Forum International de la Cybersécurité 24 et 25 janvier 2017 à LILLE

	Forum International de la Cybersécurité 24 et 25 janvier 2017 à LILLE

Lille grand palais accueille à partir de ce mardi 24 janvier à 09:30 la 9ième édition du Forum International de la Cybersécurité.

Favoriser l'innovation

Résolument tournée vers l'innovation, les écoles Epitech ont développé au sein de chaque campus des Innovation, des espaces dédiés aux expérimentations, au prototypage et au développement de projet innovants. Ces Hub reposent sur une méthodologie collaborative et transversale, reposant sur 5 domaines de compétences permettant de balayer le champ des innovations dont celui de la sécurité.

Ainsi, situé au sein de l'Espace Carrières, réunissant des écoles spécialisées, des étudiants d'Epitech et des encadrants pédagogiques proposeront des démonstrations d'attaques/défense lors des Hacking Trucks du Forum.

Les démonstrations proposées par l'Epitech :

• Démonstration de la facilité d'interception et d'altération des communications sur le(s) réseau(x) GSM et/ou Wi-Fi, par l'interception de SMS, de conversations vocales (pour le GSM) et autres communications quelconques (pour le Wi-Fi),

• Démonstration Ransomware : Démonstration du mode opératoire et des conséquences d'une campagne d'attaque par rançongiciel,

• Hacking Live : Démonstration d'une attaque en live d'une plateforme CMS Web, de la découverte de la faille Web jusqu'à la prise de contrôle du serveur l'hébergeant,

• Poisontap : À l'aide d'un matériel peu coûteux, il suffira de quelques minutes à nos étudiants démonstrateurs pour siphonner les communications d'un ordinateur, même verrouillé.

Ces démonstrations ont pour but de sensibiliser tout visiteur sur la protection des données, notamment avec le développement des usages et des nouvelles technologies afin que les consommateurs soient de plus en plus soucieux de leur sécurité tout en gardant un confort d'utilisation. Le FIC est un événement gratuit dont l'inscription est soumise à la validation des organisateurs…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : Lille FIC 2017

La coopération Internationale renforcée dans le Cloud

	La coopération Internationale renforcée dans le Cloud

« Le quinzième anniversaire de la Convention de Budapest sur la cybercriminalité est un tournant dans la mesure où la Convention atteint maintenant les « nuages », a déclaré le Secrétaire Général du Conseil de l'Europe Thorbjørn Jagland lors de l'inauguration de la Conférence Octopus 2016.

Les données et donc les preuves électroniques sont de plus en plus stockées sur des serveurs relevant de juridictions étrangères, inconnus ou multiples. C'est pourquoi, il peut être extrêmement difficile pour les autorités chargées de la justice pénale d'obtenir régulièrement de telles preuves. Faute de celles-ci, les délinquants qui opèrent dans le cyberespace ne peuvent être poursuivis.
Le Secrétaire Général a salué le jeu de recommandations adoptées par le Comité de la Convention sur la cybercriminalité lors de sa réunion des 14-15 novembre, dans lesquelles il voit une réponse véritable au problème de l'informatique en nuage (cloud computing). Les recommandations prévoient la négociation d'un protocole additionnel à la Convention à partir du milieu de 2017.
« La coopération entre les Etats s'est considérablement améliorée. Cela est dû pour beaucoup au travail du Comité de la Convention. Les notes d'orientation adoptées par le Comité ont aidé à préserver la pertinence et l'actualité de la Convention, à renforcer notre capacité de combattre le terrorisme, le vol d'identités ou les attaques contre des infrastructures d'informations critiques », a déclaré le Secrétaire Général, qui a invité les gouvernements à mieux protéger les droits des particuliers dans le cyberespace.
« Nous avons élaboré une sorte de « triangle dynamique » – Convention, Comité et renforcement des capacités – si bien que la Convention de Budapest reste aujourd'hui le traité international le plus important sur la cybercriminalité et la preuve électronique », a-t-il conclu.
A l'occasion de la conférence, Andorre a ratifié la Convention en présence d'Eva Descarrega Garcia, Secrétaire d'Etat andorrane à la Justice et à l'Intérieur.
68 Etats sont soit déjà parties à la Convention de Budapest, soit se sont formellement engagés à la respecter. Au moins 70 pays de plus ont pris la Convention comme source d'inspiration pour élaborer leur législation interne.
[Discours de Thorbjørn Jagland (*anglais*)]

