale, cela est moins évident à l'échelle internationale. Différentes approches existent, approches encadrées par différentes dispositions législatives. Dans son dernier rapport, l'INHESJ et le CIGREF proposent une analyse de ces différentes approches, afin de permettre aux entreprises d'anticiper les risques liés à l'ingérence des législations étrangères.

[ANSSI] « Shellshock », vulnérabilité critique du shell GNU Bash

L'ANSSI a attiré l'attention sur la vulnérabilité « Shellshock », vulnérabilité considérée comme critique et affectant les équipements et environnements Linux, Mac OS X et Windows. La divulgation de codes d'exploitation renforce le risque d'une utilisation de cette vulnérabilité à des fins malveillantes.

[Infosecurity Magazine] Royaume-Uni : quatre millions de Livres pour développer les PME du secteur de la cybersécurité.

Vince Cable, ministre des Affaires, de l'Innovation et du Savoir-faire du Royaume Uni, a annoncé la mise en place d'un fonds de quatre millions de Livres Sterling pour les entreprises du secteur de la cybersécurité. Annoncé durant le « US-UK Global Cyber Security Innovation Summit » de Londres, le projet de financement va permettre au Royaume Uni de maximiser son potentiel dans le secteur de la cybersécurité. Les fonds seront alloués aux entreprises qui proposent des solutions innovantes.

[Europa.eu] La Commission Européenne s'engage dans un combat pour un internet libre et gratuit.

Dans son dernier communiqué, laCommission Européenne propose un bilan de la réunion sur la Gouvernance d'internet début septembre à Istanbul. Il y est fait état d'un soutien sans conditions à la liberté d'expression sur internet, et

d'une volonté plus importante de transparence des institutions publiques vis-à-vis des pratiques de surveillance. Les Etats signataires rejettent fermement l'idée d'un contrôle étatique d'internet et veulent développer un système sécurisé plus abouti.

[Numerama] Deux nouveaux commissaires européens chargés du numérique.

Andrus Ansip, Estonien, et Günther Oettinger, Allemand, sont les deux nouveaux commissaires européens chargés du numérique. Le poste, précédemment dévolu à Viviane Reding, sera occupé par deux représentants, travaillant sur des questions différentes. Andrus Ansip aura pour mission de prendre en charge le marché unique numérique, alors que Günther Oettinger sera rattaché à l'économie et à la société numérique.

[Cyberwarzone] Les membres du collectif Anonymous Serbie identifient des djihadistes dans les Balkans.

Des membres du collectif Anonymous Serbie ont décidé de participer à l'identification de djihadistes dans les Balkans, en révélant la présence de certains contenus à destination de propagande terroriste sur les réseaux sociaux. Les unités de la cyberpolice serbes ont ainsi pu mettre la main sur l'identité des jeunes djihadistes qui opéraient en Serbie. Les membres du collectif aident ainsi les forces de l'ordre à démanteler ces cellules étrangères de l'Etat Islamique.

[CyberTinel] Opération Harkonnen : identification d'une campagne de cyberespionnage active depuis 12 ans.

Une campagne de cyberespionnage et de datamining – l'opération Harkonnen – a été dévoilée 12 ans après son lancement. Les banques, sociétés et institutions publiques d'Allemagne, de Suisse et d'Autriche auraient été victimes de cette campagne. L'information a été rendue publique par CyberTinel, société de cybersécurité israélienne. Les pirates auraient pénétré les infrastructures victimes depuis 2002 et les dommages subis par les sociétés seraient trop conséquents pour être évalués.

[Hack Read] Wikileaks révèle des informations confidentielles sur le spyware Fin Fisher.

Le site Wikileaks dévoile de nouvelles informations importantes sur l'utilisation du programme d'espionnage développé et commercialisé par Gamma Group International, Fin Fisher. Les utilisateurs peuvent découvrir les documents d'utilisation de ce spyware et son fonctionnement dans son intégralité. La liste des pays, et les institutions, utilisant ce spyware a aussi été mise en ligne sur Wikileaks.

[Numerama] L'OTAN prévoit une réaction militaire contre les cyberattaques.

Considérant qu'une attaque contre un des pays membre de l'organisation est une agression contre tous, l'OTAN prévoit que cette attaque pourrait engager une réponse militaire de tous les pays membres. Le secrétaire Général de l'OTAN, Anders Fogh Rasmussen, a évoqué cette question récurrente en insistant sur le fait que l'OTAN allait placer les questions de cybersécurité au cœur des priorités de l'organisation.

