

## Éditorial

### Insistance tenace !

JOSEPH ILLAND

Fonctionnaire de Sécurité de Défense du CNRS

La revue Sécurité Informatique avait déjà traité du chiffrement dans son édition d'avril 1999 (n° 24), puis en décembre 2005 (n° 55), et de nouveau en décembre 2007 (n° 62).

« Sécurité de l'information » digne héritière de « Sécurité Informatique » consacre encore une fois le présent numéro au chiffrement !

Harcèlement de nos lecteurs ?

Non, plutôt insistance tenace à mettre l'accent sur un sujet majeur et passablement complexe.

La protection des données sensibles, qu'il s'agisse de données scientifiques, techniques, comptables ou de données à caractère personnel, est un impératif qui n'est plus à démontrer.

Les entreprises, les laboratoires de recherche, les administrations regorgent d'informations dont la compromission peut nuire gravement à leurs intérêts, quand ce n'est pas aux intérêts nationaux (technologies innovantes, recherches duales, contrats industriels, données personnelles, données médicales... la liste est longue). Il n'est que de voir au CNRS l'angoisse du directeur d'unité venant nous informer du vol de son portable qui contenait toute la vie scientifique, humaine et financière de son laboratoire, mais aussi quelques mails très privés...

Le principe est clair. On pourra pinailler sur la définition des « données sensibles », leur degré de sensibilité, mobiliser un arsenal de méthodes d'analyses de risques ; il reste que le bon sens est à mobiliser en toute première étape, sur la base, bien sûr, de réflexes de vigilance et de compréhension des enjeux. Il sera temps plus tard de passer à une phase plus analytique pour sérier le niveau de sensibilité, le degré de priorité et chercher des parades adaptées.

Mais attention, l'équation « protection » = « chiffrement » est inexacte. Le chiffrement est une solution de protection parmi d'autres, elle n'est pas la seule et le recours à cette solution est plein d'embûches. On sait bien que le diable se cache dans les détails et en matière de chiffrement, c'est tout l'enfer qui œuvre en catimini.

Parmi ces risques, l'un des plus graves est sans doute la perte de données par incapacité de redéchiffrer. C'est le cas, par exemple, lors de pertes de clé de chiffrement, sans mécanisme de secours ou de recouvrement. L'illusion tranquille d'être sous bonne protection est, pour sa part, bien pernicieuse lorsque le chiffrement mis en place est, de fait, aisément contournable. Les vulnérabilités sont multiples : divulgation de codes personnels, existence de chemins d'accès en clair aux données chiffrées (dans des fichiers temporaires ou même des fichiers effacés, espionnage du poste...)... Les utilisateurs peuvent aussi être désarmés face à des problèmes d'utilisation si un appui technique immédiat fait défaut. Des freins psychologiques peuvent aussi entraîner un rejet d'une

>>>> suite page 6

## Opération « protection des données » en Midi-Pyrénées

Roland Dartiguepeyron

Coordinateur SSI région Midi-Pyrénées

**À l'image des autres structures du CNRS, la délégation régionale Midi-Pyrénées voit se multiplier les postes mobiles et les échanges de données sensibles, avec les laboratoires, les fournisseurs, les partenaires, les diverses parties prenantes mais surtout avec les différentes directions (générale, fonctionnelle, scientifique).**

**Cet article décrit le cheminement de notre réflexion sur la question de la protection des données à partir des études menées par les groupes de travail auxquels j'ai participé. L'expérimentation décrite dans cet article s'inscrit dans la politique de sécurité des systèmes d'information du CNRS qui rappelle notamment la nécessité de protéger les données sensibles.**

### ► Caractéristiques de l'opération

Les données de la délégation régionale sont stockées soit sur un serveur de fichier soit sur des stations de travail, fixes ou mobiles. Un état des lieux rapide montre que ce type de données ne relève pas seulement du domaine de la recherche, de la gestion administrative ou de la valorisation de la recherche mais aussi du management : des informations stratégiques circulent donc dans nos réseaux et sur nos systèmes informatiques. Or, les vulnérabilités des machines que nous utilisons sont importantes. D'abord parce que les accès physiques au poste de travail ne sont pas suffisamment bien protégés. Ensuite parce que l'utilisation des postes mobiles (ainsi que les PDA, « smartphone ») en bureau nomade s'est très largement répandue ces dernières années, cette mobilité augmente les vulnérabilités. Enfin, les applications, les systèmes d'exploitation eux-mêmes, ne sont pas toujours correctement mis à jour. Bref, malgré les enjeux (stratégiques, politiques, image de l'organisme, financiers, ...), la protection des données nous semble souvent insuffisante.

