



Communiqué de Presse

CONTACT PRESSE – AL'X COMMUNICATION

Tél. : 06 68 42 79 68

Le 4ème Forum International sur la Cybercriminalité dévoile son programme

Paris, Lille, le 11 janvier 2010 – A l'initiative de la Gendarmerie nationale et avec le soutien de l'Union européenne, le FIC – Forum International sur la Cybercriminalité – propose un cycle de débats, conférences et ateliers, dans le cadre d'une coopération publique/privée. Afin de permettre une mobilisation encore plus forte, cette 4ème édition se déroulera sur 2 jours, les 31 mars et 1er avril 2010.

Renforçant sa reconnaissance sur la scène internationale, le FIC 2010 aura le grand plaisir d'accueillir en son sein un colloque organisé par l'Organisation pour la sécurité et la coopération en Europe (OSCE) pour conduire avec un panel d'experts, une réflexion sur les moyens de sécuriser l'espace numérique.

L'événement ouvert au public est une occasion unique de débattre avec les meilleurs experts nationaux et internationaux, pour mieux appréhender les défis de la cybercriminalité. Contre cette menace qui ignore les frontières, le FIC s'inscrit pleinement dans le cadre du renforcement de la lutte contre la cybercriminalité. Une priorité établie d'une part, par le programme de Stockholm 2010-2014 (plan d'action quinquennal pour la coopération policière et judiciaire européenne), et d'autre part dans l'esprit des objectifs assignés à l'Union européenne par les Conseils européens de Lisbonne et de Göteborg ; par une approche globale, fondée sur la coopération internationale.

Outre son rôle de sensibilisation et d'information sur les dangers de l'espace numérique, l'objectif du FIC est d'offrir un terrain d'échanges et de réflexion, de relayer les bonnes pratiques et fédérer les initiatives publiques et privées destinées à rassurer les usagers, tout en dissuadant et réprimant les activités illicites.

Lancé en 2007 le FIC devient peu à peu le rendez-vous annuel incontournable des acteurs de la lutte mondiale contre le cybercrime. L'Eurométropole lilloise est un pôle d'excellence en la matière. De par les synergies et la mobilisation des acteurs, le FIC a vocation à devenir un laboratoire d'idées européen, force de proposition pour la mise en place de politiques anticipant de nouveaux risques numériques.

Par son programme et le public attendu, le FIC 2010 est aussi une invitation à poursuivre le maillage entre les services d'enquêtes et l'institution judiciaire. Il offre une place de choix pour favoriser les échanges autour du renforcement de la coopération internationale.

Le programme de conférences et ateliers

Le programme sera organisé autour de trois pôles distincts :

- **Justice sécurité défense** : pour informer et réfléchir sur les réponses institutionnelles nationales et internationales.

- **Entreprises** : pour sensibiliser aux risques numériques et développer un partenariat public-privé. Il sera l'occasion de la diffusion du "guide pratique du chef d'entreprise face au risque numérique ».

- **Collectivités** : pour déterminer les enjeux du développement de la société numérique (e-démocratie, libertés publiques...)

Une animation permanente rythmera ces deux journées : Salon des exposants, Web TV et ateliers d'experts.

Discours d'introduction

**Par le Directeur général de la gendarmerie nationale,
sous le patronage du Ministre de l'Intérieur, de l'Outre-mer et des Collectivités Territoriales.**

Conférence plénière d'ouverture

« La mobilisation européenne et internationale pour la lutte contre la cybercriminalité »

La conférence plénière accueillera les hauts représentants de :

- l'unité de coopération judiciaire de l'Union européenne, Eurojust
- l'agence répressive de l'UE, Europol
- la Direction générale des droits de l'Homme et des affaires juridiques du Conseil de l'Europe
- la Commission européenne
- l'association internationale de lutte contre la cybercriminalité

Colloque OSCE

Une approche globale de la cyber-sécurité

Les moyens mis en oeuvre, ou que l'on peut souhaiter pour améliorer la sûreté de la toile en mettant l'accent notamment sur l'approche globale mise en place par l'Organisation pour la sécurité et la coopération en Europe (OSCE), ses bonnes pratiques, les tendances à venir dans le domaine, les partenariats privé-public, le cadre légal international...

