

# **Vers une Stratégie Belge pour la Sécurité de l'Information**

Par des associations privées et le monde académique

Septembre 2008

## Organisations signataires



### Rédacteurs de ce document:

Jean-Luc Allard	Vice-président Information Security, ISACA Belgium, ISO/IEC JTC1 SC27 Belgian Shadow Committee (coordinateur wg3)
Georges Ataya	VP international ISACA et ITGI, Professeur à la Solvay Business School
Gautier Dallons	Coordinateur de l'équipe Sécurité et chef de projet R&D, CETIC
Alain De Greve	ISO/IEC JTC1 SC27 Belgian Shadow Committee (coordinateur wg1/wg4 – série 2700x)
Marijke De Soete	Vice-présidente ISO/IEC JTC1 SC27, Membre du Conseil d'Administration de LSEC
Bart Moerman	President, ISSA Brussels European Chapter
Bart Preneel	Professeur K.U. Leuven, ESAT/COSIC, Président du Conseil d'Administration de LSEC, ISO/IEC JTC1 SC27 Belgian Shadow Committee (wg2)
Ulrich Seldeslachts	CEO LSEC
Thierry Villers	Directeur, INFOPOLE Cluster TIC

### Ont revu et commenté ce document:

Dany Van de Ven, Général de Brigade e.r., Agoria/BSDI

...

# Vers une Stratégie Belge pour la Sécurité de l'Information

Version 2

## Introduction

Ce livre blanc a pour origine le besoin identifié par nos organisations constituantes (toutes sans but lucratif) directement impliquées dans le domaine de la sécurité de l'information dans tous les domaines économiques. Ce besoin concerne la promotion, la sensibilisation et l'amélioration de la coordination des initiatives dans ce domaine...

Les organisations signataires de ce document sont:

- CETIC
- Les experts belges impliqués dans les activités de l'ISO/IEC JTC1 SC27, un comité international de standardisation des techniques de sécurité de l'information, y compris les aspects de Management de la Sécurité de l'Information (ISMS)
- INFOPOLE Cluster TIC
- Le Chapitre belge de l'ISACA
- Le chapitre Brussels-European de l'ISSA
- K.U.Leuven, ESAT/COSIC
- LSEC (Leaders in Security)
- Solvay Business School

Ces organisations représentent plus de 3000 professionnels de la sécurité de l'information dans plus de 500 organisations privées, publiques et de recherche.

Les organisations signataires ont rencontré, dans leurs activités quotidiennes, un nombre de problèmes et d'insuffisances dans la structure, la réglementation, l'éducation ainsi que dans la communication des menaces dans le domaine de la sécurité de l'information dans notre pays. Sur la base leurs nombreux contacts professionnels et de leurs réseaux, ils ne peuvent que constater que la Belgique est en retard sur la plupart des autres pays européens et, pour certains aspects, encore moins développé que certains pays de l'est européen. Cette situation n'est pourtant pas due à une absence de connaissance et d'expertise puisque nos experts nationaux sont reconnus dans le monde entier.

Les initiatives gouvernementales et parlementaires actuelles, comme celle de la Commission de la Chambre de l'infrastructure/ et du Comité Ministériel du Renseignement et de la Sécurité (dont émane le BeNIS) montre une reconnaissance du besoin par les administrations fédérales (et régionales).

Les signataires ont identifié jusqu'à présent, six objectifs stratégiques qui sont présentés dans la suite de ce document et qu'ils considèrent comme extrêmement pertinentes pour la Belgique.

## Antécédents

Notre société est extrêmement dépendante des informations et des processus informationnels. Ils exigent, tous les deux, un niveau de qualité prédéfini pour atteindre leurs objectifs. La Sécurité de l'Information a pour mission d'assurer que ce niveau de qualité ne soit pas mis en danger par des risques inacceptables. Les Technologies de l'Information et de la Communication (TIC) sont aujourd'hui le support incontournable de ces processus informationnels et devraient les rendre plus fiables et efficaces. La Sécurité de l'Information détermine les objectifs à atteindre tandis que la réponse précise dépend des domaines spécifiques ou technologiques dans lesquels ces objectifs doivent être atteints.

