

Un service de coffres forts électroniques

Serge Aumont

RSSI / Université de Rennes 1
Campus Beaulieu
35042 Rennes Cedex

Résumé

Le nombre de mots de passe gérés et partagés par les personnels d'une DSI est très élevé. Au sein de la DSI de l'université de Rennes 1, plusieurs centaines de mots de passe de ce type sont utilisés. Ce sont les classiques mots de passe "root" des systèmes, ceux des bases de données, ceux de services extérieurs, etc.

Les enjeux de sécurité d'une gestion globale des mots de passe partagés sont très élevés, c'est probablement pour cette raison qu'ils figurent encore dans des classeurs ou sur des bostols et sont rangés, dans le meilleur des cas, dans un coffre dont la clé est cachée dans un lieu sûr connu de tous... Passer à un service homogène de gestion des mots de passe fait peser sur ceux-ci des risques nouveaux : compromission généralisée, indisponibilité lors de la mise en œuvre du PRA (Plan de Reprise d'Activité). Ne pas le faire est probablement pire.

Nous décrivons dans cet article les choix faits par la DSI de l'université de Rennes 1 pour cette gestion de mots de passe et l'offre de service qui en a été déclinée pour nos laboratoires.

1 Constats sur une gestion empirique des mots de passe

Les équipes de la DSI de l'Université de Rennes 1 manipulent, outre les mots de passe personnels de chacun, un grand nombre de mots de passe partagés. Ce sont, bien entendu, les mots de passe "root" des systèmes, ceux de certains composants applicatifs tels que les nombreux connecteurs aux bases de données Oracle et MySQL, ceux des comptes administrateurs des équipements réseaux ou encore les comptes permettant d'accéder à l'extranet de quelques fournisseurs pour utiliser leurs outils d'assistance. Au total, plus de 300 mots de passe sont ainsi partagés par les personnels.

Certaines équipes laissaient la gestion de ces mots de passe à la discrétion de chacun. D'autres avaient tenté de les centraliser sur des supports papier, dans des classeurs entreposés dans un coffre fort. Ces pratiques présentent d'innombrables inconvénients parmi lesquels on peut citer :

- les classeurs imposent de se déplacer physiquement pour y accéder. Au fil des années, certains mots de passe n'y ont pas été maintenus ;
- le support papier fait que presque aucun formalisme n'existe pour leur notation. Il est parfois difficile d'identifier à quel service correspond exactement une entrée de ces classeurs ;
- les coffres forts dans lesquels sont stockés ces classeurs sont en nombre limité ;
- l'absence d'interface utilisateur pour manipuler les mots de passe oblige à les saisir au clavier. Cela conduit à choisir des mots de passe faciles à retenir et/ou à taper, donc peu résistants. Ainsi, certains mots de passe sont construits avec des logiques déterministes si bien que la connaissance de l'un d'entre eux permet d'en déduire un grand nombre similaire (mot de passe avec un élément variant extrait du nom du serveur) ;
- pour mettre « au propre » les tableaux de mots de passe, ceux-ci ont parfois été imprimés depuis un tableur. Nous ne savons rien de ce que sont devenus les fichiers utilisés à cette fin ;

- plusieurs agents de la DSI ont choisi une gestion alternative des mots de passe, tant et si bien que la complétude des classeurs n'est absolument pas garantie. Il existe au moins un cas où le redémarrage d'un service a été bloqué en attente du retour d'un collègue seul détenteur connu d'un certain mot de passe ;
- en pratique, la lourdeur de l'outil papier, en particulier pour le partage entre plusieurs utilisateurs, et surtout l'absence de documentation sur la procédure de renouvellement conduit à ne pas renouveler les mots de passe aussi souvent qu'il le faudrait. Certains mots de passe sont vraiment très anciens (plus de 15 ans). En effet, aucune documentation n'existe sur la procédure de changement de chaque mot de passe, si bien que l'idée même de devoir renouveler certains mots de passe fait craindre des conséquences inattendues. Or comment documenter le processus de changement de mot de passe sans avoir jamais tenté cette opération ? Dans ces conditions, combien d'anciens agents de la DSI (stagiaires, contractuels, retraités, agents affectés dans un autre service...) disposent encore « des clés du camion » ?