Conférence

“ La protection des systèmes d'information : véritable enjeu de sécurité nationale ”

Avec les interventions du Haut fonctionnaire de défense et de sécurité du Ministère de l'économie de l'industrie et de l'emploi (MEIE) et d'un représentant de l'Agence nationale pour la sécurité des systèmes d'information (ANSSI).

Conférence plénière de clôture

“ Droit à l'oubli sur le Web : ultime protection de l'identité numérique ”

Phénomène : perte de contrôle des informations mises sur les réseaux, voire leurs modifications à des fins de nuire ou de faire chanter. La fin du droit à l'oubli, les moteurs de recherche assurant le maintien des informations (en contradiction avec le droit à la réinsertion et à l'erreur).

Parmi les intervenants, la conférence accueillera des avocats spécialistes du droit des nouvelles technologies, des représentants de la Police Judiciaire et de la Direction générale de la gendarmerie nationale (DGGN).

ATELIERS

Plus de 23 ateliers répondront aux problématiques transverses de l'actualité de la lutte contre le cybercrime. Avec la participation d'experts français et internationaux, représentants du gouvernement, de l'industrie de défense, des télécommunications, de la sécurité des systèmes d'information, des secteurs bancaires, e-commerce, universitaires et de la recherche, de la police, justice, gendarmerie et également associatifs.

Programme des ateliers

“ Essor du nomadisme : une sécurité suffisante ? ”

Moyen d'accès grandissant aux vulnérabilités encore mal maîtrisées. Quelles solutions pour réduire les risques d'intrusion, de vols de données... ? Recommandations comportementales en situation de nomadisme.

“ Cyberdéfense : quelles coopérations public/privée dans le cadre du livre blanc sur la défense et la sécurité nationale ? ”

Mise en avant des aspects de la coopération européenne public/privée concernant le volet cyberdéfense des cinq fonctions stratégiques : la connaissance et l'anticipation, la prévention, la dissuasion, la protection et l'intervention.

“ Cyber infiltration ”

Cadre légal national et international, spécificité de cette mission. Différence de conception avec le monde anglo-saxon (exemple américain : Child predator units et l'émission TV “to catch a predator”).

“ Etablissements bancaires : gestion de la sécurité des opérations en ligne ”

Vols d'identité, piratage informatique, systèmes de sécurité informatique.

“ Le commerce du futur : sécurisation des données et confiance du consommateur ”

Sécurisation des informations : cryptologie des données, transmission sécurisée, traçabilité. Analyse en sciences humaines et sociales du comportement du consommateur vis-à-vis des nouvelles technologies.

“ Web 3.0, Web 2, Web objet : quel avenir pour le Net ? ”

“ Jeux d'argent en ligne : nouvel “ELDORADO” du blanchiment ”

“ Lutte anti-virale en environnement informatique ”

Infection virale et les aspects juridiques. Etude épidémiologique, diffusion de code malveillant.

“ Présentation des outils de sensibilisation aux dangers d'Internet ”

Panel d'outils existants : La prévention en famille. Jeune et éducation : présentation d'un programme national de sensibilisation “serious game 2025 machina” (sortie prévue février 2010). Pédagogie et utilisation d'Internet par les jeunes. Protection de l'enfance : logiciels de contrôle parental, animation quizz interactif. Sensibilisation des adultes aux dangers d'Internet dont leurs enfants peuvent être victimes. AFA présentation du partenariat européen.

“ Traitement du téléchargement illégal ”

Problématique et législation française comparées à celles d'autres pays de l'UE. Etat de l'art des moyens techniques : détection, filtrage, ou blocage sélectif. Constat à distance pour une riposte graduée ou autre (avec démonstration). Prospective, difficultés techniques et juridiques attendues.

“ SSI : rôle et responsabilité du chef d'entreprise ”

Question de la délégation au RSSI, responsabilité pénale (protection des données personnelles / contenu des STAD / agissements illicites des employés) mais aussi question des modalités de management comme facteur de sécurité. Une bonne politique de sécurité nécessiterait une prise de conscience débouchant sur des actions concrètes positives de l'ensemble des collaborateurs d'une entreprise. Multiplication des procédures de contrôle et de surveillance (course à la sophistication). Notion de confiance dans les relations internes de l'entreprise (passage du contrôle à la confiance).

