



Claude-Olivier Gertsch
Security & IT Manager

Sécurisation intégrale des supports de données mobiles

La mobilité des utilisateurs et la prolifération des supports de données mobiles fragilisent les méthodes de défense traditionnelles des entreprises. Selon Gartner, 47% des données corporate résident sur des supports mobiles, un chiffre qui va croissant.

Comment faire pour tirer parti des avantages de ces supports tout en limitant les risques liés à leur utilisation ? Comment protéger les données sensibles circulant sur les laptops ? Eviter les risques de perte ou de fuite d'informations liés à l'utilisation des supports de données Plug & Play ? Et comment préserver l'intégrité du réseau en présence de supports potentiellement contaminés ?



Massimiliano Cher
Security & IT Engineer

NagraID, une société du groupe Kudelski comptant 180 collaborateurs, est confrontée à ce problème. L'entreprise possède un savoir-faire unique dans les domaines de la sécurité de systèmes d'identification. Pour ses clients du monde entier, elle produit aussi bien des cartes d'identité électroniques que des cartes bancaires, des titres de transports, des skipass ou des cartes d'accès, des solutions de traçabilité de personnes ou de marchandises. NagraID est active dans des segments d'activité très divers: gouvernements, banques, industries, médical, événementiel, loisirs, etc...

Claude-Olivier Gertsch, Security & IT Manager, et Massimiliano Cher, Security & IT Engineer, sont en charge de gérer la sécurité physique et logique de NagraID, une activité critique. En effet, dans le bâtiment hautement sécurisé de la société à la Chaux-de-Fonds, où l'on n'accède qu'au terme d'un contrôle biométrique strict, la sécurité est une évidence.

La société souhaitait assurer la sécurisation intégrale des supports de données mobiles.

Pour NagraID, la solution idéale devait répondre à plusieurs exigences essentielles. Claude-Olivier Gertsch: "En cas de vol ou de perte d'un laptop ou d'une clé USB, nous voulions être sûrs que personne ne puisse exploiter les données. Ensuite, nous voulions être certains qu'une clé USB entrant dans l'entreprise n'y introduise aucun programme malveillant. Enfin, la traçabilité du contenu de la clé devait être possible. Sans

Pour NagraID, la solution idéale devait répondre à plusieurs exigences essentielles.

" La solution de Pointsec permet de protéger par cryptage les données des laptops et des supports USB et d'assurer la traçabilité des données."

exercer une surveillance permanente, nous voulions pouvoir retracer la provenance des informations en cas de soupçons. Par ailleurs, nous voulions éviter qu'un externe arrivant chez nous avec une clé USB puisse repartir avec des données sensibles."

Après avoir testé plusieurs solutions sans parvenir à réunir toutes ces fonctionnalités, le choix de MM. Gertsch et Cher s'est porté sur la solution Pointsec proposée par Navixia, "qui répond à 100% à nos besoins."

Les solutions Pointsec de protection des données ont fait leurs preuves auprès de très nombreuses entreprises dans le monde. Pour atteindre ses objectifs de sécurité, NagraID a choisi d'associer la solution **Pointsec PC** (cryptage du contenu du disque dur des laptops), avec la solution **Pointsec Protector**, qui traite la gestion des ports, le filtrage du contenu, la vérification du contenu, la traçabilité des données et le cryptage des supports mobiles.

Pointsec PC

Massimiliano Cher décrit le principe de fonctionnement de Pointsec PC: "Le cryptage du disque dur des laptops offre deux paliers de sécurité: en cas de vol, les données ne peuvent pas être lues par des tiers; et une seule personne peut se connecter au laptop, car il n'est pas possible d'en contourner la protection. Le principe: un petit système d'exploitation est exécuté avant Windows. Son accès par login/mot de passe est synchronisé avec celui de Windows, ce qui signifie que l'utilisateur introduit simplement son mot de passe un peu plus tôt qu'il ne le ferait normalement pour accéder à son bureau Windows. Il est impossible à une tierce personne d'accéder à la machine à moins de reformater complètement le disque dur." Tous les laptops de l'entreprise sont cryptés.

Pointsec PC fonctionne sous Windows ou Linux, et permet de gérer la sécurité des laptops et des PCs de manière centralisée. En dehors de l'authentification préalable au boot, Pointsec PC supporte toutes les smartcards et tokens usuels. Les certifications de sécurité obtenues par Pointsec (FIPS 140-2, Common Criteria EAL 4 et BITS) sont supérieures à celles de n'importe quelle solution du marché.

