Forum du Rhin supérieur sur les Cybermenaces

Salle des conférences de l'ENA à Strasbourg le 25 nov. 2010

"L'entreprise dans les nuages..."

Forum du Rhin supérieur sur les Cybermenaces

Salle des conférences de l'ENA à Strasbourg le 25 nov. 2010

"Les offres faites aux entreprises et premières expériences" *(Laurent SCHMERBER)*
"La sécurité physique des entreprises" *(Adj.-chef André SCHERER)*
"Les contrats et responsabilités en nuages" *(Daniel GUINIER)*
"Cybercrime et cloud computing" *(Dr Alexander SEGER)*

Table ronde

sur les menaces et opportunités du "cloud computing"

Email : rene.eckhardt@wanadoo.fr
Web : www.euro-regio-club.com

Animée par René ECKHARDT

Président de l'EURO REGIO CLUB de Srasbourg et du Rhin Supérieur
Fondateur du Cercle des DirCom du grand Est
Chef d'escadron (RC) de la gendarmerie nationale

Les offres faites aux entreprises et premières expériences

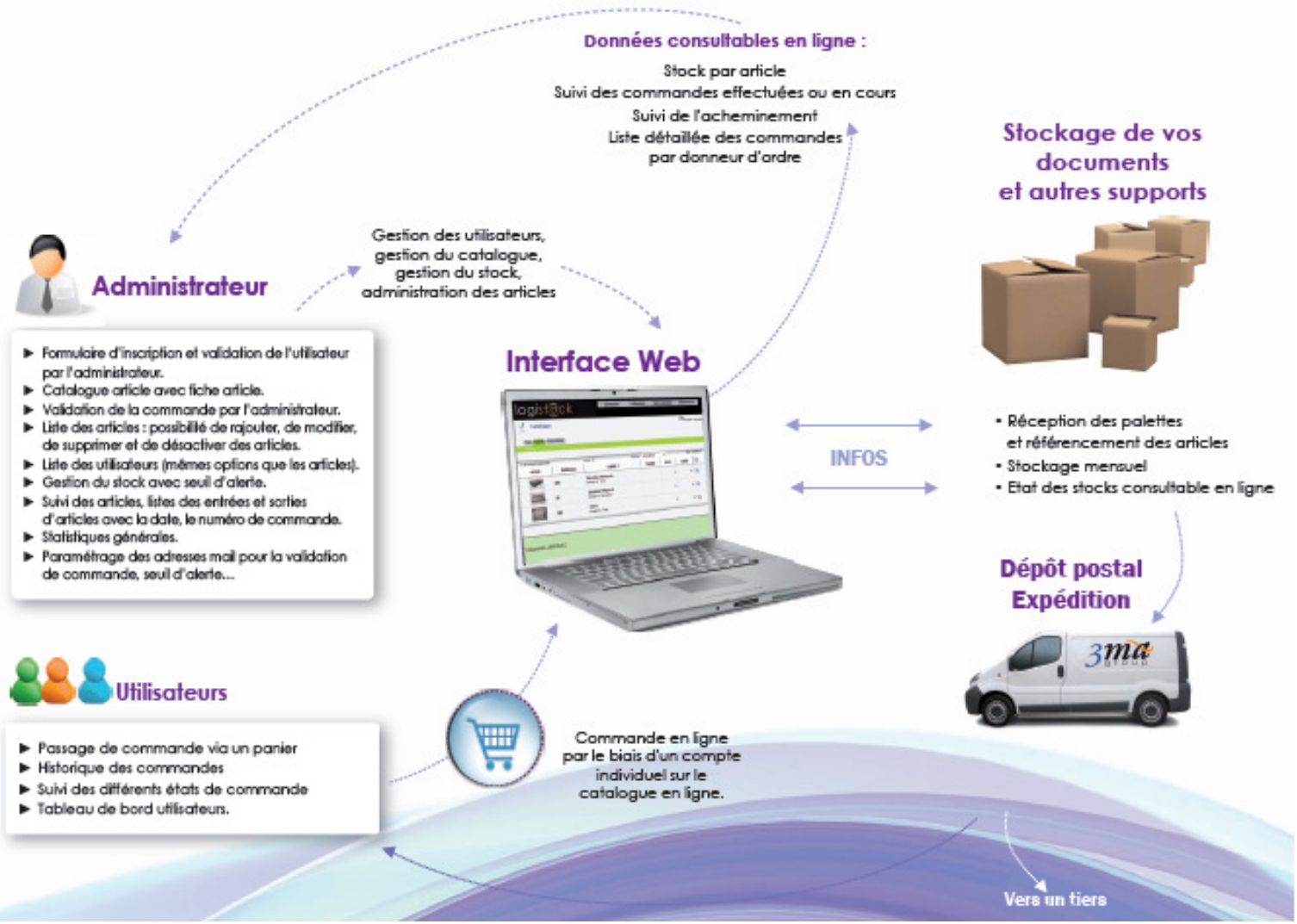
Email :laurent.schmerber@3magroup.com
Web : www.3magroup.com

par Laurent SCHMERBER

Président de 3ma Group
Président de l'UNIC Alsace (Union nationale de l'imprimerie et de la communication)
Chef d'escadron (RC) de la gendarmerie nationale

Ex. Solution de logistique en ligne

Solution de logistique en ligne



Bénéfices attendus en mode SaaS (1/2)

Réduction des coûts

- abonnement permettant de disposer d'une application
- tarifs optimisés d'affranchissement de transport et du traitement des envois à échelle industrielle
- stockage des brochures et objets dans les locaux du fournisseur

