ARVAL
Une société de BNP PARIBAS

Faire plus avec moins : Automatiser l'Analyse des Vulnérabilités dans un Environnement Réglementaire Fort et en Equipe Réduite

Pour Arval, une filiale du groupe BNP Paribas, le dilemme sécuritaire est double : il lui faut d'une part faire plus avec moins, mais elle doit en outre se conformer à un cadre réglementaire toujours plus strict. La société doit ainsi maintenir un niveau de sécurité élevé et, surtout, être en mesure de le prouver. Auditée trois fois par an par le groupe BNP Paribas, engagée dans un processus ITIL et une démarche ISO 27001, elle a tout d'une grande... mais son informatique fonctionne pourtant en effectif modeste.

> *« Si Qualys me permet de mieux cerner nos problèmes, la solution nous permet aussi de concentrer nos forces sur leur résolution (via l'Incident et le Problem management) et d'anticiper sur la conformité en donnant à l'organisme de contrôle permanent les indicateurs qui lui sont nécessaires dans le cadre des nouvelles réglementations. »*

Jean-Marc Lecoint, RSSI
Arval

"QualysGuard Enterprise me permet de consacrer mes ressources à la résolution des problèmes et non simplement à leur énumération", Jean-Marc Lecoint, RSSI d'Arval.

Le défi, bien entendu, n'est pas nouveau. Pour faire face à ses obligations Arval a déjà largement automatisé des pans entiers de sa sécurité, depuis le déploiement des correctifs de sécurité à la mise à jour des bases de signatures de ses antivirus ou même la surveillance de son réseau. Mais l'analyse des vulnérabilités échappait encore à cette automatisation. "Nous procédons à l'audit bi-annuel de quelques filiales. Nous vérifions alors le respect de la totalité de la politique de sécurité, dont l'analyse des vulnérabilités n'est qu'un aspect", explique Jean-Marc Lecoint, RSSI d'Arval.

Mais une telle approche ne permet pas réellement d'intégrer l'audit dans un processus. "Cela permet certes de corriger des problèmes dans l'immédiat. Mais ce qui nous intéresse surtout, c'est une garantie à long terme. Et cela ne passe pas par la simple correction d'une vulnérabilité mais bien par le respect d'un processus", observe Jean-Marc Lecoint. Et le RSSI d'ajouter qu'à l'inverse, un processus seul ne fait pas tout, il faut aussi disposer des moyens de contrôler sa mise en oeuvre.

Des équipes réduites

Aussi louable soit la volonté d'intégrer les analyses de vulnérabilité à un processus régulier et parfaitement contrôlé, encore faut-il en avoir les moyens. Et pour Jean-Marc Lecoint comme pour de nombreux RSSI, l'heure est plus à l'optimisation des ressources qu'à leur multiplication.

"La sécurité n'avance pas à budget constant, mais plutôt à budget réduit. Ca a été le cas pour moi, on m'enlevait deux ressources tout en me demandant de rendre un service amélioré par rapport à l'an passé", se souvient le RSSI.

Arval dispose pour cela d'un demi ETP (équivalent temps plein) dédié à la gestion des analyses de vulnérabilités et à la compilation des rapports et des indicateurs de suivi de la sécurité. "Le seul moyen d'avancer dans ces conditions est de réserver l'expertise humaine aux tâches d'analyse et non à des tâches manuelles répétitives", constate Jean-Marc Lecoint.

Il reste, bien entendu, à trouver l'outil adéquat, capable non seulement d'identifier avec précision les vulnérabilités, mais aussi d'automatiser et d'intégrer le processus à une démarche ITIL existante. Et le tout en mobilisant le moins de ressources possibles en interne.

L'externalisation s'impose

L'externalisation s'est vite imposée à Arval : "Grâce au modèle Sofware as a Service de Qualys et comparativement aux autres – c'est à dire pour le coût d'achat d'un simple logiciel – nous bénéficions à la fois de la solution, de la maintenance, du service, de la simplicité de mise en oeuvre inhérente au modèle et d'une gestion minimale. Cela nous permet de nous concentrer sur la résolution des problèmes. Mes équipes ne sont ainsi plus occupées à énumérer un certain nombre de faits problématiques, mais véritablement à en traiter les causes sous-jacentes", résume Jean-Marc Lecoint.

Le choix s'est porté sur Qualys après avoir évalué en situation réelle trois solutions du marché pendant un mois et demi. Outre la qualité et la pertinence de ses rapports, Qualys a également séduit par la disponibilité de ses équipes. "Nous attachons beaucoup d'importance à ce critère. Nous voulions un véritable acteur technique, présent à l'international et capable de déplacer des personnels en Allemagne ou en Espagne en 48 heures", détaille le RSSI.