Réagissez à cet article

Original de l'article mis en page : Cybercriminalité : vers un

Denis JACOPINI intervient au Conseil de l'Europe lors de la conférence Octopus 2016

Denis JACOPINI intervient au Conseil de l'Europe lors de la conférence Octopus 2016

A l'occasion de sa conférence annuelle consacrée à la lutte de la Cybercriminalité à travers le monde du 16 au 18 Novembre prochain au Conseil de l'Europe, Denis JACOPINI intervient au Workshop n°7

Au programme :

• La Convention de Budapest: 15e anniversaire
• Criminalité et compétence dans le cyberespace : la voie à suivre
Ateliers
• Coopération entre les fournisseurs de service et les services répressifs en matière de cybercriminalité et de preuve électronique
• L'accès de la justice pénale aux preuves dans le Cloud: les résultats du groupe sur les preuves dans le Cloud (Cloud Evidence Group)
• Renforcement des capacités en cybercriminalité: les enseignements tirés
• L'état de la législation en matière de cybercriminalité en Afrique, en Asie/Pacifique et en Amérique latine/aux Caraïbes
• Le terrorisme et les technologies de l'information : la perspective de la justice pénale
• Coopération internationale: amélioration du rôle des points de contact 24/7
• A la recherche des synergies: politiques et initiatives en cybercriminalité des organisations internationales et du secteur privé

Participation

La conférence sera l'occasion, pour les experts en cybercriminalité des secteurs public et privé ainsi que les organisations internationales et non gouvernementales du monde entier, d'échanger.

La conférence Octopus fait partie du projet **Cybercrime@Octopus** financé par les contributions volontaires de l'Estonie, du Japon, de Monaco, de la Roumanie, du Royaume-Uni, des Etats-Unis d'Amérique et de Microsoft ainsi que du budget du Conseil de l'Europe.
Agenda Octopus 2016

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : Octopus 2016

La cybercriminalité a de belles années devant elle

La cybercriminalité a de belles années devant elle

Les prochaines années laissent entrevoir de beaux moments pour les cybercriminels de tout acabit. Les raisons expliquant cela sont nombreuses. Quelles sont-elles?

Suivre la scène de la sécurité informatique a ceci de particulier : c'est à la fois fascinant et grandement décourageant. C'est d'autant plus décourageant que les tendances présentes au cours des derniers mois laissent entrevoir de beaux jours pour les cybercriminels. Essentiellement, quatre raisons expliquent cela.

La multiplication des cibles potentielles

La première raison est assez évidente : il y a de plus en plus de cibles disponibles pour les criminels. La surmultiplication du nombre de plateformes exploitant Internet a pour effet de toutes les transformer en des opportunités potentielles pour des gens malintentionnés. La manifestation la plus flagrante de cette surmultiplication se transpose dans la fulgurante montée de l'Internet des objets.

Ce nouvel eldorado porte toutefois les gènes de sa propre insécurité. En effet, le marché est meublé par une multitude de joueurs, et leur intérêt porté à la chose sécuritaire est tout aussi variable. Ainsi, alors que l'objectif est d'occuper le marché le plus rapidement possible, bon nombre de joueurs impliqués dans la course à l'Internet des objets arrivent sur le marché avec des produits qui sont, volontairement ou involontairement, plus ou moins sécurisés.

Bref, nous sommes placés devant un cercle vicieux duquel nous ne pouvons pas nous sortir : plus de technologies signifient nécessairement plus de vulnérabilités et, conséquemment, plus d'opportunités criminelles. De plus, croire que l'on puisse mettre un frein à l'évolution technologique est illusoire.

Le difficile marché de la sécurité

Le contexte actuel rend les ressources extrêmement difficiles à conserver ou à acquérir pour les petites et moyennes entreprises qui n'ont pas les moyens d'offrir des salaires élevés.