[OTAN] Nouvelle initiative de l'OTAN pour dynamiser la coopération avec le secteur privé.

Une nouvelle coopération est mise en place par l'OTAN avec le secteur privé de la cybersécurité. Le NATO Industry Cyber Partnership (NICP) a été présenté le 18 septembre dernier à l'occasion d'une conférence sur la cybersécurité en Belgique. Plus de 1500 représentants de l'industrie de la cybersécurité ont affiché leur soutien à cette initiative. L'objectif étant d'améliorer la résilience des institutions avec le soutien des technologies et des expertises du secteur privé.

[Defense News] Etats-Unis : vers des liens plus étroits entre les institutions militaires et les industriels.

Le Directeur de l'US Cyber Command - Le Lieutenant Général Edward Cardon - annonce la

nécessité pour les industriels de la cyberdéfense et le gouvernement américain de travailler de concert de manière plus rigoureuse. Ces liens devraient être renforcés notamment dans le cadre du développement d'infrastructures réseaux et le développement de nouvelles technologies sur le cyberespace.

[Hack Read] 'Treasure map' : nouvelles révélations d'Edward Snowden sur la capacité de la NSA à développer une carte du net.

Les documents dérobés par Edward Snowden dévoilent aujourd'hui un nouveau projet de la NSA : créer une carte d'internet et de tous les appareils connectés en temps réel. Le programme « Carte au Trésor » ou 'Treasure Map' autorise les différentes agences de renseignements à compiler les informations recueillies des réseaux et les intégrer dans une cartographie internationale, éditée en temps réel.

[Matthew Aid] La NSA veut déclassifier de nouveaux documents sur les cyberattaques contre les infrastructures américaines.

Le Directeur adjoint de la NSA souhaiterait que la communauté du renseignement numérique déclassifie certaines cyberattaques. Cette initiative permettrait aux institutions américaines de profiter d'expertises dans le secteur privé et de répondre plus efficacement aux potentielles menaces sur le cyberespace. Cependant, la quantité de documents classifiés est très conséquente et les services de renseignements sont conscients que les représentants politiques ne s'empareraient pas de la question, car trop peu concernés par les menaces sur le cyberespace.

[Net Security] Le malware Tinba s'attaque de nouveau à des banques américaines.

Le malware Tinba, identifié en 2012 pour avoir mis à mal des infrastructures bancaires, est réapparu sur les réseaux. Ciblant à l'origine des banques de taille modeste, le malware a été modifié pour s'attaquer à de grandes enseignes américaines et pouvoir contourner les derniers protocoles de sécurité. L'utilisation de failles dans Flash et Silverlight permet à ce malware d'infecter les ordinateurs, et de proposer un formulaire à l'utilisateur lui demandant des informations bancaires.

[Lapresse.ca] L'armée américaine met en place une nouvelle unité de cyberdéfense.

Le directeur de la NSA, Michael Rogers, a annoncé le développement d'une unité de cyberdéfense de 6 200 personnes, pleinement opérationnelle d'ici 2016. Cette unité aura pour objectif de renforcer la protection des systèmes informatique du Pentagone et ainsi répondre aux cyberattaques ciblant les infrastructures nationales.

[Infosecurity Magazine] Le trojan Citadel vise les industries pétrochimiques au Moyen-Orient.

Le trojan financier et bancaire "Citadel" a été modifié pour cibler les industries pétrochimiques des pays du Moyen-Orient. A l'origine créé pour le vol bancaire, le malware aurait, selon les experts d'IBM, connu des modifications afin de toucher un panel plus vaste de cibles. Les objectifs de Citadel sont le vol de propriété intellectuelle, l'accès aux centres de contrôle des industries et l'accès aux données confidentielles des entreprises.

[FireEye] La Syrian Malware Team utilise un BlackWorm modifié pour effectuer des attaques.

Les équipes de la SMT, principalement soutenues par le gouvernement syrien actuel, auraient récemment lancé des attaques conséquentes sur Forbes et le CENTCOM. Leur méthode a été analysée par les experts de FireEye : ils utilisent un outil dénommé BlackWorm pour s'introduire dans les réseaux. Les équipes syriennes ont modifié le malware afin de prendre le contrôle de serveurs et de consoles d'administration de sites internet.

[AP] Des pirates ont dérobés des informations sensibles dans les pays d'Amérique Latine.