Pourtant, cette gestion hétérogène et bien imparfaite n'a pas que des inconvénients. S'il est probable que des personnes aient eu la possibilité d'accès non autorisés aux mots de passe, une compromission généralisée est à l'inverse très difficilement imaginable. De même, si nous avons rencontré le cas d'une indisponibilité de mots de passe, celle-ci est restée limitée dans le temps (temps d'absence d'une personne) et elle ne peut concerner qu'un nombre très restreint de mots de passe.

En cherchant des solutions pour corriger les faiblesses constatées d'une gestion empirique des mots de passe, on arrive inévitablement à en concevoir une gestion centralisée. On doit alors évaluer les risques d'une compromission généralisée (un petit malin publie l'ensemble des mots de passe de la DSI sur internet, un cauchemar !) et ceux d'une indisponibilité totale de ceux-ci (le conteneur de mots de passe se trouve sur un serveur qu'on ne sait pas redémarrer faute de connaître un des mots de passe justement stocké dans ce conteneur...).

2 Objectifs d'un système de gestion global des mots de passe

La description de la situation de départ fixe naturellement les principaux objectifs du système de gestion à mettre en place :

- le système proposé doit être général et convenir à l'ensemble des équipes de la DSI. Pour combattre l'hétérogénéité des pratiques, l'outil qui sera le support d'une politique nouvelle pour les mots de passe partagés doit être adopté par tous. Il doit donc être séduisant car ce qui est demandé remet en cause des pratiques anciennes. Les résistances à ce changement existeront de toutes les façons. Aussi, elles ne doivent pas être renforcées en s'appuyant sur des faiblesses objectives des outils mis en place. L'ergonomie des outils doit apporter dans leurs domaines un confort que beaucoup ne connaissent pas encore ;
- bien entendu, la solidité du service doit être irréprochable. Aucun soupçon n'est acceptable sur ce point ;
- la solution doit rester disponible même en cas de sinistre majeur touchant l'ensemble des infrastructures. Elle comportera donc des dispositions permettant de récupérer l'ensemble des mots de passe depuis un poste démarré sans accès réseau et sans dépendance vis-à-vis du réseau ni d'aucun serveur ;
- les conteneurs de mots de passe doivent être partageables, de sorte que chaque mot de passe ne soit noté qu'une fois ;
- les tentatives d'écritures concurrentes ne doivent pas conduire à des pertes d'informations ou à des inconsistances. Il doit être possible de constituer plusieurs conteneurs dont les clés d'accès seront distribuées en fonction du besoin d'en connaître.

De telles exigences sont conséquentes, aussi un développement maison est exclu car il demanderait beaucoup de ressources. De même, il est même difficilement imaginable de mettre en place une telle plateforme pour les besoins stricts de la DSI car les efforts de celle-ci doivent être tournés prioritairement vers les utilisateurs de l'université. Les objectifs mentionnés sont des réponses à des besoins génériques qui existent aussi dans les laboratoires de l'université. Le système choisi, s'il répond à ces objectifs pourra entre autre être utilisé pour le service de recouvrement des conventions de chiffrement, fonctionnalité requise dans le contexte du chiffrement des disques durs des postes de travail que demande le CNRS pour ses laboratoires¹.

¹ Note [Not11Y159DSI](#) de M. Alain Fuchs du 16/01/2011 rappelée le 21/12/2012

La politique de gestion de ces mots de passe doit être auditable. Ainsi, l'amélioration des pratiques doit pouvoir être constatée et les manquements aux règles définies repérés afin de les corriger. En particulier, on doit pouvoir mesurer l'ancienneté des mots de passe (le non renouvellement de ceux-ci étant une des mauvaises pratiques constatées les plus inquiétantes). L'outil doit permettre de documenter la procédure de renouvellement de chaque mot de passe (liste des scripts et fichiers de configuration pour lesquels une intervention est requise, liste des tests pour vérifier que le changement a bien été répercuté partout, etc.). À défaut de pouvoir analyser automatiquement le contenu de cette documentation, son absence doit être repérable. Enfin, chaque accès en lecture ou en écriture doit être journalisé.

