CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

CLOUD Computing

Point de situation - points de vigilance

CNIS magazine
Paris, 1er juillet 2010

Pascal LOINTIER
Président du CLUSIF
CHARTIS Conseiller sécurité de l'information, CHARTIS

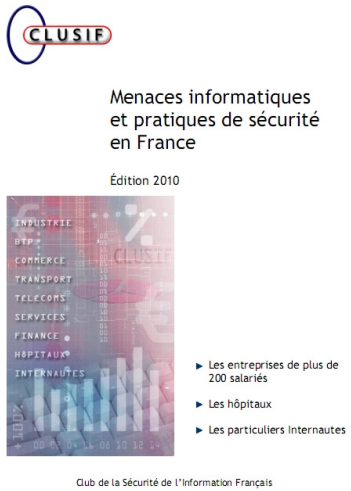
Point de situation

Une rentabilité des ressources offreurs présentée, pour certains, comme la panacée pour les utilisateurs

L'« informatique dans les nuages » permet aux entreprises de réduire leurs coûts en délocalisant leurs contenus et en utilisant des applications à distance. Mais « c'est un cauchemar pour la sécurité et elle ne peut pas être traitée par les méthodes traditionnelles », a estimé John Chambers, PDG de Cisco (01net, 27/04/2009

« Seul 10% des entreprises ont placé leur S.I. sous infogérance et quand c'est le cas, près d'une sur trois ne met pas en place d'indicateurs de sécurité!.. » (source MIPS 2010)

Pas de catastrophisme mais garder les pieds sur terre quand on a la tête dans les nuages



Dépendance et soumission à la variation d'offres

- Réversibilité. Pour les Grands Comptes, il est important de commencer par la fin : comment sortir d'un prestataire ?..

- Prix (d'appel). Comment gérer un changement de modèle économique ? Cf. le bi-bop, les co-processeurs arithmétiques bridés, le tatoo, etc.

- Le « choix » de contrat (par adhésion pour une PME)

« ta ton tatoo » et la tribu communicante… **recevoir en temps réel des messages** d'amour ou la liste des courses, être informés d'un changement de rendez-vous ou du retard de maman à l'école, à condition d'être équipés d'un pager ».
(L'Express, 07/03/1996)

Disponibilité, « aggravation du risque »

(terme d'assurance et non catastrophisme ;-))

Concentration de ressources, un incident de sécurité devient beaucoup plus impactant (nombre de clients et/ou nombre de ressources)

- Le cloud n'est pas dans le ciel mais dans un centre informatique (souterrain)
- 4 fév. 2010 - XXX ouvre un centre d'hébergement de 10.000 m2 à Seclin (source Silicon.fr)

Arrêt électrique toujours d'actualité…

- **Power Failure KOs Intuit Sites for 24 Hours**
  June 16th, 2010 : Rich Miller A major site outage that knocked Intuit web sites offline for more than 24 hours was caused by a data center power failure during routine maintenance, the company said tonight. The downtime affected the Intuit.com web site and thousands of small business customers ... An accidental power failure during that procedure affected both our primary and backup systems (source : www.datacenterknowledge.com)

[in Panorama 2009] câbles et ruptures de services

Avril, Californie (USA) : sectionnement malveillant des fibres, optiques sur deux sites de la Silicon Valley. Forte dégradation des appels aux services d'urgence, téléphonie commutée, distributeurs de billets et connexions Internet. Des dizaines de milliers d'utilisateurs impactés et, entre autres Sprint, Verizon et AT&T qui offre une récompense de 100 000 Dollars… AT&T informe via http://twitter.com/attnews/ ☺

Janvier, Phoenix (USA) : sectionnement accidentel des câbles en fibre optique à proximité d'un centre informatique d'une compagnie aérienne. Perturbation du système de gestion et retards pour une centaine de vols

[in Panorama 2009] câbles et ruptures de services

Novembre, Californie : coupure malveillante des câbles des caméras de surveillance.

