SONICWALL

PRÉSENTATION : POURQUOI LA SÉCURISATION DES APPLICATIONS WEB EST NÉCESSAIRE

Comprendre les risques inhérents aux sites Web des entreprises

Résumé

Les applications Web sont plus que jamais indispensables aux entreprises mais elles peuvent pourtant impliquer des risques importants. Cette présentation examine des exploits et des attaques basés sur le Web que les équipes informatiques se doivent de prendre au sérieux, notamment :

- injection de code/inclusion de code à distance
- vulnérabilités XSS (cross-site scripting)
- détournement de sessions Web
- authentification et autorisation insuffisantes

Introduction

À notre époque peuplée d'applications, les applications Web constituent des éléments clés pour la majorité des entreprises en concurrence, dans un environnement numérique disputé dans le monde entier. Cela est vrai notamment en termes d'identité de marque, de publicité, de compétitivité et d'acquisition de clientèle.

Entreprises, institutions et gouvernement subissent une pression constante pour innover et développer des applications Web utiles et permettant de nourrir un besoin d'accès instantané aux informations, aux services et au support.

La croissance explosive des applications Web dans l'entreprise

Les utilisateurs d'Internet représentent désormais plus de la moitié[1] de la population mondiale. Quatre-vingt treize pour cent[1] de tous les utilisateurs d'Internet ont une activité en ligne, et y restent éventuellement plus longtemps, avec des appareils mobiles plutôt qu'avec un ordinateur. En outre, l'apparition de l'Internet des objets (IoT) a fait surgir des dizaines de milliards[2] d'appareils déjà connectés, qui communiquent et échangent aujourd'hui des données via des applications Web et mobiles : TV, objets numériques prêts-à-porter, voitures, consoles de jeu et unités de vente, et toutes sortes d'appareils intelligents.

Par conséquent, les entreprises font de leur mieux pour fournir une expérience de service et un engagement aussi élevés que possible à l'aide de différents types d'applications Web interactives et d'applications mobiles pensées pour l'utilisateur.

Les applications Web sont ainsi devenues plus indispensables que jamais et les entreprises doivent veiller à ce qu'elles restent toutes en ligne et en sécurité.

Des problématiques de sécurité inhérentes

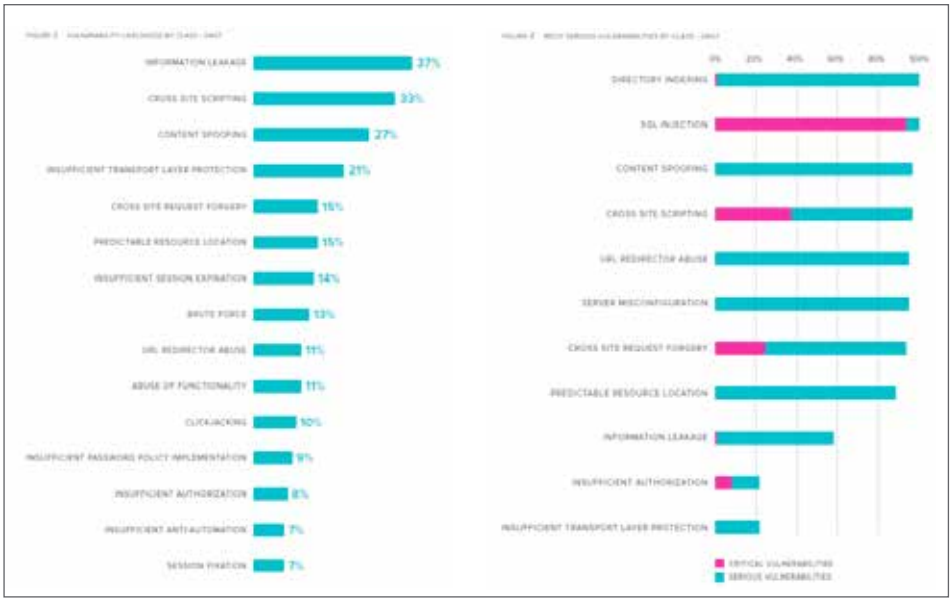
Chaque fois qu'un logiciel d'application Web est déployé avec les données auxquelles il a besoin d'accéder, un risque se pose en matière de sécurité. Il s'agit en effet d'un point d'entrée potentiel pour les pirates cherchant à s'emparer de ces données ou à étendre leur accès à des parties plus sensibles du réseau. Chaque application Web déployée expose les entreprises à un éventail très large d'exploits et d'attaques Web potentiels.

