monext
Transactions de la vie moderne

Monext automatise ses tests PCI-DSS avec QualysGuard

L'important pour Monext n'est pas seulement d'être sécurisé, c'est aussi de pouvoir le prouver. La société a donc souhaité automatiser ses audits de vulnérabilités, mais aussi la génération des rapports PCI-DSS.

"QualysGuard nous donne un 'feux vert / feu rouge' sur notre périmètre PCI. C'est vital pour nous."

Grégoire Maux, RSSI
Monext

En tant qu'acteur majeur du paiement électronique, Monext est exposé à un tir croisé d'audits : "Nous sommes régulièrement audités par nos clients, bien sûr. Mais nous devons aussi passer des audits réglementaires commandés par le GIE Cartes Bancaires et Visa-Mastercard. Sans compter que les banques nous reportent leurs obligations PCI-DSS", explique Grégoire Maux, RSSI de Monext.
Et comme l'a constaté Monext, un tel paysage réglementaire exige une approche méthodique des audits de vulnérabilités. "Nous travaillions par le passé de manière autonome, avec des scripts développés en interne et des audits commando sur certaines portions de notre parc. Mais nous pouvions améliorer notre vision du parc : certaines parties étaient bien connues et d'autres beaucoup moins. Nous avons alors souhaité pouvoir travailler de manière plus transverse et surtout de manière industrielle", poursuit le RSSI.

Difficile bien entendu d'industrialiser la pratique sur la base des outils développés en interne, et Grégoire Maux se met donc à la recherche d'une solution tierce capable de lui offrir une vision globale de son parc et ses vulnérabilités.

Le RSSI a déjà à ce stade une idée très précise de ce qu'il recherche : "Il fallait que la solution retenue soit certifiée "Approved Scanning Vendor PCI-DSS", qu'elle soit en outre présente dans le Magic Quadrant du Gartner, mais aussi référencée chez d'autres grandes banques. Et enfin, que son moteur de rapports puisse s'adapter souplement à plusieurs populations, techniques et managers notamment", se souvient Grégoire Maux.

La société consacre alors six mois à observer le marché et établir une liste de candidats potentiels, en y incluant aussi les solutions de contrôle de conformité. Premier écrémage: ces derniers se révèlent bien trop rigides pour Monext. Pour le reste, plusieurs éditeurs s'excluent eux-mêmes de la course en ne répondant tout simplement pas aux requêtes de Monext.

Seuls quatre fournisseurs restent alors en lice, dont Qualys. "Nous avons alors éliminés les scanners uniquement locaux et ceux qui ne fournissaient pas d'appliance", précise le RSSI. C'est en définitive Qualys qui sera sélectionné.

Un déploiement basé avant tout sur PCI-DSS

La mise en œuvre de la solution QualysGuard se calque alors sur l'effort PCI-DSS de la société. "Nous suivons le plan de déploiement PCI-DSS et profitons de ces interventions pour y déployer le scanner. Nous mettons l'outil en oeuvre comme un point PCI-DSS parmi d'autres", explique Grégoire Maux. L'approche a le mérite d'être pragmatique : le réseau de Monext est très segmenté, ce qui permet de réduire les portions qui doivent être conformes PCI-DSS et par tant, de réduire également les déploiements du scanner.

Dans une telle configuration, QualysGuard est donc étroitement lié aux obligations PCI-DSS de Monext, et ce n'est pas un hasard : "PCI-DSS est vital pour notre activité. Nous nous devons d'être en conformité avec les standards du marché" assène Grégoire Maux.

Le scanner, tant dans son exploitation que dans ses rapports, se plie donc avant tout aux exigences de la conformité. “PCI-DSS nous oblige à un scan par trimestre sur l’ensemble du périmètre concerné. Nous avons voulu automatiser ce contrôle au maximum. Nous utilisons le modèle de rapport PCI-DSS par défaut fournit par l’application afin d’avoir une réponse PCI Pass / PCI Fail. C’est notre coeur de métier. L’approche feux vert / feu rouge est idéale pour nos besoins”, détaille le RSSI.

Rapports PCI-DSS et bonnes pratiques

Chaque trimestre, les rapports PCI Pass sont présentés aux auditeurs. Ils sont pour cela rapatriés en local au format PDF, les auditeurs ayant besoin de les verser à leur rapport.

Le traitement des rapports PCI Fail donne de son côté lieu à une ventilation particulière des vulnérabilités. Monext répartit en effet les failles remontées par le scanner en deux familles (mauvaise configuration et absence de correctif) et trois catégories : systèmes d’exploitation, bases de données (essentiellement Oracle, avec un peu de Sybase et du MySQL) et exploitation (Apache / Tomcat pour l’essentiel). Cela permet de répartir les actions de correction aux équipes directement concernées.