Pointsec Protector

La solution Pointsec Protector, quant à elle, permet de détecter et de contrôler l'utilisation des supports USB dans l'environnement informatique de l'entreprise. Le système permet d'assurer un contrôle précis des types de périphériques et de fichiers autorisés. Le cryptage assure la confidentialité des données; un contrôle de contenu avec recherche de virus est effectué pour toute donnée entrante afin d'assurer l'intégrité du réseau. Des règles configurables permettent aux administrateurs de trouver le meilleur équilibre entre le niveau de sécurité, les coûts d'exploitation et l'impact sur les utilisateurs.

Massimiliano Cher: "Pointsec fournit un historique de tous les fichiers qui ont transité sur chaque clé. Ce suivi se fait par l'intermédiaire d'un échange d'informations entre le PC qui a autorisé la clé et notre serveur. Le suivi a lieu en temps réel si l'utilisateur de la clé se trouve dans l'entreprise. S'il est à l'extérieur, l'échange a lieu dès qu'il se connecte au réseau ou au plus tard à son retour au bureau. Nous évitons ainsi les problèmes de fichiers exécutables pouvant vulnérabiliser le réseau."



Le siège de NagraID
à La Chaux-de-Fonds

" Le cryptage du disque dur des laptops offre deux paliers de sécurité: en cas de vol, les données ne peuvent pas être lues par des tiers; et une seule personne peut se connecter au laptop, car il n'est pas possible d'en contourner la protection."

" Les outils sont très parlants, faciles à mettre en place, et ils correspondaient vraiment à ce que nous cherchions."

" Le système permet de sécuriser les utilisateurs en les embêtant aussi peu que possible, et c'est idéal. Les solutions installées correspondent à ce que nous cherchions. Nous sommes très satisfaits."

Le propriétaire d'une clé USB protégée peut accéder aux données qu'elle contient depuis n'importe quel ordinateur moyennant un login/mot de passe authentifié. En sens inverse, Massimiliano Cher relève toutefois que le contrôle des ports USB peut compliquer l'interaction avec le monde extérieur: "Cela peut s'avérer un problème pour les personnes extérieures à l'entreprise qui visitent nos locaux, puisque seules les clés authentifiées sont acceptées. Nous résolvons ce problème en mettant à disposition un PC "kiosque" non connecté au réseau, à travers lequel il est possible d'échanger des données sans faire appel à l'IT. "

Claude-Olivier Gertsch ajoute : "Tous les collaborateurs, qu'ils possèdent des desktops ou des laptops, sont soumis à la règle des clés USB cryptées. Nous avons fait le choix de ne pas crypter les desktops parce que nous considérons que les risques de vol dans l'entreprise sont infimes."

L'architecture est légère et facile à déployer, comme le confirme Massimiliano Cher: "Les outils sont très parlants, faciles à mettre en place, et ils correspondaient vraiment à ce que nous cherchions. Nous n'avons eu aucun problème avec le cryptage des laptops. Le plus long travail n'est pas l'installation, c'est la préparation préalable: définir ce qu'il faut autoriser, à qui, et gérer les exceptions. C'est la partie la plus ardue."

Claude-Olivier Gertsch et Massimiliano Cher sont satisfaits de la solution Pointsec proposée par Navixia : "Du point de vue de l'utilisateur, la solution mise en place est complètement transparente. Le seul changement pour lui, c'est que sur un autre PC que celui que NagraID lui fournit, l'utilisateur doit authentifier sa clé USB. Le système permet de sécuriser les utilisateurs en les embêtant aussi peu que possible, et c'est idéal. Les solutions installées correspondent à ce que nous cherchions. Nous sommes très satisfaits."

Les supports de données mobiles sont l'une des premières causes de fuites de données confidentielles. La solution Pointsec peut ainsi s'avérer intéressante pour toute entreprise qui souhaite se mettre à l'abri de tels risques sans pour autant compliquer la vie des utilisateurs ni ralentir leurs procédures de travail.



Navixia SA

Route du Bois 1
CH - 1024 Ecublens

Tél.:
41 (0)21 324 32 00

Fax:
41 (0)21 324 32 01

E-mail:
info@navixia.com

Web:
www.navixia.com