Alors que le domaine apparaît comme extrêmement complexe, le manque criant de main-d'œuvre est de plus en plus problématique dans les entreprises. Forbes affirme pourtant que ce secteur vaudra sous peu 75 milliards de dollars US et que le marché créera plus d'un million d'emplois.

Non seulement manque-t-il de spécialistes en sécurité, mais il manque aussi de plus en plus de pirates black hat sur le marché, faisant en sorte que les cybercriminels eux-mêmes se tournent de plus en plus vers des modèles de sous-traitance pour effectuer leurs opérations.

Ce manque d'expertise a pour effet de rendre l'économie globalement plus ou moins axée sur la sécurité. Certes, certains secteurs ont les moyens de leurs ambitions, mais le contexte actuel rend ces ressources extrêmement difficiles à conserver ou à acquérir pour les petites et moyennes entreprises qui n'ont pas les moyens d'offrir des salaires élevés. Les effets sont bien sûr conséquents : la situation engendre une sécurité bien inégale, avec le lot de vulnérabilités qu'elle impose.

La rentabilité évidente

Autre point extrêmement important pour expliquer pourquoi la cybercriminalité aura le vent dans les voiles? C'est lucratif. La logique criminelle est relativement simple : il s'agit de faire le plus d'argent possible, le plus facilement possible. En somme, c'est le capitalisme en action.

Dans le domaine de la cybercriminalité, cela fonctionne décidément. On estime à 445 milliards de dollars US le marché de la cybercriminalité. Bon, je vous entends déjà geindre et dire que c'est fort de café. Soit. Admettons que ce soit la moitié moins, c'est tout de même 222 milliards, batinse!

Pour rappel, le budget du Canada est d'environ 290 milliards de dollars CA. C'est donc payant, et c'est bien dommage, mais les conséquences de la cybercriminalité sont minimes. Les chances d'arrêter les criminels sont plutôt basses (voir point suivant) et les peines encourues ne sont pas adaptées.

L'incapacité d'action des agences d'application de la loi

Les cybercriminels ont donc le beau jeu, puisque le risque de se faire prendre est extrêmement bas. En effet, les forces policières sont mal équipées pour confronter la cybercriminalité, faisant en sorte que trop souvent, elles doivent capituler devant les actions commises par les criminels. Dans les cas les plus extrêmes, les agences tenteront de déployer les efforts nécessaires pour faire culminer une enquête, mais cela se fera à grands coups de contrats avec le secteur privé afin de se procurer l'expertise nécessaire pour résoudre le crime en question. Le fait que le FBI ait versé un montant de 1,3 million à un groupe de «chercheurs en sécurité», considérés par plusieurs comme ayant des mœurs on ne peut plus douteuses, pour accéder aux données présentes dans l'iPhone du terroriste de San Bernardino en est, en soi, la manifestation la plus éloquente.

Lutter contre la cybercriminalité demande essentiellement quatre choses. Une culture particulière, une collaboration internationale, des moyens et des techniques disponibles, et des compétences de pointe dans le domaine des technologies. Le dur constat qu'il faut faire, c'est qu'outre la collaboration internationale, les autorités compétentes n'ont pas les moyens pour atteindre les trois autres prérequis. Par conséquent, la vaste majorité des corps policiers ne s'attaqueront aux cybercrimes que lorsque les infractions sont trop exagérées.

La somme de toutes les peurs

Au final, ce qui est le plus inquiétant dans cette situation, c'est que plus le temps avance, plus les réseaux de cybercriminels deviennent solides, sophistiqués et ont de plus en plus de moyens. Les laisser agir en toute impunité a pour effet de les rendre toujours plus coriaces, ce qui rendra la tâche de lutter contre eux d'autant plus difficile à long terme. Il faudra que l'on prenne le problème à bras le corps une fois pour toute, sinon, nous risquons d'avoir de mauvaises surprises dans les prochaines années.