>>>> suite page 2

Lors de la participation de la délégation régionale aux différents groupes de travail sur le chiffrement, nous nous sommes posés la question de la nature des informations à protéger en interne.

### Identification des données, périmètre de l'opération

Le rapport du premier groupe de travail sur l'évaluation du logiciel de chiffrement ZoneCentral préconisait de commencer toute opération de protection des données par les questions suivantes :

- Quelles données protéger ?
- Quelle est leur localisation (lieu de stockage) et leur parcours ?
- Qui est habilité à accéder à ces données ?
- Quelle est leur classification ou leur type ?
- Quel est le type de menace ?
- Quelles sont les conséquences d'une divulgation ?

### Analyse sommaire de risque

Le périmètre de sécurité a été défini au démarrage de l'expérimentation avec l'objectif de protéger les données des ordinateurs portables, conduisant ainsi à restreindre à trois types les menaces à prendre en compte :

- vol matériel : principalement des ordinateurs portables, plus vulnérables à ce type de menace qu'ils soient éteints, en marche ou en veille ;
- écoute sur le réseau (WiFi ou réseau hôte) ;
- perte de données.

Cette appréciation des risques a montré que les données les plus sensibles se trouvaient essentiellement au service « Partenariat et Valorisation » de la recherche, mais elle a montré aussi qu'il en existait également dans d'autres services, comme par exemple, les données « à caractère personnel » que nous avons l'obligation de protéger (pas seulement en confidentialité !). Par ailleurs, la quasi-totalité des ordinateurs portables contiennent des données sensibles. Protéger ces matériels en cas de vol a donc été considéré comme prioritaire et notamment les portables de la déléguée régionale et du responsable du service partenariat-valorisation.

### ► Solution technique retenue

#### Choix du logiciel

Lors du premier groupe de travail, une réflexion et une évaluation des solutions de

chiffrement a été menée à travers plusieurs critères qui ont été définis puis les solutions existantes évaluées. Ces critères sont aussi bien techniques qu'organisationnels afin d'être en adéquation avec l'organisation de notre organisme. On peut les rappeler brièvement ici :

- Les choix et la robustesse des algorithmes cryptographiques
- L'ergonomie et usage
- Le chiffrement des données en vue de leur transmission
- Chiffrement des fichiers temporaires et du « swap »
- L'utilisation d'autres programmes de sécurité
- La gestion des clés d'accès
- Le recouvrement des données
- Les systèmes de fichiers supportés
- Le prix
- Critères liés à l'environnement : facilité de déploiement et d'organisation.

Lors d'un premier groupe de travail auquel participaient deux délégations régionales et plusieurs unités de recherche<sup>1</sup>, la délégation Midi-Pyrénées a travaillé à l'évaluation d'une solution de chiffrement commerciale. Le produit qui répondait le mieux aux critères ci-dessus s'est révélé être « ZoneCentral » de l'éditeur « Prim'X ». L'objectif de ce groupe de travail était de produire des recommandations générales sur le chiffrement mais aussi de proposer des recommandations spécifiques à ce produit. Cette opération a permis de définir un certain nombre de recommandations organisationnelles et techniques détaillées plus loin.

Un deuxième groupe de travail a ensuite expérimenté ce même produit dans des environnements différents<sup>2</sup>. Sept laboratoires de Midi-Pyrénées ont participé à ce déploiement « in vivo ». Les recommandations du précédent groupe de travail ont été mises en place, éventuellement ajustées aux environnements et enfin testées et validées. Des échanges sécurisés entre les sites ont aussi été expérimentés avec succès ainsi que des opérations de recouvrement. Le bilan est positif et fait ressortir un net besoin dans les structures participantes. L'aspect organisationnel a été mis en avant en particulier pour les accès de

recouvrement des données, point essentiel dans la pérennité des données.

