Qualys franchit les portes de l'entreprise

Qualys associe un boîtier à son service en ligne de détection de failles, pour repérer les vulnérabilités internes de l'entreprise.

Aussi prisés soient-ils, les services en ligne de détection de vulnérabilités se heurtent au coupe-feu de l'entreprise. En effet, le plan de route de leurs scanners distants suit la topologie du réseau tel qu'il est vu depuis Internet, ils évaluent donc seulement la sécurité des éléments frontaux (serveurs web, relais de messagerie, etc.). Pour auditer les éléments internes, tout en conservant la souplesse d'un service en ligne, Qualys associe à son service QualysGuard, un boîtier utilisant sa technologie de scan, à installer derrière le coupe-feu. Dépourvue de console ou d'interface web, cette « boîte noire » se configure par le biais d'un pavé numérique, grâce auquel on lui attribue une adresse IP fixe, ou automatiquement par DHCP.

SSL, SSH et PKI

Intranet Scanner doit cependant communiquer avec la plate-forme distante de Qualys pour connaître ses prochaines tâches, récupérer ses mises à jour logicielles et les nouvelles vulnérabilités recensées dans la base de Qualys (2 000 signatures à ce jour). Cryptés par SSL, ces échanges transitent par le port 443 du coupe-feu (dédié par défaut à HTTPS), qui reste ouvert pour que les employés accèdent à des sites sécurisés. Qualys joue néanmoins la prudence : « *Outre SSL, les communications sont encapsulées dans un tunnel SSH et les données rapatriées signées par Qualys grâce à une infrastructure à clé publique* [PKI, Ndlr]. *De plus, seule une requête du boîtier autorise l'import d'informations* », précise l'éditeur. Comme pour QualysGuard, l'entreprise gère ses scans et ses rapports en ligne. Pouvant être importés en XML, ceux-ci rassemblent les vulnérabilités détectées sur les postes, bases de données, serveurs de messageries, etc.) et leurs parades. Selon Qualys, le boîtier peut scanner jusqu'à 5 000 hôtes par jour.

Julie de Meslon

▸CARACTÉRISTIQUES

Intranet Scanner de Qualys : boîtier 1U de détection des vulnérabilités internes couplé à QualysGuard ; configurable par DHCP ou par saisie manuelle d'adresses IP ; échanges cryptés avec la plate-forme de Qualys par le port 443 ; gestion des scans et reporting en ligne ; rapports XML importables.
Prix : 2 995 € ht puis à partir de 15 215 € ht par an pour 32 adresses IP.

▸PRINCIPAUX CONCURRENTS

SecureScan SP de **VIGILANTe** audite les éléments externes et internes, mais ses agents sont sous forme logicielle.

S'attaquer aussi aux vulnérabilités internes