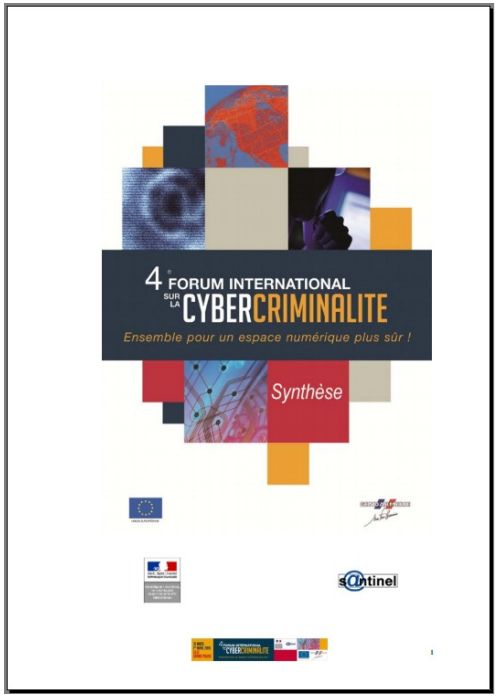
Décembre, (Etat de N-Y) : coupure de fibre optique affectant toute la région et notamment les services de billetteries et le traitement des transactions bancaires

Avril, Massachussetts : le FBI utilise un spyware (CIPAV, *Computer and Internet Protocol Address Verifier*) pour confondre une tentative de rançons contre Verizon et Comcast après coupures de 18 câbles (2005)

Sans oublier la connexion au CLOUD à partir du poste client…

Services Généraux sur IP

Il s'agit de l'ensemble des services nécessaires au fonctionnement normal d'une entreprise: achats de matériels, de fournitures, achat de terrains, construction de bâtiments, gestion des locaux techniques et des fluides: électricité, froid, chauffage, entretien des bâtiments. L'expression "Services Généraux" est généralement réservée à une activité interne de l'entreprise. Lorsque cette activité est externalisée, l'expression "Multi-service" est souvent employée. En anglais on appelle ce service "**Facility Management**" ou "**Facilities Management**". Il existe des entreprises spécialisées dans ce domaine. (source Wikipedia)



