BNP PARIBAS FACTOR

BNP Paribas Factor Assurer une sécurité intégrale à temps partiel... et réussir les audits !

“Sans le service de Qualys nous ne ferions tout simplement pas d’audit de nos vulnérabilités, nous n’avons pas le temps. Alors qu’aujourd’hui, non seulement nous gagnons un temps incroyable, mais nous n’avons encore jamais eu de remarques sur la sécurité de nos serveurs à l’issue de nos audits.”

Laurent Bertin, responsable sécurité, administration et réseau **BNP Paribas Factor**

Filiale d’un établissement bancaire, BNP Paribas Factor est largement contrôlée en matière de sécurité. Mais si elle doit être au même niveau que ses grandes soeurs, la petite filiale d’origine Marseillaise n’a cependant guère les mêmes moyens humains que ces dernières. *“Mon titre exact est responsable sécurité, exploitation, administration et réseau. Dans les faits, je ne consacre environ que 15% de mon temps à la sécurité”*, explique Laurent Bertin, en charge de la sécurité. Il a certes une équipe de neuf personnes pour l’épauler, depuis l’administrateur de bases de données jusqu’à l’ingénieur Unix, mais eux aussi sont loin de pouvoir se consacrer exclusivement à la sécurité. *“Personne ne fait de la sécurité à plein temps, car nous sommes tous surchargés par nos projets de production et d’infrastructure, notamment dans le domaine de la virtualisation actuellement”*, poursuit-il.

La sécurité n’est bien entendu pas oubliée pour autant : un prestataire spécialisé s’est chargé de mettre en œuvre l’architecture du réseau de la filiale et de l’intégration des outils sécurités. En cohérence avec les exigences d’architecture du groupe BNP Paribas, plusieurs pare-feux protègent ainsi trois DMZ dédiées respectivement aux serveurs de présentation Web et Citrix, aux serveurs applicatifs et aux bases de données. Par ailleurs un système d’authentification forte a été mis en oeuvre afin de renforcer l’accès distant au Système d’Information via les serveurs Citrix. Le prestataire vient enfin inspecter l’architecture une fois par mois et il se charge de la maintenance des outils sécurité, notamment en y appliquant les derniers correctifs.

Mais lorsque BNP Factor a souhaité aller plus loin et connaître exactement son niveau d’exposition aux attaques, le prestataire a reconnu que ce n’était pas son métier et a conseillé la solution externe. *“De notre côté, nous n’avions clairement pas les ressources nécessaires pour que quelqu’un chez nous fasse de la veille, ni l’expertise sécurité requise d’ailleurs”*, reconnaît bien volontiers Laurent Bertin.

Une vision indépendante du niveau de sécurité

Parfaitement conscient qu’une vision extérieure, indépendante, est la plus adaptée dans un tel contexte, le prestataire recommande Qualys.
BNP Paribas Factor décide alors d’évaluer la solution, et il suffit d’une démonstration pour emporter la décision. *“Ce n’est pas non plus un projet structurant, et c’est surtout une solution peu chère. Nous avons donc rapidement signé pour 500 analyses annuelles”*, se souvient Laurent Bertin. La société a depuis fait évoluer son contrat vers une formule illimitée pour 128 adresses IP.

Dès la première utilisation, la solution prouve son utilité. *“Notre premier rapport complet faisait cinq mille pages ! Et parmi elles de très nombreuses vulnérabilités de niveau 4 et 5, dites critiques”*, se souvient le responsable sécurité. La tâche de l’équipe de production est alors de réduire ces vulnérabilités et de les mettre sous contrôle. Pour cela, elle instaure un processus itératif d’analyses régulières suivies des corrections prioritaires avec l’aide de son prestataire. *“Nous faisons une analyse par mois, lorsque notre prestataire passe contrôler notre infrastructure. Il étudie avec nous le rapport et nous oriente, car le document peut parfois être intimidant lorsqu’il y a beaucoup de vulnérabilités détectées. Toutes ne méritent pas la même attention et il faut être capable de faire le tri”*, détaille Laurent Bertin.

Avec l'assistance de son prestataire, l'équipe de production de BNP Paribas Factor consacre entre une à deux journées par mois à l'analyse du rapport afin de déterminer les vulnérabilités à corriger en priorité, et préparer l'application des correctifs. *"Nous n'avons pas de plate-forme de test, c'est donc une opération délicate. Outre l'expertise de notre prestataire, les conseils de remédiation fournis par Qualys dans les rapports nous sont précieux au moment de décider quoi corriger"*, explique Laurent Bertin.