3 Le produit retenu

Nous avons d'abord recherché une solution web nous dispensant de déployer une application sur les postes clients. Citons [webKeePass²](#) que nous avons testé. Pour des raisons de sécurité assez évidentes, le chiffrement et le déchiffrement sont assurés sur le poste client via une applet JAVA (et non sur le serveur ce qui entrainerait des risques importants dans le contexte du navigateur). Toutefois, cette architecture présente de nombreux inconvénients dans notre contexte : sa sécurité dépend beaucoup trop de celle des postes de travail. En outre, l'ergonomie ne peut être qu'en retrait (exemple : absence de fonction de saisie automatique des mots de passe vers les applications qui les réclament).

[KeePass³](#) est un produit dédié au stockage de mots de passe. Il est déjà utilisé par quelques personnes au sein de la DSI de l'université. La version 2 de KeePass a reçu la "[Certification de sécurité de Premier Niveau](#)" (CSPN) de l'ANSSI⁴. KeePass est un logiciel libre et multiplateforme. Même si seule une version pour Windows a fait l'objet d'une certification, l'aspect multiplateforme est un atout important puisque l'outil doit être utilisé par l'ensemble des agents de la DSI.

KeePass permet de gérer des coffres-forts de mots de passe de manière sécurisée et chiffrée. Tous les mots de passe sont stockés dans une base de données, verrouillée avec une clé maîtresse ou un fichier clé. Il suffit de se rappeler du mot de passe maître ou de sélectionner le fichier clé pour accéder à la base de données. L'objet même du logiciel correspond aux objectifs que nous nous fixons (ce n'est pas une adaptation plus ou moins imparfaite d'un produit pensé pour d'autres usages). Cette spécialisation est rassurante du point de vue de la sécurité ; ainsi, par exemple, le rapport de certification montre qu'une attaque de l'image mémoire du processus KeePass ne permet pas d'accéder aux mots de passe en clair. Nativement, la plupart des fonctionnalités qu'on peut attendre d'un gestionnaire de mots de passe sont présentes :

- possibilité d'un cycle de vie complet d'un mot de passe sans jamais l'afficher (génération automatique, accès par le presse-papier via la fonction « copy password », expiration et renouvellement ;
- l'affichage est possible sur demande express de l'utilisateur. Il est à noter que la copie dans le presse-papier est un point faible : pour cette raison, nous paramétrons KeePass pour que le presse-papier soit automatiquement effacé après 30 secondes ;
- il est aussi possible d'utiliser un raccourci clavier encore plus pratique que le presse-papier grâce à la fonction « autotype ». Celle-ci est configurable pour sélectionner automatiquement le mot de passe en fonction du titre de la fenêtre ciblée ou de l'URL de la page web dans laquelle un mot de passe est demandé ;
- organisation de métadonnées sur les mots de passe (date de création, date de renouvellement, date d'expiration, note explicative qui au besoin peut renvoyer à une page web) ;
- journalisation des accès et historique des valeurs de chaque mot de passe ;
- organisation en dossiers des différents mots de passe d'un même coffre ;
- ouverture de plusieurs coffres sous forme d'onglets, etc.

3.1 Partage des coffres

L'utilisation de KeePass n'est possible dans notre contexte que si nous disposons d'un stockage des fichiers chiffrés au format « kdbx » partagé par l'ensemble des utilisateurs potentiels. Cette contrainte est facilement satisfaite grâce aux

² <http://sourceforge.net/p/webkeepass/wiki/Home/>

³ <http://keepass.info>

⁴ Certification de sécurité de Premier Niveau" (CSPN) de l'ANSSI

fonctions de KeePass « open URL » et « save URL » qui permettent d'ouvrir en lecture ou en écriture un fichier accessible en *ftp* ou *https*. *Ftp* sur SSH a été éliminé car nous ne souhaitons pas ouvrir des accès SSH vers le serveur de stockage des coffres. Le stockage sur le serveur de fichiers généraliste de l'université n'est pas jugé assez sûr car ce service est accessible en CIFS ou NFS depuis l'ensemble du réseau de l'université et même depuis Internet. Quand bien même les coffres sont chiffrés, cette exposition réseau est trop importante pour un service aussi sensible. Un serveur webdav dédié, en *https*, est donc retenu.

La configuration du serveur ne permet pas les accès avec un client autre que KeePass. En particulier, nous ne voulons pas d'accès avec un navigateur conventionnel et une association avec l'application KeePass gérée sur le poste de travail. En effet, dans ce cas, un fichier temporaire contenant une copie du coffre est créé dans le contexte du navigateur. Nous ne voulons pas exposer de multiples copies des coffres sur des postes de travail dont nous ne maîtrisons pas la sécurité.