Gain de temps

- commandes de documents en ligne via Internet (service disponible 24 h/24, 7 j /7)
- externalisation de la gestion de la documentation permet aux clients de se recentrer sur leur cœur d'activité

Bénéfices attendus en mode SaaS (2/2)

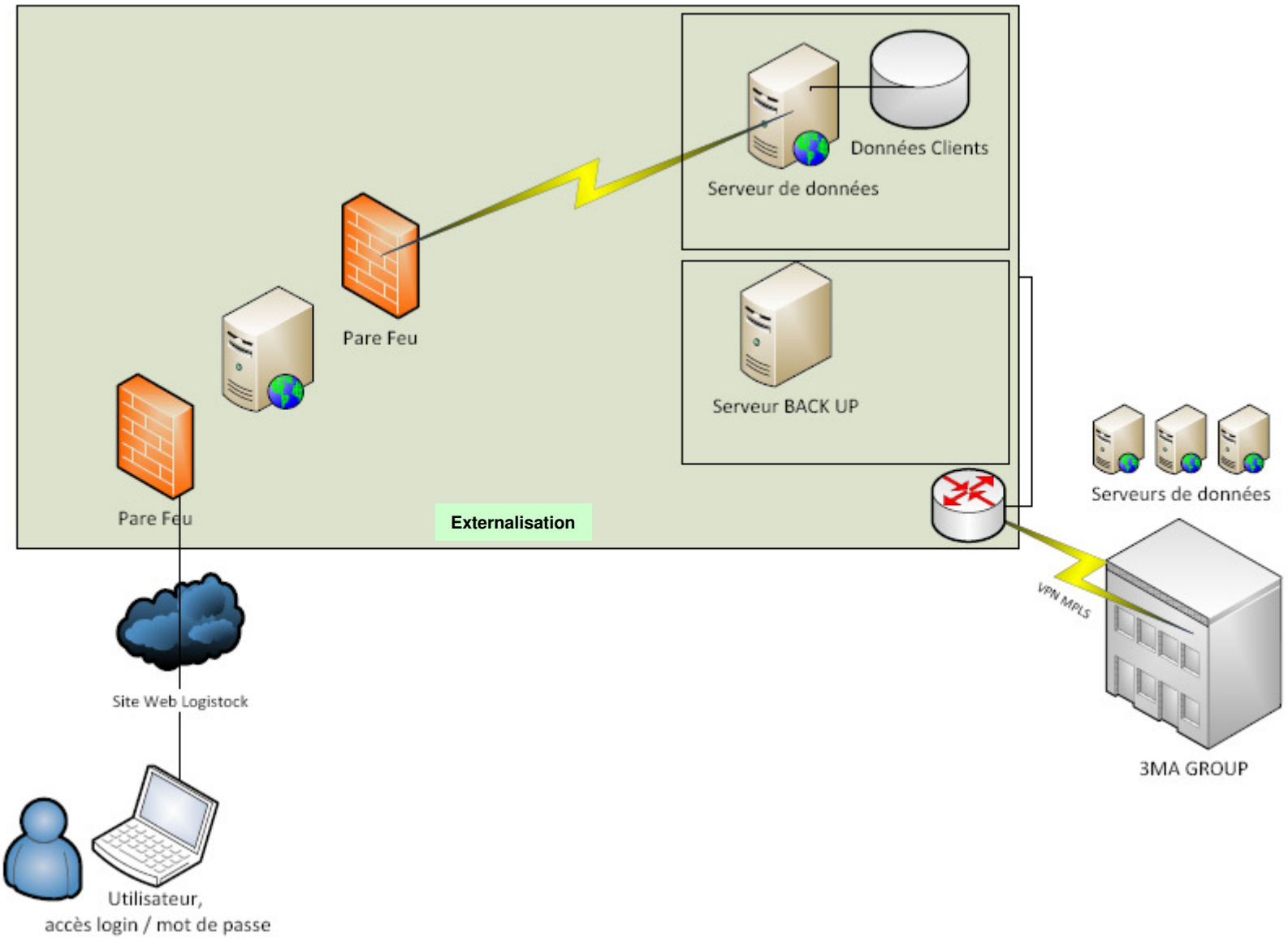
Maîtrise du processus

- visibilité 24h/24h des commandes : *quantités, date de commande, etc.*
- possibilité de mettre des quotas, budgets, seuils d'alerte.

Solution évolutive

- adaptation aux besoins même les plus complexes
- accompagnement de l'évolution du client

Schéma de l'architecture Saas



La sécurité physique des entreprises

Email : andre.scherer@gendarmerie.interieur.gouv.fr
Web : www.gendarmerie.interieur.gouv.fr

