100% des sites web français restent vulnérables aux mêmes failles

Entre juin 2016 et juin 2017, Wavestone a mis à l'épreuve la sécurité de 155 sites web (117 sur Internet et 38 sur des réseaux privés d'entreprises) à travers des tests d'intrusion (*pen test*) de 70 organisations françaises issues de tous les secteurs d'activités (banque, santé, défense, énergie, administration, télécoms…) dans le cadre de son activité de conseils.

Similaires pour chaque intrusion, les tests visent à vérifier le contrôle d'accès, la qualité du chiffrement, la diffusion d'informations techniques superflues, le traitement des communications, etc., à travers l'exploitation de 47 failles connues.

A la veille de l'ouverture des Assises de la sécurité à Monaco, le résultat que vient de présenter le cabinet de conseils IT est alarmant : 100% des sites web testés sont vulnérables, indépendamment du contexte ou du secteur. Un taux inchangé par rapport à celui de 2016.

Failles graves en baisse

Par vulnérables, il faut entendre qu'ils hébergent au moins une faille de sécurité. Laquelle peut être mineure. Mais 54% sont affectés d'une vulnérabilité grave qui permet d'accéder aux contenus et/ou de compromettre des serveurs. Malgré ce taux alarmant, des progrès notables sont faits alors que, en 2016, les failles graves touchaient 60% des sites audités.

En revanche, les failles importantes sont en hausse, de 39% en 2016 à 45% cette année. Elles permettent d'accéder aux informations d'autres utilisateurs, présentent des faiblesses dans le chiffrement ou encore ouvrent la possibilité de faire réaliser des actions malveillantes à l'insu d'un utilisateur.

Les failles mineures (absence de sécurisation des cookies, déconnexion non effective…) touchent pour leur part 1% des sites. Un taux invariable d'une année sur l'autre.

Ce tableau inquiétant est la conséquence du manque d'intégration de la sécurité dès le début du développement des projets. Inexcusable à l'heure du modèle DevOps de développement continu en lien avec les métiers.

« Il est plus que jamais nécessaire d'investir dans les compétences des équipes, en particulier des développeurs, pour que la sécurité soit bien plus qu'une étape dans des processus peu suivis, mais bien une réalité de

chaque instant », note Wavestone dans son rapport.

Tous les paramètres à revoir dans moins d'un tiers des cas

D'autant que le mal peut être facilement corrigé. A titre d'exemple, sur une faille XSS (qui permet d'exécuter du code dans un navigateur), moins d'un tiers (31%) de l'ensemble des paramètres sont à revoir. Dans 47% des cas, entre 5 et 10 paramètres sont vulnérables et un seul pour 22% des sites. *« La correction sera simple »*, assure le cabinet issu du rapprochement de Solucom et Kurt Salmon.

Côté recommandations, Wavestone incite par exemple à développer les sites à partir d'un CMS plutôt que directement en PHP. Seuls 30% des premiers sont touchés par des failles graves contre 50% pour les seconds. Ou encore bien sécuriser les fonctionnalités de type « dépôt de pièce jointe » alors que 56% d'entre elles permettent de déposer du code (potentiellement malveillant) sur le serveur. Et surtout de bien cloisonner les applications. 45% des tests réalisés à partir d'un compte utilisateur standard ont permis d'accéder à des données ou des fonctions non autorisées.

Sectoriellement, le commerce électronique est la plus impactée alors que 58% des sites audités sont victimes d'une, ou plusieurs, failles majeures.

Mais la Banque et Assurance n'est pas en reste avec 56% des sites concernés tandis que 52% des services web de l'Energie, du Transport et des Télécoms ne sont pas mieux lotis.

Lire également
Wavestone tente de privatiser le Bug Bounty
Une faille dans PHPMailer fragilise des CMS et des millions de sites web
Une faille de sécurité dans TCP permet de pirater la plupart des sites Web