Confer « Services Généraux sur IP » à FIC2010

2007 : CNN et groupe électrogène

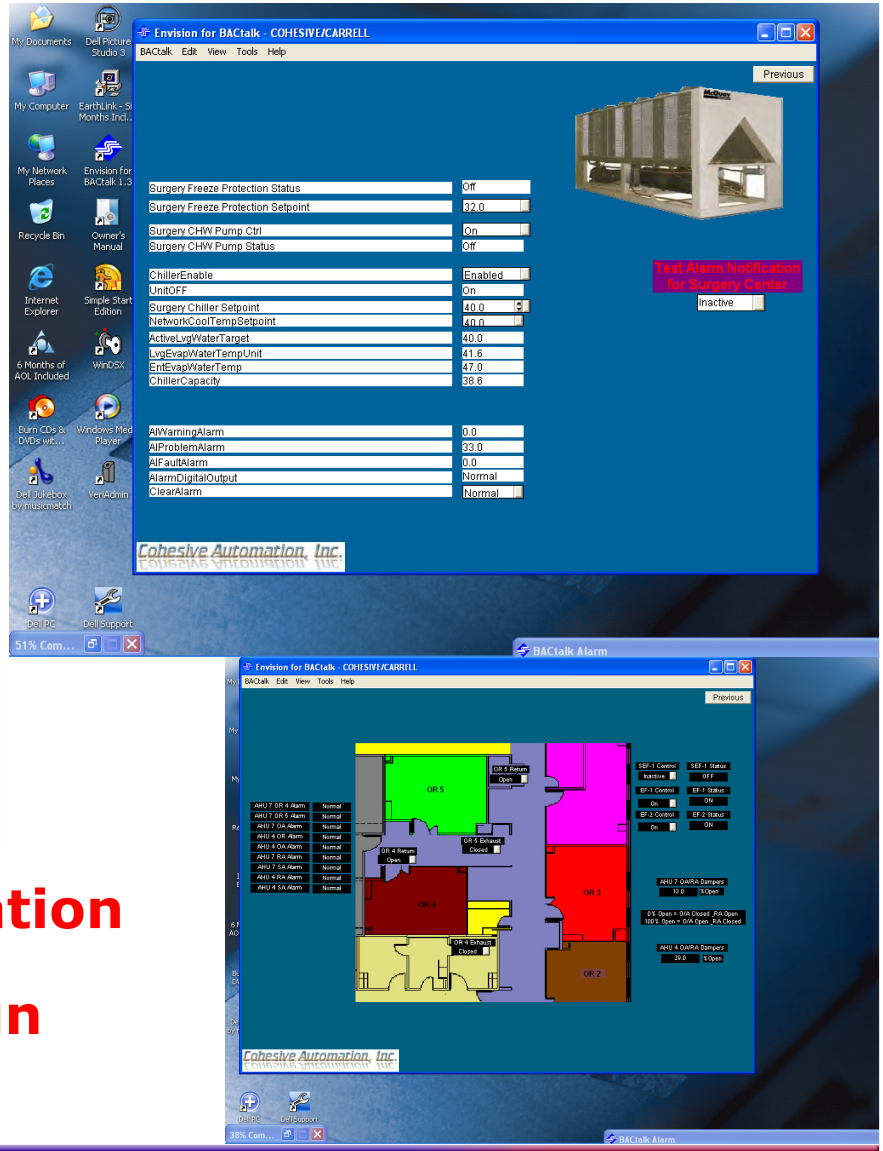
Septembre 2007 – Idaho (E-U): la chaîne CNN demande à des experts du DHS (*Department of Homeland Security*) de provoquer à distance la destruction d'u groupe électrogène. Cette action est rendu possible par l'injection de commandes numériques sur un équipement sans correctifs de sécurité (source Panorama 2007)

2009 : hacking de la ventilation dans un hôpital

FACTS IN SUPPORT OF AFFIDAVIT

6. On 6/24/2009, The Dallas Division of the FBI was contacted by Special Agent Charles Provine of the FBI in the Jackson Division of the FBI regarding a computer intrusion of a Heating Ventilation and Air Condition (HVAC) computer system at a Dallas, TX hospital, the Carrell Clinic located at 9301 North Central Expressway, Dallas, Texas. This was believed to present a risk to health and safety as the Hospital was a facility that kept patients around the clock who could be adversely affected by the cooling if it were turned off during Texas summer weather conditions and the hospital also maintained drugs which could be adversely affected by the lack of proper cooling if the intruder were to disturb the HVAC system. SA Provine stated that he was in contact with Lieutenant (LT) Lannie Hilbolt, Texas Attorney General's office and CW-1, a network