Un groupe de hackers péruviens aurait infiltré différents réseaux militaires et gouvernementaux en Argentine, Colombie, Chili, Pérou et au Venezuela. Les pirates ont ainsi procédé au

défacement de sites internet et à l'extraction de données jugées sensibles. Les informations ont été divulguées sur les réseaux à destination d'autres groupes de hackers qui voudraient acquérir ces données.

[WILEY] Parution d'un nouvel ouvrage sur les capacités de cybersécurité de la Chine.

Dans son dernier ouvrage, paru en juillet 2014, Daniel Ventre analyse les capacités de cybersécurité et de cyberdéfense de la Chine. Ce pays peut actuellement faire face à de nouvelles menaces, du fait de son rapide développement numérique.

[Security Week] Deux campagnes distinctes de cyberespionnage chinoises mises en parallèle.

Les chercheurs de FireEye ont mis à jour deux campagnes de cyberespionnage d'origine chinoise. Il semblerait que les deux groupes distincts, qui ont des objectifs et des méthodes spécifiques, aient reçu le même entrainement et soient dotés des mêmes capacités techniques. Les toolkits employés pour les attaques sont identiques et les deux groupes feraient partie d'un même scénario de campagne de cyberespionnage.

Cybersécurité et aide à la décision

Les études montrant que les petites et moyennes entreprises sont les principales victimes de la cybercriminalité économique se sont multipliées ces dernières années[1][2]. Passé le soupçon initial quant à l'origine et aux objectifs marketings de ces études), la question des coûts associés à leur sécurisation reste inéluctablement un frein.

Même si les campagnes de sensibilisation peuvent aider ces structures de taille modeste à mieux prendre en compte le risque cyber, l'expert en sécurité reste une denrée rare et onéreuse, tandis que les solutions logicielles efficaces nécessitent un certain niveau d'expertise pour être opérées. Le problème est encore exacerbé dans le cas des startups, qui combinent à la fois innovation et incapacité d'investir dans une cyberprotection alors même que leur capital informationnel est très attractif pour un cyberattaquant.

Dans un contexte économique difficile, comment concilier le besoin croissant de cybersécurité des petites et moyennes entreprises avec leur budget ? Ne serait-il pas intéressant de créer des systèmes d'aide à la décision adaptés à leur taille et donc à leur niveau d'expertise cyber ?

Aide à la décision & systèmes experts

L'aide à la décision, aussi appelée recherche opérationnelle, est l'ensemble des méthodes et des techniques rationnelles permettant d'opter pour la meilleure prise de décision possible. Grâce à une modélisation conceptuelle et mathématique, elle vise à analyser des situations complexes en vue de donner aux décideurs la capacité d'arbitrer sans avoir besoin de maîtriser l'ensemble des concepts derrière la problématique posée.

Le système expert représente la version logicielle de l'aide à la décision, reproduisant les mécanismes cognitifs d'un expert de son domaine. Il est capable de répondre à des questions en mettant en relation faits et règles à l'aide d'un moteur d'inférence reposant essentiellement sur le syllogisme.

En matière de cybersécurité, les SIEMs (Security Information and Event Management) et les IDS (Intrusion Detection System) sont des logiciels experts. Dans le cas des SIEMs par exemple, un moteur de corrélation permet de relier plusieurs évènements à une même cause, simplifiant la tâche des experts qui l'emploient en effectuant ainsi un travail qui leur revenait auparavant. Même si ces logiciels sont de simples outils, il faut bien comprendre qu'ils intègrent et mettent en pratique un premier niveau d'expertise et de raisonnement.

Accessibilité de la cybersécurité : niveau minimum de sécurité à atteindre

Si l'expertise humaine est trop onéreuse et si les outils de sécurité restent destinés aux experts, alors apparaît le besoin d'une solution logicielle permettant aux petites structures de se protéger en se rapprochant de la prestation d'un expert.

En se penchant sur les logiciels de sécurité, on remarque plusieurs choses :

[1] http://www.trendmicro.fr/media/misc/small-business-is-big-business-in-cybercrime-fr.pdf

[2] http://www.symantec.com/fr/fr/about/news/release/article.jsp?prid=20130416_01

- On retrouve toutes les solutions nécessaires dans le domaine des logiciels libres pour établir une cartographie détaillée d'un réseau et de son environnement logiciel, détecter des failles de sécurité et même détecter des intrusions.
- Ces logiciels ne présentent pas les informations de façon intelligible pour le béotien, et n'offrent pas de solution claire à un problème qu'ils sont pourtant en mesure d'identifier.

