Akamai

WHITE PAPER

L'elenco OWASP Top 10

Come Akamai aiuta a proteggere dalle vulnerabilità più comuni

Introduzione

L'elenco OWASP (Open Web Application Security Project) Top 10 comprende le vulnerabilità più comuni riscontrate nelle applicazioni web, per incrementare la consapevolezza delle organizzazioni. Per sfruttare al massimo l'elenco OWASP Top 10 è necessario comprendere dove, come e quanto i fornitori di servizi di sicurezza possono aiutarvi a migliorare le pratiche di sviluppo. Il seguente dettaglio delle vulnerabilità OWASP Top 10 descrive ciascuna di esse e spiega come Akamai può sostenere le organizzazioni con le soluzioni per la sicurezza sull'edge, i servizi gestiti e la più grande Intelligent Edge Platform al mondo.

Prodotti Akamai

OWASP Top 10		Account Protector	Akamai Guardicore Segmentation	App & API Protector	Bot Manager	Enterprise Application Access	Enterprise Threat Protector	Identity Cloud	Managed Security Services	Akamai MFA	Page Integrity Manager
Controllo degli accessi danneggiato	A01			✓	✓	✓		✓		✓	
Errori crittografici	A02			✓		✓	✓				✓
Injection	A03			✓							
Progettazione non sicura	A04			✓		✓					
Errata configurazione della sicurezza	A05		✓	✓	✓						
Componenti vulnerabili e obsoleti	A06		✓	✓							✓
Errori di identificazione e autenticazione	A07	✓		✓	✓	✓		✓		✓	
Errori di integrità di software e dati	A08		✓	✓			✓				✓
Errori di registrazione e monitoraggio della sicurezza	A09		✓	✓		✓	✓		✓		
Falsificazione richieste lato server	A10		✓	✓							

Le OWASP Top 10 sono categorie di rischi, non singoli rischi. Le soluzioni Akamai affrontano queste categorie di rischi in molteplici modi. Leggete il nostro white paper per maggiori informazioni.

A01: controllo degli accessi danneggiato

> "Il controllo degli accessi applica policy che impediscono agli utenti di agire al di fuori delle loro autorizzazioni. In genere, gli errori portano alla divulgazione non autorizzata delle informazioni, alla modifica o distruzione di tutti i dati o all'esecuzione di una funzione aziendale che esula dai limiti dell'utente".
>
> - Fonte: owasp.org

Il contributo di Akamai

Se da una parte le organizzazioni devono ottimizzare il loro modello di controllo degli accessi per poter gestire al meglio le vulnerabilità che ne conseguono, la competenza di Akamai nelle soluzioni WAAP può aiutarle a individuare e contrastare alcuni dei vettori di attacco che cercano di sfruttarlo:

- **Enterprise Application Access** offre un modello di accesso basato sul privilegio minimo per gli utenti aziendali, consentendo solo agli utenti autenticati la visibilità e l'accesso alle applicazioni autorizzate, supportando un modello di sicurezza Zero Trust.
- **Akamai MFA** fornisce servizi di autenticazione avanzati basati sugli standard tecnologici FIDO2 resistenti al phishing.
- **App & API Protector**, la soluzione WAAP di Akamai, può aiutare a bloccare gli attacchi di forza bruta ai browser verificando l'intestazione del "referer" e applicando l'autenticazione per le API per rafforzare il controllo degli accessi con l'Akamai API Gateway.
- **Identity Cloud** fornisce controlli granulari degli accessi ai dati degli utenti finali, consentendo l'accesso basato sul privilegio minimo per utenti o sistemi interni.
- **Bot Manager** previene gli attacchi automatizzati agli strumenti e gli attacchi alle credenziali di accesso.