Les systèmes TIC deviennent de plus en plus envahissants dans notre société: chaque citoyen et organisation voient leur dépendance aux services et applications TIC croître. Ceci a un impact sur tous les acteurs économiques, y compris les administrations publiques et les infrastructures critiques (par exemple l'énergie, le transport, la santé et les télécommunications). Dans ce nouvel environnement émergent sans cesse de nouvelles menaces : des attaques à grande échelle peuvent être lancées de partout dans le monde pour atteindre ces systèmes TIC. Nous entendons parler de diverses attaques à la fois contre les individus (p.ex. les virus et les spam) et des cas plus globaux : attaques par Déni de Service (*Denial Of Service* [DOS] (par exemple contre l'Estonie en 2007 [1]), espionnage économique et industriel (par exemple les accusations selon lesquelles la Chine chercherait à pénétrer les systèmes nationaux des pays de l'Union Européenne [2]) et la fraude (p.ex. dans le secteur bancaire [3]).

Des investissements substantiels dans la recherche, le développement, le déploiement et l'audit ont été réalisés au cours des vingt dernières années; il en résulte une amélioration de la protection contre certaines de ces menaces mais, malheureusement, de nombreux incidents montrent que la sécurité plus générale de l'information n'est pas réellement accrue. Plusieurs éléments influencent cette tendance :

- 1) Nos systèmes d'information évoluent rapidement et deviennent plus complexes (nous interconnectons les ordinateurs constitués de centaines de millions de petits composants dans des réseaux de centaines de millions d'ordinateurs); et l'homme n'excelle pas à gérer et à sécuriser les systèmes complexes qui présentent beaucoup de modes de défaillances;
- 2) Comme de plus en plus d'applications fonctionnent 'en ligne', les enjeux financiers stimulent des comportements criminels en ligne qui ne cessent de s'accroître; il est également important de noter que, dans cet environnement, nous ne pouvons pas être suffisamment informés des problèmes car les criminels agissant pour des motifs financiers n'ont pas intérêt à rendre leurs exploits publics ;
- 3) La sécurité de l'information est hautement interdisciplinaire. Développer des solutions exige une approche managériale intégrée qui combine technologie et réglementation interne et externe à l'organisation). L'étude des facteurs humains et économiques joue également un rôle important. Un progrès ne sera possible que s'il se base sur une collaboration étroite entre le gouvernement, les entreprises et les instituts de recherche.

Le développement et le déploiement de systèmes TIC sécurisés exigent le développement de normes, l'évaluation de produits et de systèmes, ainsi qu'une coordination et une mise en vigueur globale. Beaucoup de ces questions nécessitent un traitement au niveau

international. Cependant, il est également que les gouvernements nationaux ont une responsabilité essentielle. A cet égard, il est à noter que la Belgique ne dispose pas d'une Agence de sécurité de l'information émettant des recommandations et soutenant les administrations, les institutions et les organisations, à tous niveaux, contrairement à tous les pays qui nous entourent, y compris la plupart des pays d'Europe de l'est [voir Annexe A]. Ceci signifie que les actions concrètes dans ce domaine ne sont ni cohérentes, ni compatibles, ni efficaces.

Il n'y a pas non plus de schéma belge de certification de produits et services de sécurité, par exemple basé sur les Critères Communs, comme c'est le cas dans tous les pays voisins et d'autres comme le Grèce, la Pologne et la Hongrie [Voir Annexe B]. Cela induit que, très souvent, l'industrie belge ne peut pas participer à des appels d'offre internationaux, et que, si nous voulons tout de même y participer, notre savoir-faire national fuit vers d'autres pays. Ceci est la cause de pertes d'emploi ou de délocalisations.