Ayant toutes les cartes en main, il est possible d'imaginer un logiciel capable de déterminer et d'analyser la topologie réseau d'une entreprise, puis de suggérer les modifications à apporter afin d'améliorer le niveau de sécurité. Il s'agirait d'associer les capacités d'analyse des logiciels existants avec une documentation pédagogique, intégrée, pour guider pas à pas le néophyte dans les actions correctives à opérer.

La base de faits et de règles d'un tel système expert intégrerait les vulnérabilités connues et les règles techniques fondamentales de la sécurité informatique (fermeture des ports non-utilisés, maintien à jour de l'environnement logiciel, etc.). Ceci compléterait les campagnes de sensibilisation mises en œuvre afin de réduire les manquements humains à l'hygiène et à la sécurité informatique (on pense notamment au besoin de vigilance vis-à-vis des pièces jointes).

L'aide à la décision dans la réaction à une cyberattaque

Toujours dans l'optique d'apporter un certain niveau de protection aux néophytes, il conviendrait de s'intéresser à la réaction en cas d'attaque : toute entreprise sera, à un moment ou un autre, l'objet d'une attaque. Comme les premiers secours pour l'humain, la rapidité et l'efficacité de la réaction détermineront les impacts de l'attaque.

La première réaction à portée de l'utilisateur informé est d'isoler un élément compromis. Cependant le confinement peut aussi concerner un élément sensible dont l'intégrité et la confidentialité doivent être conservées, quitte à sacrifier sa disponibilité dans un premier temps (en attendant l'intervention d'un CERT).

C'est aussi l'occasion de rappeler à l'utilisateur les bons réflexes[3]en cas d'attaque : conservation des preuves, ne pas éteindre les postes infectés afin de préserver les informations en mémoire sur le malware, etc.

Ce logiciel pourrait être créé par un éditeur qui y verrait l'occasion de promouvoir ses propres solutions, par exemple en les mettant en avant parmi un panel de solutions gratuites. On peut également l'imaginer sous la forme d'un logiciel modulaire, selon un modèle commercial éprouvé : une version de base gratuite et des versions payantes plus avancées en termes de fonctionnalité (qui incluraient un IDS et l'aide à la décision dans la réaction). Ce schéma permettrait ainsi de suivre les entreprises dans leur développement, en les fidélisant dès leur « enfance ».

Au-delà des cyberattaques visant le gain immédiat (vol de données clientes, ransomware), l'innovation dont les petites structures font preuve attirent les convoitises. D'autre part, les sous-traitants constituent souvent le maillon faible pour un attaquant sérieux qui souhaite pénétrer la sécurité d'une grande entreprise. Il devient alors stratégique pour un Etat, comme pour un grand donneur d'ordres privé, de s'assurer que les petites entreprises ont les moyens de se protéger jusqu'à atteindre une taille critique qui lui permettra enfin d'accéder aux services d'un expert en sécurité.

[3] http://www.cert.ssi.gouv.fr/site/CERTA-2002-INF-002/index.html

Envisager une défense automatisée peut sembler utopique. Ce raisonnement est pourtant à l'œuvre côté attaque. La DARPA américaine projette ainsi de créer un système offensif automatisé[4]. S'il est possible de rendre un tel système efficace, alors la faisabilité d'un équivalent défensif est uniquement une question de moyens.

