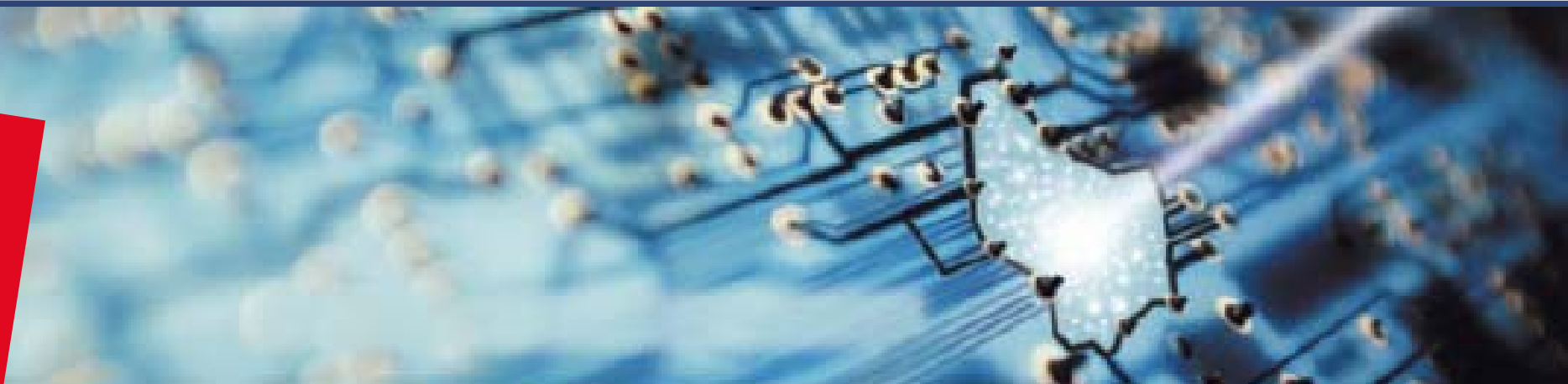




LE GOUVERNEMENT
du Grand-Duché de Luxembourg



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie
et du Commerce extérieur



LE GOUVERNEMENT
du Grand-Duché de Luxembourg

www.CASES.lu

(Cyberworld Awareness and Security Enhancement Structure)

CASES – une initiative luxembourgeoise pour
réduire la fracture numérique dans le domaine de
la sécurité de l'information

Internet Security Day - 26.03.2007



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie
et du Commerce extérieur

Agenda



1. Introduction
2. La stratégie nationale
3. CASES : L'approche
4. CASES+ (au-delà de CASES)
 - 4.1. CNLSI (ANSIL)
 - 4.2. Honey-nets/malware ...
5. LuCSIRT



La situation actuelle au Luxembourg

- Les TIC offrent de nombreuses opportunités pour les secteurs public et privé
- Les PME investissent dans les TIC, mais pas dans le B2C
 - Intensif en ressources
 - Manque de savoir-faire
 - Crainte des risques
- Les citoyens adoptent principalement les TIC pour des besoins récréatifs
 - Manque de confiance
 - Bas niveau de savoir-faire

La situation actuelle au Luxembourg

- Nous observons que:
 - Les PME et les citoyens n'utilisent les TIC qu'en interne
 - Le commerce électronique ne se développe pas autant que prévu
 - Les services en ligne ne sont pas autant employés que prévu
 - Le ROI est souvent mauvais dans le commerce électronique
 - La fracture numérique liée à la sécurité s'accroît rapidement
- Cependant, nous constatons:
 - De très haut taux de connexion, et donc, d'exposition
 - Un très bas niveau de savoir-faire, même pour le plus rudimentaire
 - De nombreux incidents liés à la sécurité
 - Les réactions imprévisibles des PME et des citoyens – pas de culture commune de la sécurité

La situation dans le monde

- Nous observons que:
 - Convergence des technologies et donc des vulnérabilités
 - Professionnalisation des menaces
 - Les attaquants travaillent de plus en plus en réseau
 - Cibles ne sont plus seulement les « grands »
 - Croissance forte du nombre de Vulnérabilités critiques (130 MS)
 - Croissance forte du nombre de 0-day exploits (entre 21 et 48 MS)
 - Croissance forte des zombies (bots avec capacités Rootkit)

Nous observons que les mêmes techniques d'attaque fonctionnent depuis 25 ans.