Un défaut de l'organisation pré-existante est l'absence de contrôle d'accès sur les répertoires de mots de passe au sein de la DSI. Grossièrement, on peut dire que tous les personnels de la DSI ont accès à tous les mots de passe. Nous avons donc travaillé sur l'inventaire des mots de passe d'une part et sur « le besoin d'en connaître » d'autre part afin de définir une série de coffres dont les clés sont distribuées aux personnels qui en ont besoin. Une application stricte du principe de limitation en fonction du besoin d'en connaître nous aurait conduits à un trop grand nombre de coffres. Nous poursuivions plusieurs objectifs parfois contradictoires :

- chaque mot de passe ne doit être noté que dans un seul coffre ;
- chacun doit avoir un petit nombre de coffres à connaître (pas plus de 3 ou 4) pour ne pas induire des gestions individuelles empiriques des clés de ces coffres ;
- quand une personne recherche un mot de passe, la logique d'organisation de ceux-ci doit lui permettre d'identifier immédiatement dans quel coffre celui-ci est stocké.

Ces critères nous ont conduits à créer :

- un coffre pour chaque équipe (système, réseau, système d'information, direction, équipe administrative) ;
- un coffre spécifique pour chacun des trois domaines d'activités jugés les plus sensibles : ressources humaines, application financière et SSI.

L'équipe EXAS (EXploitation des Applications et des Services) ayant des missions transversales est celle dont les membres ont accès au plus grand nombre de coffres (en dehors des RSSI qui ont accès à tous les coffres pour pouvoir en assurer le recouvrement). Nous avons créé les coffres dont nous avons réglé les droits d'accès webdav pour refléter cette restriction des partages. Nous en avons distribué les clés de chiffrement via des messages utilisant S/MIME avec des certificats personnels TCS. Ces messages peuvent être archivés, mais il est demandé aux personnes de ne pas les imprimer.

3.2 Traitement des écritures concurrentes

Dans KeePass, les opérations d'ajout ou de modification ne sont effectives que lorsque l'utilisateur sauve son travail. Dans le contexte de coffres partagés, chacun travaille sur une copie en mémoire du coffre qu'il a ouvert. On peut donc redouter que si plusieurs personnes travaillent en parallèle sur un même coffre, la version finalement sauvée soit celle du dernier qui enregistre son travail (en écrasant celui de ces collègues). KeePass détecte ces conflits d'écriture et propose à l'utilisateur lors d'une opération « save », de faire une fusion avec la version modifiée postérieurement à l'ouverture du coffre. L'opération « merge » est faite sur la version de travail de l'instance de KeePass qui l'a détectée. L'utilisateur doit malgré tout terminer par un « save » pour que le résultat soit enregistré. Ce traitement est sûr si les utilisateurs lisent effectivement le popup d'alarme de KeePass. Il est fonctionnellement plus performant qu'un simple verrouillage en écriture puisqu'il permet de travailler à plusieurs, ce qui s'est avéré particulièrement utile lors de la phase d'initialisation de notre projet.

3.3 KeePass2 KeePassX et les multiples plateformes.

Au sein de la DSI, les utilisateurs se répartissent entre Windows et divers Unix. La version KeePass V2 sous Windows est la version native de KeePass. C'est la plus confortable et la plus sûre. Les versions Linux sont satisfaisantes mais cependant, elles requièrent le « framework » Mono pour la compatibilité avec « .net ». Ce portage est probablement responsable de quelques bugs d'affichage dont le plus gênant concerne une différence entre la position effective du curseur de saisie et la position affichée de celui-ci. Pour cette raison, nous conseillons d'opérer les grosses opérations

de saisie de mot de passe dans les coffres depuis un poste de travail Windows (principalement pour éviter les erreurs de saisie des mots de passe).

Au quotidien, l'utilisation en lecture d'un coffre avec KeePass depuis un poste linux Ubuntu ou autre sont parfaitement raisonnables.