## Objectifs stratégiques

### 1. Un Forum de Sensibilisation à la Sécurité de l'information

Afin d'améliorer la sensibilisation et fertilisation croisée (*cross-fertilization*), un Forum belge sur la sécurité de l'information devrait être créé. Ce Forum devrait permettre l'échange d'information sur les initiatives, les normes relatives à la Sécurité de l'Information ainsi que les expériences de mises en œuvre et de certification, incluant le management de la sécurité de l'information, le management des risques, les techniques de sécurisation des informations et des TIC. Il devrait également servir comme plateforme de communication effective et opérationnelle pour toutes les initiatives émanant du gouvernement fédéral et de ses organes tels que la police fédérale ou des institutions européennes telles que l'ENISA [4].

Idéalement, ce Forum devrait se baser sur une coopération avec les organisations spécialisées en sécurité de l'information, telles que les organisations signataires, et le gouvernement, l'industrie, les services, l'éducation et la recherche.

De plus, la création d'un groupe de réflexion (*think tank*) national sur la sécurité de l'information, qui aurait une fonction d'avis vis-à-vis de l'Agence belge de sécurité de l'information dont il sera question plus loin est recommandé. Il devrait être lié au Forum mentionné ci-dessus.

Le Forum sur la Sécurité de l'Information pourrait également créer des WARPs (Warning, Advise and Reporting) en sécurité de l'information à l'exemple de ce qui est fait au Royaume-Uni [5] et aux Pays-Bas [6].

### 2. Standardisation en Sécurité de l'Information

Des exigences minimales de sécurité de l'information et des TIC, basées sur des normes internationales [voir Annexe C] devraient être édictées et totalement intégrées dans les nombreuses réglementations des secteurs industriels. Elles devraient inclure des sujets comme le management de la sécurité de l'information et des structures, le management des risques, la gestion des incidents, la continuité des activités, l'évaluation et l'audit, le *reporting* et la conformité, etc..... Les exigences devraient également mentionner le besoin d'homologation des systèmes critiques. Dans ce domaine, l'Administration pourrait montrer l'exemple à l'industrie et aux organisations privées où l'homologation ne fait pas partie de la mise en œuvre des solutions de sécurité.

Nombre de normes relatives à la sécurité de l'information permettent l'évaluation et la certification. Aujourd'hui, les fabricants et les organisations belges doivent aller à l'étranger pour faire certifier les produits et services de sécurité de l'information. Face au professionnalisme croissant du secteur et l'émergence d'une demande pour des produits et services certifiés, la Belgique devrait créer son propre cadre de certification de la sécurité de l'information, basé sur les normes internationales et conforme aux lois et réglementations. A cet égard, l'organe belge BELAC devra accréditer les organismes de certification et d'évaluation chargés d'évaluer la conformité des produits et services la sécurité de l'information requise ainsi que les centres d'évaluation. Cette autorité gouvernementale de certification de la sécurité de l'information serait alors en mesure de

produire les certificats des produits et services. L'initiative déjà démarrée dans ce domaine devrait continuer à recevoir le soutien nécessaire à l'atteinte de ses objectifs.

L'organe accrédité de certification de la sécurité de l'information devra établir une collaboration avec les autres organes de certification nationaux existant au sein de l'Union Européenne au travers du Common Criteria Recognition Agreement [7]. Le but est la création d'un cadre harmonieux de certification avec les autres états membres pour la transposition de normes à mettre en vigueur dans le programme de certification national au départ des directives européennes. Sur une plus grande échelle (mondiale) cet organe doit établir le cadre de la reconnaissance croisée avec les organismes pairs.

Une meilleure coordination est nécessaire pour soutenir pour les efforts belges dans le cadre de la normalisation internationale relative à la sécurité de l'information. Bien que de l'excellent travail soit réalisé par les experts belges dans ces forums, il n'y a pas de soutien ni de reconnaissance de la part de l'organe national belge de normalisation (lisez NBN). Ce rôle de coordination pourrait, par exemple, être rempli par Agoria, point de contact unique pour le secteur des TIC (en tant qu'opérateur sectoriel). Ces activités coordonnées devraient être supervisées par le Ministère des Affaires Economiques et par le département de la Politique Scientifique.