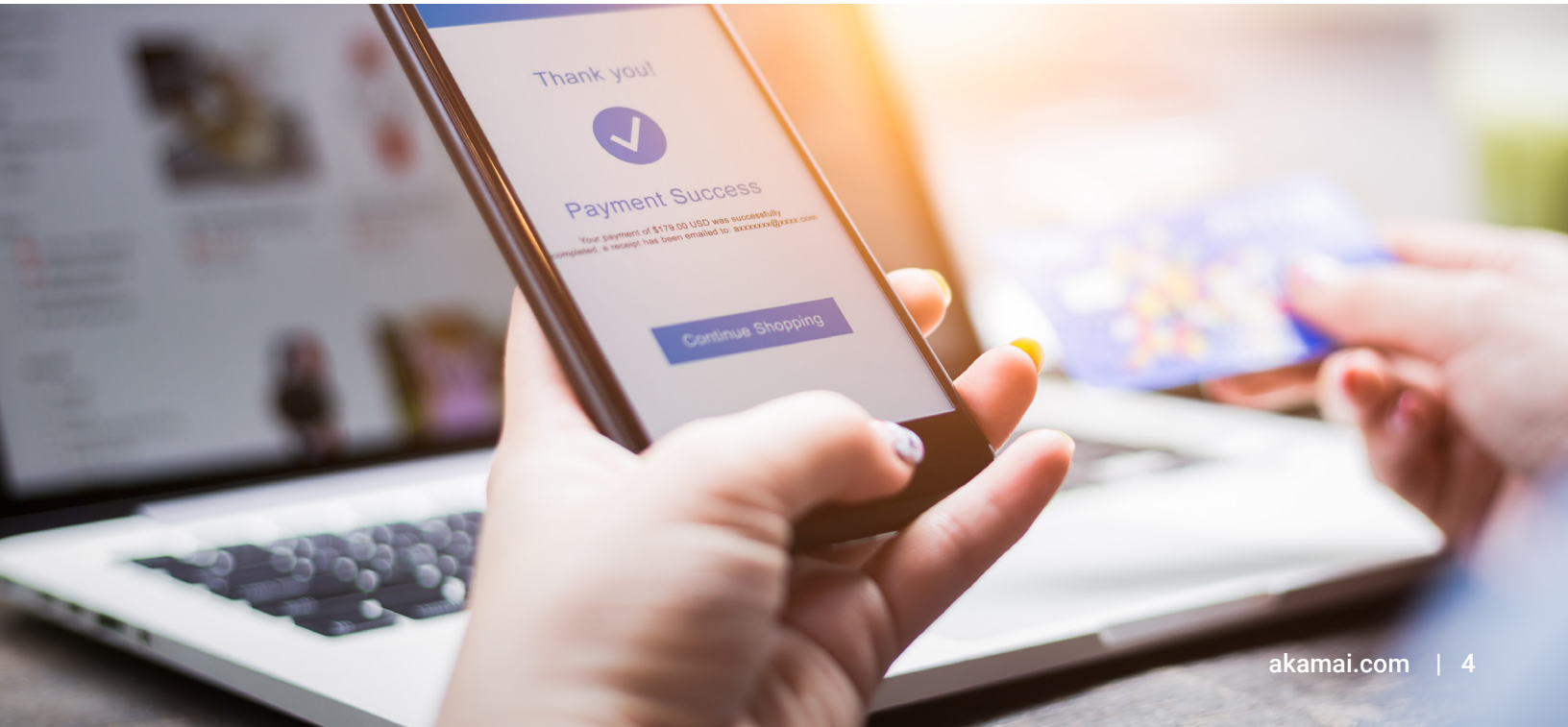
A02: errori crittografici

> "L'attenzione è rivolta agli errori relativi alla crittografia (o alla mancanza di essa), che porta spesso all'esposizione di dati sensibili. … Ad esempio, password, numeri di carte di credito, cartelle cliniche, informazioni personali e segreti commerciali richiedono una protezione extra, soprattutto se i dati sono coperti dalle leggi sulla privacy".
>
> - Fonte: owasp.org

Il contributo di Akamai

Le organizzazioni non possono difendersi al meglio dagli errori crittografici affidandosi a un'unica soluzione di sicurezza. D'altro canto, la combinazione di varie soluzioni aiuta a gestire alcuni aspetti di questa vulnerabilità.
È questo il caso delle seguenti soluzioni Akamai:

- **App & API Protector** crittografa e protegge i dati sensibili in transito con le versioni più recenti di TLS e una crittografia robusta. Aiuta anche a:
  - Mantenere la conformità PCI agendo esclusivamente da una CDN sicura che supporta tutti i certificati TLS brandizzati e protegge le chiavi private dei clienti.
  - Offrire una CDN che sia protetta dalla sicurezza fisica e operativa, ad esempio con rack protetti e rilevatori di movimento, che concedono l'accesso ai server solo al personale autorizzato.
  - Individuare e prevenire la perdita di dati sensibili con l'apprendimento delle informazioni di identificazione personale tramite API.
- **Enterprise Application Access** può proteggere l'accesso remoto crittografando la comunicazione e nascondendo i dati riservati da sguardi indiscreti sulla rete.
- **Enterprise Threat Protector** può aiutare a prevenire l'esposizione dei dati sensibili.
- Anche **Page Integrity Manager** rileva la perdita di informazioni di identificazione personale tramite l'uso improprio del codice JavaScript, che può provocare errori crittografici.



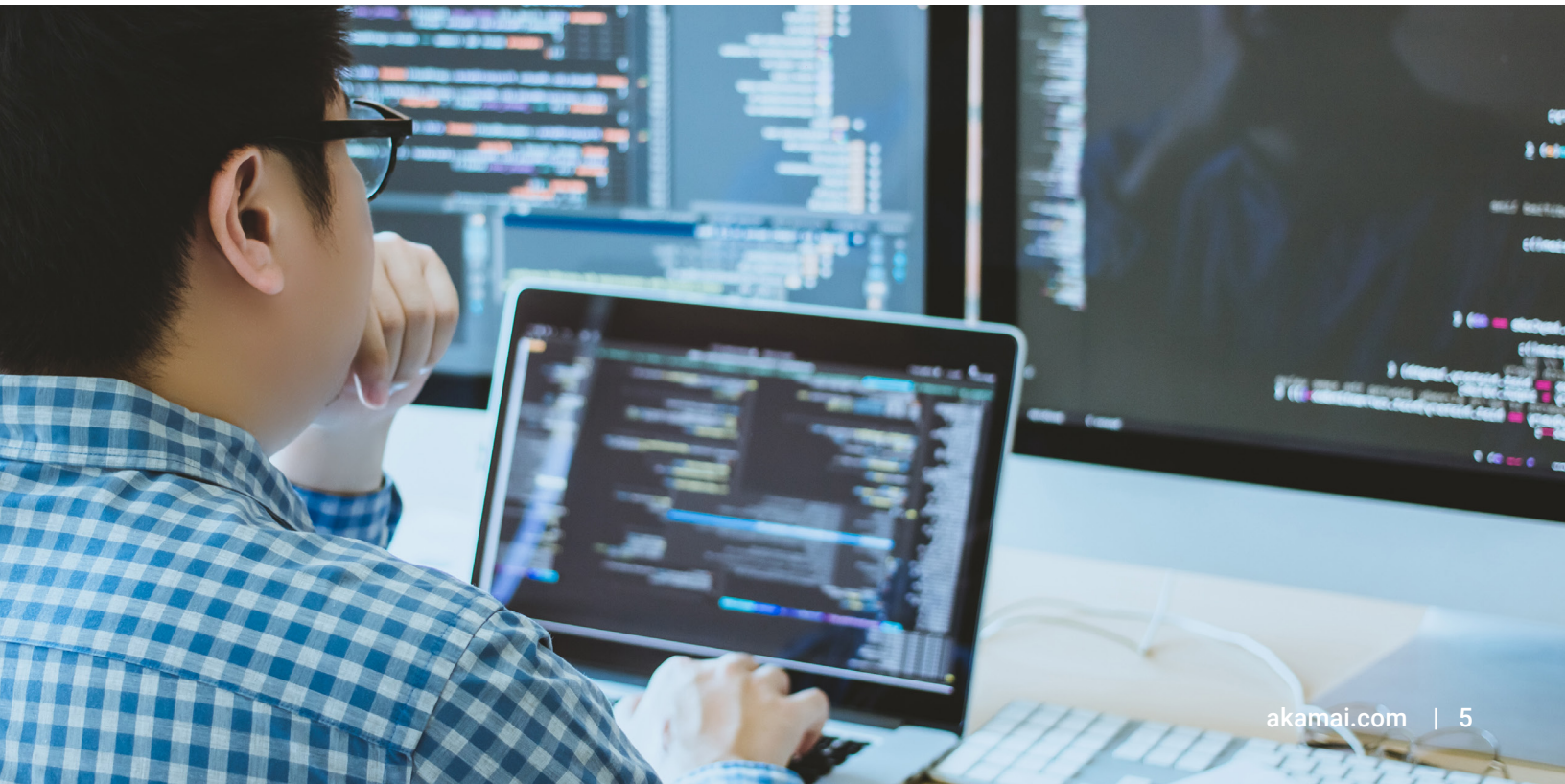
A03: injection

> "Gli attacchi injection, come SQL, NoSQL, OS e LDAP, si verificano quando vengono inviati dati inattendibili a un interprete come parte di un comando o una query. I dati dannosi dell'autore dell'attacco possono portare l'interprete ad eseguire comandi indesiderati o ad accedere a dati senza un'adeguata autorizzazione".