Toutefois, un [bug assez grave de KeePass](#)⁵ a été constaté avec la version 3 de "Mono" . Il conduit à la perte pure et simple d'un coffre lors d'une opération « save ». À ce jour, Mono V3 est installé par défaut sur FreeBSD. Nous avons donc interdit l'utilisation de KeePass sur FreeBSD. De même, ne connaissant pas les surprises que contiennent les portages de KeePass pour MacOS X, iPhone, Android, Blackberry ou Windows phone, l'utilisation de ces produits est interdite sur les coffres de la DSI. Ces limitations sont acceptables au sein de la DSI car il existe peu ou pas de demandes pour cet usage sur smartphone.

Concernant le service ouvert aux laboratoires, l'acceptation de ces contraintes est moins certaine. En outre, compte-tenu d'un usage de KeePass probablement bien moins fréquent, des inconsistances du contenu d'un coffre pourraient passer inaperçues assez longtemps. Un outil permettant de vérifier que le nombre de mots de passe de chaque coffre varie peu chaque jour est à l'étude. Nous sommes protégés des dégâts d'éventuelles corruptions d'un coffre via les sauvegardes comme pour tout autre fichier.

3.4 Le coffre RSSI

Le coffre des RSSI contient quelques mots de passe spécifiques à la SSI. Surtout, il contient les « passphrases » d'ouverture de tous les autres coffres. Ceci est requis essentiellement pour être en mesure d'assurer le recouvrement de n'importe quel coffre si la passphrase de celui-ci venait à être perdue. Ce besoin est essentiel dans le contexte des coffres proposés aux laboratoires, en particulier si ceux-ci sont utilisés pour stoker les clés de chiffrement de disques durs comme le demande le CNRS. Le recours à la procédure de recouvrement pourrait aussi être indispensable au sein de la DSI si, par exemple, un maladroît changeait la passphrase d'un coffre sans s'en souvenir.

3.4.1 Sensibilité du coffre RSSI

Le coffre des RSSI est donc particulièrement sensible ; sa compromission jetterait le doute sur l'ensemble des autres coffres. Aussi avons nous décidé d'utiliser la fonction « composite key » qui permet de chiffrer un coffre KeePass avec une clé à 2 composants dont l'un est dans un fichier et l'autre est une passphrase classique. Pour ouvrir le coffre RSSI, il faut donc d'une part posséder une copie du fichier de clé et d'autre part connaître la passphrase du coffre. Ces 2 éléments (détenus par chacun des trois RSSI dans un message S/MIME chiffré) constituent une authentification à double facteur. Cette solution a été préférée à un plugin permettant de chiffrer un coffre KeePass partagé avec des certificats personnels, une deuxième approche qui aurait eu l'avantage d'individualiser le dispositif d'ouverture du coffre. Cela aurait été particulièrement contraignant pour assurer la disponibilité du coffre en l'absence des RSSI. Enfin, faute d'un support matériel dédié pour la gestion des certificats personnels, ceux-ci ne sont protégés que par le mot de passe du magasin de certificat utilisé.

3.4.2 Applications du coffre RSSI

L'accès au coffre RSSI permet d'ouvrir l'ensemble des autres coffres. C'est donc sur ce dispositif que sont basés les outils de surveillance des coffres. En effet, une API de KeePass permet de manipuler par programme un ou plusieurs coffres⁶. Celle-ci est utilisée pour ouvrir le coffre RSSI puis, un à un, l'ensemble des autres coffres afin de compter les mots de passe présents, de vérifier leur ancienneté ainsi que la présence du champ de documentation de ceux-ci.

4 Disponibilité des coffres

Un des enjeux important du projet est d'assurer que les coffres restent disponibles même en cas de sinistre majeur de l'infrastructure de la DSI (les coffres contiennent des mots de passe indispensables pour la mise en œuvre du PRA de la DSI). À cet effet, une copie périodique des coffres est faite sur des clés USB (modèle choisi pour sa fiabilité due aux qualités de la technologie « SLC » autorisant un très grand nombre d'écritures) ; elles sont stockées dans une armoire-

⁵ [bug assez grave de KeePass](#)

⁶ Sur suggestion de François Dagorn que nous remercions pour son aide, nous avons retenu le module CPAN File::KeePass pour nos scripts.

forte spécifique aux RSSI. Le rangement de ces clés USB dans un coffre fort impose une opération manuelle ; la sauvegarde est donc couplée au script de monitoring du contenu des coffres qui doit être lancée par une personne détenant les clés de ce coffre.