Page 4 of 18



Absence de ventilation = évacuation

Arrêt du refroidissement dans un centre informatique = …

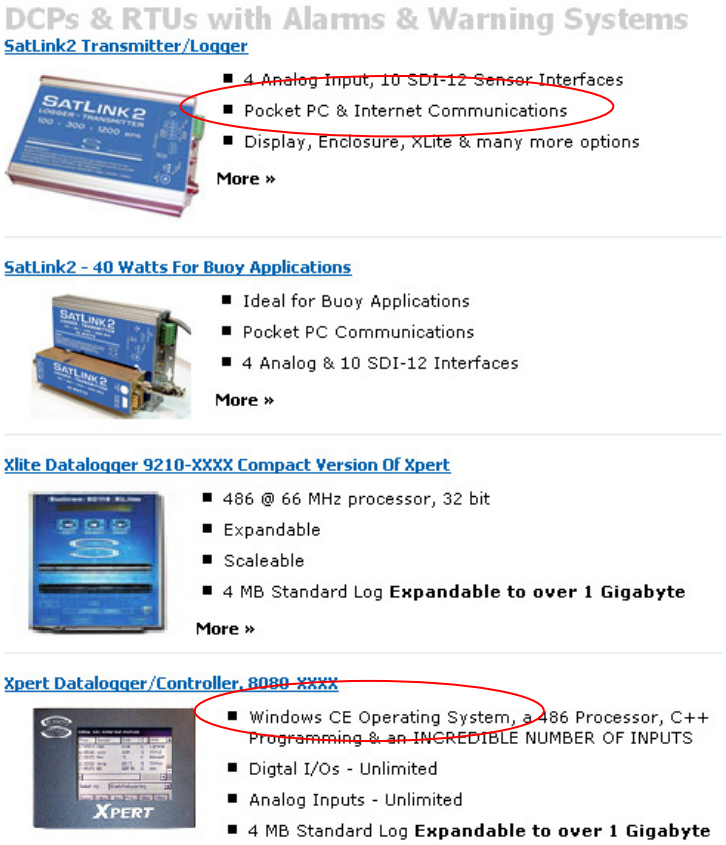
La migration IP continue…

… Surveillance et accès (portes, badgeuses, caméras, détecteurs présence, détecteurs incendie, humidité…)

La redondance physique des ressources (serveurs, électricité, réseaux) exposée à des défaillances logicielles.

Le MTBF (*Mean Time Between Failure*) concerne l'alea des pannes physiques, pas le déploiement simultané sur toutes les ressources redondantes mais à l'identique

- Mauvaise configuration (cf. incident HLR d'un opérateur télécom)
- Correctif bloquant (cf. … vous avez le choix ☺),
- Intrusion par la télémaintenance



Cloud computing, virtualisation : haute indisponibilité… parfois !

Haute disponibilité

La haute disponibilité est un terme souvent utilisé en informatique, à propos d'architecture de système ou d'un service pour désigner le fait que cette architecture ou ce service a un taux de disponibilité convenable (source Wikipedia)

- Pour mesurer la disponibilité, on utilise souvent un pourcentage essentiellement composé de '9' :
  - 99% désigne le fait que le service est **indisponible** moins de 3,65 jours par an
  - 99,9%, moins de 8,75 heures par an
  - 99,99%, moins de 52 minutes par an
  - 99,999%, moins de 5,2 minutes par an
  - 99,9999%, moins de 54,8 secondes par an
  - 99,99999%, moins de 3,1 secondes par an
  - Etc.

Et pourtant…

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Cloud computing, virtualisation : haute indisponibilité… parfois !

L'incendie de Lausanne n'est pas circonscrit

28.09.2009 22:24

De l'eau a été pompée directement du lac Léman pour inonder les sous-sols. [Keystone]

Cloud computing, virtualisation : haute indisponibilité… parfois !

Quelque part dans le monde (cloud ☺) pendant l'année 2009 mais pour des entreprises prestigieuses : Air New Zealand, Amazon (dont EC2), Barclay's, eBay (Paypal), Google (Gmail entre autres), Microsoft, Over-blog, Rackspace, RIM, Twitter…

- ☞ Panne électrique (UPS) et crash disques au redémarrage
- ☞ Feu électrique, destruction du générateur de secours et de l'UPS, commutateurs électriques, etc.
- ☞ Mise à jour corrective qui bogue
- ☞ Mauvaise configuration du routage entre 2 Data Center
- ☞ Attaque en DDoS ciblant des ressources DNS dans un Data Center spécifique

Cloud computing, virtualisation : haute indisponibilité… parfois !

