Maitriser les données confidentielles et informer l'ensemble des utilisateurs

Support des cinq établissements de santé du GHT18, le CH de Bourges a opté pour la solution de notification automatisée NetSupport Notify et pour la solution de sécurité des données DriveLock de Query Informatique. Frank Moussé, RSSI et DPO du GHT, nous explique pourquoi.

Pour réduire les risques d'infection de code malveillant, mais aussi le transport de données confidentielles (personnelles et de santé) non protégées sur clé USB ou support amovible, notre politique générale de sécurité des systèmes d'information de santé (PGSSIS) recommande de verrouiller les ports USB sur l'ensemble des établissements.

Flexibilité dans le blocage des ports USB

Or, il y a trois ans, il était encore possible d'insérer n'importe quelle clé sur les postes de travail du CH, ce qui était un risque critique et dangereux. « *Dans un premier temps, pour sécuriser ces postes, nous avons complètement verrouillé les ports USB par GPO, mais ce n'était pas adapté, surtout quand quelqu'un avait besoin d'un accès rapide* », a expliqué Franck Moussé. Il fallait une solution pour gagner du temps et faciliter le maintien en condition opérationnelle. « *Voilà un an que notre choix s'est porté sur DriveLock de Query Informatique, car il offrait plusieurs avantages : d'abord, il nous a permis de déployer rapidement sur tous les postes un agent qui autorise exclusivement et sur demande les clés USB fournies par le CH* ».

Chaque clé, ou support amovible, est chiffrée et les autorisations sont gérées à partir d'une console. « *Globalement, on autorise une clé USB sur un poste de l'établissement uniquement si elle est autorisée dans DriveLock et si elle est chiffrée avec DriveLock Encryption 2-go ou BitLocker, la solution de chiffrement de Microsoft* ». Désormais, DriveLock permet au SIS de réduire les risques d'infections, de fuites d'informations non maitrisées et de confidentialité en cas de perte d'une clé, ou d'un disque externe, contenant des données de santé. DriveLock permet aussi le déverrouillage de port USB à distance, sans être connecté. « *Cette fonction est assez intéressante, car on peut ainsi autoriser une personne qui se trouve à l'extérieur de l'établissement à accéder au contenu de sa clé* ». Autre point important souligné par le RSSI : l'enrôlement des clés dans le système via le numéro constructeur IMEI, qui permet, grâce à des exceptions, d'utiliser un port USB avec un dongle, mais aussi d'avoir des traces des actions réalisées sur les clés et sur les supports.

Une solution d'information instantanée

Avant NetSupport Notify, le service informatique envoyait ses messages d'information et d'alerte par courriel, ou des moyens détournés, ce qui n'était pas très efficace. Désormais, il peut informer instantanément tous les utilisateurs ou un groupe d'utilisateurs grâce au couplage Active Directory en un clic via un pop-up sur l'écran, qui apparaît directement sur la machine. Par exemple, le support technique peut informer de l'indisponibilité d'une application à un moment donné s'il a besoin de procéder à une mise à jour et avertir dès que l'application est à nouveau accessible. L'opération est très simple, d'autant que Notify propose des messages préformatés.

Un autre usage de Notify concerne les alertes : les services techniques ont constaté, lors d'un exercice de cellule de crise, qu'ils avaient du mal à informer les utilisateurs. « *Dorénavant, grâce à un accès à la console, la cellule de crise peut envoyer des messages d'alerte préformatés sur tous les postes et atteindre tout le monde* ». L'accès à la console a même été étendu au PC Sécurité, qui peut avoir besoin dans certaines circonstances d'informer les services ou tout l'hôpital de la présence d'un intrus ou d'un risque d'agression (Vigipirate). « *Le service de communication peut aussi envoyer des messages d'information sur un tas de sujets, et moi-même, je peux demander de déconnecter les postes ou de débrancher les câbles pour résoudre un problème de cybersécurité* ».

Selon Frank Moussé, ces deux solutions parfaitement indépendantes répondent complètement aux besoins actuels du GHT18. « *Sur les 5 établissements, un seul est en attente de basculement prochain vers la solution NetSupport Notify* ». Globalement, le déploiement via une GPO ou via SCCM a été très rapide et totalement transparent pour l'utilisateur. « *L'agent communique soit avec la console Notify ou avec la console DriveLock* ». Au fur et à mesure de l'évolution des risques qui pèsent sur les établissements, le RSSI et DPO du GHT pourraient ajouter de nouvelles capacités à Drivelock, notamment un module pour la protection des fichiers. ■

Centre Hospitalier Jacques Cœur à Bourges