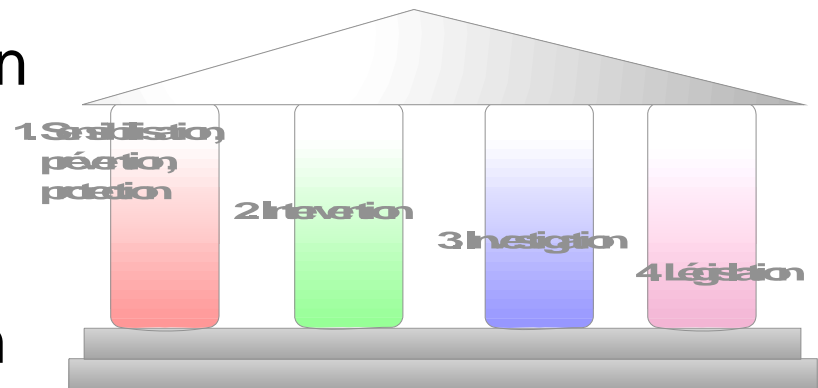
La stratégie nationale - sensibilisation

- Nos objectifs:
 - Augmenter le savoir-faire
 - Responsabiliser les PME et les citoyens
 - Renforcer la confiance
 - Mettre en place une culture de la sécurité pour changer les réactions imprévisibles des PME et des citoyens en des actions réfléchies et responsables
 - Favoriser la coopération et coordonner les plans d'action des différents partenaires impliqués afin de les maintenir en ligne avec la stratégie nationale.

La stratégie nationale

La stratégie est basée sur quatre piliers:

1. Sensibilisation et prévention
2. Réaction sur incidents
3. Investigation et répression
4. Législation et normalisation

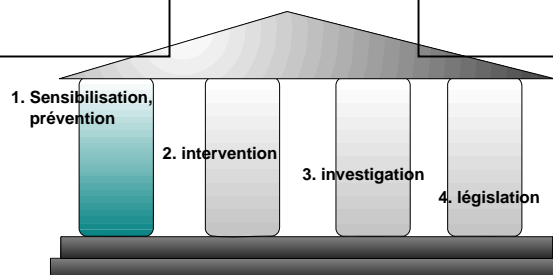


Structures permanentes

- CASES
- LuxTrust
- Organismes de Certification
- Honey-nets/malware – CSRRT-LU
- Veille technologique
- Veille normative
- Etc.

Délivrables

- Transfert de savoir-faire
- Guides pour PME et citoyens
- E-commerce certified
- Protection des infrastructures critiques
- E-learning
- Etc.



Intérêt stratégique

- Devenir proactif (meilleure défense)
- Protéger les investissements
- Contraintes internationales
- Accroître la confiance

Actions nécessaires

- Sensibilisation et prévention
- “Culture de sécurité” OCDE
- Donner le sens des responsabilités
- Certification vs. régulation

CASES – Réduire la fracture numérique en sécurité :

Missions :

- Sensibiliser
- Promouvoir l'utilisation de mesures de sécurité
- Promouvoir la confiance via le savoir-faire et la coopération

Public cible :

- enfants
- citoyens
- PME
- Administrations



L'inconscience et le manque de savoir-faire représentent les vulnérabilités majeures auxquelles nous devons faire face, puisqu'elles sont continuellement exploitées.