par l'adjudant-chef André SCHERER

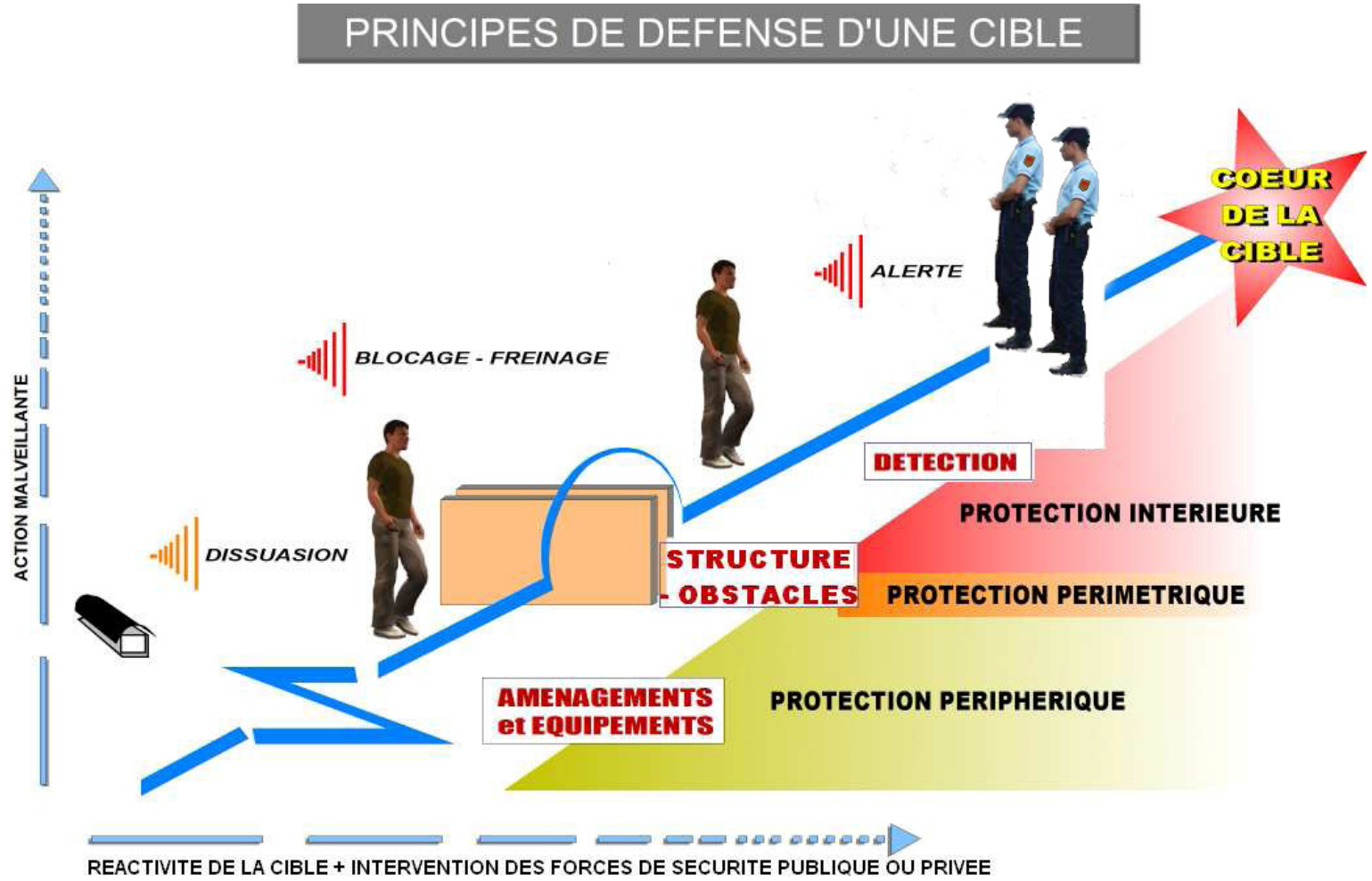
Référent Sûreté - Prévention situationnelle et vidéoprotection
Adjoint au Commandant de la brigade territoriale autonome de STRASBOURG
Région de Gendarmerie d'Alsace – Groupement de Gendarmerie Départementale du Bas-Rhin

La Prévention Technique de la Malveillance (PTM) appliquée à la protection physique des entreprises

- Son BUT est de :
  - **DÉTECTER** : les failles dans le domaine de la sûreté des lieux ;
  - **ANALYSER** : apporter l'expertise et l'expérience d'un professionnel ;
  - **PRÉCONISER** : proposer des solutions au maître des lieux.
- Elle repose sur un POSTULAT : le malfaiteur est un être rationnel
  - son objectif est d'obtenir un maximum de gain,
    en prenant le minimum de risque,
    dans un laps de temps restreint.
- Elle suppose une METHODE :
  - obligeant le malfaiteur à augmenter ses efforts pour parvenir à ses fins ;
  - faisant peser sur lui le risque d'être plus facilement détecté, identifié, arrêté ;
  - diminuant l'intérêt financier de la cible en réduisant les gains potentiels.

La PTM recouvre l'ensemble des mesures techniques, et humaines visant à prévenir la commission d'actes délictueux ou à les rendre moins profitables, et permet d'établir une stratégie de défense passive ou de protection active, après analyse des vulnérabilités constatées sur site.

La Prévention Technique de la Malveillance (PTM) appliquée à la protection physique des entreprises



L'objectif idéal est que le délai de réactivité de la cible soit inférieur à la durée de l'action malveillante

Méthode systémique et concentrique

- Périphérie du site
  - Vulnérabilités *(environnement, topographie, accessibilité, etc.)*
  - Stratégie de défense *(partenariat avec Ets voisins, gestionnaire du site, collectivités, etc.)*
  - Préconisations *(visibilité, lisibilité, etc.)*
- Périmétrie de l'entreprise
  - Limites de propriété *(de la résistance physique du périmètre, premier rempart, découle généralement le passage à l'acte malveillant)*
  - Stratégie de défense appliquée aux zones et vecteurs à risques *(parkings, stockage matériaux, structures des bâtiments, ouvrants, toitures, contrôleurs d'accès, réseaux énergie, réduction des facilitateurs…)*
  - Préconisations *(moyens mécaniques, techniques, chimiques, gestion des flux, vidéoprotection, etc.)*
- Volumétrie des espaces intérieurs
  - Sécurisation homogène des espaces internes, et de façon accrue des locaux stratégiques et du cœur de cible *(local coffre-fort, serveur réseau, etc.)*
  - Stratégie de défense *(réaménagement des espaces, proportionnalité entre les valeurs à protéger et les moyens de défense, etc.)*
  - Préconisations *(idem ci-dessus, favoriser la conformité aux normes des moyens de protection, etc. (ex. certification A2P)*