[4] http://www.darpa.mil/Our_Work/I2O/Programs/Plan_X.aspx

Découvrez le portail OMC. Pour y accéder, rendez-vous sur : https://omc.ceis.eu/

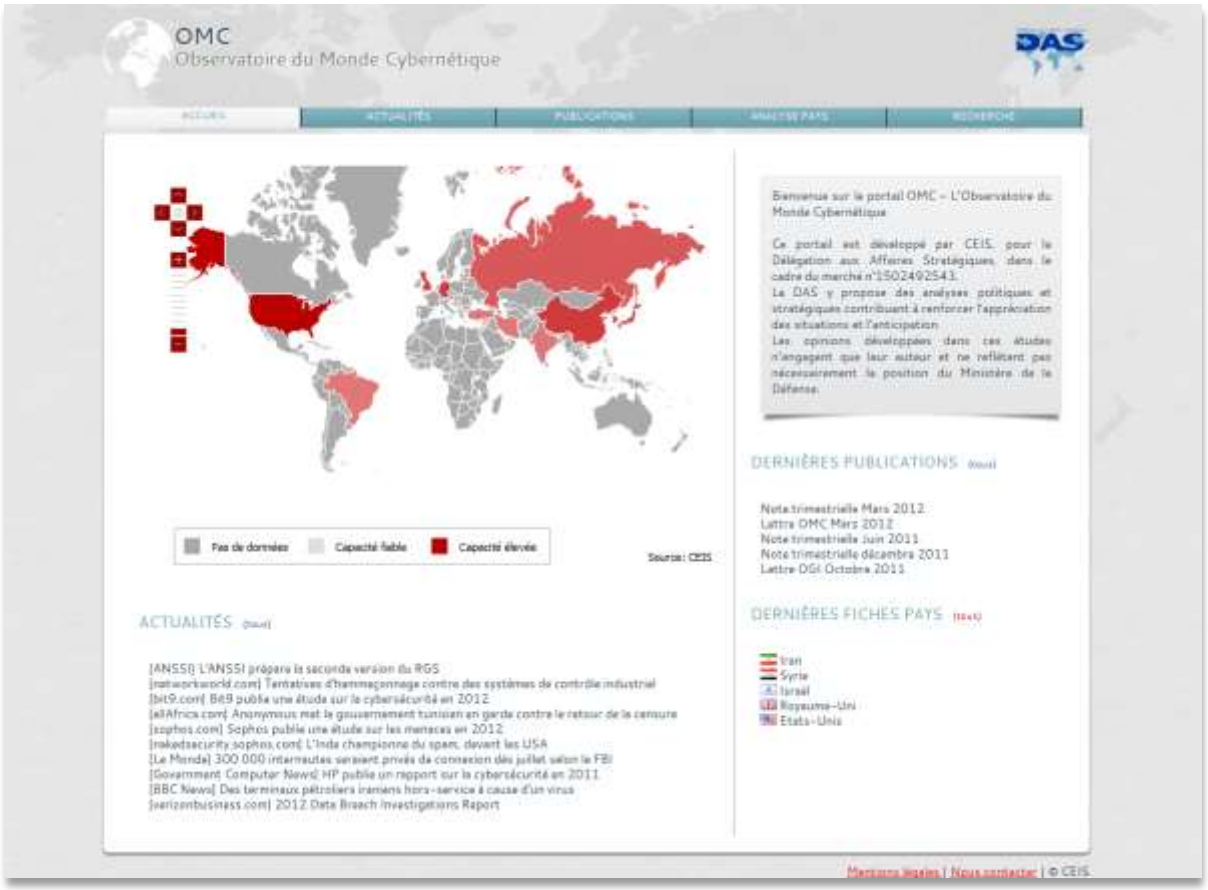

Figure 1. Page d'accueil du portail OMC - https://omc.ceis.eu/

Pour vous y connecter, n'hésitez pas à demander vos identifiants à CEIS.

Contact : Barbara Louis-Sidney - blouis@ceis.eu et omc@ceis.eu

Les Assises de la Sécurité	Monaco	1 - 4 octobre
Cybersecurity in Romania	Sibiu	2 - 3 octobre
OVH Summit 2014	Paris	7 octobre
IP Cyber Security EXPO	Londres	8 – 9 octobre
International Conference on Information Security and Cyber Forensics	Maylaysia	8 – 10 octobre
ISSE 2014 – Securing Assets Across Europe	Bruxelles	14 – 15 octobre
System Safety and Cyber Security 2014	Manchester	14 – 16 octobre
Black Hat Briefings & Training Europe	Amsterdam	14 - 17 octobre
X.25 Ethical Hacking Conference	Mexico	17 octobre
Cyber Security Summit 2014	Minneapolis, MN	21 - 22 octobre
USDA Cyber Security Symposium and Expo 2014	Washngton, DC	28 – 29 octobre

CEIS

Compagnie Européenne
d'Intelligence Stratégique

Téléphone : 01 45 55 00 20
Télécopie : 01 45 55 00 60
E-mail : gtissier@ceis.eu

Les opinions exprimées dans cette lettre n'engagent que la responsabilité de leurs auteurs.

Retrouvez cette lettre et l'ensemble des articles cités sur le portail
https://omc.ceis.eu/
(Accès soumis à authentification)

La Délégation aux Affaires Stratégiques 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 DAS a confié à la **Compagnie Européenne d'Intelligence Stratégique (CEIS)** 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 de la défense et des anciens combattants
Délégation aux Affaires Stratégiques
Sous-direction Politique et Prospective de Défense
14 rue St Dominique 75700 PARIS SP 07