ISPPC
Intercommunale de Santé Publique du Pays de Charleroi

Client
ISPPC hôpitaux

Secteur
Santé

Personnel
+/- 4.600

Solution
- Trend Micro OfficeScan
- Trend Micro Deep Discovery Analyzer
- Trend Micro ScanMail for Exchange
- Trend Micro Deep Discovery Inspector
- Trend Micro Deep Discovery Analyzer
- Interscan Web Security Virtual (IWSva)
- Interscan Messaging Security Virtual (IMSva),
- Trend Micro Control Manager
- Deep Security

Avantages
- Meilleure protection
- Gestion et supervision centralisées

Prodata Systems et Trend Micro garantient la bonne santé de l'environnement IT du CHU de Charleroi

Synopsis

L'Intercommunale de Santé Publique du Pays de Charleroi (ISPPC) a pour raison d'être de procurer des soins de qualité en continu. L'association gère le CHU de Charleroi, hôpital public, ainsi qu'une série d'autres établissements, en ce compris trois maisons de repos et de soins, un centre d'aide à la jeunesse qui assure notamment un accueil extra-scolaire et des crèches. Le groupe gère 77 sites au total. Au niveau du CHU de Charleroi, cinq hôpitaux sont concernés, représentant un effectif total de 4.200 employés et plus de 400 médecins affiliés.

L'IT joue un rôle sans cesse plus important dans le cadre d'un hôpital. « Son rôle est même critique dans la mesure où un hôpital cesserait de fonctionner sans IT. Après tout, tout est numérique - depuis le Dossier Patient Informatisé (DPI) jusqu'aux communications (VoIP) en passant par le fonctionnement du labo. La surveillance des patients (cardiologie, néonatologie…) et des bâtiments (détection d'incendie, température…) est tout aussi importante - voire souvent vitale », déclare *Pierre Jaradin*, administrateur réseau à l'ISPPC. Le Real Time Healthcare System (RTHS), développé en interne, qui collecte, analyse et intègre des données est un exemple d'initiative récente qui illustre parfaitement l'importance de l'informatique dans l'hôpital. Parallèlement, ce dernier évalue les potentiels de l'Internet des Objets: surveillance de la température des réfrigérateurs, jumelage avec tous les systèmes d'alerte et de communications possibles et imaginables (incendie, appel infirmier, gestion technique, contrôle d'accès).

« Les produits de Trend Micro procurent une défense à tous les niveaux (réseau, système, passerelle) tandis que diverses fonctionnalités nous soulagent de certaines tâches. »

Pierre Jaradin,
Network Administrator at ISPPC

Défis

L'un des grands défis que doit relever le CHU de Charleroi consiste à réconcilier la multitude des sites avec le caractère ouvert d'une informatique hospitalière. « Nous veillons à une accessibilité maximale de nos systèmes d'information: notamment pour le personnel médical, les patients mais aussi les visiteurs. Multiplicité des points d'accès et réseaux, nombre croissant de dispositifs devant être connectés au réseau, volume exponentiel de données… le défi consiste à garantir que tout est parfaitement sécurisé et que seules les personnes autorisées aient accès aux données sensibles des patients. »

Voilà pourquoi le CHU de Charleroi avait besoin d'une solution de sécurité globale entièrement intégrée, incluant la sécurité réseau (IPS / IDS), la gestion de correctifs virtuels (virtual patching), la mise en "bac à sable" (sandboxing) et une supervision consolidée (SIEM - security information and event management). « Notre solution devait être la plus proactive possible », souligne *Pierre Jaradin*. Défi supplémentaire pour le département IT: les ressources financières disponibles dans le secteur public sont limitées, sans commune mesure avec celles dont dispose par exemple le secteur financier.
« Et pourtant, nous sommes sans doute le deuxième secteur le plus vulnérable et le plus ciblé, juste derrière le secteur bancaire. »

