Sécurité des sites Web : solutions à distance vs solutions intégrées (reflectiz.com)

Sécurité des sites Web : pourquoi les solutions à distance sont meilleures que les solutions embarquées

Surface d'attaqueVie privéeRisque lié aux tiers

28 mars 2023 Temps de lecture: 5 minutes

Il existe deux approches courantes de la sécurité des sites Web : les solutions à distance et les solutions intégrées. Reflectiz a choisi une solution à distance qui utilise une plate-forme de surveillance à distance propriétaire pour sécuriser les actifs en ligne. Reflectiz a opté pour l'exécution à distance car c'est le moyen le plus sûr, le plus rapide et le plus rentable de fournir une visibilité sur les menaces et d'offrir une sécurité maximale aux clients. Cela contraste avec d'autres solutions qui reposent sur l'intégration de scripts sur les sites Web des clients, ce qui introduit de nombreux risques et inconvénients non gérés.

Les aspects négatifs des solutions embarquées

Voici un résumé de ces inconvénients, suivi d'une exploration approfondie –

Accès aux données des utilisateurs – Le script intégré, qui est une partie indissociable du site Web, a accès aux données personnelles et professionnelles tout comme les applications Web qu'il surveille. De plus, il doit se conformer à toutes les réglementations en matière de confidentialité et de sécurité de l'information, qui nécessitent une maintenance constante.

Surface d'attaque plus large – Le script peut servir de point vulnérable pour les attaques potentielles, et sa simple présence amplifie la surface d'attaque numérique de l'organisation, augmentant ainsi le nombre de vecteurs d'attaque à gérer.

Manque de visibilité – Les scripts intégrés ont des capacités de surveillance limitées, et ils ne peuvent pas surveiller les iFrames et le code qu'ils contiennent, ce qui est regrettable car c'est exactement à partir de là que la plupart des trackers et de nombreuses Attaques d'écrémage Web ont été initiées. Cette lacune technologique peut entraîner une couverture insuffisante lors de l'utilisation de solutions de script embarquées.

Problèmes de performances – Le script intégré affecte probablement les performances et l'expérience utilisateur du site Web. Tout travail intensif, tel que la surveillance de tout le code exécuté sur une page donnée, aura un impact négatif sur les performances et affectera très certainement les revenus. De plus, les composants Web sont constamment mis à jour, vous devrez donc vous assurer que le script de sécurité intégré est toujours compatible avec tous, ce qui implique des coûts supplémentaires.

Exploration approfondie

Examinons en profondeur les raisons de l'utilisation d'une solution de sécurité de site Web à distance plutôt que de solutions intégrées:

Accès aux données des utilisateurs

Chaque fois qu'un script est installé sur un site Web, il a accès à la page et aux données personnelles et activités des utilisateurs, c'est pourquoi nous avons créé Reflectiz: pour surveiller ces scripts. Nos outils garantissent que les scripts tiers n'ont pas accès aux données sensibles.

Le problème avec les outils de sécurité intégrés traditionnels est que leurs scripts ont également accès aux données de votre site Web. Avec cette méthode, il n'y a presque aucun moyen de surveiller un site Web sans accéder à des informations sensibles, ce qui signifie que le script lui-même doit se conformer à vie privée et les réglementations en matière de sécurité de l'information telles que CCPA et GDPR. C'est également pourquoi l'organisation est obligée d'informer l'utilisateur du partage de ses données avec un fournisseur tiers – qui dans ce cas est le créateur de l'outil de sécurité lui-même. Bien que techniquement parlant, le script peut éviter ces données, s'il le souhaite, elles sont toujours sous le contrôle du fournisseur et non du client.

Surface d’attaque plus large

L’utilisation de code tiers pour résoudre les problèmes de sécurité du code tiers semble contre-productive, car le script lui-même est également une cible d’attaque. Un chaîne logistique L’attaquant qui accède au code aura un accès immédiat au site Web et aux informations qu’il contient.

La brèche SolarWinds est un exemple bien connu d’attaquants exploitant une vulnérabilité logicielle. Dans ce cas, les attaquants ont inséré du code malveillant dans le logiciel de surveillance informatique Orion de l’entreprise, qui est utilisé par des milliers d’entreprises et d’agences gouvernementales dans le monde entier. En conséquence, l’outil de surveillance a été transformé en un outil d’espionnage.