### **3. Education, formation et recherche**

Il existe un besoin urgent de coordonner les initiatives liées à l'éducation à la formation et à la recherche en sécurité de l'information. Plusieurs groupements d'universités et d'écoles supérieures en Belgique organisent leurs propres programmes avec des contenus différents. La définition et la promotion d'une base commune seraient un minimum.

Une plateforme de recherche en sécurité de l'information devrait être créée et promue (voir les exemples aux Pays-Bas [8] et en France [9]). Elle devrait prendre en considération les livrables des objectifs stratégiques définis dans ce livre blanc.

### **4. Infrastructures Critiques & CERT**

Un plan et un calendrier pour la protection de nos infrastructures critiques devraient être développé en coopération avec l'industrie et les autres pays européens, aligné sur le cadre européen actuellement en cours de préparation au sein d'un Programme Européen dédié. Ces infrastructures comprennent, en plus de l'énergie, des transports et de la santé – qui ont reçu la priorité en Europe – les finances, l'approvisionnement alimentaire, l'eau, les matières dangereuses, les télécommunications et le gouvernement [10].

Ce calendrier devrait également tenir compte du développement prévu de normes ISO ISMS spécifiquement dédiées aux aspects de sécurité de l'information des infrastructures critiques.

Le gouvernement belge devrait rédiger d'urgence un plan de crise limité qui sera développé ultérieurement sur base de scénarios plus larges et l'implication de l'industrie.

Un CERT belge (Computer Emergency Response Team) [11] et [12] doit être créé à brève échéance. Sa mission devrait être de protéger l'infrastructure Internet belge et de coordonner la protection et la réponse face aux attaques informatiques dans le pays. Cette évolution doit se faire en concertation étroite avec l'industrie et s'appuyer sur son expertise. Etablir une collaboration avec BELNET, s'inspirer des initiatives dans plusieurs secteurs (p.ex. financier), coordonné avec l'ECSA ([www.ecsa-eu.org](http://www.ecsa-eu.org)) et la CFS-CSF ([www.csf-cfs.be](http://www.csf-cfs.be)) sont des actions fortement recommandées dans ce domaine. Enfin, la loi relative aux communications électroniques (Loi du 13 Juin 2005, Art 113 et 114) est peu claire quant au rôle de l'IBPT/BIPT concernant le CERT national. Elle laisse à tout le moins place à l'interprétation, et entraîne dès lors l'inaction.

## **5. Lois & réglementation**

Plusieurs lois belges relatives aux TIC et à la sécurité de l'information (p.ex. loi sur le cryptographie, loi sur la criminalité informatique, etc.) ont besoin d'être réévaluées. Au minimum, les lois sur la criminalité informatique et la protection de la vie privée devraient être révisées afin de clarifier les buts ambigus et éviter les interprétations. Par exemple ; les sociétés offrant des services de tests de vulnérabilité des réseaux pourraient exiger un statut spécial. Le rôle des experts judiciaires dans les affaires de sécurité de l'information devrait également être mieux précisé et leur apport défini.

Une réglementation détaillée au en regard des aspects de protection de la vie privée [13]: liés aux nouvelles technologies - comme l'identité électronique, les technologies de localisation des citoyens et la biométrie - devient urgente et devrait être traitée de manière appropriée par le gouvernement. On peut en effet s'interroger sur la manière dont les organisations peuvent réellement et concrètement se conformer à la loi dans ce domaine. Cette difficulté souvent due à une terminologie et à des exigences trop vagues.

Une coordination adéquate ainsi qu'une coopération entre l'organe belge de sécurité de l'information et la Commission de Protection de la Vie Privée et indispensable. L'organe de sécurité de l'information proposé ci-dessous conseiller le gouvernement belge dans l'établissement et l'évolution du cadre légal. Les lois qui en résulteront devraient être cohérentes avec les lois et réglementations *nationales et internationales* en matière de sécurité de l'information et devraient prendre en considération la grande expertise belge en sécurité de l'information présente en Belgique.

