KICK-OFF MEETING À MUNICH. 1 JUIN 2014

De droite à gauche :

[1] Nicolas BARRET
[7] Frédérique PLAIN

↘ Chefs de projet Bertin IT

SOURCE :
Blog ECOSSIAN
http:// www.ecossian.eu/blog

ECOSSIAN veille sur les infrastructures critiques européennes

LE PROJET DE R&D EUROPEEN ECOSSIAN VISE LA CREATION D'UN SYSTEME PANEUROPEEN D'ALERTE EN TEMPS REEL ET DE VIGILANCE CYBER POUR AMELIORER LA PROTECTION DES INFRASTRUCTURES CRITIQUES. A L'ISSUE DES 36 MOIS PLANIFIES, UN PROTOTYPE PREFIGURANT LE TOUT PREMIER SOC EUROPEEN DEVRAIT VOIR LE JOUR.

La Protection des Infrastructures Critiques (PIC) en Europe - et dans le monde - est essentielle au maintien du bon fonctionnement social et économique des nations, et notamment de la sécurité et du bien-être des populations.

Comme le souligne le rapport 162 CDS 07[1] de l'Assemblée parlementaire de l'OTAN, "*dans l'environnement de sécurité actuel, les travaux en rapport avec la PIC ne peuvent être menés de manière disparate. De nombreux secteurs critiques - transports, énergie, information et communications - sont de plus en plus mondialisés et interconnectés.*"

SECTEURS D'ACTIVITE D'IMPORTANCE VITALE

- Transports (aérien, ferroviaire, routier, maritime)
- Production & distribution d'Energie
- Installations & services publics, notamment Défense, maintien de l'Ordre et services d'Urgence
- Technologies de l'Information & Communication
- Eau & Alimentation
- Secteur des Soins de Santé
- Institutions Financières

SOURCE : Rapport 162 CDS 07, *op. cit.*

Lancé en 2006 par la Commission Européenne, le **Programme Européen pour la Protection des Infrastructures Critiques** (PEPIC)[2] témoigne de la conscience au plus haut niveau d'une nécessaire coordination entre Etats membres et entre Opérateurs d'Importance Vitale (OIV) pour renforcer la sécurité de ces infrastructures, en particulier celles dont l'arrêt ou la destruction affecterait plusieurs Etats.

Le réseau d'alerte CIWIN - "Critical Infrastructure Warning Information Network", constitue l'une des premières mesures collaboratives mises en œuvre dans le cadre de ce Programme : depuis janvier 2013, un portail numérique permet aux acteurs européens de la PIC d'échanger de l'information sur les vulnérabilités et menaces, ainsi que sur les bonnes pratiques en matière de protection des infrastructures critiques.

Démarré le 1er juin 2014, **ECOSSIAN - "European COntrol System Security Incident Analysis Network"** s'inscrit dans la continuité de cette démarche. Il contribue également à l'Initiative mondiale sur la cybersécurité des Systèmes de Contrôle Industriels et des réseaux intelligents.

MISSION ? Améliorer la détection et la gestion des incidents de sécurité et des cyberattaques touchant les infrastructures critiques.

COMMENT ? Par la mise en place d'un système paneuropéen d'alerte en temps réel et de vigilance cyber doté d'installations de commande et de contrôle.

C'est donc **le prototype du tout premier SOC (Security Operation Centre) communautaire** capable de centraliser les informations provenant des différents centres au sein de l'UE qui devrait voir le jour au terme des 36 mois du projet.

AVEC QUI ? Le projet FP7 ECOSSIAN mobilise une vingtaine d'acteurs privés et publics aux expertises complémentaires. Le consortium est en effet composé d'entreprises spécialistes de la cybersécurité (Bertin IT, Airbus, Espion, …), d'OIV (réseaux ferrés portugais, fournisseur d'eau et de gaz irlandais, …), d'autorités (police judiciaire portugaise), d'universités (Louvain, Bologne) et d'instituts de recherche (Fraunhofer, AIT, …).

RÔLEDEBERTINIT

Leader sur la définition de l'architecture d'ECOSSIAN et de ses fonctions de sécurité, Bertin IT apporte aussi son expertise sur la gestion des échanges de données entre environnements informatiques et domaines de sensibilités différentes.

Fin février, Bertin IT a livré le premier document décrivant l'architecture globale d'ECOSSIAN et a entamé depuis les spécifications détaillées qui seront fournies fin 2015.

Bertin IT travaille également à l'expérimentation des passerelles sécurisées qui permettront d'interconnecter les systèmes et de garantir la sécurité et l'anonymat des échanges entre les infrastructures et les SOC nationaux ou européens.

Les développements du framework de ces passerelles ont été amorcés et se poursuivront sur 2016.

LA PROTECTION DES INFRASTRUCTURES CRITIQUES EUROPEENNES

▪ 2006

Texte fondateur initié dès 2004, le **Programme Européen pour la Protection des Infrastructures Critiques** (PEPIC) est lancé en 2006. Il énonce les grands principes d'une PIC européenne. Parmi eux :

- la **subsidiarité** : bien qu'elle concentre son action sur les IC européennes (ICE)[a], la Commission peut apporter son soutien aux IC nationales, à la demande des Etats membres
- la **confidentialité** des informations avec une diffusion limitée au *besoin d'en connaître*
- la **coopération** de tous les acteurs concernés : Opérateurs d'Importance Vitale (OIV), pouvoirs publics et autres instances compétentes
- une **approche sectorielle**, tenant compte des expériences, expertises et exigences particulières à une IC selon son secteur

Le PEPIC prévoit différentes mesures , dont la création du réseau d'alerte **CIWIN** - *Critical Infrastructure Warning Information Network.*

▪ 2008

Egalement inscrite au PEPIC, la **directive 2008/114/CE**[3] établit un processus européen de recensement et de désignation des ICE. Elle se concentre alors sur les Transports et l'Energie.

