



est une société éditant des logiciels consacrés à la sécurité informatique. Elle s'appuie sur l'état de l'art scientifique et technologique dans les domaines de la cryptographie et de la sécurité.

Probleme

Vous êtes DSI et savez que la perte ou le vol d'informations ont un coût de plus en plus important pour les organisations : perte financière directe ou bien indirecte (image, coût de reconstitution des données, perte d'avantage concurrentiel, ...).

La seule protection efficace est l'utilisation massive du chiffrement. Mais la mise en place à l'échelle des organisations est difficile : la perte d'une passe phrase ou de la clé de chiffrement peut entraîner la perte complète des informations protégées : le chiffrement est délicat à gérer et à mettre en place à l'échelle d'une organisation.



est un système logiciel permettant de **protéger les secrets de manière cryptographique et collaborative pour une organisation à l'échelle de l'organisation.**

Vous avez mis en place le chiffrement des fichiers, des disques durs ou des échanges dans votre organisation. Mais que se passe-t-il en cas d'absence ou de refus d'un collaborateur ? Vous n'avez plus accès aux données. L'utilisateur devient un risque.

Avec le **LEMS** tout utilisateur peut déposer un secret (mot de passe ou fichier) dans le système séquestre via un logiciel dédié. Le secret est alors stocké de manière chiffrée dans **LEMS**. Toutes les opérations de chiffrement sont faites sur le logiciel de l'utilisateur. Aucune donnée non chiffrée ne transite sur le réseau.

Un ensemble d'administrateurs de secrets sont attachés au système Séquestre. Pour récupérer un secret, il faut qu'un utilisateur le demande, un quorum d'administrateurs valide alors la demande de manière quasi simultanée. Le demandeur peut alors récupérer le secret. LEMS permet au chiffrement d'être généralisé en réduisant le risque utilisateur.

Avantages

- Minimisation des risques liés aux pertes d'information des utilisateurs.
- Sécurité ne reposant pas sur un individu unique, pas de SPOF (single point of failure) humain ou matériel.
- Traçabilité et contrôle par la hiérarchie des récupérations des secrets.
- Stockage de tout type de secrets (mot de passe, certificats, tout type de fichiers) pour tout logiciel ou tout système d'exploitation.
- Changement des administrateurs de secret sans déchiffrement des informations.
- Les administrateurs de secret n'accèdent pas au secret lors de la libération du secret.

Lybero.net

Votre contact : Arnaud Laprevote
 Mail : arnaud.laprevote@inria.fr
 Espace Transfert
 615 rue du jardin Botanique
 CS20101
 54603 Villers-lès-Nancy Cedex
 France
 Tel : 03 83 59 30 60

Société anonyme au capital de 37.000 € enregistrée sous le numéro 818 754 574 R.C.S. Nancy