Un gain de temps majeur et des audits simplifiés

Plus qu'un important gain de temps (*"monstrueux"*, comme le résume Laurent Bertin), l'apport de Qualys se traduit surtout par des audits largement plus digestes pour l'équipe de production. *"Nous sommes très régulièrement audités, que ce soit par les Commissaires aux Comptes, l'Inspection Générale du Groupe ou la Commission Bancaire. Lorsque nous disons aux auditeurs que nous utilisons un service d'analyse des vulnérabilités et que nous leur présentons nos rapports, c'est pour eux un gage de confiance. D'autant plus que Qualys commence a être reconnu au sein des milieux bancaires"*, poursuit Laurent Bertin. Et le responsable de sécurité d'ajouter qu'il n'a jamais eu aucune remarque sur ses serveurs depuis qu'il a souscrit au service.

De 5000 pages à l'origine, un rapport complet comporte aujourd'hui une quarantaine de pages seulement, *"essentiellement des vulnérabilités que nous surveillons et contrôlons"*, ajoute Laurent Bertin.

BNP Paribas Factor ne compte pas en rester là dans son utilisation du service QualysGuard. La société envisage dans un premier temps d'intégrer les informations issues des rapports à son framework de gestion des incidents de production, basé sur la solution Open Source Mantis Bug Tracker. Elle s'appuiera pour cela sur l'API XML fournie par Qualys pour importer directement les rapports. *"Jusqu'à présent notre priorité était de réduire les alertes de niveaux 4 et 5, les plus critiques. Maintenant que nous y sommes parvenu, nous pouvons envisager d'industrialiser notre usage de la solution"*, explique Laurent Bertin.

Autre évolution, la société s'oriente désormais vers l'analyse des vulnérabilités sur son réseau interne à l'aide d'une appliance Qualys. *"Nous n'allons pas analyser nos 300 postes de travail, car nous n'avons une licence que pour 128 adresses. Mais nous allons cibler en priorité ceux qui disposent de droits plus étendus que les autres. Ce sera la première fois que nous procéderons à un audit complet des postes de travail !"*, conclue Laurent Bertin.

LE METIER

Filiale de la banque BNP Paribas, l'activité Factor offre des services d'affacturage aux entreprises. Elle se charge du recouvrement de leurs créances commerciales après les avoir achetées et garanties , protégeant ainsi ses clients des impayés et participant à leur financement. La société offre ses services aux PME comme aux grands compte à travers plusieurs offres packagées.

LE PERIMETRE

BNP Paribas Factor emploie 300 collaborateurs répartis sur deux sites de production, à Puteaux et Marseille. Chacun est capable de seconder l'autre en cas sinistre. La société exploite un système d'information composé d'une dizaine de serveurs Unix pour ses applications métier et une quarantaine de serveurs Windows (serveurs de fichiers, de messagerie, Citrix...).
Les deux centres de production sont reliés par une liaison de 30mbs.

LE PROBLEME

Avec un RSSI à temps partiel et des équipes très occupées par des projets de production et d'infrastructure, BNP Paribas Factor a peu de temps à consacrer à la sécurité.
Un prestataire spécialisé se charge certes des missions d'implémentation d'architecture et d'intégration sécurité, mais il ne peut être juge et partie lorsqu'il s'agit d'évaluer sa propre prestation.

LE DEFI OPERATIONNEL

Filiale d'un établissement bancaire, BNP Paribas Factor est très régulièrement audité sur sa sécurité. Elle doit, avec moins de moyens que nombre d'autres filiales, atteindre un niveau de sécurité sensiblement équivalent et le prouver à chaque audit.

LA SOLUTION

QualysGuard Express, solution on demand de Qualys, délivrée en mode « Software as a Service» (SaaS), et une appliance placée sur le réseau interne afin d'analyser les postes de travail.

POURQUOI QUALYS ?

- Qualité des rapports fournis
- Rapidité et simplicité de mise en oeuvre
- Peu de ressources à y consacrer
- Coût attractif
- Solution reconnue des auditeurs du milieu bancaire

SITE WEB

https://factor.bnpparibas.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