Adapter l'Analyse de Vulnérabilités à l'Organisation de l'Entreprise

"On a beau avoir le meilleur scanner du monde, si les bonnes informations ne vont pas aux bonnes personnes, il est inutile. Il est donc certes nécessaire d'avoir un reporting standard, mais il faut également être capable d'informer directement les exploitants des machines concernées avec les informations nécessaires à la résolution du problème, sans pour autant les noyer."

Thierry Chiofalo,
RSSI du groupe
SDV Logistique Internationale

Les spécialistes de la sécurité le savent bien, la difficulté est rarement dans la technique, mais le plus souvent dans l'organisation.

Et c'est précisément l'écueil auquel devait faire face SDV Logistique Internationale, une division du groupe Bolloré, en matière d'analyse des vulnérabilités. "Nous utilisions au préalable le scanner Nessus. C'est techniquement un très bon outil mais il n'offre qu'un seul niveau de publication des résultats et pas réellement de délégation. Or, notre organisation et le périmètre du groupe font que si nous ne déléguons pas, les équipes opérationnelles passent trop de temps à gérer le scanner ou ne peuvent tout simplement pas tout scanner", résume Thierry Chiofalo, le RSSI du groupe.

"QualysGuard Enterprise s'adapte à nos besoins en matière de visibilité : il ne nous présente que les vulnérabilités pertinentes et qui méritent réellement notre attention". Thierry Chiofalo, RSSI du groupe SDV Logistique Internationale.

L'organisation informatique de SDV Logistique Internationale est en effet à plusieurs étages : une Direction des Services d'Information au niveau du groupe a pour mission de définir les normes, de préconiser et d'orienter. Mais au sein des régions ou des différentes marques rachetées au fil de la croissance du groupe, des directions informatiques locales pilotent le quotidien.

La DSI Groupe est notamment responsable des analyses de vulnérabilités. Mais outre le fait qu'il est difficile pour une seule équipe d'analyser la dizaine de filiales concernées, la correction des vulnérabilités revient malgré tout aux directions informatiques locales... qui n'ont pourtant pas accès au scanner !

C'est pour trancher ce noeud gordien que Thierry Chiofalo a fait table rase. Il s'est mis en quête d'une solution d'analyse des vulnérabilités qui permettrait d'intégrer les directions informatiques locales dans le processus d'audit, tout en conservant à la DSI Groupe son rôle de contrôle. "Je voulais un outil qui permette à la DSI Groupe de diriger les analyses, mais qui achemine ensuite automatiquement les résultats aux responsables des machines concernées. Le suivi des interventions devait toutefois rester dans le giron de la DSI Groupe afin de nous assurer que les vulnérabilités sont corrigées dans les temps", résume le RSSI.

Et il était souhaitable, bien entendu, que la nouvelle solution exige le moins de tâches d'administration possible.

La solution est hébergée

SDV Logistique Internationale entame donc une phase d'étude du marché et repère plusieurs solutions, aussi bien celle de Qualys en mode hébergé (Software as a Service, ou SaaS) que des produits logiciels commerciaux. Mais ces derniers seront rapidement écartés : "Les logiciels ne présentaient pas, en ce qui nous concerne, suffisamment de fonctionnalités supplémentaires pour justifier leur charge d'administration accrue", explique Thierry Chiofalo.

Le choix se porte alors sur QualysGuard, qui sera évalué pendant un mois sur deux adresses IP du groupe. "Nous voulions nous assurer, bien sûr, que les vulnérabilités étaient bien identifiées. Mais le plus important était surtout de déterminer si le produit était capable de s'adapter à notre organisation, et que nous pourrions l'intégrer à nos processus", résume Thierry Chiofalo.

Dont acte : la solution de Qualys s'est imposée de manière pragmatique à l'issue de cette période d'évaluation, car elle répondait au besoin de simplicité recherché par la DSI tout en étant effectivement capable de coller à l'organisation du groupe.

Une mise en oeuvre en trois étapes

Une fois la solution validée, sa mise en oeuvre s'est déroulée en trois étapes. Il a fallu tout d'abord à SDV Logistique Internationale faire l'inventaire de ses ressources accessibles depuis Internet (les adresses IP publiques). La DSI s'est appuyée pour cela sur la fonction d'asset management fournie par la solution de Qualys. "Le produit analyse des plages d'adresses IP afin de découvrir ce qui est visible. C'est à nous ensuite d'associer à ces découvertes les données métiers qui leurs correspondent (unités organisationnelles, etc...)", explique Thierry Chiofalo. Cela a demandé une journée-homme de travail.