Les espaces défendables : Périphérie - Périmétrie - Volumétrie

La gestion de l'humain et de l'organisationnel

- La communication externe et les relations
  - avec les responsables de la sécurité/sûreté des sites voisins
  - avec les collectivités locales
  - avec les forces de sécurité
- La communication interne et la gestion de l'humain
  - concevoir, communiquer, expliquer
  - contrôler les connaissances et l'application des procédures
  - sensibiliser, former, évaluer les personnels
- L'organisation et les moyens techniques
  - contrôle et vérification périodique des dispositifs
  - détection et correction des anomalies
  - vérification du bon usage des procédures
  - contrôle des opérations de maintenance

La présence humaine, la vigilance, la prise de conscience que la sécurité/sûreté est l'affaire de tous. Cette dimension est essentielle et souvent omise ou insuffisamment prise en compte, alors que les mesures de bon sens ne seraient pas génératrices de coûts.

Les moyens de protection

- Les standards :
  - Périphérie et limite de propriété
  - Périmétrie :
    - Protection mécanique
    - Protection électronique
  - Volumétrie
- Les contrôles d'accès : IAAA et gestion des flux
  - les moyens techniques usuels
  - les technologies spécifiques : RFID, biométrie
- La vidéoprotection
  - avec opérateurs humains
  - avec intelligence artificielle embarquée
- Les techniques innovantes

Aujourd'hui, on ne peut plus parler de protection sans y associer la technologie de l'image. La vidéoprotection est, si le système est maitrisé, un outil très efficace.

Les contrats et responsabilités en nuages

Email : guinier@acm.org

par Daniel GUINIER

Expert judiciaire honoraire près la Cour d'Appel de Colmar
Expert devant la Cour Pénale Internationale de La Haye
Lieutenant-colonel (RC) de la gendarmerie nationale

Préalables

- **Loi applicable** - alternative
  - lieu de résidence du responsable du traitement
  - lieu des moyens pour réaliser le traitement, hors transit
  - lieu déterminé par contrat ou obligé pour certaines données
- **Droit applicable en France**
  - droit français : *ex. LIL et conformité du 06/08/04, LCEN, LSI*
  - droit communautaire : *ex. Directive 95/46 du 24/10/95*
- **Réglementations spécifiques à certaines données**
  - sectorielles : *de santé, bancaires, de défense, etc.*
  - transverses : *à caractère personnel, de la vie privée, etc.*
    - déclaration à la CNIL pour les données dans l'Union Européenne
    - approbation de la CNIL pour les données hors de l'Union Européenne

Il faut s'interroger sur la légalité des opérations si des données ne peuvent être délocalisées ou exigent des précautions particulières, en fonction des lieux de transfert, de stockage et/ou de sauvegarde.

Responsabilités en droit français

Responsabilités du prestataire

- il est le *"gardien de la chose" (Art. 1384 du Code civil)*
- il doit conserver la chose *(ex. données), -sans perte et avec la sécurité voulue-,* et la restituer au client
- il est l'organe du traitement des données personnelles

Responsabilités du client

- il détermine les **finalités** et les **moyens** de traitement
- il est le responsable du traitement des données personnelles *(Art. 3 et Art. 5 de la Loi Informatique et Libertés (LIL))*

Coresponsabilité au vu des moyens

- ne sont plus directement déterminés et contrôlés par le client
- se sont souvent des services fournis par sous-traitance
- l'obligation d'information est exigée de part et d'autre

Il faut s'interroger sur le service ...aaS concerné et la localisation, formaliser le droit et la compétence juridictionnelle, et se poser la question de l'exequatur (*) en cas de jugement à exécuter.

(*) Procédure visant à donner dans un pays, force exécutoire à un jugement rendu à l'étranger.

Les contrats

- **Les grands principes**
  - la liberté contractuelle limitée par la loi qui s'applique
  - le consensus, ou l'adhésion, négociée ou non – *l'intuitu personæ*
  - la force obligatoire du contrat et sa résolution
- **Les contrats usuels**
  - de licence d'utilisation d'une application logicielle
  - de développement, de maintenance
  - d'infogérance, hébergement, etc.
- **Les contrats de services *…aaS***
  - de service d'exploitation d'une application logicielle *(SaaS)*
  - de convention d'un niveau de service *(SLA)* spécifique par objectif
  - de mutualisation de ressources *(ex. HaaS, FaaS),* etc.

Alors que droit de l'informatique arrivait à maturité : qualification juridique établie et jurisprudence assise, le "cloud computing" fait naître des interrogations légitimes.

Les clauses juridiques principales

- **Signataires**, **objet et périmètre** : *SaaS, PaaS, IaaS, etc.*
- **Engagement et portée** des obligations, conventions
- **Garanties**
  - licité et conformité aux réglementations
  - localisation et accès : *ressources et données*
  - prix et base de facturation : *ressources, bande passante, stockage, etc.*
  - pérennité, *intuitu personæ* et sous-traitance *ou non*
  - réversibilité : *facteurs déclencheurs, récupération des données, etc.*
- **Protection des données** et **propriété intellectuelle**
- **Assurance** et réparation en cas de faute établie
- **Confidentialité** : *contrat, signataires, etc.*
- **Résolution** du contrat et **changement de fournisseur**
- **Loi applicable**, arbitrage et **juridiction compétente**

Les clauses juridiques précisent les obligations, permettent de se prémunir et d'anticiper sur des évènements pouvant se produire, et d'envisager les mesures à appliquer.