Le choix Trend Micro

Le CHU de Charleroi recherchait une solution qui lui procure une protection maximale pour une charge de gestion minimale. Les défis cités précédemment requièrent un surcroît de ressources mais un budget n'est pas toujours disponible pour financer du personnel supplémentaire. « C'est l'une des raisons pour lesquelles nous avons opté pour une solution de sécurité intégrée globale venant de Trend Micro », explique *Pierre Jaradin*. « Les produits de Trend Micro nous procurent une défense à tous les niveaux (réseau, système, passerelle). Par ailleurs, diverses fonctionnalités nous soulagent de certaines tâches. Prenez par exemple le Control Manager: il fait office de SIEM et permet de partager les informations à propos des menaces visant tous les systèmes de sécurité. »

Solution

« Nous avons opté pour une solution de sécurité intégrée et globale parce que notre équipe doit gérer divers produits (pour le proxy, le réseau, les passerelles…). Devoir systématiquement, pour chacun d'eux, former quelqu'un à un système entièrement différent coûte du temps et de l'argent. Qui plus est, notre équipe IT opère en 24x7 dans la mesure où un hôpital ne ferme pas ses portes à 20 heures. Nos équipes ont donc besoin de soutien. Il est dès lors utile de limiter les connaissances requises aux solutions d'un minimum de fournisseurs. Le CHU de Charleroi a choisi OfficeScan (pour ses 2.100 postes de travail), ScanMail for Exchange (pour les serveurs de messagerie internes), Deep Discovery Inspector (pour surveiller les réseaux), Deep Discovery Analyzer (avec sandboxing pour tous les produits), Interscan Web Security Virtual (IWSva pour proxy Web) et Interscan Messaging Security Virtual (IMSva pour passerelle Mail), le Trend Micro Control Manager et Deep Security (pour les 600 serveurs virtuels).

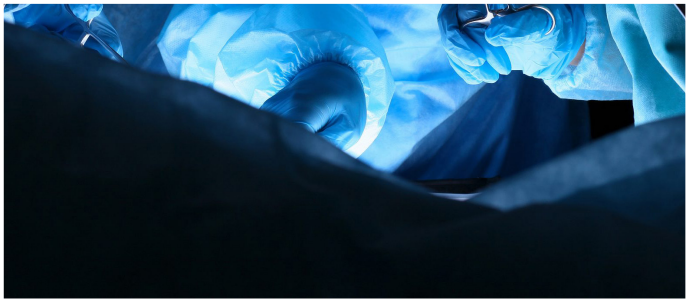
Résultats

Les différents outils ont un impact positif à plusieurs niveaux. La sécurité informatique globale de l'hôpital tire notamment parti de la fonction de sandboxing contre les menaces évoluées. « Quelque 38.000 fichiers (documents, URL…) sont vérifiés chaque mois par l'entremise du sandboxing. Au cours des trois derniers mois, 17 fichiers suspects, totalement inconnus des solutions de sécurité, ont ainsi été détectés et bloqués. La passerelle mail reçoit 780.000 courriels par mois. 15.000 d'entre eux sont des pourriels (spam). Une centaine contiennent des maliciels critiques. Désormais, tous ces fichiers sont également détectés », déclare *Pierre Jaradin*.

L'équipe IT, elle-même, tire parti de la nouvelle solution, essentiellement en raison d'une gestion simplifiée. La vue globale fournie par le Control Manager de Trend Micro, le fait que les journaux (logs) soient centralisés et la proactivité accrue en cas de possible attaque, sont une aide précieuse.

« La passerelle mail reçoit 780.000 courriels par mois. 15.000 d'entre eux sont des pourriels. Une centaine contiennent des maliciels critiques. Désormais, tout cela est détecté grâce aux solutions de Trend Micro. »

Pierre Jaradin,
Network Administrator at ISPPC



Pour en savoir plus, visitez nos customer cases sur www.prodata-systems.be/cases