Article original de branchez-vous.com

Réagissez à cet article

Original de l’article mis en page : La cybercriminalité a de belles années devant elle | Branchez-vous

---

Amnesty critique la nouvelle loi sur la cybercriminalité au Koweït

Amnesty critique la nouvelle loi sur la cybercriminalité au Koweït

---

Amnesty International a vivement critiqué mardi une nouvelle loi sur la cybercriminalité au Koweït qui, selon cette organisation, va restreindre davantage la liberté d'expression et doit être révisée.

Le texte, qui entre en vigueur mardi, « va s'ajouter à l'éventail de lois sur le web qui restreignent déjà le droit des Koweïtiens à la liberté d'expression et doit être révisé d'urgence », écrit l'organisation de défense des droits de l'Homme dans un communiqué.
La nouvelle législation prévoit la criminalisation d'une série d'expressions en ligne comportant notamment des critiques envers le gouvernement, des dignitaires religieux ou des dirigeants étrangers, relève Amnesty.
« Cette loi répressive » fait partie d'un éventail de législations destinées à « étouffer la liberté d'expression », a commenté Saïd Boumedouha, directeur adjoint d'Amnesty International pour le Moyen-Orient et l'Afrique du nord.
Des dizaines de personnes au Koweït ont été arrêtées et poursuivies en justice, certaines servant déjà des peines de prison, en vertu d'une autre législation pour des commentaires sur les réseaux sociaux.
Votée en juin, la nouvelle loi prévoit des peines de 10 ans de prison et des amendes allant jusqu'à 165.000 dollars pour des crimes en ligne, notamment ceux liés au terrorisme.
Pour le gouvernement, cette loi est nécessaire pour combler un vide juridique et réglementer l'utilisation des services en ligne tels que Twitter.
La peine minimale en vertu de la loi consiste en six mois de prison et 6.600 dollars d'amende pour celui qui ose, illégalement, « infiltrer un ordinateur ou un réseau électronique ».
« Les autorités koweïtiennes ne doivent pas appliquer cette loi jusqu'à ce qu'elle soit révisée pour se conformer aux obligations internationales du Koweït en matière de droits de l'Homme », a dit M. Boumedouha.
« Cette loi n'appartient pas au XXIe siècle », a-t-il ajouté, soulignant que « les Koweïtiens méritent mieux » qu'une telle législation.

Réagissez à cet article

Source : *Koweït: Amnesty critique la nouvelle loi sur la cybercriminalité – Internet – Notre Temps*

Vers l'adhésion de la Tunisie à la convention de Budapest sur la cybercriminalité | Le Net Expert Informatique

Vers l'adhésion de la Tunisie à la convention de Budapest sur la cybercriminalité

Le chef du gouvernement Habib Essid a présidé ce mercredi 23 septembre 2015, la deuxième réunion du Conseil stratégique de l'économie numérique, à la Kasbah.

Une batterie de mesures ont été décidées à cette occasion, dont :

- L'élargissement de la composition du conseil en y intégrant les ministres de la Défense et de la Santé. Faire participer les composantes de la société civile qui sont actives dans le domaine du numérique.
- L'approbation de l'objectif stratégique : « Un accès haut débit pour toutes les familles tunisiennes ».
- L'intensification des concertations entre les secteurs public et privé dans le but d'œuvrer à la « numérisation totale des écoles ».
- La mise en place d'une base de données topographique au service de la géo-localisation et signature, à cet effet, d'un contrat de partenariat public-privé sur une période de six mois.
- L'appui des efforts pour que la Tunisie abrite le sommet africain sur l'open enseignement « African MOOCs Summit ».
- La formation d'une équipe conjointe entre le public et le privé pour développer le cadre juridique et procédural des appels d'offre publique dans le domaine du numérique.
- L'approbation d'une série de mesures à caractère technique et structurel ayant relation avec l'e-administration tel que l'identifiant unique.
- Le lancement du projet de numérisation du patrimoine culturel.
- Le dépôt de la candidature de la Tunisie pour adhérer à la convention de Budapest sur la cybercriminalité.

Source :
http://www.jawharafm.net/fr/article/vers-l-adhesion-de-la-tunisie-a-la-convention-de-budapest-sur-la-cybercriminalite/90/27865
Par Zeyneb Dridi