Dans le cycle de vie des données à protéger, des échanges vers l'extérieur sont nécessaires. Dans la grande majorité des cas, ces données transitent en tant que pièces jointes à un courrier électronique. La confidentialité n'est donc plus assurée. Une fonctionnalité de ZoneCentral permet de répondre à ce besoin. En effet, il est possible de créer des archives chiffrées. Ces « conteneurs » ont leur propre liste d'accès ne comprenant que les accès des personnes habilitées à lire les documents. Un module gratuit aux fonctionnalités bridées est disponible gratuitement pour les destinataires, leur permettant de lire le contenu chiffré mais aussi de le modifier ou d'ajouter des documents. Ce produit de chiffrement s'adressant seulement au monde Windows, pour l'instant du moins, le problème de communication reste entier pour les autres systèmes d'exploitation. Un complément est l'utilisation de courriers électroniques chiffrés grâce à un certificat numérique (S/Mime). Ceci pose un nouveau problème organisationnel si les documents sont gardés chiffrés dans le client de messagerie. En effet, au renouvellement du certificat, les documents ne pourront plus être déchiffrés ce qui ne garantit pas la pérennité des données.

Un autre aspect important est la gestion des médias amovibles (clé usb, ...). Le produit gère ce type de média en permettant ou non l'écriture en clair (via paramétrage de stratégies).

Les versions récentes de ZoneCentral intègrent la gestion de consignes de chiffrement. Celles-ci permettent à l'administrateur de définir finement ce qui doit être chiffré sur le poste, laissé en clair ou choisi par l'utilisateur. À chaque démarrage du poste, les consignes de chiffrement sont vérifiées par le logiciel et appliquées suivant les directives de l'administrateur. Cette fonctionnalité est intéressante car elle permet de fixer dans le temps une politique de chiffrement du poste client mais surtout d'éviter l'érosion de la politique de protection.

**Depuis peu, « ZoneCentral » a reçu la certification Critères Communs (ISO/IEC 15408:2005) au niveau EAL2+<sup>3</sup> et obtenu la Qualification Standard de la DCSSI. La**

1. [https://www.urec.cnrs.fr/IMG/pdf/secu.corres.InfoT.Crypto.Rapport-Groupe\\_Travail.pdf](https://www.urec.cnrs.fr/IMG/pdf/secu.corres.InfoT.Crypto.Rapport-Groupe_Travail.pdf)

2. <https://extranet.dr14.cnrs.fr/SSI/Documentation/chiffrement/deploiementchiffrementDR14.pdf>

3. Centre d'évaluation : Oppida, rapport de certification et cible de sécurité disponible sur : [http://www.ssi.gouv.fr/archive/fr/confiance/certificats/certificat2008\\_46.html](http://www.ssi.gouv.fr/archive/fr/confiance/certificats/certificat2008_46.html)

## Une expérience de sécurisation des échanges

Durant le mois de novembre 2008, nous nous sommes intéressés à la sécurisation des échanges de données sensibles. Notre but était de sécuriser les échanges entre le service Partenariat et Valorisation de la délégation et des laboratoires grâce aux conteneurs ZoneCentral. Pour quatre laboratoires de Midi-Pyrénées, correspondant à un nombre important d'échanges de données sensibles, un correspondant valorisation est nommé dans le laboratoire. Cette opération a débuté dans une première unité après une réunion d'information réunissant les différents intervenants : gestionnaires et chargés d'affaires SPV, correspondant valorisation du laboratoire, administrateur(s) du laboratoire et de la délégation où nous avons recommandé l'installation d'un produit de chiffrement par les informaticiens du laboratoire sur les postes des « correspondants valorisation ». Cette première phase nous a permis de valider diverses procédures. Quand cela fut fait, pour pousser plus loin l'expérimentation, nous avons ajouté trois autres laboratoires parmi les plus importants de la délégation (il y a trois « correspondants valorisation » dans l'un de ceux-ci !) et utilisé des conteneurs pour transmettre des données sensibles à une direction fonctionnelle du siège (Direction des Partenariats Industriels).

La procédure appliquée aux chargés d'affaires SPV est la suivante :

1°) Les certificats X509 des « correspondants valorisation » sont mis à disposition des utilisateurs sur notre site. Un premier conteneur vide est créé avec une liste d'accès spécifique à chaque laboratoire destinataire contenant donc le (ou les) « correspondant valorisation », l'ensemble du SPV.

2°) Les accès obligatoires de recouvrement sont ajoutés automatiquement. Pour l'envoi de données sensibles, le gestionnaire ajoute à ce conteneur les documents et le joint à un courrier électronique signé numériquement.

3°) À réception, le correspondant ouvre le conteneur et déplace les documents dans son dossier coffre-fort. Pour l'envoi suivant, le conteneur est vidé puis mis à jour. Cette pratique évite de reconstruire les listes d'accès pour chaque envoi.

Elle a été adoptée sans difficulté par les utilisateurs qui ont même surnommé le conteneur « la valise diplomatique ».