Les clauses techniques principales

La sécurité des services et des données

- confidentialité des données et accès frauduleux *(Art. 323-1 du CP)*
- intégrité des installations, systèmes et données
- disponibilité par des sauvegardes et réplications distantes
- imputabilité et éléments de preuve *(Art. 1316 et suivants du Code civil)*

La continuité et la qualité des services

- convention d'un niveau de service (SLA) par objectif
- outils de mesure de l'utilisation des services
- plan de réversibilité vers d'autres prestataires
- mode dégradé et restauration : *palliatifs, délais et pénalités*
- plan de reprise ou de continuité d'activité et solution de secours

La sécurité est la première préoccupation liée à l'externalisation massive des données et aux traitements en nuages exigeant des contrôles et audits permanents selon les normes attendues.

Conclusion

- **En externalisation classique**
  - les contrats sont stables : *licence, infogérance, hébergement, etc.*
  - leur qualification juridique est acquise
  - la jurisprudence est assez bien assise
- **Avec les services en nuages**
  - les contrats sont plus complexes : *services, territorialité, etc.*
  - leur qualification juridique reste à établir et les contrats à revoir
  - il n'existe pas encore de réelle jurisprudence

Un modèle de services ...aaS et le concours d'un cabinet spécialisé seront utiles pour mieux fonder la contractualisation en matière de services en nuages.

Cybercrime et "cloud computing"

Email : alexander.seger@coe.int
Web : www.coe.int/economiccrime

par le Dr Alexander SEGER

Head of Economic Crime Division
Directorate General of Human Rights and Legal Affairs
Conseil de l'Europe

Questions

Dans une société d'information ou de réseau sans frontières

- Comment garantir la sécurité tout en conservant une procédure régulière, la liberté d'expression et la protection des données personnelles dans un contexte mondial ?
- Comment s'assurer de la sécurité et la protection des données dans les "clouds" ?
- Question spécifique : enquêtes de la cybercriminalité dans les "clouds" ?

La cybercriminalité

- **Infractions contre les données et systèmes informatiques**

  Accès illégal, interception illégale, atteinte à l'intégrité des données, atteinte à l'intégrité du système, abus de dispositifs

- **Infractions informatiques**

  Falsification informatique, fraude informatique, pornographie infantile, infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

- **Les criminels s'organisent pour obtenir des profits économiques**

- **Preuves électroniques**

- **Criminalité transnationale**

Enquêtes en cybercriminalité

- **Dans une perspective de sécurité :** nécessité de retracer l'origine d'une attaque/infraction, d'identifier le délinquant , besoin d'accéder à des données relatives au trafic, aux données relatives au contenu ou d'autres données informatiques stockées, d'obtenir des informations liées aux abonnés
- **Approche actuelle :** "Les données stockées sur un système informatique"
- **La procédure normale :** recherche, saisie, interception, préservation, production
- **Conditions et sauvegardes** en matière de données et systèmes informatiques dans le pays où se déroule l'enquête policière
- **Enquêtes internationales** : MLA + des mesures urgentes pour la préservation
- **Convention de Budapest sur la cybercriminalité**
- **Avec le "cloud computing":** *Où se situe le système informatique ? Où sont les données ? Comment obtenir un accès ?*

L'accès des services répressifs dans les "nuages"

Scénarios :

1. **Accès aux données** des "clouds" relevant de la compétence des autorités de police
2. **Accès aux données hébergées à l'étranger** : avec l'aide des autorités policières du pays d'hébergement des fournisseurs de "cloud computing"
3. **Accès direct aux données** de "clouds" hébergées "quelque part" à l'étranger sans impliquer les fournisseurs de services de "cloud computing" ou les autorités du pays d'hébergement
4. **Accès avec la collaboration des fournisseurs** de services de "cloud computing"

Question :

- **Garanties et sauvegardes procédurales** *(Convention de Budapest Art 15)*

Conclusion

Sécurité & droits fondamentaux… aussi dans les "nuages"

1. **Pleine mise en œuvre de la Convention** sur la cybercriminalité
2. **Améliorer l'efficacité de l'application des dispositions de la coopération internationale** de la Convention sur la cybercriminalité et autres instruments
3. **Développer des normes internationales supplémentaires** sur l'application de la loi d'accès aux données stockées à l'étranger et dans les "clouds"
4. **Insister sur les garanties et sauvegardes** / établir des procédures de coopération entre fournisseurs de "cloud computing" et les forces de l'ordre -> lignes directrices aux fournisseurs de "cloud computing"
5. **Etablir un cadre international fiable** pour la protection des données personnelles
6. **Les fournisseurs de "cloud computing"** qui ne peuvent pas garantir les normes de protection et la confidentialité des données et des garanties procédurales auront un désavantage concurrentiel

www.coe.int/cybercrime

Forum du Rhin supérieur sur les Cybermenaces

Salle des conférences de l'ENA à Strasbourg le 25 nov. 2010

"L'entreprise face aux subversions..."

