

## Les synthèses du CLUSIF



### *Chiffrement des données locales des moyens nomades*

*Synthèse de la conférence thématique du CLUSIF du 7 avril 2009 à Paris*

***Les pertes et vols de données sont tous les jours plus médiatisés. Si aux Etats-Unis, il y a obligation de déclarer publiquement ces incidents de sécurité, il n'en est pas de même en France. Pourtant ce phénomène touche tous les pays et tous les secteurs, constate Pascal Lointier, Président du CLUSIF et conseiller sécurité de l'information chez AIG Europe. Dans ce contexte, le chiffrement des données est une des solutions efficaces.***

Les affaires de vols ou de pertes accidentelles de données confidentielles se multiplient dans tous les domaines d'activité et en particulier dans le milieu bancaire. On peut supposer qu'il existe des mécanismes de captation de données à des fins criminelles. Aux Etats-Unis, l'obligation de divulgation de ce type d'incidents a donné naissance à l'acronyme DLP : *Data leak prevention/protection* suivant que l'on soit pessimiste ou optimiste... Dans ce pays, des *Class Action*, souvent coûteuses sont aussi engagées. Au final, ce sont des préjudices importants pour les entreprises du fait de l'atteinte à l'image, de gestion de crise (informations auprès des médias, clients), des pertes de chiffres d'affaires, et de parts de marché. En France, la CNIL depuis 30 ans a fait évoluer la réglementation sur les données à caractère personnel avec en

particulier l'article 226-17 du code pénal qui condamne le défaut de protection des données à caractère personnel, laissant l'entreprise toujours responsable même lorsque le dit traitement a été sous-traité (externalisation de l'informatique).

Les données dérobées ont une grande variété de cible : les numéros de cartes bancaires, les savoir-faire industriels, les données judiciaires, les informations personnelles. Les supports volés ont également évolué. On est passé des bandes de sauvegarde à des clés USB ou à des disques durs portables ; ce qui facilite grandement la tâche des pirates informatiques. Ainsi, Pascal Lointier a donné plusieurs exemples de cas de vol de données : CardSystems, TGX, Hannaford et un autre cas en France.

#### **Alain Takahashi, Hermitage Solutions : les habitudes socioculturelles au cœur du chiffrement.**

Alain Takahashi, Hermitage Solutions, s'est attaché à caractériser les différents moteurs et freins qui accompagnent le déploiement de solutions de chiffrement en entreprise. En préambule, il a souhaité

clarifier l'acronyme PGP : « *Pretty Good Privacy* ». C'est avant tout une norme de cryptographie et un format d'échange, OpenPGP (RFC4880). Depuis 1996, c'est aussi une société, créée par Phil

Zimmermann qui compte aujourd'hui 250 personnes. En outre, PGP est associé à différents produits logiciels interopérables qui supportent la norme OpenPGP, tels que GnuPG, Utimaco, SSH, Véridis, Voltage... Par ailleurs, les approches et offres de chiffrement sont variables selon les pays. Ainsi, les deux éditeurs français, Arkoon et PrimX, ne supportent pas cette norme, préférant utiliser de la PKI.

Les principaux moteurs du marché du chiffrement dans le monde sont : la protection des données confidentielles ou nominatives, la prévention de la perte de réputation et surtout, la protection de la responsabilité pénale du dirigeant. Aux Etats-Unis par exemple, la loi oblige la déclaration publique de pertes de données nominatives.

En 2008, le chiffre d'affaires des éditeurs de solutions de chiffrement en France est estimé à 10-15 % de celui réalisé en Allemagne ou au Royaume-Uni, eux-mêmes en retard par rapport au marché américain. Alain Takahashi souligne, de plus, l'existence d'une différence culturelle concernant le type d'informations que chaque pays souhaite chiffrer. Par exemple en France, nous avons une forte propension à vouloir chiffrer les fiches de paie, tandis qu'aux Etats-Unis, ces informations n'auront pas vraiment de valeur de confidentialité, contrairement aux bulletins scolaires.

### **Laurent Perruche, Solucom et Cyril Moneron, RSSI du Groupe Saint-Gobain : le chiffrement est une technologie mûre mais qui nécessite une organisation et l'adhésion des utilisateurs.**

Laurent Perruche, Solucom, s'est plus particulièrement attaché au chiffrement des équipements nomades en s'appuyant sur le témoignage de Cyril Moneron, RSSI du Groupe Saint-Gobain. Les équipements portables PC, clés USB, disques durs portables sont les équipements les plus exposés aux risques de perte de données. Pour s'en prémunir, le chiffrement constitue un moyen de protection avancé.