Dans le scénario Web, les pirates auront un accès complet aux informations personnelles et autres entrées sensibles via une application tierce malveillante, qui sera complètement invisible pour les contrôles de sécurité standard tels que WAF et DAST. L’attaque Ticketmaster est un excellent exemple de compromis et d’utilisation d’un fournisseur de code tiers pour injecter du code malveillant. Dans ce cas, le logiciel du fournisseur est devenu le point d’entrée de l’attaque. Le tribunal a statué que l’organisation, plutôt que le fournisseur tiers, est responsable de la protection des renseignements personnels des utilisateurs. Par conséquent, si vous utilisez une solution tierce et que son code compromet la sécurité de votre site, la responsabilité vous incombe.

En revanche, la solution de surveillance de Reflectiz est externe, il n’y a donc pas d’exposition à ce type de risque.

Manque de visibilité

Un script de sécurité installé sur un site Web ne peut pas accéder aux composants iFrame tiers et aux scripts qu’ils contiennent. En raison des limitations de navigation, les scripts n’ont accès qu’à leurs propres scripts origine. Bien que cette approche ait été créée pour augmenter la sécurité des composants Web, elle crée également des limitations pour JavaScript installé afin de fournir une sécurité complète, car ces iFrames incluent des trackers, des pixels et plusieurs scripts tiers non gérés.

Le script de sécurité installé ne peut pas mapper tous les trackers, découvrir les fuites de données ou créer un inventaire fonctionnel des applications et scripts tiers, donc des activités critiques, telles que la détection de CVE pour les frameworks JS, pixels de suivi comme Meta et TikTok, les empreintes digitales et

la mauvaise configuration des balises - sont limités car ces composants sont rendus inaccessibles.

Il convient de rappeler que quelques recours collectifs ont déjà été intentés contre des organisations de soins de santé en réponse à l'Utilisation de Meta pixel tiers qui a envoyé des données provenant de zones spécifiques nécessitant une authentification. Cette exigence s'applique également au code responsable de la protection de votre site Web, ce qui en fait un autre casse-tête de conformité. Qu'il utilise iFrames ou non, la responsabilité incombe toujours au propriétaire du site Web.

Récemment, une grande société de services financiers a choisi Reflectiz pour la surveillance de son site Web et notre solution a détecté une activité suspecte liée au pixel TikTok. L'équipe d'enquête de Reflectiz a fourni des mesures d'atténuation claires pour mettre fin immédiatement à l'activité non approuvée du pixel. En conséquence, l'entreprise se sent suffisamment confiante dans notre service pour continuer à utiliser les nouveaux outils de marketing et trackers qui lui permettent de s'adresser à son public cible, sachant qu'elle ne compromettra pas la posture de sécurité de son site Web.

Problèmes de performances

Afin de surveiller le code sur un site Web, il est généralement nécessaire d'installer le script dans la section d'en-tête, de sorte qu'il s'agisse du premier composant chargé, sinon il ne pourra pas garder un œil sur le code qui a été chargé avant lui. Mais comme c'est le premier script à charger, cela crée un retard, et il peut également casser d'autres scripts et trames s'il existe une collusion de code entre eux. Les problèmes peuvent inclure des temps de chargement plus longs, des performances médiocres, des problèmes d'utilisabilité et des activités non prises en charge.

De nombreuses recherches (comme celle-ci) Analyse de la recherche Walmart ou ceci Rapport de synthèse Cloudflare) ont montré qu'il existe un lien direct entre les temps de chargement et les taux de conversion des sites web. Le temps de chargement initial de votre site Web est critique pour l'entreprise. Même un retard d'une seconde peut avoir un impact sur les revenus jusqu'à 2%.

Avec la surveillance externe de Reflectiz, aucun script de sécurité n'est chargé sur le site Web, il n'y a donc pas de baisse des performances ou de l'expérience utilisateur. Le seul « fardeau » est quelques impressions supplémentaires par jour.

En outre, un script de surveillance doit pouvoir répondre à tous les utilisateurs du site Web, il doit donc être compatible avec toutes les plates-formes matérielles et logicielles possibles, qui sont bien sûr toujours mises à jour vers de nouvelles versions. Pour assurer une compatibilité continue, l'organisation devra investir dans des mises à jour sans fin de son système et de ses composants tiers pour assurer la sécurité du site Web et optimiser l'expérience utilisateur, et elle devra également vérifier auprès du fournisseur qu'elle prend en charge toutes les versions requises pour toute nouvelle version. C'est un autre coût à considérer lorsque vous n'optez pas pour des solutions de numérisation externes comme Reflectiz.

Réserver une démo aujourd'hui et voyez par vous-même comment Reflectiz peut aider votre organisation à toujours rester protégée.

Distribué en France par AMC SOFT
https://amcsoft.fr
Email : contact@amcsoft.fr
Tel : +33680741316