L'année 2009 n'est peut-être pas spécifiquement exceptionnelle mais les incidents sont de plus en plus visibles : alerte *via* blogs, réseaux sociaux, Twitter…

Des effets secondaires

- Délais et ordonnancement du redémarrage des serveurs
- Crash des disques
- Destruction par incendie, le reste par inondation pour extinction…
- Pénalités (Rackspace contraint de payer entre 2,5 et 3,5 millions de dollars à ses Clients)
- Saisie des serveurs (FBI chez Core IP Networks, Texas)
- Perte de contrats (prestataire mais aussi pour l'entreprise commerciale vis-à-vis de ses propres clients)
- Twitter « interdit » de mise à jour par une Administration le dimanche de juin d'une élection ☺…
- …

Points de vigilance, « aggravation du risque »

(terme d'assurance et non catastrophisme ;-)

La responsabilité (pénale, économique) n'est pas externalisée ;-)

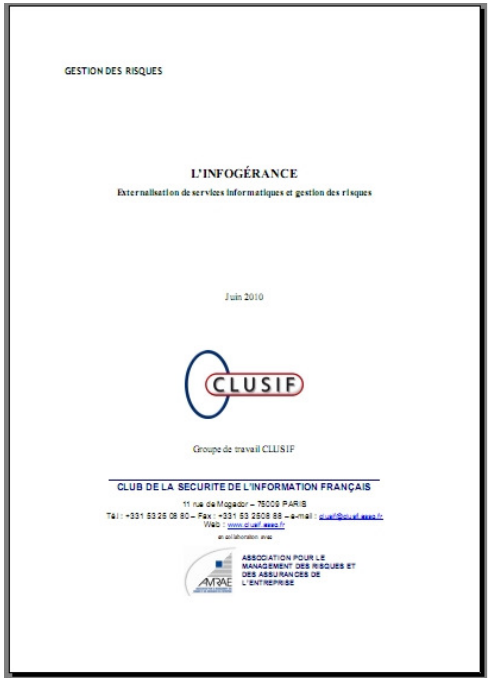
- Art 226-17 – « Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende. »
- Responsabilité Civile des Mandataires Sociaux (RCMS, D&O) et le *due diligence*

Points de vigilance, « aggravation du risque »

(terme d'assurance et non catastrophisme ;-)

Maîtrise des ressources et infogérance

- Clauses du contrat d'infogérance, à lire par le Département juridique, l'informatique (et la SSI) mais également par les Responsables métiers pour valider les délais de reprise sur incident
- Contrôler les procédures de sécurité effectives
- Identifier les sous-traitances et relocalisations possibles et parfois non signifiées au client
- Apprécier la capacité de reprise sur incident avec des systèmes mutualisés
- Traçabilités
  - Requête judiciaire
  - Chaîne de responsabilité au civil
  - Maintenir/prouver une conformité (réglementaire)


GESTION DES RISQUES

L'INFOGÉRANCE

Externalisation de services informatiques et gestion des risques

Juin 2010

CLUSIF

Groupe de travail CLUSIF

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

Solution souvent ressassée : travailler dans la confiance

1er semestre 2010…

- GMail autorise les audits internes de son infrastructure par la NSA
  - 🕮 Google to enlist NSA to help it ward off cyberattacks (source WahsingtonPost, 04/02/2010)
- Google Street view et le wardriving des WiFi mal sécurisés en Europe
  - 🕮 Dix autorités de protection de la vie privée interpellent Google (source Le Monde 20/04/2010)
- Google Android et le téléchargement et contrôle des téléphone à l'insu des usagers
  - 🕮 Google can kill *or install* apps on citizen Androids (source The Register 28/06/2010)

Conclusion :
on n'arrête pas un courant (commercial ☺)…
on le dévie !