Un rapport récent[3] indique que près de 50 pour cent des applications Web sont toujours vulnérables, tout au long de l'année. Ces failles nuisibles peuvent être les suivantes : fuite d'informations (37 %), cross-site scripting (33 %), usurpation de contenu (27 %), protection insuffisante de la couche de transport (21 %) et attaques CSRF (Cross-Site Request Forgery) (15 %). En termes d'impact stratégique sur l'activité de l'entreprise, l'injection SQL se classe comme la vulnérabilité la plus grave, suivie du cross-site scripting (XSS), du cross-site request forgery (XSFR) et de l'insuffisance d'autorisation.

Ces résultats indiquent que les applications Web continuent de rencontrer de sérieux problèmes de qualité du code source et de sécurité. Les équipes de développement Web semblent ne pas encore avoir entièrement intégré les pratiques de sécurité nécessaires au développement de leur code. Selon Gartner[4], « Les développeurs vont continuer à développer du code non sécurisé et on ne peut rien y faire. C'est une bataille perdue d'avance contre les pirates. »

Un mauvais processus de développement Web, ainsi que des correctifs de sécurité insuffisants, font peser des risques sur les données de conformité. Par conséquent, les entreprises ne sont pas capables de respecter les exigences règlementaires des contrôles de sécurité, notamment PCI, HIPPA et RGPD. Des vulnérabilités logicielles sont régulièrement signalées et sont exploitées dans des applications comme CMS (Content Management Systems), dans des forums et sur des portails utilisés par des entreprises de toutes tailles et de tous secteurs.

L'utilisation de nombreux protocoles dans des applications Web, par exemple HTTP(S), JSON, XML et SOAP, vient exacerber ce problème, ainsi que la nature non restreinte et ouverte de l'interface utilisateur. Par ailleurs, les entreprises ont fait peser des risques sur leurs applications Web en attendant que leurs développeurs logiciels internes et/ou tiers fournissent des correctifs à ces systèmes.



Scénarios d'attaque

Examinons par exemple un formulaire Web type conçu avec un langage de développement Web populaire tel que JavaScript ou PHP.

Ce formulaire accepte différents paramètres permettant aux applications Web de traiter les informations recueillies. Si l'application manque de mécanismes de protection, par exemple analyse et validation des données entrantes, les pirates peuvent potentiellement exploiter l'application et compromettre le service en publiant un contenu arbitraire dans le formulaire.

Dans ce scénario, il est possible qu'une ou plusieurs vulnérabilités courantes pour les applications PHP permettent aux pirates d'inclure leur propre code dans l'application Web ciblée. C'est ce qu'on appelle habituellement un type d'attaque par inclusion de code locale ou distante.

Aujourd'hui, les serveurs Web type hébergent de multiples applications Web sur un hôte unique et sont accessibles via un port unique (port 80 pour HTTP et 443 pour HTTPS). Cela génère une vaste surface d'attaque que les entreprises doivent protéger.

Conclusion

Les entreprises ne peuvent pas s'en remettre à leur équipe de développement Web pour proposer des applications Web parfaites. Sur une année, le nombre de tentatives d'attaques Web peut se compter en centaines de milliers voire en millions : il appartient donc aux administrateurs informatiques de se saisir des questions de sécurité.

En savoir plus. Lisez notre dossier Pratiques d'excellence pour les pare-feux d'applications Web ou rendez-vous sur www.sonicwall.com/web-application-firewall.

[1] https://thenextweb.com/contributors/2017/04/11/current-global-state-internet/
[2] https://cdn.ihs.com/www/pdf/IoT-ebook.pdf
[3] https://info.whitehatsec.com/rs/675-YBI- 674/images/WHS%202017%20Application%20Security%20Report%20FINAL.pdf
[4] https://sdtimes.com/automation/stop-fighting-yesterdays-software-security-wars/

À propos de nous

SonicWall s'engage depuis plus de 25 ans dans la lutte contre la cybercriminalité, défendant PME et grands comptes dans le monde entier. Notre alliance de produits et de partenaires nous a permis de mettre sur pied une solution de cyberdéfense en temps réel, adaptée aux besoins spécifiques de plus de 500 000 entreprises dans plus de 150 pays, leur permettant de se concentrer sans crainte sur leur cœur de métier.

Pour toute question concernant l'usage potentiel de ce document, contactez :

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Consultez notre site Internet pour plus d'informations.
www.sonicwall.com