Pour revenir aux solutions, PGP serait utilisé par 84 % des sociétés Fortune 100 US, 65 % des sociétés du CAC 40 et 50 % des sociétés du SBF 250. Néanmoins, certains secteurs de PME sont pourtant précoces dans le chiffrement en France : les preneurs d'ordres et sous-traitants des grands groupes, les banques d'affaires, les sociétés de gestion du patrimoine, les cabinets d'audit et de conseil, les cabinets d'avocat, les départements des RH, ou encore les PME ayant vécu un vol ou une perte de données. Cependant, même quand le chiffrement est déployé, il n'est pas toujours bien utilisé ou moins utilisé par rapport au projet d'origine défini par la direction ou le fournisseur. Dans certains cas, c'est le chef d'entreprise qui n'en voit pas l'utilité ; dans d'autres, ce sont les utilisateurs qui freinent le déploiement.

Pour conclure, quelques conseils peuvent contribuer à un déploiement réussi :

- Bien définir les données que l'on veut protéger.
- Sensibiliser les utilisateurs finaux aux risques de la sécurité informatique,
- En ce qui concerne le chiffrement de messagerie, comprendre les tenants et les aboutissants d'un système qui se met en rupture de flux : que veut-on chiffrer ? Comment va-t-on échanger les clés publiques ?

Ce dernier repose sur une donnée protégée : la clef de chiffrement, sécurisée par un ou plusieurs facteurs d'authentification qui peut être un mot de passe, un code PIN, un *token*, un certificat, une carte à puce ou encore une solution de biométrie.

En amont du déploiement d'une solution de chiffrement, il faut mettre en œuvre une stratégie qui repose sur le pragmatisme :

- Cadrer ses besoins et ses contraintes : identifier les données à protéger (comment sont-elles manipulées, stockées ? Qui les manipule ?), les menaces (vol, perte, accès non autorisé), et les risques (atteinte à l'image, désavantage concurrentiel, extorsion, manquement aux obligations légales).

- Tenir compte des aspects légaux et réglementaires. L'anticipation est nécessaire, à ce sujet, de manière à répondre à l'ensemble des contraintes auxquelles l'entreprise est soumise. Si la solution de chiffrement est utilisée à l'étranger, il faut se renseigner auprès des différents pays sur leurs aspects légaux d'utilisation du chiffrement. En effet, il n'y a pas d'harmonisation, chaque pays dispose d'un contexte général d'usage de la cryptographie et des réglementations spécifiques. En Chine, par exemple, les solutions de chiffrement doivent être utilisées avec une licence d'utilisation validée par une commission gouvernementale.

Cyril Moneron, chez Saint-Gobain, a fait une enquête auprès des 350 sociétés du groupe. Il en est ressorti que le risque majeur concernait les PC portables et les clés USB. Toutefois, il a été décidé que chaque entreprise du groupe devait choisir sa politique de données à sécuriser. Aujourd'hui, un tiers des PC portables sont protégés, en particulier tous les postes de R&D. En revanche, Saint-Gobain n'a pas encore résolu le problème de la protection des clés USB. En effet, la solution technologique retenue pour les PC n'est pas tout à fait adaptée aux clés USB.

Pour Laurent Perruche les différentes solutions techniques du marché, propriétaires et Open Source, sont aujourd'hui mûres. Le produit choisi peut répondre aux questions suivantes : quels sont les besoins à couvrir et quelles solutions sont alors envisageables ? Faut-il du chiffrement intégral, unitaire de fichiers et de répertoires ou autonome avec mot de passe ? Toutefois, il faut être conscient de l'impact d'une solution de chiffrement sur l'exploitation et le support utilisateur.

L'aspect disponibilité ne doit pas être négligé et doit même être pensé en amont car chiffrement suppose recouvrement (des clefs). Comme les données doivent être accessibles en cas de dysfonctionnement, il faut donc le plus souvent prévoir un support 24/7 car les personnels VIP sont les premiers à voir ces solutions déployées sur leur poste. Tout cela a été mis en place par Cyril Moneron qui a aussi déployé un système de traçabilité pour identifier chaque demande et les actions menées. Un des enjeux clef d'un tel déploiement est de gagner l'adhésion des utilisateurs. Il est donc nécessaire de les sensibiliser et d'accompagner ces changements : comment la solution fonctionne ? Qu'est-ce que ça change pour eux ? Il faut savoir qu'un outil peu ergonomique sera mal ou non utilisé. On en perd donc les bénéfices.

En conclusion, pour Laurent Perruche, les solutions de chiffrement sont mûres et intéressantes pour protéger les informations sensibles, mais les impacts psychologiques, organisationnels et techniques complexifient leur mise en œuvre. Dans ce contexte, la préparation et l'accompagnement s'avèrent essentiels.

