groupecarrefour

QualysGuard pour Animer la Communauté Sécurité

> ***"Nous avons obtenu des indicateurs compréhensibles par les non-informaticiens, et donc pu pousser la sécurité auprès des managers qui ne sont pas techniques."***

Nicolas Burtin, Responsable SSI, **Groupe Carrefour**

Le groupe Carrefour a déployé des boîtiers QualysGuard afin d'auditer ses vulnérabilités sur le WAN (Wide Area Network). A l'heure du bilan, la solution permet non seulement de mesurer le niveau d'exposition de manière quantifiable, mais elle est aussi devenue un lien entre les responsables sécurité du groupe.

Le groupe Carrefour, organisé en de nombreuses Business Units, exploite un WAN important. Dans le courant de l'année 2007, le Groupe Carrefour décide de renforcer son analyse des vulnérabilités. "*Nous souhaitions connaître de manière quantifiable notre exposition à ce type de risques*", indique Nicolas Burtin, en charge de ces aspects au sein de la Direction de la Sécurité des Systèmes d'Information du Groupe Carrefour.

La DSSI Groupe procède alors à une évaluation du marché en commençant par les logiciels libres d'analyse des vulnérabilités dont l'industrialisation s'avère rapidement insuffisante. Des produits commerciaux, à déployer en local, sont également considérés. "*Le fait qu'il s'agisse d'outils locaux nous rassurait, car externaliser les données sécurité nous semblait antinomique !*", reconnaît Nicolas Burtin. Mais les solutions étudiées manquent d'ergonomie et relèvent des soucis d'installation durant la phase de maquette.

Externaliser la sécurité

"*Une solution Software as a Service, à l'inverse, nous paraissait très souple tant en termes de déploiement que d'utilisation. Mais il restait le problème de l'externalisation. Après une série d'échanges avec la société Qualys, nous avons été convaincus que la confidentialité était au rendez-vous*", détaille Nicolas Burtin. Seul regret : l'incapacité, pour le moment, d'utiliser les clés de chiffrement générées par Carrefour à la place de celles fournies par Qualys.

Contrairement à de nombreuses entreprises qui choisissent de commencer par analyser une portion réduite de leur infrastructure, le Groupe Carrefour a préféré des analyses moins nombreuses mais plus vastes. Un choix qui montrera tout son intérêt à l'heure du bilan.

La solution a beau être en mode SaaS, analyser un réseau privé exige la présence des boîtiers sur l'infrastructure. "*Cela s'est fait très simplement : j'ai remis la mallette contenant le boîtier aux RSSI des BU qui devaient avoir leur propre appliance, lors de leur passage à Paris. Une fois les boîtiers installés, ils sont gérés automatiquement par des comptes distincts créés à l'avance*", souligne Nicolas Burtin.

Une utilisation à plusieurs niveaux

Les analyses conduites régulièrement génèrent une masse d'information qu'il faut traiter. C'est là que l'organisation mise en place par la DSSI Groupe de Carrefour parvient à créer du lien avec la communauté des RSSI locaux et à renforcer le rôle de ces derniers auprès des DSI locales.

"*Nous trions les informations remontées afin d'isoler les vulnérabilités les plus critiques (de niveaux 4 et 5) et parmi elles, celles qui sont les plus nombreuses. Cela nous donne une liste plus courte que nous envoyons au RSSI du pays ou de la BU en question, qui peut alors l'étudier avec la DSI locale. Car l'objectif est aussi de créer le lien entre le RSSI et l'opérationnel*", explique Nicolas Burtin.
De même, le suivi des améliorations est fait de telle sorte qu'il implique fortement le RSSI local : le Groupe procède à des revues régulières avec chaque pays afin d'évoquer les actions nécessaires et consulte les statistiques QualysGuard relatives à la Business Unit en question. "*Mais pour le reste, c'est localement que chaque RSSI détermine les priorités.*

C'est un moyen de responsabiliser les RSSI locaux, et de faire en sorte qu'ils s'approprient l'infrastructure. On a simplement établi avec eux la liste des actifs critiques, et ils doivent y veiller", poursuit Nicolas Burtin.

Après un an d'exploitation, la solution QualysGuard a désormais "fait le tour du monde" chez Carrefour, en analysant l'Amérique, l'Europe et l'Asie. Au total, environ 500.000 adresses IP ont été détectées durant la phase de cartographie du réseau, et 16.000 d'entre elles constituent le périmètre à analyser. Carrefour est parvenu à réduire de 20% le nombre de ses vulnérabilités cette première année.

Certes, la DSSI convient qu'il aurait été plus facile de démarrer sur un périmètre plus réduit, et donc plus facile à maîtriser. "*Mais nous avons fait d'emblée le choix d'un périmètre large car nous voulions obtenir aussi un véritable effet de sensibilisation. Stratégiquement, ce projet n'aurait pas eu le même impact s'il avait été mené sur un périmètre réduit*", justifie Nicolas Burtin.

Car l'objectif de la DSSI Groupe était aussi de crédibiliser la sécurité auprès des autres interlocuteurs du SI : "*Il fallait montrer que les vulnérabilités constituent un problème concret et faire la démonstration que cet outil pouvait aider à le régler. Et cela ne peut se faire à petite échelle, ou du moins ça n'aurait pas marqué les esprits de la même manière. Alors que désormais tous les RSSI sont impliqués et nous avons pu obtenir des indicateurs clairs, accessibles aux non-informaticiens. Cela nous permet donc aussi de pousser le rôle de la sécurité auprès des managers qui ne sont pas de culture technique*", conclut Nicolas Burtin.

Au delà de la seule gestion des vulnérabilités, c'est ainsi une véritable opération de communication que la DSSI Groupe a pu mener, aussi bien auprès de ses RSSI locaux que des responsables métiers.

LE METIER

Le groupe Carrefour est l'un des premiers acteurs de la grande distribution dans le monde (premier distributeur européen et second dans le monde). Le groupe compte 15.000 magasins, depuis les enseignes de proximité jusqu'aux hypermarchés.

LE PERIMETRE

Le groupe Carrefour est organisé en Business Units réparties à travers le monde : chaque pays est une BU, ainsi que certaines entités spéciales, telle la branche Hypermarchés France ou l'entité Groupe elle-même. Toutes communiquent à travers un réseau mondial de type WAN.

LE PROBLEME

Carrefour souhaitait formaliser sa gestion des vulnérabilités et disposer d'indicateurs clairs de son exposition aux risques sur son réseau interne WAN.

LE DEFI OPERATIONNEL

La solution devait permettre d'impliquer les RSSI locaux, valoriser leur rôle auprès des DSI locales et souligner l'importance de la sécurité auprès des responsables non techniques

LA SOLUTION

Quatre boîtiers QualysGuard Enterprise.

POURQUOI QUALYS ?

- Simplicité de déploiement et d'utilisation
- Qualité des analyses
- Mode Software as a Service
- Automatisation des rapports

SITE WEB

http://www.carrefour.com

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