Il a été jugé préférable de renouveler tous les certificats des utilisateurs du SPV de façon à faire se correspondre au mieux leur date d'échéance. Ainsi, les listes d'accès pourront être mises à jour globalement et non au coup par coup à chaque certificat périmé.

La sensibilisation des utilisateurs sur les contraintes du chiffrement (en particulier, la création de fichiers temporaires dans des zones non protégées, le risque de perte de données lorsque les clés d'accès arrivent à échéance, etc.) et de l'utilisation des conteneurs (un conteneur ouvert n'est plus protégé, il a un caractère éphémère, etc.) a été entrepris dès le départ : les outils de chiffrement mal utilisés n'apportent qu'une illusion de protection.

Il faut aussi informer : les informations en ligne sur notre site sécurisé ont été complétées afin de mieux répondre aux différentes questions techniques courantes. On peut trouver aussi parmi ces informations, les certificats X509 des utilisateurs et une liste d'accès contenant tous les membres du service SPV (pour permettre aux laboratoires de les ajouter aux conteneurs envoyés à la délégation). D'un point de vue organisationnel et bien que chaque chargé d'affaires du service Partenariat Valorisation traite un portefeuille de laboratoires, une telle liste a son intérêt durant les vacances où il faut assurer la continuité de service.

L'échange de « valises diplomatiques » entre le service partenariat-valorisation et les correspondants valorisation des 4 laboratoires (LAAS, LCC, CEMES, IPBS) fonctionne ainsi de façon satisfaisante. Pour ceux qui ne disposent pas d'un système Windows nous leur proposons de communiquer en S-Mime.

Cette procédure fonctionne jusqu'à maintenant de façon satisfaisante car les acteurs du service SPV ont compris notre message et sensibilisent à leur tour leurs interlocuteurs sur la nécessité de protéger les données sensibles (négociation amont de contrats, déclarations d'inventions,...). Cette sensibilisation de l'utilisateur final – éternel maillon faible – est essentielle pour la solidité de la chaîne complète.

La réussite de l'opération doit beaucoup au soutien des hiérarchies, tant dans la délégation régionale que dans les unités.

certification, lourde et coûteuse pour un éditeur, apporte une assurance de sécurité supplémentaire à l'utilisateur qui doit en conséquence encourager cette démarche.

## Coût de l'opération

Le coût financier pour l'acquisition des licences nécessaires, dans le cadre des accords logiciels négociés par le LOGCRI, est très abordable pour une Unité. Il inclut les mises à jour logicielles pendant 5 ans et l'accès au support de l'éditeur.

## Mode de chiffrement retenu

Deux types de fonctionnalités sont proposés (qui peuvent être utilisés simultanément pour cumuler les avantages de l'une et de l'autre).

1. Tout d'abord, le chiffrement au niveau du répertoire permet de chiffrer à la volée tous les fichiers enregistrés et de déchiffrer de la même manière ceux qui sont ouverts légitimement. Les données sont donc protégées même lorsque la machine est allumée tant qu'on n'a pas ouvert un répertoire protégé.
2. Ensuite, le chiffrement de surface agissant au niveau d'une partition ou d'un disque complet assurant une protection en cas de vol de la machine. Cette solution est simple à mettre en œuvre et transparente pour les utilisateurs mais l'authentification étant effectuée à l'ouverture de la session ou au premier accès à une partition chiffrée, il n'y a plus de protection une fois celle-ci effectuée.

Le chiffrement par répertoire et la possibilité de l'étendre au poste complet présente l'avantage d'être transparent sans nécessité de réorganiser les partitions. L'impact sur les habitudes de travail des utilisateurs est presque inexistant. La possibilité d'étendre le chiffrement à l'ensemble des données stockées sur la machine apporte une protection – transparente pour l'utilisateur – des fichiers temporaires générés par le système. L'application gère une liste d'exceptions qui permet de ne pas chiffrer certains fichiers système. Cette fonctionnalité introduit la notion de « droit d'en connaître ». Cette notion est parfois négligée mais est essentielle dans le processus de protection des données. En effet, un poste contenant des données protégées peut tomber en panne et donc nécessiter l'intervention d'une personne non habilitée à lire les données mais ayant des droits de lecture étendus. Lorsque le système n'est pas entièrement chiffré, aucune clé d'accès

## La suite ...

Durant le dernier trimestre 2009, une formation au Système de Management des Systèmes d'Information sera organisée à la délégation à l'intention notamment des coordinateurs régionaux de sécurité des systèmes d'information (CRSSI), des chargés de sécurité des systèmes d'information (CSSI), internes et pour quelques unités, des responsables SSI d'autres tutelles, notamment des Universités.