>
> - Fonte: Akamai

Il contributo di Akamai

La soluzione WAAP consente di mitigare il rischio di attacchi injection indirizzati alle applicazioni web e alle API. Tuttavia, le organizzazioni sono tenute ad applicare sempre le patch alle applicazioni web, per gestire eventuali vulnerabilità rilevate sulla base dei cicli di sviluppo.

- **App & API Protector** offre una soluzione WAAP leader nel settore grazie a un Adaptive Security Engine (ASE), che fornisce ampia protezione dagli attacchi injection usando regole esistenti e pronte all'uso. Il penalty box ASE può bloccare temporaneamente tutto il traffico in arrivo da client che hanno tentato di sferrare di recente un attacco injection usando una soluzione WAAP.
- L'applicazione di patch virtuali con regole personalizzate permette di gestire rapidamente vulnerabilità di tipo injection emergenti o nuove vulnerabilità emerse a seguito delle modifiche alle applicazioni, finché non sarà possibile applicare le patch. Le organizzazioni di sicurezza possono inoltre automatizzare l'applicazione di patch virtuali e integrarla nei processi DevSecOps sfruttando le funzionalità API di Akamai.
- **Client Reputation** può aiutare a identificare e bloccare gli attacchi injection e offre un punteggio di rischio per i client dannosi fortemente attivi nella categoria Autori di attacchi web.