Les objectifs énumérés ci-dessus ne seront vraiment coordonnés et efficaces que lorsqu'une stratégie centralisée et contrôlée sera établie. Ceci requiert la définition d'un sixième objectif.

## **6. Agence Belge de Sécurité de l'Information**

Une Agence gouvernementale belge de sécurité de l'information devait être fondé (en analogie avec, par exemple le BSI en Allemagne). Cette Agence aura pour charge de déterminer la politique et la stratégie concernant la sécurité de l'information en Belgique, en coopération étroite avec l'industrie et les autres départements gouvernementaux. Elle

devrait ensuite définir les normes auxquels les gouvernements, l'Administration et leurs fournisseurs (de service) devraient souscrire en matière de sécurité de l'information. La création de cette Agence pourrait s'appuyer sur l'expertise de l'IBPT/BIPT ou de tout autre agence fédérale. Mais elle nécessite clairement la création d'un comité indépendant impliquant des experts belges de la sécurité de l'information (à la fois de l'industrie et de la recherche) et inspiré éventuellement des expériences dans les pays voisins et de l'ENISA si nécessaire. La stratégie devrait être alignée sur la structure européenne et avoir des liens directs avec les organes européens comme l'ENISA ou les agences nationales des autres pays Européens.

Cette Agence devrait être créé par le gouvernement fédéral indépendamment des entités publiques concernées (IBPT.BIPT, ANS/NVP, etc.) mais associée à celles-ci. Il rassemblera toutes les entités pertinentes au sein de l'Administration (fédéral, communautés et régions) afin de définir, avec l'industrie, une stratégie pour la Sécurité de l'Information tout en déterminant les directions futures pour les services gouvernementaux, l'Etat fédéral et les régions.

Cette Agence devrait également assurer la coordination avec les différents organes belges responsables de la recherche en matière de sécurité de l'information.

Cette Agence devrait enfin coordonner la représentation belge dans les groupes internationaux dans lesquels notre intérêt national exige notre présence

Les organisations signataires de ce livre blanc sont disposées, dès à présent, à former le comité indépendant d'experts en sécurité de l'information proposé ci-dessus, jusqu'à ce qu'il soit officiellement institué.

## **Conclusion**

Les organisations signataires en appellent au gouvernement belge afin que les actions urgentes soient entreprises par les parties prenantes intéressées afin d'atteindre les objectifs stratégiques mentionnés ci-dessus.

Les organisations signataires sont prêtes à s'impliquer et à assumer leurs responsabilités afin d'amener la Sécurité de l'Information en Belgique à un niveau adéquat.

Plus d'informations concernant ce document et l'initiative peuvent être obtenues auprès des représentants des organisations signataires : Jean-Luc Allard (ISACA) et Bart Moerman (ISSA).

## Références:

- CAWET Werkgroep 55: Beveiliging van Digitale Informatie, 26 oktober 2007, <http://www.kvab.be/downloads/CAWET/beveiliging%20van%20digitale%20informatie.pdf>
- “Pour une politique nationale de sécurité de l’information”, *Livre Blanc* élaboré par la plateforme de concertation sur la sécurité de l’information (BeNIS)“
- DOC 52 0898/001, Chambre 2e Session de la 52e Législature - Kamer 2de Zitting van de 52de Zittingperiode 2008 2007, Commission de l’Infrastructure, des communications et des entreprises publiques, par Monsieur Heer Roel Deseyn.