Webographie

Ruptures de câbles

http://news.smh.com.au/breaking-news-technology/computer-problem-delays-us-airways-flights-20090130-7tdo.html

http://www.eweek.com/c/a/VOIP-and-Telephony/ATT-Offers-100000-Reward-for-Conviction-of-Bay-Area-Telecom-Vandals-437552/

http://www.datacenterknowledge.com/archives/2009/04/09/cable-cut-cited-in-silicon-valley-outage/

http://www.pcmag.com/article2/0,2817,2344762,00.asp

http://www.theinquirer.fr/2009/01/30/cable-sectionne-les-vols-us-airways-cloues-au-sol.html

http://www.varmatin.com/ra/derniere-minute/233072/vols-de-cables-jusqu-a-1h30-de-retard-sur-le-reseau-tgv?utm_source=rss&utm_medium=feed&xtor=RSS-220&

http://www.umpguingamp.over-blog.org/article-les-vols-de-metaux-en-augmentation-un-fleau-pour-les-transports-39597879.html

http://www.coltethernet.com/global_network_map.php

http://www.indybay.org/newsitems/2009/11/30/18630970.php

http://www.networkworld.com/news/2009/042009-fbi-used-spyware-to-catch.html

Webographie

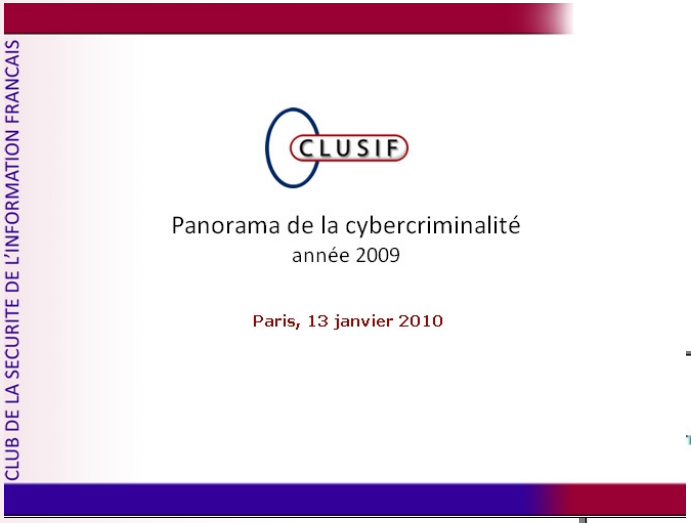
Centres informatiques et Cloud computing

http://www.datacenterknowledge.com/archives/2009/11/04/inside-a-cloud-computing-data-center/
http://www.datacenterknowledge.com/archives/2009/12/16/major-data-center-outages-of-2009/
http://www.datacenterknowledge.com/archives/2009/07/06/the-day-after-a-brutal-week-for-uptime/
http://cloudsecurity.org/
http://www.datacenterknowledge.com/archives/2009/12/23/dns-issues-cause-downtime-for-major-sites/
http://www.informationweek.com/story/showArticle.jhtml?articleID=222001992
http://www.networkworld.com/news/2009/101209-sidekick-cloud-computing-outages-short-history.html
http://www.infoworld.com/print/105435
http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853
http://www.networkworld.com/news/2009/040609-cloud-computing-security.html
http://www.theregister.co.uk/2009/10/05/amazon_bitbucket_outage/
http://www.computerworld.com/s/article/9130283/Backup_provider_Carbonite_loses_data_sues_vendor
http://www.tdg.ch/feu-avenue-provence-fermez-fenetres-2009-09-25http://www.tsr.ch/tsr/index.html?siteSect=200001&sid=11279188
http://www.theregister.co.uk/2009/06/17/barclays_gloucester_outage/
http://www.theinquirer.fr/2009/07/02/panne-electrique-sur-un-centre-de-donnees.html
http://www.networkworld.com/news/2009/071009-rackspace-ceo-speaks.html
http://www.theregister.co.uk/2009/08/04/paypal_offline_again/
http://www.theregister.co.uk/2009/06/24/paypal_uk_down/
http://www.theregister.co.uk/2009/08/05/cisco_2hour_outage/
http://www.theregister.co.uk/2009/10/19/swissdisk_failure/
http://www.silicon.fr/articles/printView/fr/silicon/news/2009/12/10/des_hackers_s_introduisent_dans_ec2__l_offre_de_cloud_d_amazon