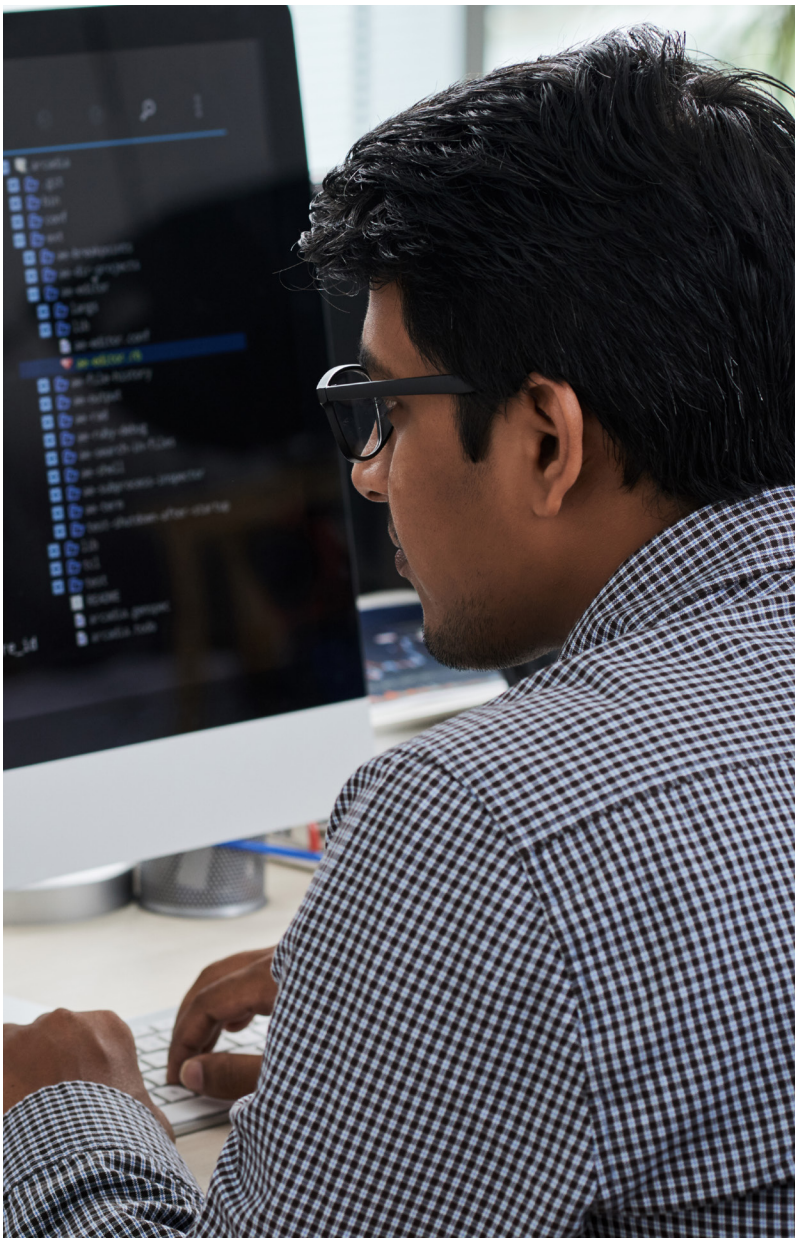
A04: progettazione non sicura

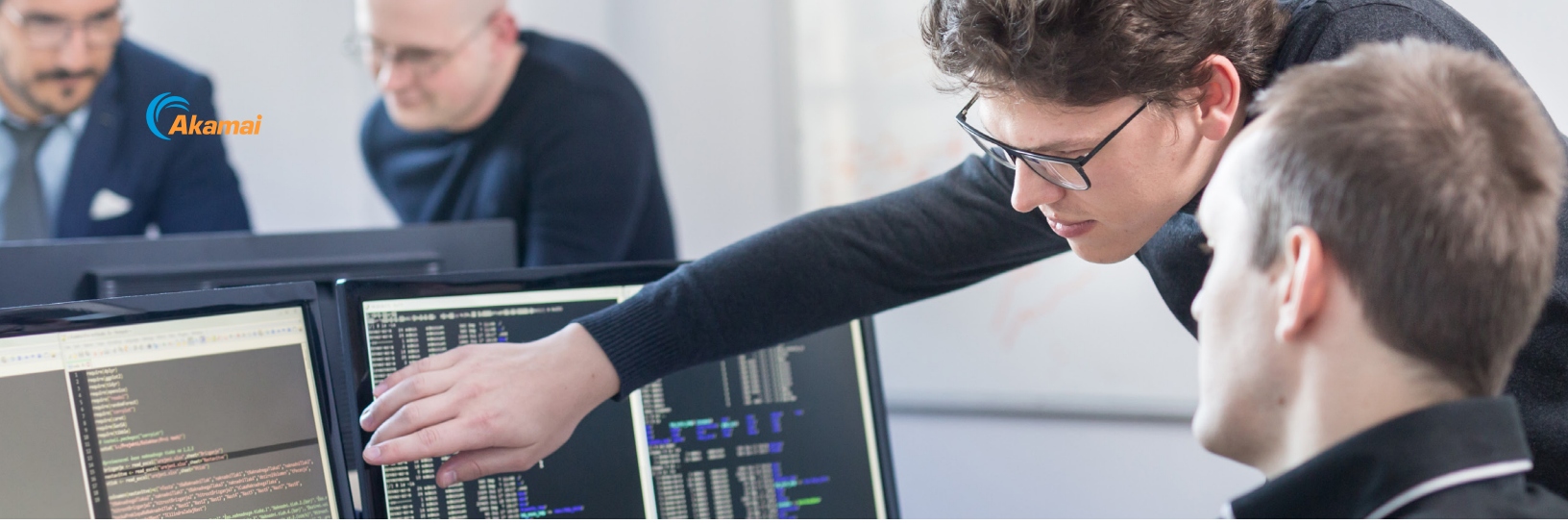
> "La progettazione non sicura è un'ampia categoria che include diversi punti deboli e può sintetizzarsi nell'espressione "progettazione dei controlli mancante o inefficace". C'è differenza tra progettazione non sicura e implementazione non sicura. Una progettazione non sicura può avere comunque dei difetti di implementazione che causano vulnerabilità che potrebbero essere sfruttate. Una progettazione non sicura non può essere corretta da un'implementazione perfetta in quanto, per definizione, i controlli di sicurezza necessari per difendersi da attacchi specifici non sono mai stati creati".
>
> - Fonte: owasp.org