### **Charles d'Aumale, Ercom : la carte à puce, une réponse aux enjeux de sécurité en situation de mobilité.**

Charles d'Aumale, responsable marketing et commercial d'Ercom, a présenté Cryptosmart, sa solution de sécurisation des terminaux mobiles, PC, PDA et Smartphones. Pour remédier aux menaces, Ercom propose une solution basée sur la carte à puce : carte de type bancaire, USB, micro SD (carte à puce bancaire associée à une zone de stockage chiffrée). Cette solution protège quasiment tous les types de mobiles. Elle inclut un PUK sécurisé avec 10 codes générés aléatoirement lors de la création de la carte. Ercom propose aussi une « box » pour la protection des

communications pour voitures, bateaux et avions. Charles D'Aumale a ensuite présenté la plupart des situations de communications sécurisables par cette solution : appel chiffré, e-mail sécurisé, vidéoconférence, flux de données, fax sécurisé... Il a conclu son intervention par la présentation du cas d'une PME dans le domaine de la sécurité physique qui a organisé la sécurisation de ses communications avec cette solution.

### **Cette session s'est conclue par un débat animé par Fred Messika, Fondateur de Sekoia.**

Pour introduire cet échange, Philippe Blot de la DCSSI (ANSSI) qui fait partie du SGDN, un service du Premier Ministre, a rappelé son rôle dans l'homologation des produits, l'intelligence économique, l'exploitation des technologies sensibles... Il a annoncé que son service allait devenir une agence et voir son effectif multiplier par deux d'ici à 2012. La DCSSI a plusieurs centres d'intérêts dont la sécurité des produits, la cyberdéfense, la gestion des réseaux interministériels sécurisés pour la gestion de crise. Philippe Blot a en charge la réglementation comme le Référentiel Général de Sécurité (RGS) mais aussi les produits de sécurité utilisés par les administrations et les produits commerciaux. Depuis 2003, la DCSSI a mis en place la qualification des produits avec la définition d'un niveau de sécurité et d'un référentiel. On y trouve la cible et le périmètre d'évaluation. Plus d'une dizaine de produits sont déjà qualifiés : Arkoon PrimX, Bull, Thalès, TrueCrypt ou encore Blancco dans le domaine de l'effacement. En effet, il ne faut pas oublier que l'effacement des données est aussi important, en particulier lors de la fin de vie des disques durs.

Emmanuel Forgues, chef du produit « Globull », de Bull, a décrit le concept de

cette nouvelle solution : transporter des données en les sécurisant par du chiffrement tout en se libérant du PC. En effet, les certificats sont stockés dans le processeur cryptographique. Ce périphérique ne pèse que 120 g et peut s'adapter sur n'importe quel PC. Ainsi, lorsqu'un employé prend ses fonctions dans une entreprise, on lui remet un Globull et une somme forfaitaire pour acquérir le PC et l'OS de son choix. Ce produit simplifie la tâche des administrateurs et rend la politique de sécurité applicable de façon homogène et transparente. Il permet aussi de supprimer certains comportements des utilisateurs comme la copie des données sur des clés USB.

### **Fred Messika : Monsieur Moneron, Alain Takahashi a évoqué les problèmes culturels à l'origine de la faible adoption du chiffrement en France ; n'y a-t-il pas plutôt un problème organisationnel ?**

Cyril Moneron : Je pense qu'il y a un problème technique, en particulier pour les transferts par e-mail et l'insuffisance de la généralisation des standards de crypto. Au niveau organisationnel, nous sommes confrontés à la réticence des utilisateurs. Quant à la mise en place d'une

organisation, elle doit faire partie intégrante du déploiement de la solution technique.

**Alain Takahashi : Monsieur Blot, pouvez-vous nous préciser la différence entre la certification Critères Communs et la qualification des produits ?**

Philippe Blot : Les critères communs sont régis au niveau international. Il y a des pays émetteurs, dont la France fait partie, mais tous ne sont pas habilités. Dans certains secteurs, comme la banque ou les administrations, on s'en sert pour sélectionner des produits de sécurité. L'Etat a décidé de se référer aussi à la qualification qui permet de vérifier que le produit répond à un besoin des administrations. Les Critères Communs n'imposent pas d'évaluations pour la crypto, cette partie est laissée à chaque Etat. Ainsi, pour la crypto, nous avons défini un référentiel particulier et nous faisons une cotation de ses mécanismes : bon usage des algorithmes, des modes, de

la génération d'aléas, d'effacement des clés... Nous évaluons aussi des solutions qui ne mettent pas en œuvre une PKI. La certification d'un produit n'est pas une recommandation à l'inverse d'une qualification. De plus, il y a aussi une alternative aux Critères Communs : la CSPN - Certification de Sécurité de Premier Niveau. C'est une évaluation du produit en boîte « grise » qui peut même se faire à l'insu du développeur. Nous déterminons une cible mais nous ne pouvons attester de l'environnement de développement du produit. Elle est adaptée aux produits étrangers ou Open Source. Enfin, la qualification elle-même a plusieurs niveaux dans le RGS, en fonction des besoins de sécurité : de l'élémentaire à la renforcée, en passant par la standard. Ainsi, les passeports électroniques vont passer de la qualification standard à la qualification renforcée.

*Retrouvez les vidéos de cette conférence et les supports des interventions sur le web CLUSIF*  
<http://www.clusif.asso.fr/fr/infos/event/#conf090407>.