LISTE DE CONTRÔLE D'AKAMAI

Liste de contrôle des fonctionnalités de protection des applications Web et des API

Déployer une solution de sécurité des applications Web et des API tout en planifiant, en mettant en œuvre ou en optimisant votre stratégie de sécurité de l'information permettra à votre entreprise de comprendre ses risques uniques, de cibler ses lacunes en matière de sécurité et de détecter les menaces. Il vous faut une solution de protection des applications Web et des API (WAAP) vous offrant une visibilité constante, avec des informations exhaustives, et étant pleinement capable d'identifier et de bloquer les attaques les plus sophistiquées.

Cette liste de contrôle peut être utilisée pour évaluer les capacités des fournisseurs ou comme liste d'exigences nécessaires pour mettre en œuvre une solution WAAP efficace.

Catégorie 1 : exigences en matière de plateforme

Il existe des entreprises de toutes formes et de toutes tailles, avec différents besoins. Votre solution de sécurité des applications Web doit être flexible, évolutive et facile à gérer.

- [ ] Une évolutivité répondant aux demandes de trafic et fournissant une protection continue sans perte de performances
- [ ] Une architecture capable de relever les défis d'applications géographiquement dispersées
- [ ] Des fonctionnalités de journal d'audit garantissant une utilisation adaptée
- [ ] Une protection des serveurs d'origine sur site, privés ou sur cloud public (y compris multicloud ou cloud hybride)
- [ ] Une atténuation des attaques par déni de service (DDoS) distribuées de la couche réseau [L3/4] avec un accord de niveau de service de zéro seconde
- [ ] Une visibilité sur l'auteur, la fréquence et la gravité des attaques grâce à un système collaboratif d'informations sur les attaques sur toute la plateforme
- [ ] Un proxy inverse avec un trafic Web via les ports 80 et 443
- [ ] Une protection de la confidentialité du réseau grâce au chiffrement SSL/TLS

Catégorie 2 : protection adaptative des applications Web et contre les attaques DDoS

La sécurité des applications Web doit s'étendre au-delà de la traditionnelle détection basée sur les signatures, vers des formes plus avancées de protection adaptative des applications Web et contre les attaques DDoS pour des résultats plus précis et plus fiables en matière de sécurité.

- [ ] Une détection étendue au-delà des attaques basées sur les signatures avec une notation basée sur les anomalies et les risques
- [ ] Des fonctions d'apprentissage automatique, d'exploration de données et de détection heuristique pour identifier les menaces à évolution rapide
- [ ] Des mises à jour automatiques des règles de Web Application Firewall (WAF) avec des informations en temps réel sur les menaces fournies par des chercheurs en sécurité
- [ ] La possibilité de tester les règles de WAF nouvelles ou mises à jour sur du trafic réel avant de les déployer à la production
- [ ] Une protection (au minimum) contre les attaques de types injection SQL, cross-site scripting, inclusion de fichiers, injection de commandes, SSRF, SSI et XXE
- [ ] Des règles prédéfinies entièrement personnalisables pour répondre aux exigences spécifiques des clients
- [ ] Une protection contre les attaques par déni de service (DoS) volumétriques de la couche applicative [L7] conçues pour surcharger les serveurs Web avec une activité récursive des applications
- [ ] Des règles de WAF entièrement gérées pour éliminer le besoin de configuration et de mises à jour continues
- [ ] Une notation et des informations sur la réputation du client pour les adresses IP individuelles et partagées
- [ ] Des règles personnalisées pour une protection rapide contre des modèles de trafic spécifiques (correctifs virtuels)
- [ ] Une limitation du taux de demandes pour assurer une protection contre le trafic de bots automatisé ou excessif
- [ ] Une protection contre les attaques ciblées visant directement l'origine
- [ ] Des contrôles IP/géographiques via plusieurs listes de réseaux pour bloquer ou autoriser le trafic provenant d'adresses IP, de sous-réseaux ou de zones géographiques spécifiques
- [ ] Une protection contre les clients automatisés, telle que l'analyse des failles de sécurité et les outils d'attaque Web

Catégorie 3 : visibilité, protection et contrôle des API

Les protections des API sont devenues un élément essentiel de la sécurité des applications Web. Pour atténuer les failles des API et réduire votre zone de risque, vous avez besoin d'une solution WAAP dotée de puissantes fonctionnalités de détection, de protection et de contrôle des API.

- [ ] Une détection et un profilage automatiques des API inconnues et/ou en cours de modification (y compris les points de terminaison, les caractéristiques et les définitions des API)
- [ ] Une inspection automatique des demandes XML et JSON pour détecter les attaques basées sur les API
- [ ] Des règles d'inspection API personnalisées pour répondre aux exigences spécifiques de l'utilisateur
- [ ] La possibilité de prédéfinir des formats d'objet XML et JSON acceptables qui limitent la taille, le type et la profondeur des requêtes API
- [ ] Une protection des infrastructures API back-end contre les attaques de type « low-and-slow » conçues pour épuiser les ressources (par exemple, Slow POST, Slow GET)
- [ ] Des alertes, rapports et tableaux de bord en temps réel au niveau des API
- [ ] Des contrôles de fréquence (limites) pour les points de terminaison d'API basés sur une clé API
- [ ] Des listes de réseaux API (listes blanches/noires) basées sur l'IP/l'emplacement
- [ ] Une gestion du cycle de vie de l'API et des versions
- [ ] Une authentification et une autorisation sécurisées via la validation par jetons Web JSON (JWT)
- [ ] Une définition des demandes API autorisées par clé (quota défini indépendamment pour chaque clé) pour un contrôle total de la consommation
- [ ] Une intégration des API grâce aux définitions d'API standards (Swagger/OAS et RAML)

Catégorie 4 : gestion flexible

Vous avez besoin de flux de travail simples et automatisés pour optimiser votre investissement et améliorer votre efficacité opérationnelle. Qu'il s'agisse de protéger les applications nouvelles ou en cours de modification, d'adopter de nouvelles règles de WAF ou d'étendre les protections aux API, le processus doit être fluide et intuitif.

- ☐ Des API ouvertes et une interface de ligne de commande (CLI) permettant d'intégrer les tâches de configuration de la sécurité aux processus CI/CD
- ☐ Une intégration aux applications de gestion des événements et des informations de sécurité (SIEM) sur site et dans le cloud
- ☐ Un environnement de test (staging) complet et la capacité de mettre en œuvre le contrôle des modifications
- ☐ Des protections de sécurité à réglage automatique qui s'adaptent à votre trafic
- ☐ Des tableaux de bord, rapports et fonctionnalités d'alerte heuristiques en temps réel
- ☐ Une interface utilisateur centralisée pour accéder à la télémétrie détaillée des attaques et analyser les événements de sécurité
- ☐ Une flexibilité de gestion de la WAAP via des contrôles de proximité et/ou des protections entièrement automatisées
- ☐ Des services de sécurité entièrement gérés pour délester ou renforcer votre gestion de la sécurité, votre surveillance et votre atténuation des menaces

Akamai Connected Cloud collecte des informations auprès de millions d'attaques d'applications Web, de milliards de requêtes de bots et de milliers de milliards de requêtes API chaque jour. Cette masse d'informations, associée à un apprentissage automatique avancé et à la recherche sur les menaces, nous permet de nous améliorer constamment, de détecter de nouvelles menaces et de développer des capacités innovantes.

Pour en savoir plus, rendez-vous sur akamai.com ou contactez votre équipe commerciale Akamai.

 | Assistance | Publication : 10/23