Approche choisie dans CASES :

- Rechercher la coopération avec les parties intéressées
- Utiliser un langage simple (très difficile) et rester positif
- Adopter une approche globale
- Considérer les interdépendances, et pas seulement, les singularités

Structurer le savoir-faire

Risque = Vulnérabilité * Menace * Impact

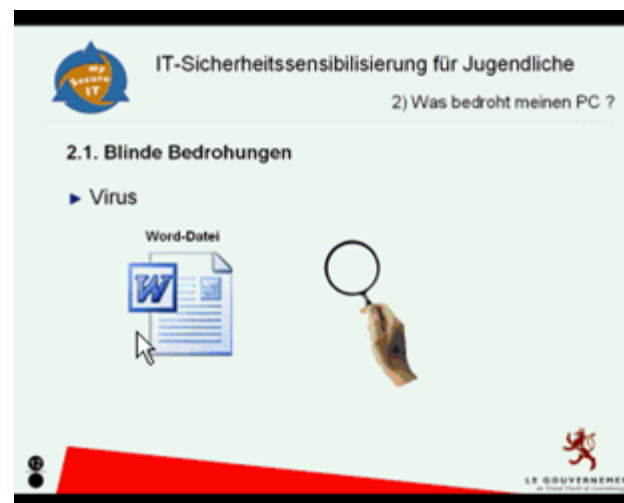
CASES – Combattre les vulnérabilités :

Outils utilisés :

- Glossaire
- Fiches thématiques
- Dossiers thématiques
- Règles de comportement
- Politiques

Canaux de distribution :

- Portail Internet
- Plate-forme E-learning
- Documents
- Workshops
- Conférences
- Affiches



CASES – Combattre les vulnérabilités :

Exemple: Campagne de sensibilisation intergouvernementale

- Analyse des besoins en sécurité (EBIOS)
- Formations
- Politique de sécurité
- Campagne



CASES – Combattre les vulnérabilités :

Exemple: Campagnes pour enfants

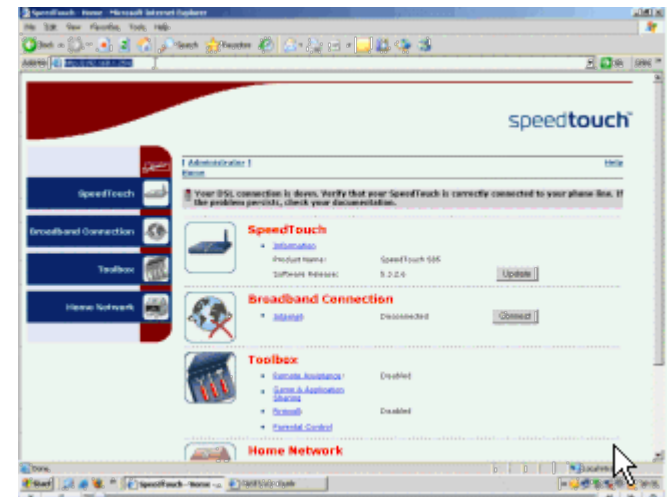
- Internet driving license : <https://pwws.cases.lu>
- Fiches pour enfants
- Présentations pour enfants



CASES – Combattre les vulnérabilités :

Exemple : Le WiFi au Luxembourg

- Fiche thématique sur le WiFi
- Fiche thématique sur le Bluetooth
- Dossier thématique sur le WiFi
- Document sur le Bluetooth cracking
- Analyse des WiFi-Routers vendus au Luxembourg



CASES – Combattre les vulnérabilités :