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

CLUSIF

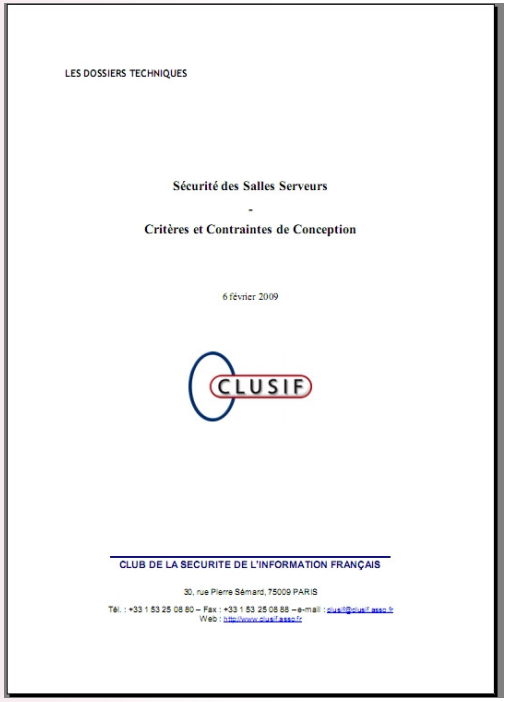
www.clusif.asso.fr


CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

CLUSIF

Panorama de la cybercriminalité
année 2009

Paris, 13 janvier 2010


LES DOSSIERS TECHNIQUES

Sécurité des Salles Serveurs
-
Critères et Contraintes de Conception

6 février 2009

CLUSIF

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

30, rue Pierre Sémard, 75009 PARIS


'ION DES RISQUES

L'INFOGÉRANCE

Externalisation de services informatiques et gestion des risques

Juin 2010

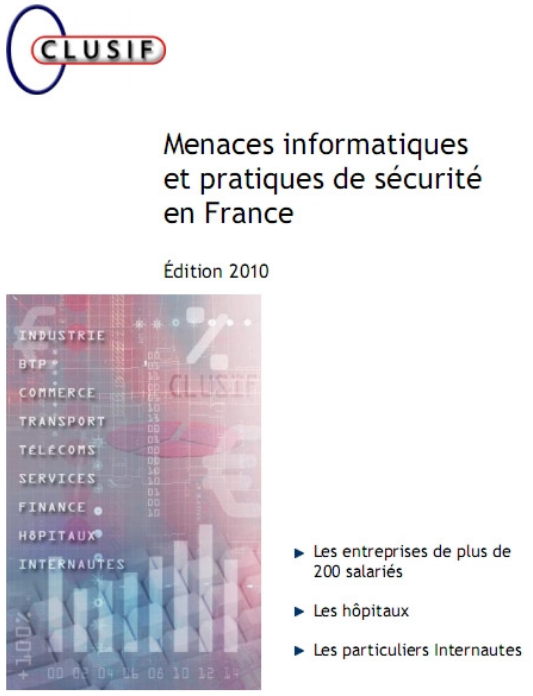
CLUSIF

Groupe de travail CLUSIF

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11 rue de Mogador – 75009 PARIS

ASSOCIATION POUR LE MANAGEMENT DES RISQUES ET DES ASSURANCES DE L'ENTREPRISE


CLUSIF

Menaces informatiques
et pratiques de sécurité
en France

Édition 2010

INDUSTRIE
BTP
COMMERCE
TRANSPORT
TELECOMS
SERVICES
FINANCE
HÔPITAUX
INTERNAUTES

- Les entreprises de plus de 200 salariés
- Les hôpitaux
- Les particuliers Internautes

Club de la Sécurité de l'Information Français