



SUR UN CAMPUS UNIVERSITAIRE, LES PLUS GRANDES MENACES VIENNENT DE L'INTERIEUR

Créée en 1971, Hasselt est une université jeune, innovatrice et dynamique. La population étudiante avoisine les 3000 personnes, et le personnel compte 800 personnes. Hasselt est réputée pour son enseignement actif et dynamique, une recherche de haut niveau dans des secteurs de pointe, un esprit d'entreprise et d'innovation, et une orientation internationale. Elle adhère aux principes de liberté universitaire et scientifique, d'engagement social et de franchise idéologique.



Interview avec Marc Thoelen

Responsable Réseau



L'UNIVERSITE D'HASSELT



UN RESEAU OUVERT ET UNE TECHNOLOGIE AVANCEE AMENENT DES RISQUES

Il y a environ six ans, l'Université d'Hasselt apprit pour la première fois que son réseau devait rester protégé lorsqu'un incident était causé par une des sociétés de son Programme Incubateur. Les sociétés hébergées dans l'Incubateur de l'Université sont de petites entreprises innovatrices offrant des services et des produits basés sur l'informatique et l'Internet. Ces start-ups innovatrices partagent des ressources, y compris celles du réseau de l'Université. Un seul incident suffit à justifier l'achat du premier firewall NETASQ de l'Université.

Il est très vite apparu évident que les étudiants, eux aussi, représentaient une menace. Comme ils devenaient plus actifs sur le réseau et commençaient à utiliser Linux sur leurs PCs et ordinateurs portables, il est devenu impératif d'installer plus de pare-feu NETASQ entre les salles de cours et le réseau. "Je suis moi-même enthousiasmé par Linux," déclare Thoelen, "mais plus un système est puissant à utiliser, plus cela devient dangereux. C'est comme conduire un char, c'est très puissant mais tout aussi dangereux."

Bien sûr, il y a aussi des tentatives d'intrusion délibérées. Les étudiants aiment expérimenter et le réseau doit

être protégé contre ces expériences. Des incidents mêmes négligeables peuvent survenir. "Nous avons eu, il y a quelques semaines, un virus provenant de l'ordinateur portable infecté d'un membre du personnel. Notre personnel n'est pas spécialisé en informatique, mais ils aiment vraiment explorer ce domaine avec leurs ordinateurs portables. Ou ils achètent des équipements externes dont nous ne sommes pas au courant », ajoute Thoelen. « Si vous ne pouvez pas faire confiance à vos utilisateurs, et que vous n'avez pas beaucoup de temps à perdre à administrer votre réseau et vos utilisateurs, alors procurez-vous un pare-feu NETASQ. »

Les groupes de travail étudiants doivent aussi être contrôlés et le réseau doit être protégé de certains secteurs étudiant comme la cafétéria et le restaurant. Et Thoelen d'ajouter, "Il existe des points de connexion partout. Les étudiants achètent leurs ordinateurs portables personnels et bien que nous les pressions de mettre à jour leur logiciel antivirus régulièrement, nous ne pouvons pas vérifier s'ils l'ont effectivement fait. Nous devons donc anticiper, voilà pourquoi nous avons commencé progressivement à installer plus de firewalls. »

Maintenant, nous avons cinq équipements juste pour protéger le réseau des utilisateurs en interne. »

« Si vous ne pouvez pas faire confiance à vos utilisateurs, et que vous n'avez pas beaucoup de temps à perdre à administrer votre réseau et vos utilisateurs, alors procurez-vous un pare-feu NETASQ .»

Marc Thoelen, Responsable Réseau

UNE PERFORMANCE ELEVEE GARANTIT UNE ASSURANCE DE SECURITE

Un ingénieur à temps plein et un ingénieur à temps partiel gèrent le réseau de toute l'Université. Chaque jour, les équipements NETASQ envoient 15 à 20 notifications de tentatives d'intrusion ou dénis de service. "Il y a des tentatives constantes, mais nous y sommes habitués et nous ne leur y prêtons peu d'attention. Nous laissons simplement les équipements en mode « critique », dit Thoelen.

"Chaque fois que nous avons eu un incident sérieux sur le réseau qui survenait d'un côté des équipements NETASQ, nous découvrons que nous devons nettoyer l'intégralité du réseau excepté pour les équipements placés derrière les pare-feu NETASQ. Nous n'avons jamais besoin d'y toucher grâce à la façon dont ils sont installés. Nous avons trouvé que NETASQ nous facilitait la vie, nous avons l'assurance que si quelque chose se passait sur le réseau, nous n'aurions aucun problème derrière les pare-feu NETASQ. »

"Les pare-feu NETASQ offrent de meilleures performances que les pare-feu classiques ACL parce qu'ils scannent les flux tcp/udp/icmp/...à un niveau plus profond pour stopper les menaces qui utilisent les ports service normaux, par exemple pour obtenir l'accès aux serveurs de FTP illégaux par le port Web 80," ajouta Thoelen.

"Nous avons trouvé que NETASQ nous facilitait la vie, nous avons l'assurance que si quelque chose se passait sur le réseau, nous n'aurions aucun problème derrière les pare-feu NETASQ."

Marc Thoelen,
Responsable Réseau

QUALITE SUR UN BUDGET UNIVERSITAIRE

"Prendre en considération les coûts est toujours important pour une Université, mais l'Université d'Hasselt n'est pas encline à accepter un compromis sur la qualité. Une fois qu'il a été décidé que les pare-feu étaient nécessaires, cinq fabricants de pare-feu ont été invités sur site pour les tests. Nous avons réalisé que le coût variait significativement selon les fabricants. Après avoir intensivement mis plusieurs firewalls à l'épreuve, l'Université d'Hasselt a constaté que les firewalls NETASQ leur apportaient à la fois qualité et économie. »

LES AVANTAGES CLIENT SONT :

- L'assurance d'un réseau à la fois sécurisé et accessible
- Une technologie fiable pour exclure toute menace
- Gain de temps pour les ingénieurs pour sécuriser le réseau
- Atteindre le coût le plus bas sans accepter de compromis sur la qualité



ABOUT NETASQ

Fondée en 1998, NETASQ est le premier constructeur européen de solutions de sécurité unifiée destinées aux entreprises de toutes tailles : PME-PMI, Grands Comptes et Administrations. La société conçoit et commercialise des appliances qui associent une technologie unique de Prévention d'Intrusion en Temps Réel, l'ASQ (« Active Security Qualification ») aux fonctions de pare-feu réseau et applicatif, VPN IPSec et SSL, filtrage de contenu et sécurisation de la VoIP. Véritable innovateur technologique, NETASQ offre ainsi toutes les fonctions de sécurité indispensables, intégrées dans un seul et même boîtier.

NETASQ HEADQUARTERS

3 rue Archimède 59650 Villeneuve d'Ascq (Lille)
Tel: +33 3 20 61 96 30 – Fax: +33 3 20 61 96 39

www.netasq.com