Dans son processus correctif, Monext capitalise également sur les solutions fournies par les rapports de vulnérabilités Qualys. “Nous alimentons une base de connaissances interne notamment grâce aux recommandations des rapports d’audit du scanner. Cela nous permet de créer des documents de bonnes pratiques que nous remettons aux administrateurs”, détaille Grégoire Maux.

L’outil QualysGuard permet d’alimenter - avec d’autres sources - la base de connaissances et les “best practices” sécurité de Monext, et permet par ailleurs d’en contrôler la bonne application lors du déploiement de nouveaux serveurs. “S’il y a un souci sur un serveur fraîchement déployé, c’est que nos consignes n’ont pas été suivies”, poursuit le RSSI.

Stress applicatif en prime

Un effet de bord original noté par Monext durant les audits de vulnérabilités est la capacité à stresser les applications. “Il arrive que, par exemple, des applications de paiement qui reçoivent généralement des requêtes séquentielles se retrouvent en difficulté face au scan. C’est parfois révélateur de leur développement ! Mais cela nous permet de les connaître et d’être plus vigilants avec elles en période de charge”, reconnaît Grégoire Maux.

Enfin, à terme, Monext envisage de surveiller d’autres équipements de réseau et sécurité (reverse proxy, répartition de charge, application delivery, etc) et de pouvoir contrôler leurs analyses directement depuis l’interface d’administration de l’outil d’analyse.

LE MÉTIER

Monext est un acteur majeur du paiement électronique en France. La vocation de Monext est de faciliter les transactions de paiement électronique, avec ou sans carte, sur le point de vente, sur Internet ou sur mobile. Monext développe des solutions sécurisées, fiables et immédiates, destinées aux établissements financiers et à la distribution.
Monext opère 10 millions de cartes chaque année (bancaires, privatives et transport) et plus de 550 millions de transactions.

LE PÉRIMÈTRE

Monext héberge ses propres infrastructures pour la fourniture des services de monétique. L’ensemble est réparti sur deux centres de données, pour un total d’environ 500 serveurs. Il s’agit essentiellement de serveurs Linux et Unix (Red Hat et HPUX respectivement) mais aussi de plusieurs serveurs sous Windows.

LE PROBLÈME

La société souhaitait renforcer la vision de son parc et de ses vulnérabilités en bénéficiant d’un aperçu plus complet de son périmètre notamment en industrialisant et en automatisant les audits de vulnérabilités.

LE DÉFI OPÉRATIONNEL

La conformité à la norme PCI-DSS est cruciale à l’activité de Monext. Outre la seule détection de ses vulnérabilités, la société doit être en mesure de présenter des rapports spécifiques à la norme tels qu’attendus par ses auditeurs, sur un périmètre bien identifié.

LA SOLUTION

QualysGuard Enterprise, solution on demand de Qualys, délivrée en mode « Software as a Service » (SaaS) et associée à des boîtiers appliances sur le réseau interne. Utilisation des modèles de rapports PCI-DSS fournis par défaut par l’application.

POURQUOI QUALYS ?

- Solution certifiée “Approved PCI Scanning Vendor”.
- Solution déjà présente chez d’autres grands acteurs du monde financier.
- Moteur de reporting souple et adaptable à différentes populations de l’entreprise.
- Association cohérente du mode SaaS et de boîtiers locaux pour l’audit du LAN.

QUALYS®
www.qualys.com

USA – Qualys, Inc. • 1600 Bridge Parkway, Redwood Shores, CA 94065 • T: 1 (650) 801 6100 • sales@qualys.com
Royaume-Uni – Qualys, Ltd. • 224 Berwick Avenue, Slough, Berkshire, SL1 4QT • T: +44 (0) 1753 872101
Allemagne – Qualys GmbH • München Airport, Terminalstrasse Mitte 18, 85356 München • T: +49 (0) 89 97007 146
France – Qualys Technologies • Maison de la Défense, 7 Place de la Défense, 92400 Courbevoie • T: +33 (0) 1 41 97 35 70
Japon – Qualys Japan K.K. • Pacific Century Place 8F, 1-11-1 Marunouchi, Chiyoda-ku, 100-6208 Tokyo • T: +81 3 6860 8296
Hong Kong – Qualys Hong Kong Ltd. • 2/F, Shui On Centre, 6-8 Harbour Road, Wanchai, Hong Kong • T: +852 2824 8488

ON DEMAND SECURITY