Exemple : L’E-learning

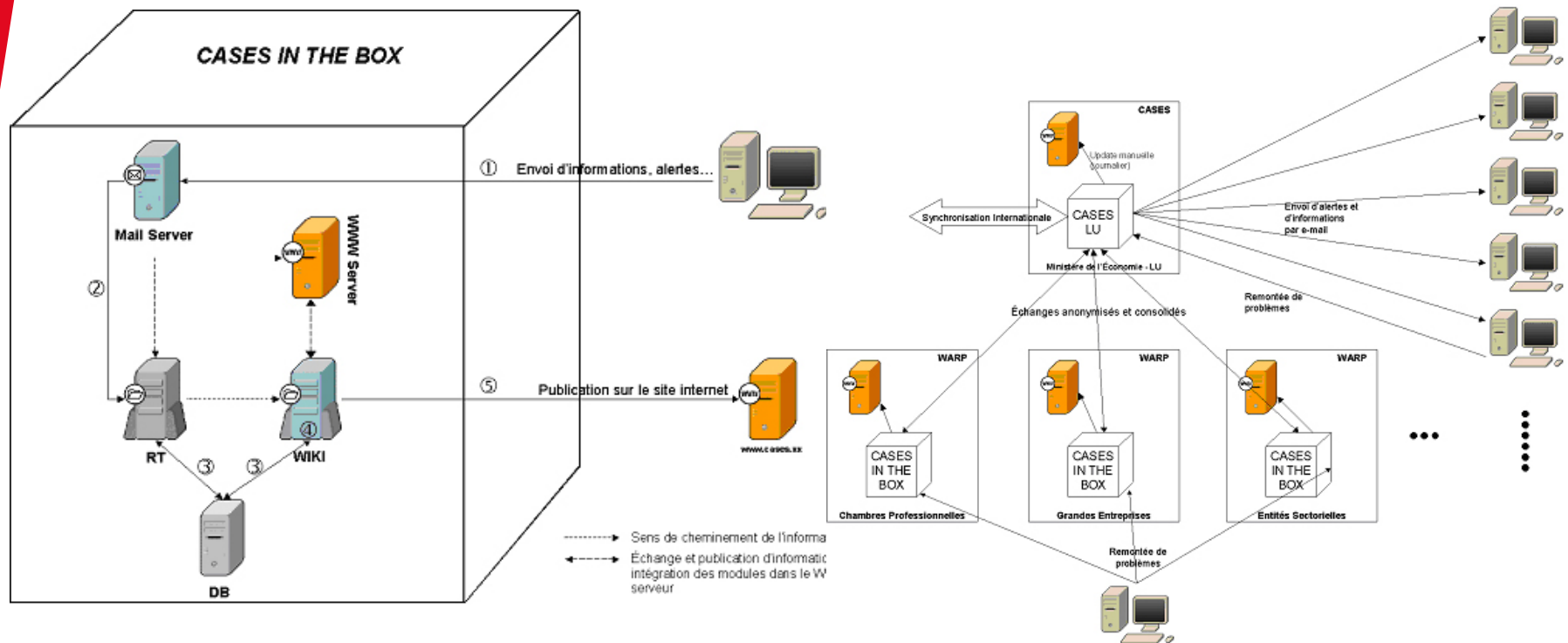
Fusionner l’expertise des domaines de la sécurité et du Technology Enhanced Learning pour fournir une plateforme d’E-learning innovatrice afin de réduire la fracture numérique liée à la sécurité:

- Citoyens : 13 modules
- PME : 25 modules
- Plate-forme innovante basée sur Php, mysql,
- <https://elearning.cases.lu/> (powerd by AnaXagora)



CASES – La coopération nationale :