### Antécédents

#### [1] Cas d’attaques: Estonie

- Assessing the Cyber Security Threat (SDA Monthly Roundtable), A Security & Defence Agenda Rapporteur: John Chapman, Year of publication: 2008, Bibliothèque Solvay, Brussels

#### [2] Cas d’attaques: China (présumée)

- Belgische Kamer van Volksvertegenwoordigers – Chambre des Représentants de Belgique
  - CRIV 52 PLEN 035 – Plenumvergadering/Séance plénière donderdag/jeudi 08-05-2008 (pm)
- CRABV 52 COM 209 – Commissie voor Landsverdediging/Commission de la Défense Nationale woensdag mercredi 14-05-2008 (avond/soir)

#### [3] Money mules dans le secteur bancaire :

[http://www.ecp.nl/nieuws/id=101482/Banken\\_pakken\\_money\\_mules\\_aan\\_met\\_start\\_campagne.html](http://www.ecp.nl/nieuws/id=101482/Banken_pakken_money_mules_aan_met_start_campagne.html)

### Forum de Sensibilisation à la Sécurité de l’Information

#### [4] Référence ENISA sur la Sensibilisation à la Sécurité de l’Information:

[www.enisa.europa.eu/pages/ENISA\\_Working\\_Group\\_on\\_Awareness\\_Raising.htm](http://www.enisa.europa.eu/pages/ENISA_Working_Group_on_Awareness_Raising.htm)

#### [5] WARP au Royaume Uni : [www.warp.gov.uk](http://www.warp.gov.uk)

#### [6] WARP aux Pays-Bas: [www.onderwijswarp.nl](http://www.onderwijswarp.nl), [www.ictu.nl](http://www.ictu.nl) (NICC) et [www.samentagencybercrime.nl](http://www.samentagencybercrime.nl)

### Standardisation en Sécurité de l’Information

#### [7] Pour le CCRA - <http://www.commoncriteriaportal.org/members.html>

### Education et recherche

#### [8] Exemples aux Pays-Bas: Veilig Verbonden:

[http://www.ictregie.nl/iip/pdf\\_pagina.php?pageId=34](http://www.ictregie.nl/iip/pdf_pagina.php?pageId=34)

#### [9] Exemples en France: ANR programme Sécurité et Sûreté Informatique

### Infrastructure Critique, CERT, CSIRT

#### [10] Infrastructures Critiques: <http://europa.eu/scadplus/leg/en/lvb/l33259.htm>

#### [11] Pour une vision complète des CERT en Europe :

[http://www.enisa.europa.eu/cert\\_inventory/index\\_inventory.htm](http://www.enisa.europa.eu/cert_inventory/index_inventory.htm)

#### [12] “Successful cyber defense requires a coordinated national approach” by Miguel De Bruycker, Belgian Defense, Computer Incident Response Capability & Urs E. Gattiker, CyTRAP Labs, (<http://papers.weburb.dk/frame.php?loc=archive/00000149/>)

### Lois & Règlements

#### [13] Recommandations sur les aspects de protection de la Vie Privée (Privacy):

- [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/lawreport/walrave\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/walrave_en.pdf)
- [http://www.enisa.europa.eu/doc/pdf/Country\\_Pages/Belgium.pdf](http://www.enisa.europa.eu/doc/pdf/Country_Pages/Belgium.pdf)

## Annexe A

### Liste des Organes de Sécurité de l'Information en Europe

Certains de ces Organes sont intégrés à l'Autorité Nationale de Sécurité, d'autres pas.

Espagne	CNI	<a href="http://www.cni.es">http://www.cni.es</a>
Italie	AISE	
Royaume Uni	CESG	<a href="http://www.cesg.gov.uk/">http://www.cesg.gov.uk/</a>
France	DCSSI	<a href="http://www.ssi.gouv.fr">http://www.ssi.gouv.fr</a>
Pays-Bas	MIVB	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Allemagne	BSI	<a href="http://www.bsi.bund.de">http://www.bsi.bund.de</a>
Estonie	Information Board	....
Pologne	ABW	<a href="http://www.abw.gov.pl">http://www.abw.gov.pl</a>
Roumanie	ORNISS	<a href="http://www.orniss.ro">http://www.orniss.ro</a>
Suède	Utrikesdepartementet SSSB	...