Il contributo di Akamai

Le organizzazioni dovrebbero integrare la sicurezza fin dalle primissime fasi della progettazione. Tuttavia, i team di sviluppo potrebbero non essere in grado di farlo quando la sicurezza è difficile da integrare. I prodotti Akamai permettono di velocizzare lo shift left, per impedire che la mancanza di sicurezza della progettazione comprometta app e API.

- **App & API Protector**, che comprende la nostra soluzione WAAP e ASE, può inoltre rilevare e risolvere alcuni difetti di progettazione prima di passare alla produzione. Sfruttando l'automazione, inoltre, permette di snellire e semplificare le attività di routine, lasciando alle persone quelle che richiedono un'analisi umana e automatizzando invece aggiornamenti, ottimizzazione, rilevamento delle API, programmabilità semplificata e user experience.
- **Enterprise Application Access** garantisce solo agli utenti autorizzati di poter accedere alle applicazioni. Questo approccio basato sul privilegio minimo previene il movimento laterale verso altre applicazioni, il che può avvenire facilmente con le soluzioni di accesso alla rete, come le VPN.





A05: errata configurazione della sicurezza

> "[Dalla] precedente edizione, è stato esaminato il 90% delle applicazioni, alla ricerca di qualche forma di configurazione errata, con un tasso di incidenza del 4% e oltre 208.000 occorrenze di una CWE (Common Weakness Enumeration) in questa categoria di rischio. Senza un processo di configurazione della sicurezza concertato e ripetibile, i sistemi corrono un rischio molto più elevato".
>
> - Fonte: owasp.org