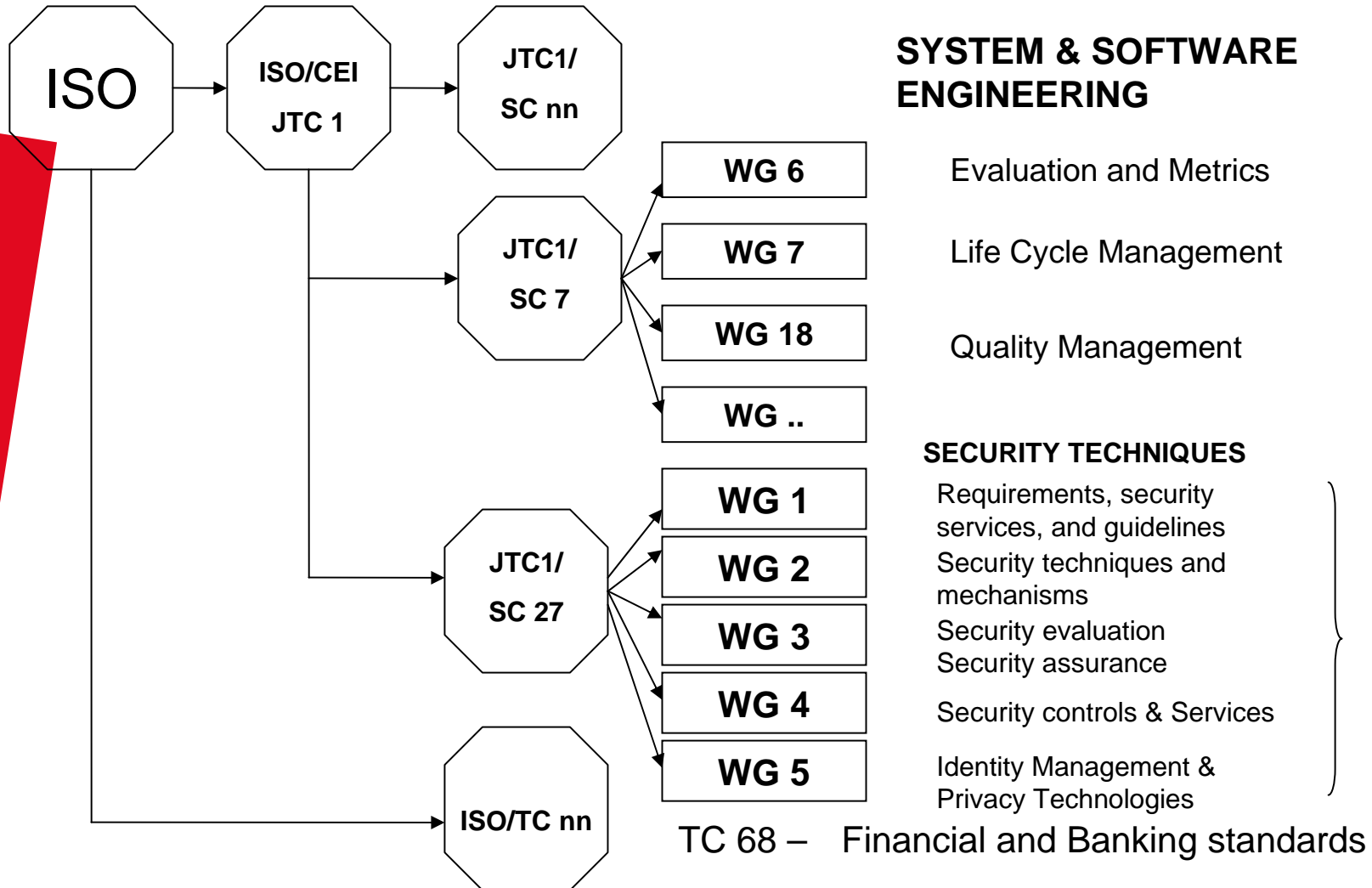
Networking tools : CASiX - CASES in the box



CASES – International Cooperation :

- Coopération au niveau ministériel avec la Suisse
- Coopération au niveau ministériel avec le Canada
- Coopération avec la DCSSI du SGDN en France
- Coopération avec l’IBPT en Belgique
- Coopération avec différents pays au niveau CASES
- ...