Vient ensuite la sélection, parmi les éléments découverts précédemment, de ceux qui seront observés par QualysGuard. Tous en effet ne méritent pas d'être analysés régulièrement (toutes les interfaces publiques d'un même serveur, aucun service attaquable, etc...).

"Chaque élément restant est alors associé à une personne qui en sera responsable au sein de l'informatique locale. C'est à elle que seront envoyées les alertes de sécurité, et elle sera notre contact si des correctifs restent à appliquer, par exemple", détaille le RSSI.

Il reste enfin à configurer la gestion des tickets d'incidents, qui sera la pierre angulaire de l'organisation mise en place par Thierry Chiofalo. Cela se fait en ligne via une interface fournie par Qualys. Il s'agit de créer des règles qui stipulent que lorsqu'une vulnérabilité est détectée au delà de tel niveau de gravité, un ticket d'incident est ouvert.

"Les correspondants locaux reçoivent quotidiennement un rapport par courrier électronique. Il indique si de nouvelles vulnérabilités ont étés découvertes dans le périmètre dont ils ont la charge. Si c'est le cas, le correspondant se connecte à l'interface sécurisée de QualysGuard. Il y verra alors toutes les vulnérabilités encore actives, dont les nouvelles. En cliquant sur l'une d'elles, il découvrira les informations de correction proposées", détaille Thierry Chiofalo. Enfin, lorsque la vulnérabilité liée à un ticket aura été résolue, ce dernier sera automatiquement fermé à la prochaine analyse.

Bien entendu chaque correspondant n'a accès qu'aux tickets ouverts pour les systèmes dont il a la charge. Par ailleurs, SDV Logistique Internationale a souhaité séparer l'information d'ouverture du ticket de son contenu technique, afin d'avoir une information plus granulaire encore. "L'information liée au ticket nous permet de mesurer notre réactivité, tandis que le détail des incidents nous donne une vision de notre niveau de vulnérabilité. Ce sont deux approches complémentaires : sommes-nous vulnérables, et si oui, réagit-on suffisamment vite ?", précise le RSSI.

Mission accomplie

Avec une telle organisation Thierry Chiofalo a atteint son objectif : la DSI Groupe contrôle entièrement les analyses de vulnérabilités, qu'elle peut déclencher à loisir ou automatiser. A l'issue de ces dernières les résultats sont envoyés automatiquement aux responsables techniques des machines vulnérables et un ticket d'incident ouvert. Enfin, de son poste d'observation la DSI Groupe peut contrôler leur cycle de vie et s'assurer que ses recommandations sont suivies et sa politique de sécurité appliquée.

Une tâche qui sera d'ailleurs bientôt encore plus aisée : "Nous attendons un dernier développement de Qualys qui nous offrira un rapport encore plus synthétique. Nous verrons alors chaque mois, pour chaque direction informatique locale, combien de tickets ont étés ouverts, combien ont étés résolus et combien restent ouverts", prévoit Thierry Chiofalo.

LE METIER
SDV Logistique Internationale est une division du groupe Bolloré. Elle assure des missions de logistique internationale. Le groupe SDV est implanté dans 88 pays et compte 445 agences et 26.000 collaborateurs. Il a acheminé en 2006, 510 000 tonnes de fret aérien et 630 000 conteneurs.

LE PERIMETRE
Né d'une croissance essentiellement externe et implanté sur cinq continents, le groupe SDV Logistique Internationale dispose d'un Système d'Information réparti sur de nombreuses implantations. La DSI Groupe oriente et préconise, mais elle s'appuie sur les directions informatiques locales (géographiques ou organisationnelles) pour l'opérationnel.

LE PROBLEME
Intégrer l'analyse des vulnérabilités dans l'organisation multi-niveaux de l'entreprise. La DSI Groupe doit conserver le contrôle des analyses, mais la correction des failles doit être réalisée par les directions informatiques locales. Ces dernières doivent également disposer d'un système de gestion des tickets d'incidents, utilisé notamment par la DSI Groupe afin de suivre leurs interventions.

LE DEFI OPERATIONNEL
La solution doit être considérée comme un service et non comme une contrainte par les directions informatiques locales. Sa valeur ajoutée doit être perçue immédiatement.

LA SOLUTION
QualysGuard Enterprise, solution on demand de Qualys, délivrée en mode « Software as a Service » (SaaS)

POURQUOI QUALYS ?
- Gestion des tickets d'incidents
- Délégation des rapports d'analyse
- Découverte et prise en charge des assets physiques sur le réseau.
- Faible besoin d'administration et simplicité de mise en œuvre, de part son modèle SaaS.

SITE WEB
www.sdv.com

QUALYS®
www.qualys.com

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

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

Allemagne – Qualys GmbH
Aéroport de Munich
Terminalstrasse Mitte 18
85356 Munich
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