SODEXO RENFORCE LA SÉCURITÉ DES SI DE SES FILIALES AVEC QUALYSGUARD

"Cinq ans plus tard nous utilisons toujours la même solution, mais sur un périmètre, géographique et fonctionnel, beaucoup plus vaste. C'est la force du modèle Software as a Service que d'avoir su tenir compte et intégrer, de manière continue et transparente pour nous, l'évolution de nos besoins spécifiques, ainsi que ceux du marché en général."

Abdellah Cherkaoui,
Chief Information Security Officer
Sodexo

Compléter les audits sur site ponctuels par une analyse automatisée et continue des vulnérabilités de chaque filiale.

C'était le tonneau des danaïdes : après avoir audité et aidé les équipes de ses trente filiales dans le monde à améliorer la sécurité de leur SI, l'équipe d'audit Groupe de Sodexo Chèques & Cartes de Services (CCS) ne pouvait matériellement pas répéter l'exercice plus d'une fois tous les deux ans, en moyenne. "*Entre temps, les configurations des SI ayant évolué au rythme rapide imposé par les besoins du métier et de nos clients, il était souvent nécessaire de reprendre à zéro*", explique Abdellah Cherkaoui, Chief Information Security Officer de l'activité CCS du Groupe. Certes, l'audit sur site offrait une vision détaillée du niveau de sécurité des SI de la filiale, ainsi qu'une liste de recommandations pour l'améliorer, mais un tel fonctionnement pouvait difficilement s'adapter à la croissance soutenue de l'activité et à l'apparition de nouvelles filiales, et encore moins offrir au siège une vision immédiate de son exposition au risque. "*Nous ne pouvions pas faire d'audits plus fréquents, et nous ne souhaitions pas mettre en place des équipes locales, qui n'auraient alors plus été indépendantes de la filiale à auditer*", poursuit Abdellah Cherkaoui. Il fallait donc trouver autre chose.

Le Groupe s'est alors mis en quête d'une solution technique capable de seconder l'équipe d'audit entre deux passages et offrir ainsi une vision continue de l'exposition des filiales. Cela relève cependant du grand écart fonctionnel : la solution doit être capable de s'adapter à toutes les filiales, de la plus grosse qui réalise à elle seule une part importante du volume d'émission de l'activité jusqu'à la plus petite. "*Mais une solution simple adaptée à cette dernière ne sera pas nécessairement assez complète pour répondre aux besoins de la première, et vice-versa*", observe le responsable de la sécurité. De plus, la solution doit également pouvoir être administrée simplement, et permettre une vue centralisée du niveau de risque et de la gestion des vulnérabilités des SI des filiales, sans toutefois nécessiter de présence locale dédiée dans la filiale. Enfin, la solution doit apporter des recommandations effectives et continuellement mises à jour, permettant aux équipes locales de corriger les vulnérabilités au fur et à mesure de leurs apparitions.

"*Nous avons fait le tour du marché, où s'opposaient l'approche logicielle et celle de Software as a Service. Mais nous avions décidé de commencer par analyser notre exposition depuis l'extérieur, et le modèle SaaS nous semblait le plus adapté pour cela. Bien entendu le fait de n'avoir rien à déployer en interne ni aucune organisation à créer pour supporter la solution a également joué en la faveur de ce modèle*", justifie Abdellah Cherkaoui.

Modéliser l'organisation de l'entreprise

Les équipes chargées du projet identifient alors plusieurs solutions basées sur le mode SaaS afin de choisir celle qu'ils évalueront de manière plus approfondie. "*De toutes les solutions étudiées, celle de Qualys était en avance sur deux points : d'abord par son interface, qui permettait une organisation très flexible et très adaptable, par exemple par filiale, par type d'équipements ou encore par niveau de risque. Cette flexibilité de l'interface nous permettait de vraiment coller à notre organisation géographique. Ce service se distinguait ensuite par la qualité de ses rapports très diversifiés, très granulaires, ainsi que par l'offre de recommandations précises pour la correction des vulnérabilités. Ce dernier point est vital pour des équipes locales avec des compétences sécurité limitées. Elles peuvent prendre le rapport tel quel et savoir ce qu'elles doivent faire et où trouver l'information complémentaire si nécessaire.*", poursuit le CISO.

Sodexo demande alors une licence d'évaluation et met le service à l'épreuve du terrain. "*Nous avons tout simplement comparé les résultats des analyses aux rapports très complets*

fournis par notre équipe d'audit". Et le résultat est à la hauteur des attentes de l'équipe en termes de qualité d'analyse. Mais il reste toutefois un dernier frein au déploiement : la crainte de voir des données confidentielles hébergées par un prestataire externe. Une intrusion chez le prestataire ou une malveillance interne pourrait en effet révéler la totalité des points vulnérables de l'architecture de Sodexo.

"*Nous avons mené une analyse de risque afin d'évaluer l'impact de la perte de notre liste de vulnérabilités par rapport au gain que le service nous offre. Car il faut être réaliste : le fait d'avoir une liste de vulnérabilités chiffrée chez un prestataire reconnu dont c'est le coeur de métier est largement moins risqué que de rester avec des vulnérabilités béantes comme c'était le cas à l'époque*", admet Abdellah Cherkaoui. Par ailleurs, Sodexo a décidé d'auditer Qualys. "*Nous avons procédé à des visites sur site et exigé de consulter les rapports d'audits indépendant déjà réalisés. Nous avons été rassurés par les contrôles internes mis en place, et par le fait que toutes les données clients sont chiffrées par la clé privée de ces derniers. Personne chez Qualys ne peut lire nos données de vulnérabilités*", explique le responsable sécurité.