Une autre formation suivra courant 2010. Ces formations nous permettront d'appréhender la problématique liée à la mise en place de la politique de sécurité des systèmes d'infor-

mation pour une Unité et notamment l'aspect « analyse de risque ». L'affinement de ce critère par rapport à notre approche devrait nous permettre de compléter le périmètre de l'information à protéger et nous donnera les pistes à suivre pour continuer à déployer en interne cette technologie. Les CSSI des Unités auront également en leur possession les arguments pour commencer à mettre en place une protection des données sensibles et pour échanger de façon sécurisée avec la délégation ou d'autres partenaires (notamment industriels) des informations sensibles.

ne sera nécessaire à l'équipe informatique ou au prestataire extérieur. Ainsi les interventions sont donc possibles sans donner accès aux données confidentielles.

### Modalités de déploiement

Les premiers postes nomades d'utilisateurs ont été déployés en conformité avec une architecture technique et organisationnelle quasi définitive. Les postes clients étant intégrés à un Active Directory, le paramétrage complet de ZoneCentral est effectué via stratégies de domaine. Le modèle d'administration fourni avec le logiciel se révèle être extrêmement complet.

Le paramétrage du logiciel s'exprime par des « polices »<sup>4</sup> référencées « Pxxx » dans l'outil. Nous ne rentrerons pas dans les détails mais citerons les principales fonctionnalités mises en place :

- Empêcher : les modifications locales, d'utiliser le magasin de stockage des certificats de Windows, d'utiliser les mots de passe pour accéder à des dossiers chiffrés mais pas pour des conteneurs.
- Imposer : Copie des listes d'accès personnelles sur un serveur réseau partagé, une liste de recouvrement dans les listes d'accès, un plan de chiffrement préalablement établi.
- Contrôle de la robustesse de la passphrase qui protège la clé.
- Comportement du logiciel face aux média amovibles

On trouvera sur notre extranet<sup>5</sup> un modèle de paramétrage de ZoneCentral qui reprend

4. Politique de sécurité

5. <https://extranet.dr14.cnrs.fr>

certificats ou mots de passe) pour les textes qui ont besoin d'être transmis avec un bon niveau de sécurité (c'est-à-dire suffisant pour des documents non classifiés).

### Répartition des responsabilités

Cette opération a été pilotée par le responsable des Systèmes d'Information (RSI) aidé par un agent du service des systèmes d'information et soutenue par la Déléguee Régionale. La sensibilisation, l'assistance technique, le conseil sont assurés par le RSI et un agent du service. Plusieurs laboratoires dont certains ont comme responsable informatique les coordinateurs régionaux de sécurité ont participé aux groupes de travail.

### Le choix de ZoneCentral

Nous avons vu précédemment que le choix de ZoneCentral a été fait d'abord pour la qualité de ce logiciel, mais une autre raison a été aussi déterminante : il peut chiffrer avec les certificats numériques générés par notre IGC et offrir une gestion avancée du recouvrement au sein de ses listes d'accès. D'autres fonctionnalités de ce produit nous ont paru encore utiles. Par exemple :

- le mécanisme de secours permettant à un administrateur de communiquer par téléphone un mot de passe pour ouvrir une zone protégée.
- La possibilité de transmettre des conteneurs chiffrés : à partir de l'annuaire LDAP de l'IGC un utilisateur peut télécharger le certificat X509 de son correspondant afin de l'intégrer à la liste d'accès du conteneur.

### Procédure de recouvrement

« On ne sort jamais d'un problème que par un autre problème ». S'il était besoin d'illustrer cette fameuse loi de la systémique, le chiffrement y suffirait à lui seul. Par exemple :

- un incident en écriture sur un disque dur chiffré peut entraîner une catastrophe irréversible pour les données qu'on voulait protéger ;
- la perte de la clé privée (ou l'oubli de la passphrase) a pour conséquence de se trouver dans l'impossibilité de récupérer ses précieuses données.

Ainsi le chiffrement, peut sur le plan de la disponibilité, aggraver le risque plus qu'il ne le diminuait sur celui de la confidentialité. Par ailleurs, une institution comme la nôtre doit pouvoir assurer la continuité du service en cas d'absence ou de départ du propriétaire des données. Elle doit aussi pouvoir

répondre à des exigences légales comme, par exemple, une requête judiciaire. La sauvegarde de ses données est indispensable (elle est effectuée chiffrée de bout en bout) ainsi que le recouvrement des clés. Le problème, purement technique au début, devient organisationnel !