Arval a donc souscrit au service QualysGuard Enterprise, qui lui garanti des analyses de vulnérabilités mensuelles récurrentes ainsi qu'autant de tests nécessaires lors de la mise en production de projets sensibles. La solution on demand repose sur la plate-forme de services en mode SaaS de Qualys associée à quatre boîtiers installés chez Arval afin de scanner le réseau de l'intérieur comme de l'extérieur. Le tout fonctionne également dans un environnement multi-sites à l'échelle internationale. "Nous déployons actuellement une filiale à l'étranger par mois, il nous faut donc une solution capable de suivre cette expansion", fait remarquer Jean-Marc Lecoint.

Une approche formelle de la gestion des vulnérabilités

Mais disposer d'une vision claire et régulière de ses vulnérabilités n'est qu'un début. Il faut ensuite être en mesure d'exploiter cette information et de l'intégrer aux processus de contrôle en vigueur dans l'entreprise.

"Ce qui fait la force de la solution de Qualys, ce sont ses indicateurs. Cela permet de prendre en charge toute la chaîne du traitement des vulnérabilités et d'en diffuser le produit aux décideurs concernés en fonction de leurs besoins", entame Jean-Marc Lecoint. Mais il va plus loin : "Car pourquoi les vulnérabilités ne devraient-elles être traitées que par la DSI ? Le responsable métier, par exemple, est aussi concerné. Mais lui ne parle pas le langage de la DSI, seulement celui des risques et des coûts". Et c'est précisément parce que la solution QualysGuard Enterprise prend en charge la notion d'assets management (inventaire des serveurs et des équipements) pour les actifs physiques, qu'elle permet de fournir des rapports en ce sens, utiles à toute la chaîne métier et non plus seulement aux seuls informaticiens.

La flexibilité des rapports fournis par QualysGuard Enterprise a eu une autre incidence positive sur Arval : "Cela nous a permis d'aller voir le Contrôle Permanent (une entité du groupe chargé des audits internes) et leur demander les Points de Surveillance Fondamentaux (PSF) qu'ils souhaitent contrôler chez nous. La solution de Qualys nous permet ensuite de les leur donner régulièrement, dans une démarche proactive", se félicite Jean-Marc Lecoint.

Enfin, dans le cadre d'ITIL, QualysGuard Enterprise permet l'identification des incidents (les vulnérabilités) et le suivi de leur résolution, s'intégrant ainsi dans une démarche de gestion du changement.

"Le CAB (Change Advisory Board) va valider les demandes de changement pour la résolution des incidents en tenant compte des impacts potentiels", explique le RSSI.

De l'identification à la résolution, en passant par un processus de gestion du changement formel, la vulnérabilité est ainsi ré-intégrée dans le cadre d'une démarche structurée d'analyse et de suivi de la performance.

LE MÉTIER

Filiale de BNP Paribas, Arval est en charge du financement de parcs automobiles et des locations longue durée. Elle est l'un des six pôles d'activité du groupe BNP Paribas.

LE PÉRIMÈTRE

Arval est présent dans plus de trente pays. La société emploie 5500 personnes et gère environ 3000 serveurs. L'informatique est très fortement répartie.

LE PROBLÈME

Faire passer l'analyse de vulnérabilités de l'ère de la pratique manuelle à celle d'un composant automatisé parfaitement intégré à des processus stricts, solidaire d'une démarche ITIL et des contraintes réglementaires.

LE DÉFI OPÉRATIONNEL

Faire plus avec moins ! Avec un budget réduit d'un exercice à l'autre et des obligations métier de plus en plus nombreuses, la solution doit être automatisée, simple à administrer et à intégrer aux processus existants.

LA SOLUTION

QualysGuard Enterprise, solution on demand de Qualys, délivrée en mode « Software as a Sercice » (ASP) et associée à des boîtiers clés-en-mains disposés sur le réseau interne.

POURQUOI QUALYS ?

- Analyses de vulnérabilités performante,
- Des rapports aux formats spécifiques adaptés au management, à l'opérationnel ou à l'audit interne,
- Présence internationale de Qualys, disponibilité et forte réactivité des équipes techniques,
- Découverte et prise en charge des assets physiques sur le réseau,
- EFaible besoin d'administration et simplicité de mise en œuvre, de part son model Software as a Service (SaaS).

WEBSITE

www.arval.com

QUALYS®
www.qualys.com

USA – Qualys, Inc.
1600 Bridge Parkway
Redwood Shores
CA 94065
Tél : 1 (650) 801 6100
sales@qualys.com

UK – Qualys, Ltd.
224 Berwick Avenue
Slough, Berkshire
SL1 4QT
Tél : +44 (0) 1753 872101

Germany – Qualys GmbH
München Airport
Terminalstrasse Mitte 18
85356 Münich
Tél : +49 (0) 89 97007 146

France – Qualys Technologies
Maison de la Défense
7 Place de la Défense
92400 Courbevoie
Tél : +33 (0) 1 41 97 35 70

ON DEMAND SECURITY