Forum du Rhin supérieur sur les Cybermenaces

Salle des conférences de l'ENA à Strasbourg le 25 nov. 2010

"Rumeurs, attaques réputationnelles et déstabilisation d'entreprise" *(M Emmanuel LEHMANN)*
"Les menaces liées aux réseaux sociaux" *(M Pascal GADEN)*
"Les menaces liées aux déplacements à l'étranger" *(M Philippe JOLIOT)*
"Le cadre légal et les risques judiciaires" *(Colonel Alain SEVILLA)*

Table ronde

sur les menaces subversives contre les entreprises

Email : rene.eckhardt@wanadoo.fr
Web : www.euro-regio-club.com

Animée par René ECKHARDT

Président de l'EURO REGIO CLUB de Srasbourg et du Rhin Supérieur
Fondateur du Cercle des DirCom du grand Est
Chef d'escadron (RC) de la gendarmerie nationale

Rumeurs, déstabilisations, attaques réputationnelles

Email : elehmann@gmail.com
Web : www.emmanuel-lehmann.com

***par* Emmanuel LEHMANN**

Expert en sécurité et déploiement économiques

L'attaque et ses objectifs

- Décrédibiliser un concurrent
  - Auprès de ses partenaires
  - Auprès de ses clients et prospects
  - Auprès de ses fournisseurs
- Affecter le cours d'une entreprise
  - Pour mieux la racheter (OPA)
  - Pour la mettre en difficulté
  - Pour jouer sur les cours
- Déstabiliser un projet
  - En délégitimant l'entreprise auprès des parties prenantes
  - En stigmatisant des éventuelles failles
  - En portant le débat sur la place publique

Méthodologie de l'attaquant

- La désinformation
- L'arme de la rumeur
- L'attaque réputationnelle
- L'instrumentalisation des acteurs et des parties prenantes

=> Une bataille autour de la légitimité

Gérer la crise

❑ Ne jamais répondre à chaud!

- Retracer une attaque :
- Analyser l'ensemble des signaux
- Identifier les lieux de l'attaques, les arguments et la montée en puissance
- Profiler les sources d'information et les acteurs
- Reconstruire la *"timeline"* de l'attaque
- Déterminer le commanditaire et l'*EFR* de l'attaque

❑ **Répondre** : Quel message et quel moyen de réaction ?

- Identifier les parties prenantes
- La gestion des arguments
- Utiliser/impliquer les leaders d'opinion
- Gérer les contradicteurs
- Anticiper les éventuelles contre-attaques

Anticiper et mieux connaître son environnement

- Identifier les angles d'attaque potentiels
- Identifier les acteurs et leurs liens relationnels
  - Par la veille
  - En relevant tous les acteurs *(actifs, passifs, neutres, hésitants, contradicteurs, opposants, adversaires, ...)* : l'ensemble des parties prenantes
  - En analysant leurs caractéristiques
  - En analysant les liens relationnels et d'influence
- Anticiper/imaginer les scénarios de crises
- Préparer les réponses à apporter
- **S'approprier la méthodologie pour mieux se développer**
  - Maîtriser son environnement
  - Connaître tous les acteurs
  - Identifier de nouvelles opportunités
  - Modeler la réalité

Les menaces liées aux réseaux sociaux

Email : pascal.gaden@adira.com
Web : www.adira.com

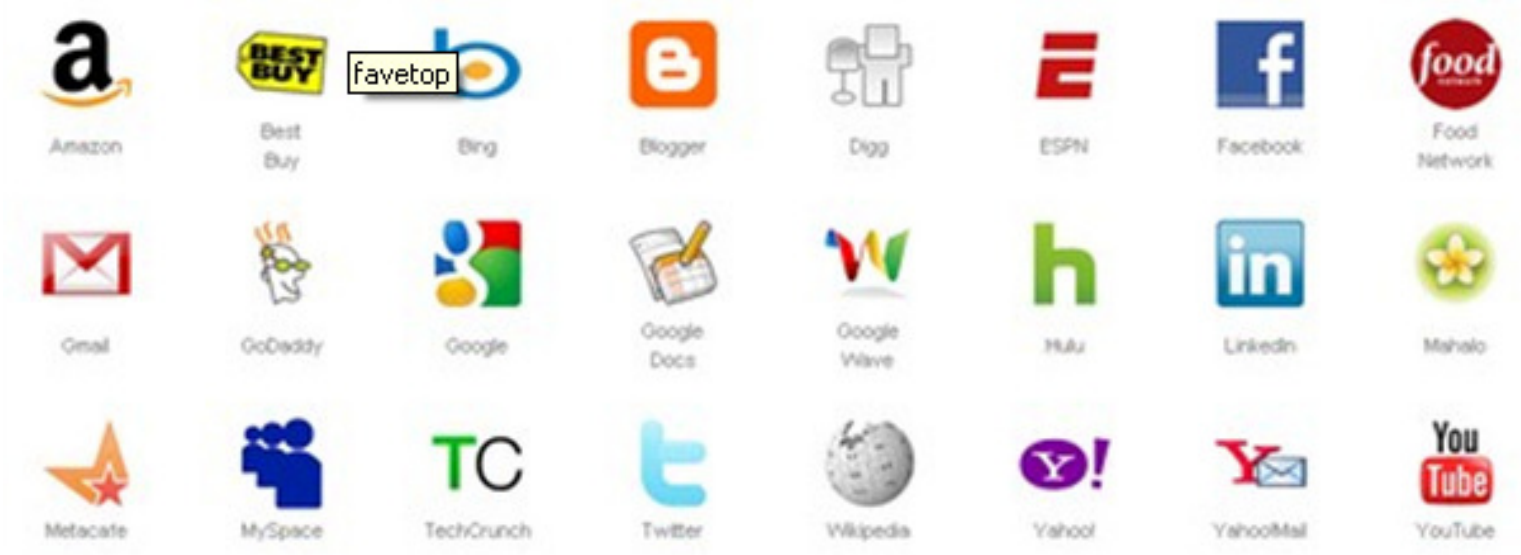
***par* M Pascal GADEN**

ADIRA – Agence de développement économique
Chef d'escadron (RC) de la gendarmerie nationale

Les réseaux sociaux

Qu'est ce qu'un réseau social sur Internet ?