Un service offert aux filiales

Une fois la décision prise, la mise en oeuvre du service s'avère rapide. Après avoir acquis une licence pour une centaine d'adresses IP, l'équipe Sodexo modélise petit à petit l'organisation du groupe dans l'interface d'administration et programme les analyses de tous leurs points d'accès externes. Bien que la configuration de l'outil soit centralisée, le rapport, en revanche, est entièrement destiné aux filiales. "C'est une vente ! Nous avons dit aux filiales "*ce rapport est pour vous. Je vous apporte un outil local, vous ne le payez pas. Cela va vous expliquer comment régler vos vulnérabilités. Toutes les mises à jour sont prises en charge, vous n'avez qu'à identifier vos frontaux. Et nous, on continue à vous supporter par des audits techniques sur site comme d'habitude*", explique Abdellah Cherkaoui. Et les filiales vont se prendre au jeu. Elles s'approprieront rapidement l'outil, aussi bien lors d'analyses régulières que pour la mise en ligne de nouveaux serveurs. Et il sera apprécié au point que certaines filiales décident de s'offrir les services de consultants externes afin de les aider à corriger leurs vulnérabilités plus efficacement.

De son côté, le siège surveille les tendances depuis l'interface centralisée. "La règle est qu'une vulnérabilité de niveau 4 ou 5 (urgente ou critique) ne doit pas rester sans correction plus d'un mois. De plus, grâce aux améliorations apportées, l'outil devient de plus en plus pointu et précieux, car il peut procéder aujourd'hui à une certaine corrélation qui permet de mieux noter l'importance des vulnérabilités : une faille critique qui aurait comme pré-requis l'exploitation d'une vulnérabilité inexistante serait par exemple rétrogradée", poursuit Abdellah Cherkaoui.

L'émergence de nouveaux besoins

Au fil de l'utilisation du service, deux besoins nouveaux ont émergés : l'analyse des systèmes internes, d'abord. "*Le demande est venue des filiales. A ce moment, Qualys proposait une appliance à déployer sur le LAN, que nous avons décidé de tester. Et entre des configurations laissées par défaut ou des correctifs non appliqués, nous avons immédiatement vu l'intérêt du boîtier !*", reconnaît le CISO. Sodexo décide alors de déployer une appliance par filiale, à la condition que ces dernières s'engagent à agir sur les rapports d'analyses internes et à obtenir une décrue de leurs vulnérabilités internes.

Dernier besoin nouveau, enfin, le respect de la réglementation Sarbanes-Oxley et du contrôle interne. "*Nous avons identifié une quinzaine de contrôles essentiels. Nous avons rapidement vu que Qualys pouvait aider les filiales à automatiser et rendre le suivi de certains des contrôles beaucoup plus simple et effectif. Un exemple très parlant est celui de la gestion des configurations par défaut. Nous avons, grâce à Qualys, pu créer un modèle de rapport personnalisé qui ne présente que ces configurations par défaut, que nous avons ensuite partagé instantanément avec toutes les filiales*", explique Abdellah Cherkaoui, avant de conclure "*C'est la force du modèle SaaS : nous utilisons toujours le même produit depuis cinq ans, mais il a su s'adapter à nos nouveaux besoins*".

LE METIER

Avec 310.000 entreprises et institutions clientes, 20,2 millions d'utilisateurs et plus de 1 million de partenaires affiliés dans 30 pays, le Groupe Sodexo est le numéro 2 mondial de l'activité Chèques et Cartes de Services.

LE PERIMETRE

Répondant aux besoins et contraintes locales, les Systèmes d'Information des filiales de Sodexo Chèques & Cartes de Services sont à l'image de ses implantations: hétérogènes, souvent multi-vendeurs et multi plates-formes.

LE PROBLEME

Le Groupe souhaitait améliorer sa connaissance et la gestion des vulnérabilités de tous ces Systèmes d'Information distribués, réparti à travers la planète au sein de filiales très décentralisées.

LE DEFI OPERATIONNEL

Des audits techniques sur site sont réalisés en moyenne une fois tous les deux ans, ce qui est largement insuffisant pour suivre de manière efficace les vulnérabilités et leur correction. Une présence locale dédiée à l'audit n'est cependant pas imaginable, car elle serait difficilement indépendante de la production. De plus, les ressources locales sont concentrées sur le support quotidien des opérations, n'ayant souvent ni le temps ni les compétences nécessaires pour découvrir, analyser et corriger les vulnérabilités des SI.

LA SOLUTION

QualysGuard Enterprise, solution on demand de Qualys, délivrée en mode « Software as a Service » (SaaS) et associée à des boitiers « plug-and-play » au sein de chaque filiale. Analyse illimitée et à la demande de tous les équipements présents sur le réseau, du routeur à la base de donnée en passant par les serveurs et les stations de travail, multi-vendeur, multi-plate-forme.

POURQUOI QUALYS ?

- Qualité, richesse et souplesse des rapports d'analyse
- Capacité à modéliser l'organisation du Groupe dans l'interface de la solution
- Sécurité de la plate-forme chez Qualys pour y héberger des données confidentielles
- Pertinence des analyses de vulnérabilité
- Source directe de connaissance pour les ressources locales des filiales du Groupe

SITE WEB

http://www.sodexo.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