## **Annexe B**

### **Listes des pays membres du CCRA (Common Criteria Recognition Agreement)**

#### Europe:

Suède, Espagne, Norvège, Pays-Bas, Italie, Hongrie, Grèce, Allemagne, France, Danemark, Tchéquie, Autriche, Royaume-Uni, Finlande

#### World:

Etats Unis d'Amérique, Turquie, Singapour, Malaisie, Corée (Sud), Japon, Israël, Inde, Canada, Australie/Nouvelle Zélande (ensemble).

## Annexe C

### Liste de normes potentielles à promouvoir au sein de l'Administration belge

#### ISO

- la série ISO/IEC 2700x (e.g. 27001 'ISMS requirements' et 27002 'ISMS Good Practices') et série ISO 2701X (mise en œuvre spécifique de la norme ISO 27002, p.ex. Opérateurs de Télécommunication, Infrastructures critiques)
- ISO/IEC 15408 (Common Criteria for security evaluation) et normes liées
- ISO/IEC 21827 (System Security Engineering – Capability Maturity Model)

#### ISF

- Standard of Good Practice for Information Security

#### ISACA

- CobIT 4.1

#### ENISA

- [http://www.enisa.europa.eu/rmra/files/D1\\_Inventory\\_of\\_Methods\\_Risk\\_Management\\_Final.pdf](http://www.enisa.europa.eu/rmra/files/D1_Inventory_of_Methods_Risk_Management_Final.pdf)

Et de nombreuses autres éditées par les organes nationaux (Annexe A) ou les instituts nationaux de normalisation (comme le NIST aux Etats Unis :).

NIST SP 800 : <http://csrc.nist.gov/publications/PubsSPs.html>

NIST FIPS : <http://csrc.nist.gov/publications/PubsFIPS.html>

## Qui sommes-nous ?

- Le CETIC, (Centre d'Excellence en Technologies de l'Information et de la Communication) est actif en recherche appliquée pour le développement d'applications, les technologies GRID et les systèmes électroniques. Le CETIC est un agent de communication qui a pour but le transfert de technologie entre la recherche universitaire et les industries.
- Le chapitre belge de l'ISACA, une organisation professionnelle internationale destinée à soutenir les professionnels de la gouvernance des TIC par la recherche et l'éducation en Assurance et d'audit des TIC, -en gouvernance des TIC et en Management de la sécurité de l'information. L'ISACA certifie des Managers de la sécurité de l'information [CISM] plus de 8000 professionnels certifiés dans le monde et 40 en Belgique) et est active en Belgique depuis 1986. Des documents majeurs sont régulièrement publiés et distribués gratuitement afin d'améliorer la sensibilisation à la sécurité de l'information et la gouvernance appropriée.
- Le chapitre "Brussels-European" de l'ISSA, une organisation professionnelle internationale qui supporte les professionnels de la sécurité des systèmes d'information en mettant à disposition une plateforme d'éducation, de sensibilisation et de formation professionnelles continues
- LSEC (Leaders in Security), une asbl belge, association de l'industrie de la sécurité de l'information dont les membres sont issus des instituts de recherche, des professionnels individuels et une large gamme d'entreprises.
- INFOPOLE Cluster TIC, le réseau wallon des professionnels des TIC (entreprises, universités, centres de recherche,...) dont un certain nombre sont actifs dans le domaine de la sécurité de l'information.
- K.U.Leuven, ESAT/COSIC, active dans de nombreux domaines de sécurité des TIC, organise un programme de 'post-graduat' en sécurité de l'information.
- Solvay Business School, réalise le lien entre la technologie de l'information et le monde des affaires. SBS organise des Masters ou programmes de post-graduats en IT Governance et IT Audit and Security
- Le Groupe d'Experts belges impliqués auprès de ISO/IEC JTC1 SC27, un Comité International de Standardisation dédié aux techniques de sécurité de l'information et traitant du 'Système de Management de la Sécurité de l'Information [ISMS] (WG1), les systèmes cryptographiques (WG2), l'évaluation, la certification et l'assurance (WG3), les technologies de la sécurité (WG4) et le management de la Privacy et des Access (WG5).