“ La révélation des failles de sécurité, risques et enjeux ”

Quel cadre légal et contractuel pour les tests ? (Etude comparée européenne).
Quid de l'obligation de dénonciation ?

“ Sécurité des chaînes de production et des services généraux informatisés ”

Sensibilisation sur la sécurité des systèmes de contrôle de processus. Prise de contrôle, chantage au sabotage.

“ E-démocratie : opportunités et menaces pour les collectivités territoriales ”

Enjeu, développement et protection. Manipulation de données sensibles, de l'expression publique...

“ Contrefaçon sur le Net : quelles solutions ? ”

La contrefaçon outre son impact économique présente également des risques pour la sécurité des personnes. Internet facilite la dispersion mondiale de ces productions, quelle responsabilité pour les e-commerçants ?

“ Cybersécurité, entre frein et support à la créativité et à la performance dans l'entreprise ”

Problématique de l'ouverture de l'entreprise sur le monde, se laisse découvrir et pénétrer au risque de se voir piller ses atouts et savoir-faire. Jusqu'où une entreprise doit-elle s'ouvrir dans la conquête des marchés mondiaux ? Est-il encore judicieux de se protéger (brevets, procédures contentieuses) alors que les progrès techniques rendent les processus caducs très rapidement ? Réflexion et interrogation dans le domaine de la cybersécurité pour éviter de se préparer à la guerre d'hier.

“ Plate-forme de signalement de contenus illicites : vers une plate-forme européenne ”

Présentation de la plus value de ces plates-formes et incitations des états membres de l'Union européenne à adopter cette solution conformément aux conclusions du Conseil prises sous la Présidence Française de l'Union européenne en 2008.

“ E-réputation et Social engineering : nouvel enjeu de société ”

Importance de la veille pour préserver son image contre des atteintes par la rumeur ou la désinformation facilitées par les réseaux sociaux. Perte de frontière entre vie privée et vie professionnelle.

“ Quel profil pour les futurs responsables sécurité des systèmes d'information ”

Recrutement des futurs RSSI : Quels profils ? Quelles compétences ? Quelles formations ?

“ Données sensibles : quelles solutions de stockage sécurisé ? ”

Enjeux et risques de l'externalisation.

“ Haine et intolérance sur le Net : quelle réponse ? ”

Courants extrémistes qui se développent en Europe et les problèmes d'intolérance à l'immigration. Développement de réponses légales ou autres.

“ La cybercriminalité s'intéresse à votre santé ”

Organisation du secteur SSI Santé (initiative d'une certification professionnelle) afin de se préserver contre les atteintes cybercriminelles alors que le monde de la santé effectue sa révolution numérique. La santé publique est un domaine impacté par la cybercriminalité (vente/contrefaçon de médicaments, autodiagnostic médical, escroquerie à l'assurance maladie et sécurité sociale, informations de santé...).

* * * *

Le FIC 2010 est soutenu par le Ministère de l'Intérieur, de l'Outre-mer et des Collectivités Territoriales, la Préfecture de la région Nord-Pas-de-Calais, la Région du Nord-Pas-de-Calais, Lille Métropole Communauté Urbaine et la Ville de Lille.

23 pays sont partenaires de l'événement : Afrique du Sud, Algérie, Belgique, Bulgarie, Canada, Chine, Chypre, Espagne, Estonie, Grande-Bretagne, Hongrie, Irlande, Italie, Japon, Lettonie, Pologne, République Tchèque, Roumanie, Russie, Serbie, Ukraine, USA.

Egalement partenaires, des institutions européennes et internationales : Conseil de l'Europe, OSCE, Commission européenne, Eurojust, Europol.

Pour en savoir plus sur l'événement, et consulter les horaires du programme : www.fic2010.fr

CONTACTS PRESSE & ACCREDITATIONS : AL'X COMMUNICATION

Véronique Loquet

vloquet@alx-communication.com
06 68 42 79 68

Emilie Viel

eviel@alx-communication.com
06 68 54 79 68