17 millions d'utilisateurs en France 49% des internautes et 75% des 18/24 ans



Le facteur humain

- Le personnel de l'entreprise
- Il constitue par conséquent une cible privilégiée
- Un profil en ligne est souvent très éloquent
- Canaliser les élans de vos collaborateurs

L'ingénierie sociale

- Définition
- Quelques point faibles liés au facteur humain
- Un exemple de vulnérabilité dérivé de l'ingénierie sociale sur les réseaux

Les solutions pour chaque risque (1/4)

- **La récurrence des informations, le vol d'identité**
- **Attention à ce que vous postez ou téléchargez**
  - Choisissez avec précaution quelles images, vidéos ou informations vous publiez
  - Pas d'information sensible
  - Utilisez un pseudo

Les solutions pour chaque risque (2/4)

- **Les *"spams"*, les intrusions inamicales, les chevaux de Troie, la compromission**
- **Choisir ses amis avec soin**
  - N’acceptez pas les requêtes d’amis que vous ne connaissez pas
  - Vérifiez tous vos contacts

Les solutions pour chaque risque (3/4)

- **Protéger son environnement professionnel et éviter les risques réputationnels**
  - Utilisez votre email personnel sur les réseaux sociaux
  - L'image en ligne que vous donnez de votre entreprise
  - Ne mélangez pas vos contacts personnels et professionnels
  - Attention à ce que vous publiez à propos de quelqu'un
  - Qui fourni le service, l'application, le jeu ou le réseau ?

En première instance, le jugement du Conseil des Prud'hommes de Boulogne-Billancourt indique que faire preuve de mauvais esprit sur une page Facebook est un motif valable de licenciement.

Les solutions pour chaque risque (4/4)

- Protégez votre vie privée
- N'interdisez pas l'usage des réseaux sociaux
- Définissez des règles de sécurité appropriées

Conclusion

Le seul morceau de fromage
vraiment gratuit
se trouve sur les attrape-souris

(Proverbe russe)

Les menaces liées aux déplacements à l'étranger

Email : pjoliot@wanadoo.fr

***par* M Philippe JOLIOT**

Ingénieur – PDG de PCM Assistance et dirigeant de Tracip
Expert à la Cour d'Appel de Nancy
Président de l'AFSIN (Association Francophone des Spécialistes de l'Investigation Numérique)