En juin 2012[4], le Parlement européen envisagera qu'elle s'étende aux TIC, aux services financiers, à la santé, à l'approvisionnement en eau et en nourriture, à la recherche et l'industrie nucléaires.

a- Les infrastructures critiques dites 'européennes' (ICE) sont celles dont l'arrêt ou la destruction aurait un impact sur plusieurs Etats membres.

▪ 2009

Le plan d'action pour la **Protection des Infrastructures d'Information Critiques (PIIC)**[5] vise à "protéger l'Europe des cyberattaques et des perturbations de grande envergure" en améliorant l'état de préparation, la sécurité et la résilience des Etats membres.

Le rôle de l'ENISA[b] - Agence Européenne chargée de la sécurité des réseaux et de l'information, y est central.

Parmi les principales réalisations de ce plan, on notera :

- la définition d'une **base minimale de capacités et services que les CERT** - "Computer Emergency Response Team" (équipes d'intervention en cas d'urgence informatique) des Etats membres doivent posséder pour soutenir efficacement la coopération paneuropéenne ;
- le lancement d'un **partenariat public-privé** européen pour la résilience (EP3R) et la création du **Forum européen** des Etats membres ;
- la réalisation d'**exercices paneuropéens** portant sur des incidents de grande envergure affectant la sécurité des réseaux (Cyber Europe 2010, 2012, 2014).

La nécessité d'une approche coopérative de la PIIC se verra réaffirmée en 2011 à travers une seconde Communication - **"Réalisations et prochaines étapes : vers une cybersécurité mondiale"**[6]. Celle-ci se verra elle-même largement approuvée par la résolution du Parlement du 12 juin 2012.

b- Créée en 2004, l'ENISA - "European Network and Information Security Agency" a pour mission de sécuriser à un niveau élevé la société de l'Information en Europe et de favoriser l'émergence d'une culture dans ce domaine. Elle soutient activement la coopération entre les CERT à travers l'Europe.

▪ 2010

Le chapitre 'Confiance & Sécurité' de la **Stratégie Numérique pour l'UE**[7] définit des actions pour une réponse européenne coordonnée face aux cyberattaques. Certaines se sont concrétisées :

- [2011] avec la mise en place d'un **CERT européen** (CERT-EU) permanent, chargé de prévenir les attaques sur les réseaux et systèmes des institutions de l'UE, et de proposer une réponse en cas d'urgence.
- [2013] et l'installation d'un **Centre européen de lutte contre la Cybercriminalité** dans les locaux d'Europol pour faciliter le partage entre États d'informations liées à la cybercriminalité.

▪ 2013

La **Stratégie de Cybersécurité pour l'UE**[8] expose cinq priorités, dont celles d'élaborer une politique et des moyens de cyberdéfense relevant de la politique de sécurité et de défense commune (PSDC) et de développer les ressources industrielles et technologiques nécessaires à la cybersécurité.

Elle s'accompagne d'un projet de **directive sur la Sécurité des Réseaux et de l'Information (SRI)**[9]. Suivant ce projet (tel que revu par le Parlement en mars 2014), **les OIV** de secteurs tels que les services financiers, les transports, l'énergie et la santé se verraient obligés d'adopter des pratiques de gestion des risques et de **signaler les principaux incidents de cybersécurité** à l'autorité nationale compétente.

La même année, la **directive 2013/40/UE**[10] **relative à la cybercriminalité dans l'UE** vise à soutenir la sécurité des informations par le biais de législations nationales renforcées, de sanctions pénales plus sévères et d'une meilleure coopération entre les autorités compétentes.

RÉFÉRENCES

[1] Rapport 162 CDS 07 de l'Assemblée parlementaire de l'OTAN
http://www.nato-pa.int/

L'ensemble des textes européens sont consultables sur http://eur-lex.europa.eu/

[2] Programme européen de protection des infrastructures critiques
celex:52006DC0786

[3] Directive relative au recensement et à la désignation des infrastructures critiques européennes
celex:32008L0114

[4] Résolution du Parlement européen du 12 juin 2012 sur la PIIC
CELEX:52012IP0237

[5] PIIC // Protéger l'Europe des cyberattaques et des perturbations de grande envergure (…)
celex:52009DC0149

[6] PIIC // Réalisations et prochaines étapes: vers une cybersécurité mondiale
celex:52011DC0163

[7] Une stratégie numérique pour l'Europe
celex:52010DC0245
Voir aussi : http://ec.europa.eu/digital-agenda/

[8] Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé
celex:52013JC0001

[9] Proposition de directive pour un niveau élevé commun de SRI dans l'UE
celex:52013AE1414

[10] Directive relative aux attaques contre les systèmes d'information
celex:32013L0040

LIEN UTILES // en savoir +

Site de l'ENISA
http://www.ecossian.eu

Site du projet ECOSSIAN
http://www.ecossian.eu