La chance du CNRS est de s'être doté très tôt d'une infrastructure de gestion de clé (IGC) et d'une organisation d'autorités d'enregistrement qui permettent de distribuer des certificats de confiance. Cette organisation a eu le temps de se roder depuis sa mise en place au début des années 2000 et, pour une fraction significative du personnel, l'utilisation de certificats numériques X509 n'est plus une nouveauté. Le choix d'utiliser l'IGC du CNRS et l'organisation des autorités d'enregistrement s'est donc naturellement imposée simplifiant ainsi considérablement les contraintes organisationnelles, en particulier pour le recouvrement.

Nous avons choisi une durée de validité de deux ans pour ces certificats (cinq ans pour les certificats de recouvrement) ; ils peuvent être révoqués à n'importe quel moment si un problème de sécurité a été rencontré ou si le propriétaire quitte sa structure ou l'organisme. Ils sont associés à une clé privée, stockés au format pkcs12 et protégés par une passphrase<sup>6</sup>... ce qui ne peut se faire sans information et sensibilisation du personnel.

En l'occurrence, la qualité de la procédure de recouvrement, garantie par des tests, est essentielle. Aussi, les accès de recouvrement sont-ils imposés aux utilisateurs et clairement indiqués dans les listes d'accès personnelles (non-masquage des accès obligatoires). Un certificat nominatif particulier (d'une durée de validité de cinq ans), généré par l'IGC du CNRS, est attribué aux agents de recouvrement qui ont été habilités<sup>7</sup> (au moins un agent dans chaque unité). Pour des raisons de sécurité évidentes, les certificats et leur clé privée sont stockés au format PKCS12 sur une clé USB rangée dans le coffre fort du service Système Information avec leurs passphrases sur un autre support. Pour les accès utilisateurs, une liste personnelle est utilisée et pointée vers un certificat personnel CNRS-standard. Ce certificat est stocké lui aussi au format

PKCS12 et protégé par une passphrase solide (voir les critères de robustesse, note 6). Les certificats CNRS-Standard ont maintenant une durée de validité de 2 ans. Ceci espace les interventions pour le renouvellement des clés d'accès.

Bien qu'un accès de secours soit prévu dans le produit, toujours dans le but d'optimiser le recouvrement des données chiffrées, les listes d'accès personnelles doivent être stockées dans un dossier partagé d'un serveur. Elles ne sont modifiables que par leur propriétaire.

**Il est important de noter que l'utilisation de ZoneCentral permet de mettre en œuvre une architecture de recouvrement extrêmement robuste puisque, outre le recouvrement qui doit être assuré au niveau local, on met en place un recouvrement régional (un troisième niveau de recouvrement n'est pas justifié).**

#### ► Déroulement de l'opération

Le déploiement du produit ZoneCentral à la délégation régionale s'est déroulé en plusieurs étapes. Tout d'abord, le logiciel a été testé sur les postes du SSI lors du premier groupe de travail afin de l'évaluer dans notre environnement et d'acquérir l'expérience technique avant la mise en place d'un support utilisateur. Puis plusieurs points ont été testés comme le paramétrage de l'application, le recouvrement des données, la sauvegarde des données chiffrées sur serveur puis sur support amovible (DLT, DAT) via un logiciel de sauvegarde spécialisé et la restauration de celle-ci sous forme chiffrée.

#### Choix de mise en œuvre

Dans notre organisation interne, les données professionnelles des utilisateurs sont stockées dans un répertoire bien précis. La messagerie électronique contient aussi des données à protéger et est, elle aussi, stockée dans un dossier particulier. Dans un premier temps, ces deux dossiers ont été chiffrés ainsi que le répertoire correspondant au profil de l'utilisateur (celui-ci est chiffré car certaines applications y créent des répertoires ou des fichiers temporaires qui sont autant de failles dans la protection des données s'ils ne sont pas eux aussi chiffrés). Par défaut et dès l'installation de ZoneCentral, le fichier d'échange du système (swap) est lui aussi chiffré. Deux autres outils sont ajoutés par ce logiciel : un effacement sécurisé des fichiers par surcharge et un pilote de clavier propriétaire afin de contrer un éventuel logiciel espion

