Bezema accroît la protection de ses données

Etude de référence IBM Security Network Intrusion Prevention System GX

Le client : Bezema AG, Montlingen

Sise à Montlingen dans le canton de Saint-Gall, Bezema AG est une entreprise du groupe international CHT. Elle fournit des produits novateurs et de haute qualité à ses clients issus de l'industrie d'ennoblissement et de l'entretien textiles ainsi que de la chimie du bâtiment. Le siège de la société se trouve dans la vallée du Rhin, aux confins de la Suisse, de l'Allemagne et de l'Autriche, une région à la longue tradition textile, de renommée mondiale.

« Avec l'implémentation de l'appliance de sécurité IBM, nous sommes en mesure de réagir immédiatement aux attaques et maliciels, de limiter les dommages et d'améliorer encore la sécurité informatique au sein de notre entreprise. »

Peter Bossart, responsable informatique de Bezema AG

Points forts

- **Facilité d'intégration :** Au niveau technique, la solution IPS fonctionne comme un pont classique et a pu être implémentée sans problèmes au sein de Bezema. Aucune modification de la structure réseau n'a été nécessaire.

- **Implémentation rapide :** L'ensemble de la solution IPS a pu être installé sur site en une journée de travail. Le réglage a été effectué par la suite via une connexion VPN sécurisée.

- **Disponibilité élevée :** Grâce à la fonctionnalité « fail open » (ouvert en cas de panne) intégrée dans l'appliance GX, la disponibilité de l'infrastructure serveurs est garantie même en cas de panne du matériel mis en œuvre.

- **Reporting :** Le management reçoit régulièrement des rapports sur l'état de la sécurité et les éventuels incidents et est ainsi en situation d'avoir un bon aperçu des investissements réalisés.

Le défi

Suite à une attaque de maliciels en 2009, le département informatique se demandait comment remédier au problème et se protéger de futurs piratages.
Comme dans bien d'autres entreprises, Bezema était à l'époque équipée de composants de sécurité classiques tels que pare-feu et protection anti-virus des postes de travail individuels.
Pour aggraver encore les choses, outre son réseau principal, la société avait dû intégrer deux réseaux supplémentaires externes ; par ailleurs, l'entreprise compte un nombre important de commerciaux en déplacement à travers le monde avec leur ordinateur portable.
Protéger une telle infrastructure requiert beaucoup d'efforts et un travail de réflexion important. Bezema a vite réalisé qu'il ne suffisait pas de combattre les maliciels et qu'il fallait avant tout prendre des mesures afin d'éviter de telles attaques.

La solution

Bezema a opté pour l'implémentation d'un système de prévention des intrusions (Intrusion Prevention System, IPS) par le partenaire commercial IBM Mips Computer AG.

Une solution IPS moderne peut détecter les attaques déjà au niveau du protocole et, au contraire d'un pare-feu, comprend le langage des protocoles courants (http, ftp, SMTP, etc.). Ainsi, si un pirate procède à une attaque par force brute pour essayer d'obtenir un mot de passe, l'IPS déclenche une alarme et bloque l'intrus.

Chez Bezema, la solution IPS a été installée sur le périmètre du réseau. Elle contrôle ainsi l'ensemble du trafic de données entre le réseau principal, les réseaux externes et Internet.

Cependant, un système de prévention des intrusions n'est pas un ensemble statique. C'est pourquoi l'équipe de recherche X-Force d'IBM introduit en permanence les résultats de ses dernières découvertes dans la solution, augmentant ainsi le niveau de sécurité en continu. Pour pouvoir fonctionner de manière optimale, il est important qu'un système IPS fasse l'objet d'un suivi attentif.

Chez Bezema, la solution tourne depuis maintenant près d'une année et a permis de découvrir et de contrecarrer plusieurs attaques de maliciels.

Les avantages de la solution IPS Proventia GX

- **Détection et compréhension de plus de 200 protocoles :** Grâce à la technologie IBM X-Force, la version actuelle du module d'analyse (des protocoles) comprend plus de 200 protocoles. Elle est ainsi à même de contrôler l'ensemble du trafic et de réagir en conséquence.

- **Protection préventive avec la technologie IBM Virtual Patch :** Cette technologie protège les systèmes exposés en empêchant les attaques sur leurs points faibles. Elle permet ainsi de gagner un temps précieux qui peut être utilisé pour tester et déployer des mises à niveau et des patchs de sécurité grâce auxquels les vulnérabilités pourront à leur tour être éliminées.

- **Sécurité des applications Web :** Protège les applications Web telles que les serveurs Web, les boutiques en ligne et les applications Web 2.0 en offrant le niveau de sécurité d'un pare-feu d'application Web.

- **Invisibilité aux yeux des pirates :** L'appliance de sécurité étant située sur la deuxième couche du modèle ISO-OSI, elle peut être intégrée sans problèmes dans n'importe quelle infrastructure réseau existante.

- **Performances :** Différents modèles permettent une analyse du flot de données jusqu'à 8 Gbit/s, avec une latence de moins de 200 microsecondes.

- **Gestion centralisée et reporting :** Combinées avec la console de gestion SiteProtector, les solutions de sécurité d'IBM peuvent être gérées de manière centralisée. La solution comprend par ailleurs des fonctions de reporting performantes.

Contacts :

IBM Suisse
Markus Böck
Vulkanstrasse 106
Case postale
8010 Zurich

Mips Computer AG
Roger Schmid
Oberdorfstrasse 13
Case postale
6340 Baar