La disponibilité des coffres KeePass est uniquement dépendante de celle de ces clés USB. Des mesures organisationnelles permettent d'assurer celles-ci même en l'absence des RSSI. Ainsi, le FSD (Fonctionnaire de Sécurité de Défense) dispose du fichier de clés composite du coffre RSSI, le DSI disposant lui de la passphrase. **Ensemble**, ils peuvent donc ouvrir le coffre RSSI et les autres coffres.

5 L'offre de service pour les laboratoires de l'université

La majorité des laboratoires dispose de moyens informatiques propres. Ils sont donc confrontés dans le domaine de la gestion des mots de passe aux mêmes besoins que la DSI. En outre, la mise en œuvre de la directive du CNRS sur le chiffrement des postes de travail implique qu'un service de recouvrement des données soit assuré. La technique probablement la plus simple pour atteindre cet objectif est de disposer d'un séquestre des passphrases de chiffrement (et de sauvegardes des fichiers chiffrés).

Nous proposons aux laboratoires qui le souhaitent d'utiliser la plateforme technique des coffres de la DSI pour répondre à ce besoin. Une convention d'utilisation de ce service stipule que les RSSI peuvent procéder au recouvrement des mots de passes stockés dans les coffres, sur réquisition judiciaire, sur décision du chef d'établissement, du directeur de l'unité ou à la demande du correspondant technique « coffre » du laboratoire. La convention précise l'identité des correspondants techniques pour ce service, leurs rôles (ils sont les seuls détenteurs des clés du coffre au sein de la composante titulaire du coffre et donc seuls capables de le consulter ou de l'alimenter).

Les laboratoires n'ont pas la liberté de modifier la clé de chiffrement de leurs coffres sans communiquer celle-ci aux RSSI. Cette disposition est destinée à garantir que les clés de chaque coffre figurent bien dans le coffre RSSI ; elle est vérifiée grâce au script de monitoring des coffres. Au cas où il serait impossible d'ouvrir un coffre avec les informations contenues dans le coffre RSSI, il serait demandé au correspondant technique responsable de ce coffre de rétablir la situation, faute de quoi le coffre serait détruit. Cette disposition qui peut sembler radicale, est le moyen de s'assurer que l'université peut s'acquitter si le besoin se présente de l'obligation légale de recouvrement. Nous n'empêchons pas les laboratoires de créer leurs propres coffres KeePass, mais nous leur expliquons les contraintes légales et techniques auxquelles ils doivent se soumettre afin que leur politique de gestion de ces coffres ne mette pas en faute l'université.

6 Premier bilan

Il est trop tôt pour tirer des conclusions sur l'utilisation de ce service au sein des laboratoires. Concernant la DSI, le déploiement initial des coffres a été l'occasion pour plusieurs agents de mesurer et de rectifier les travers des habitudes passées. Par exemple, le fait de formaliser le partage des mots de passe en devant les dispatcher dans les coffres selon la visibilité de ceux-ci a permis de pointer que certaines tâches n'étaient pas prises en charge par l'équipe qui en a formellement la responsabilité.

Passés les premiers efforts de prise en main de KeePass, les personnes ont pu apprécier les qualités très pratiques de cet outil ce qui en facilite l'adoption. Toutefois, un des points demandés dans cette nouvelle politique de gestion des mots de passe partagés semble poser plus de difficultés : l'obligation de documenter les procédures de renouvellement. Il n'y a pas de bénéfice visible immédiatement pour les intéressés à procéder au renouvellement des mots de passe. Il y a, par contre, un surcroît de travail lié à cette mesure, alors même que l'initialisation des coffres demande un certain investissement. Prenons notre temps, nous nous appuyerons sur le mécanisme d'expiration prévu dans KeePass pour faire évoluer cette situation.

La mise en place du service a été accompagnée d'une formalisation de la politique de gestion des mots de passe partagés. La déclinaison de cette politique pour le service des coffres lui-même se doit d'être l'exemple de ce que les RSSI demandent aux équipes de la DSI dans ce domaine. Elle est très exigeante envers les RSSI et elle permet de prendre la mesure des difficultés qui sont liées aux bonnes pratiques : distribution sûre des « passphrases », renouvellement de celles-ci, etc. sont difficiles. La visibilité sur les pratiques dans le domaine des mots de passe partagés a permis aux RSSI de faire montre d'un peu de pédagogie, voire de demander en urgence la correction des problèmes les plus critiques.