de type keylogger. Cette organisation en répertoires « coffre fort » donne de bons résultats en protégeant « à minima » le poste client, mais les systèmes se complexifiant, elle devient insuffisante. En effet, des éléments peuvent être oubliés comme le répertoire de stockage des données hors connexion du système (répertoire CSC). Une évolution logique de cette organisation que nous avons donc appliquée est de chiffrer la partition système ou même des disques complets. Lors de cette extension du chiffrement, ZoneCentral utilise une liste de fichiers et d'extensions (paramétrable) à ne pas traiter afin de ne pas chiffrer entièrement le système d'exploitation. D'autre part, le produit est capable de travailler dans une architecture client-serveur où les fichiers de données se trouvent sur un partage réseau. Ce lieu de stockage peut être chiffré. Le déchiffrement des données s'effectuant sur le poste utilisateur, les données circulent donc sous forme chiffrée sur le réseau.

#### Périmètre

Les ordinateurs portables ont été traités en priorité ainsi que tous les postes (mobiles ou non) du service Partenariat et Valorisation. Le déploiement de ZoneCentral a été effectué poste par poste et non par déploiement automatique (lot MSI) qui est possible.

#### Mesures de sensibilisation et d'accompagnement

Avant ce déploiement, une réunion d'information réunissant les utilisateurs impactés a été effectuée. À cette occasion, la PSSI, la sensibilisation au traitement des données sensibles et la finalité du chiffrement ont été largement abordées. Un temps important fut aussi consacré aux questions-réponses et a permis d'éclairer les utilisateurs sur certains points obscurs ou sur la sécurisation de certaines de leurs habitudes de travail. L'installation poste par poste avec participation de l'utilisateur a permis de lui apporter une aide technique, des conseils (comme le choix d'une passphrase solide) et surtout un accompagnement personnalisé dans la prise en main du produit.

Cette première étape de sensibilisation était couplée avec notre participation au second groupe de travail dont l'objectif était de tester in vivo le déploiement d'une solution de chiffrement. Grâce à notre participation au groupe de travail précédent, nous

6. Au moins 10 caractères alphanumériques et caractères spéciaux et 12 recommandés

7. Dans les faits, ce sont les mêmes que ceux qui sont « autorités d'enregistrement » dans la délégation.

avions déjà identifié des pré-requis organisationnels et techniques.

### Action de formation menée

Il nous a semblé indispensable d'accompagner le déploiement en proposant une formation technique sur le produit à destination des Administrateurs Système et Réseau (et/ou aux autorités de recouvrement). Cette formation a été effectuée par l'éditeur du logiciel.

### Moyens techniques d'appui

Une assistance a également été mise en place via la mise en ligne sur notre site extranet sécurisé<sup>8</sup> d'informations organisationnelles et techniques à destination des Administrateurs Système et Réseau. D'autre part, les demandes de support de premier niveau sont traitées par le service Système Information. Le but est qu'une fois le déploiement démarré, les utilisateurs finaux aient toujours un appui technique à disposition immédiate.

### Les leçons

Depuis trois ans dont douze mois d'utilisation étendue, nous pouvons dresser un bilan intermédiaire positif pour ce déploiement interne. En effet, le produit est très stable, aucune incompatibilité avec une autre application n'a été constatée. Mais surtout l'impact sur les habitudes de travail des utilisateurs est minime. Les renouvellements de certificat (et donc renouvellement de la clé d'accès) dans les listes d'accès personnelles ont été effectués sans difficulté. ZoneCentral se révèle ergonomique et simple au point qu'un utilisateur même non averti est capable d'effectuer seul ce changement. Nous avons eu à restaurer à plusieurs reprises des données chiffrées sauvegardées (boîtes mail en particulier) et aucune perte de donnée n'est à déplorer.

8. <https://extranet.dr14.cnrs.fr>

Le seul point faible que nous avons noté dans la version actuelle du logiciel concerne la protection des données lors de l'hibernation (ou la mise en veille prolongée) d'une machine.

### ► En conclusion

Le but initial était de protéger les postes itinérants, cibles principales de pertes ou de vols de données. Le déploiement de cette solution de chiffrement nous a permis de sécuriser la détention de données sensibles. Dans notre environnement homogène, le logiciel ZoneCentral se révèle adapté, stable, ergonomique et grandement configurable via stratégies de domaine active directory ou locales. Les possibilités sont en effet très étendues et permettent une gestion fine des différents paramètres logiciels. Plus important, les points jugés importants au déploiement d'une solution de chiffrement sont présents, comme la gestion avancée du recouvrement, sont bien pris en compte par cet outil. L'ergonomie et les performances ont fait qu'il a été bien accepté par les utilisateurs.