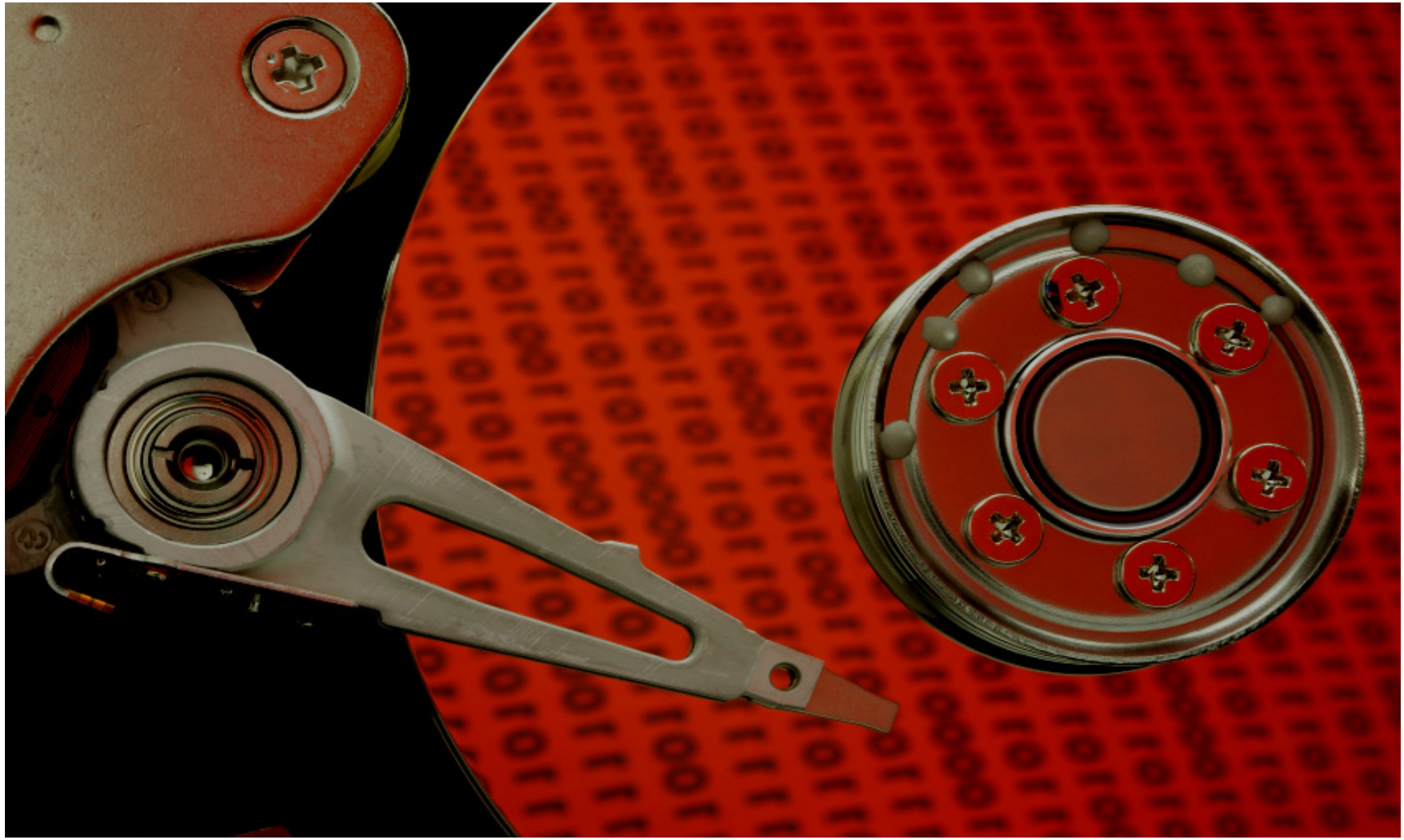
Les données numériques

- Déplacements à l'étranger et données numériques

Les données numériques

- **Le bon sens**
  - Minimiser les données et pas de données sensibles
  - Contrôle permanent des supports
  - Répartir les données sur différents supports

Les données numériques



Les moyens de communication

- **Les connections à distance**
  - Bureau à distance
  - VPN
- **Les connections WIFI**
  - Débit
  - Sécurité
- **La téléphonie**
  - 3G
  - Satellite

Les moyens de communication

- Merci de votre attention

Le cadre légal et les risques judiciaires

Email : alain.sevilla@gendarmerie.interieur.gouv.fr
Web : www.gendarmerie.interieur.gouv.fr

***par* le Colonel Alain SEVILLA**

Chef d'état-major de la région de gendarmerie d'Alsace

La diffamation publique

- **Définition** :
  - Allégation ou imputation de mauvaise foi d'un fait déterminé qui porte atteinte à l'honneur ou à la considération de la **personne physique ou morale** à laquelle ce fait est imputé
- **En matière pénale** : Art. 29 de la loi du 29 juillet 1881
  - La diffamation qualifiée est punie jusqu'à un an d'emprisonnement et d'une amende de 12000 € à 45000 €
- **En matière civile** : Arts. 1382 et 1383 du Code civil
  - Une action en responsabilité civile peut être intentée en cas de préjudice subi

L'action en diffamation se prescrit après trois mois, à compter de la première émission ou publication de l'écrit qualifié de diffamatoire.

La défiguation de sites

- **Définition** :
  - La défiguration *(pour "defacement")* est une **action délibérée et dirigée** en dégradant, modifiant ou détruisant une ou plusieurs pages d'un site Web, *souvent la page d'accueil*
- **En matière pénale** : Arts. 323-1 et 323-2 du Code Pénal
  - Atteinte au système de traitement automatisé de données *(STAD)*
  - Résulte :
    - d'une **altération des données** par suppression ou modification,
    - *ou* d'une **atteinte au fonctionnement** même du système,
  - Accès et maintien frauduleux à l'aide d'un programme *ad hoc*

    (Art. 46 de la LCEN, Art. 323-3-1 du Code Pénal)
- **En matière civile** : Arts. 1382 et 1383 du Code civil
  - Une action en responsabilité civile peut être intentée en cas de préjudice subi

L'entreprise doit supprimer les failles présentes par une veille et une mise à jour au fur et à mesure avec les correctifs appropriés.

L'usurpation d'identité

- **Définition** :
  - **Utilisation délibérée de l'identité d'un tiers** dans le but de réaliser une **action frauduleuse** : accéder à des droits de façon indue et aux finances de la personne, commettre en son nom un délit ou un crime
- **En matière pénale** : Art. 434-23 du Code pénal
  - **L'usurpation d'identité** est punie jusqu'à 5 ans d'emprisonnement et de 75 000 € d'amende
  - **L'usurpation d'identité électronique** est une incrimination qui sera l'objet d'une loi nouvelle
- **En matière civile** : Arts. 1382 et 1383 du Code civil
  - Une action en responsabilité civile peut être intentée en cas de préjudice subi

Les incriminations d'usurpation d'identité et d'usage de faux documents sont différentes, et peuvent se cumuler.

Usurpation d'identité électronique

- **Définition** :
  - **Utilisation délibérée de l'identité d'un tiers**, *ou de données de toute nature permettant de l'identifier*, sur un réseau de communication électronique **dans le but de nuire** en troublant la tranquillité d'un tiers ou portant atteinte à son honneur et à sa réputation
- **En matière pénale** : Art. 2 de la nouvelle loi LOPPSI II (*)
  - L'usurpation d'identité numérique est punie jusqu'à un an d'emprisonnement et de 15 000 € d'amende pour un particulier, et 5 fois plus pour une personne morale

    (Arts. 222-16 1 et 222-16 2 du Code Pénal)
- **En matière civile** : Arts. 1382 et 1383 du Code civil
  - Une action en responsabilité civile peut être intentée en cas de préjudice subi

(*) **LOPPSI** : Loi d'Orientation et de Programmation pour la Performance de la Sécurité Intérieure

Ces dispositions visent l'envoi de courriels et la publication de messages sur un blog ou un réseau social, et seront des moyens de lutte contre le "spam", et le "phishing".

Conclusion

- **Les menaces subversives sont** :
  - induites par les TIC
  - renforcées par les messageries et les réseaux sociaux
  - liées à des risques pour les particuliers et les entreprises
  - associées à des incriminations judiciaires
  - etc.

Il appartient à l'entreprise de s'en prémunir et de s'en protéger, de l'intérieur comme de l'extérieur.