- **CNLSI – Extension normative de CASES**
- **CNLSI** = Comité de Normalisation Luxembourgeois pour la Sécurité de l'Information (CNLSI)
- **CNLSI** = Comité technique ISO/SC27 Luxembourg
- Composition : experts de la sécurité de l'information – G-D de Luxembourg
- Rôle : commentaires et votes sur les normes ISO/SC27, en regard des spécificités et intérêts du G-D de Luxembourg



➤ Rapport de la Commission européenne (octobre 2006)

➤ ***“Les PME et la normalisation en Europe, 23 bonnes pratiques pour promouvoir la participation de l’artisanat et des PME à la normalisation et l’utilisation des normes (EIM Business & Policy Research)”***

➤ G-D de Luxembourg parmi les 23 exemples de bonnes pratiques listés (Chapitre 6)

➤ Lien fort avec le portail de la sécurité de l’information du G-D de Luxembourg : <http://www.cases.public.lu>

ANSIL (Association de Normalisation pour la Société de l'Information du Luxembourg)

Objectifs (extraits des statuts):

- d'étudier, d'analyser toutes formes de documents normatifs,
- de constituer ... des groupes d'experts ... (comités),
 - ... intérêts économiques du Grand-Duché de Luxembourg,
 - travailler par consensus,
- ... interface entre ... acteurs ... et ... institutions officielles,
- ... sensibiliser ... promouvoir ... encourager la normalisation,
- ... participer à des projets de recherches ...,
- ... services d'expertise ...,
- ... en conformité avec l'ISO/IEC, le CEN/CENELEC




ANSIL
ASSOCIATION DE NORMALISATION POUR LA
SOCIÉTÉ DE L'INFORMATION LUXEMBOURG

Faire faces aux menaces

Outils utilisés :

- Projet de recherche R2SIC
- Honey-pots et Honey-nets – CSRRT-LU
- Déploiement d'un outil de malware collection : CSRRT-LU

 statistics | nepenthes logfile | google map

(Sorted by FirstSeenDate, descending) Hash: < previous page next page > (page 1/218)

Hash V	First Seen V	Last Seen V	Hits V	Virus	Norman Result	Hexdump	File
56e3960ab3645e2b49613c0438e3ac16	19.09.2006 17:36:17	19.09.2006 17:52:20	8	no	yes (-)	browse	download
1c9681e0860159bf9cc3e48c525ecceb	19.09.2006 17:29:26	19.09.2006 17:46:39	8	no	yes (-)	browse	download
42623e7330a0f8eb95hef520834b2b11	19.09.2006 16:37:01	19.09.2006 18:27:56	4	yes (4)	yes (+)	browse	download
13ff667bebcc58253faba2313dce7b89	19.09.2006 16:31:55	19.09.2006 16:32:11	1	yes (3)	yes (+)	browse	download
81cb60384c7a55679288edfe38daacef	19.09.2006 15:59:15	19.09.2006 17:01:19	3	yes (3)	yes (+)	browse	download
bfaeaacd3acfb02b4f5d96214e7d882e	19.09.2006 15:19:37	19.09.2006 17:33:13	2	yes (3)	yes (+)	browse	download
72aec55cb267ebcd1f798deb599e70fe	19.09.2006 14:53:21	19.09.2006 14:54:46	12	no	yes (-)	browse	download
02de24cfe3d31763e78bf6414010449b	19.09.2006 14:48:07	19.09.2006 18:19:46	8	yes (1)	yes (+)	browse	download
a385b5ca070397859e0f530c8b19c66f	19.09.2006 14:04:23	19.09.2006 14:04:38	1	yes (4)	yes (+)	browse	download

Computer Security Research and Response Team – Luxembourg : CSRRT.ORG.LU

LuCSIRT (Luxembourg Computer Security & Incident Response Team)

Objectifs/bénéfices :

- Traitement systématique d'incidents informatiques.
- Support technique pour le recouvrement après incident.
- Consolidation et collection d'information sur des incidents (vue globale, panorama).
- Centre de compétence pour toutes les questions de sécurité.

Démarche :

- basée sur le questionnaire (Observatoire des menaces)
- mise en place d'une entité gouvernementale,
 - services réactifs (interne)
- evolution vers une structure nationale
 - services proactifs pour le grand public

Merci pour votre attention

**François Thill
Pascal Steichen**

**francois.thill@eco.etat.lu
pascal.steichen@eco.etat.lu**

www.cases.lu