Dans le cycle de vie des données sensibles, le stockage est un aspect mais les échanges vers des correspondants externes sont fréquents et souvent indispensables. La possibilité d'échanger des conteneurs chiffrés est une valeur ajoutée importante que nous explorons depuis quelques mois. Néanmoins, à ce jour, ZoneCentral n'est pas disponible pour d'autres plate-formes que Windows. Ceci nous amène à expérimenter de façon complémentaire les échanges par messages chiffrés via S/Mime avec quelques unités.

Au travers de notre participation aux différents groupes de travail et à cette expérimentation, il ressort très clairement que l'aspect organisationnel est le paramètre clé dans le déploiement d'une solution de chiffrement.

[roland.dartiguepeyron@dr14.cnrs.fr](mailto:roland.dartiguepeyron@dr14.cnrs.fr)

### »» suite de l'Éditorial, page 1

solution de chiffrement imposée hâtivement sans démarche d'accompagnement.

Le CNRS a, dès l'origine, opté pour une démarche mesurée et prudente, fondée sur l'expérimentation et la consolidation progressive des acquis.

Disposer d'expériences significatives, dans des situations professionnelles variées, et selon des déploiements différenciés (logiciels et politiques d'implémentation), c'est pouvoir :

- 1) dégager les meilleures pratiques ;
- 2) disposer de « références » incontestables pour formuler des recommandations techniques et surtout organisationnelles et aussi sensibiliser, convaincre et adapter les moyens de soutien (sensibilisation, formation, guides...).

Une dizaine d'expériences de chiffrement sont actuellement en cours dans les laboratoires du CNRS, ce qui n'interdit pas, loin s'en faut, de garder un œil sur les expériences de chiffrement menées ailleurs, dans un bon souci d'analyse comparative.

Les leçons sont encore loin d'en être tirées. Mais le travail engagé avec passion et ténacité par les équipes de la délégation régionale de Midi-Pyrénées du CNRS offre sans doute aujourd'hui la référence la plus achevée et la plus riche d'enseignements.

Cette référence a bien sûr ses limites, elle ne concerne qu'un seul logiciel (ZoneCentral), un environnement informatique unique (Windows) et un contexte plutôt administratif.

Sécurité de l'Information consacre l'ensemble du présent bulletin à cette expérience, décrite en détail par les responsables SSI de la délégation.

Le débat n'est pas clos et d'autres expériences sont en cours, dont on reparlera.

L'enjeu de la protection des données scientifiques, techniques, commerciales ou personnelles... vaut qu'on y revienne sans repos et sans répit.

[joseph.illand@cnrs-dir.fr](mailto:joseph.illand@cnrs-dir.fr)

## En bref : La DCSSI est morte, vive l'ANSSI !

La nouvelle Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), a été officiellement créée par un décret publié au Journal Officiel du mercredi 8 juillet 2009. Son existence vise à renforcer les moyens de la lutte contre les attaques informatiques venant d'États ou de groupes criminels, l'une

des priorités stratégiques définie par le Livre Blanc de la défense nationale. L'agence, placée sous l'autorité du Secrétariat Général de la Défense Nationale, rattaché au premier ministre, se verra allouer un budget de 90 millions d'euros. On peut visiter son site Internet à l'adresse [www.anssi.gouv.fr](http://www.anssi.gouv.fr)

### SÉCURITÉ DE L'INFORMATION

**Sujets traités :** tout ce qui concerne la sécurité informatique. Gratuit.  
**Périodicité :** 4 numéros par an.  
**Lectorat :** toutes les formations CNRS.

**Responsable de la publication :**  
Joseph Illand

Fonctionnaire de Sécurité de Défense  
Centre national de la recherche scientifique  
3, rue Michel-Ange, 75794 Paris cedex 16  
Tél. : 01 44 96 41 88  
Courriel : [joseph.illand@cnrs-dir.fr](mailto:joseph.illand@cnrs-dir.fr)  
<http://www.sg.cnrs.fr/fsd>

**Rédacteur en chef :**

Robert Longeon  
Chargé de mission SSI du CNRS  
Courriel : [robert.longeon@cnrs-dir.fr](mailto:robert.longeon@cnrs-dir.fr)

**Impression :** Bialec, Nancy (France) - D.L. n° 72135  
ISSN 1257-8819

La reproduction totale ou partielle des articles est autorisée sous réserve de mention d'origine.