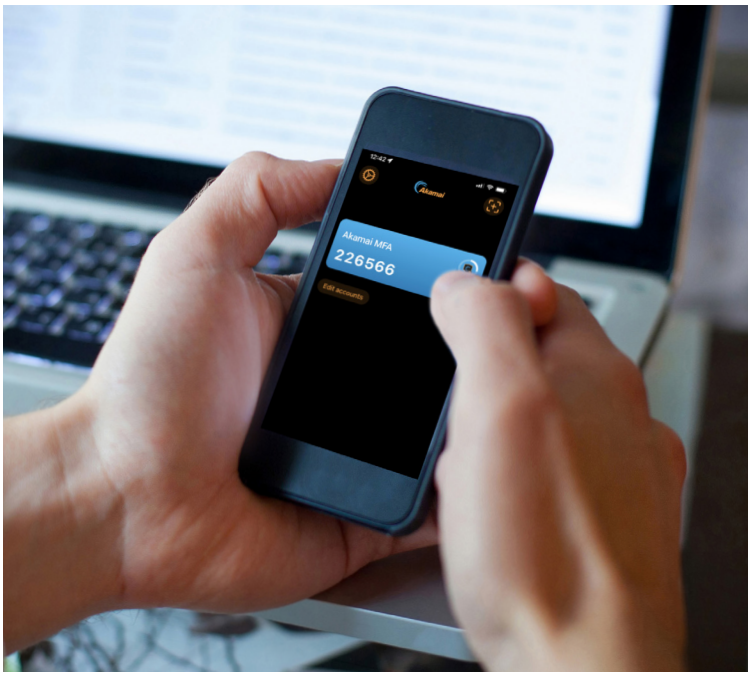
Il contributo di Akamai

Per definizione, i problemi di configurazione della sicurezza interessano molteplici aspetti, oltre a riguardare la corretta configurazione dei controlli di sicurezza da parte delle organizzazioni. I prodotti Akamai possono aiutarvi nei seguenti modi:

- Anche se non può sostituire una configurazione vera e propria, **App & API Protector** può aiutare in vari modi:
  1. Applicando gruppi di attacco alle anomalie in uscita, al fine di catturare le fughe di informazioni, come i codici di errore o il codice sorgente creato da un'errata configurazione della sicurezza.
  2. Implementando regole che possono individuare e arrestare gli attacchi XXE prima che il parser XML elabori l'entità esterna pericolosa.
  3. Implementando regole che possono individuare l'accesso a file sensibili noti lasciati dagli sviluppatori sui server di produzione.
- **Akamai Guardicore Segmentation** aiuta a proteggere dalla perdita di dati dovuta a configurazioni errate fornendo visibilità e controllo granulare su comunicazioni non autorizzate e non pianificate tra le vostre applicazioni e Internet.
- L'applicazione di patch virtuali con regole personalizzate può aiutare a gestire rapidamente le fughe di dati finché il vostro team non sarà in grado di applicare le patch.
- Con **App & API Protector** e **Bot Manager** è possibile proteggersi dagli attacchi di forza bruta effettuati con credenziali predefinite utilizzando i controlli della velocità.
- Una configurazione di sicurezza debole sulle intestazioni delle policy di sicurezza dei contenuti e altre intestazioni HTTP relative alla sicurezza può essere rafforzata sulla piattaforma Akamai.
- Con il rilevamento automatico delle API di **App & API Protector** potete rilevare ed effettuare il profiling continuo delle vostre API, inclusi endpoint, definizioni e caratteristiche di risorse e traffico.

A06: componenti vulnerabili e obsoleti

> "Componenti quali librerie, framework e altri moduli software vengono eseguiti con gli stessi privilegi dell'applicazione. Inoltre, gli script agiscono da risorse per le applicazioni affidabili con pieno accesso ai dati applicativi. Un componente vulnerabile violato può facilitare una grave perdita di dati o l'acquisizione del controllo del server".
>
> - Fonte: Akamai



Il contributo di Akamai

Le organizzazioni faticano a tenere traccia dei componenti di terze parti usati all'interno delle loro applicazioni e spesso i team di sicurezza non ne sono informati. Inoltre, le organizzazioni non hanno alcun controllo sui tempi con cui le vulnerabilità recenti vengono gestite da terzi, sempre che vengano gestite. Per mitigare la scarsa visibilità e l'incertezza servono una soluzione di sicurezza, come WAAP, e una protezione degli script come quella offerta dalle seguenti soluzioni:

- **App & API Protector** include molteplici regole progettate per risolvere le vulnerabilità note, sia nelle vostre applicazioni che nei componenti di terze parti. Offre inoltre funzionalità per proteggere le API, anche quando i componenti terzi in esse integrati le espongono ad abusi.
- Il modulo informativo **Akamai Guardicore Segmentation** vi consente di cercare le risorse presenti nella rete potenzialmente vulnerabili, mentre l'applicazione granulare inclusa consente di isolare eventuali risorse interessate dal problema finché non viene applicata la patch.
- L'applicazione di patch virtuali con regole personalizzate permette di gestire rapidamente vulnerabilità emergenti o nuove vulnerabilità emerse a seguito delle modifiche alle applicazioni, finché non sarà possibile applicare le patch.
- **Client Reputation** offre un punteggio di rischio per i client dannosi nella categoria Scansione web per la protezione dallo sfruttamento delle nuove vulnerabilità.
- **Page Integrity Manager** analizza costantemente il comportamento dell'esecuzione degli script, in sessioni con utenti reali, per identificare comportamenti sospetti o decisamente dannosi. Blocca inoltre l'esfiltrazione dei dati dagli script di prime e terze parti verso URL con vulnerabilità note usando un database CVE (Common Vulnerabilities and Exposures) aggiornato.

A07: errori di identificazione e autenticazione

> "Le funzioni delle applicazioni correlate all'autenticazione e alla gestione delle sessioni sono spesso implementate in modo errato, consentendo agli autori di attacchi di compromettere password, chiavi o token di sessione, oppure di sfruttare altri difetti di implementazione per assumere l'identità degli utenti in modo temporaneo o permanente".
>
> - Fonte: Akamai

Il contributo di Akamai

Le organizzazioni sono tenute a correggere eventuali falle per risolvere completamente questa vulnerabilità. Tuttavia, le soluzioni Akamai elencate di seguito possono aiutare a individuare e proteggere da molti dei vettori di attacco che cercano di sfruttare gli errori di identificazione e autenticazione:

- **Bot Manager** può individuare e mitigare gli attacchi automatizzati, ad esempio gli attacchi di credential stuffing.
- **Account Protector** mitiga i tentativi di controllo degli account in cui gli impostori cercano di ottenere l'accesso non autorizzato agli account degli utenti.
- **Enterprise Application Access** può delegare l'accesso alle applicazioni con un "modello di accesso basato sul privilegio minimo", riducendo la superficie di attacco dell'applicazione e ottimizzando l'accesso.
- **Akamai MFA** fornisce una robusta autenticazione usando la tecnologia FIDO2 resistente al phishing.
- **App & API Protector** offre una funzionalità di controllo della velocità, che può gestire gli attacchi di forza bruta.
- **Identity Cloud** offre una gestione sicura delle credenziali degli utenti finali e protegge le informazioni dei profili tramite l'autenticazione a due fattori e le funzionalità di autenticazione basate sui rischi.

A08: errori di integrità di software e dati

> "Gli errori di integrità di software e dati sono correlati a codici e infrastrutture che non proteggono da violazioni dell'integrità. Un esempio è quando un'applicazione si affida a plugin, librerie o moduli da fonti, archivi e CDN (reti per la distribuzione dei contenuti) non affidabili. Una pipeline CI/CD non sicura può introdurre il potenziale per un accesso non autorizzato, un codice dannoso o un sistema compromesso".
>
> - Fonte: owasp.org

Il contributo di Akamai

La soluzione WAAP consente alle organizzazioni di proteggere le applicazioni web e le API dagli errori di integrità dei dati e del software. Tuttavia, le organizzazioni sono tenute ad applicare sempre le patch alle applicazioni web per gestire eventuali vulnerabilità rilevate sulla base dei propri cicli di sviluppo.

- **App & API Protector**
  - Offre una protezione robusta dagli attacchi di deserializzazione.
  - Previene gli attacchi machine-in-the-middle che possono portare a problemi di integrità dei dati tramite l'implementazione delle versioni TLS più recenti e di una crittografia robusta.
  - Assicura l'autenticazione dell'origine dei dati e la protezione dell'integrità dei dati dei record DNS implementando DNSSEC con Edge DNS per prevenire la manomissione dei record DNS, che può indirizzare gli utenti verso fonti non affidabili.
- Il modulo informativo contenuto in **Akamai Guardicore Segmentation** consente di eseguire la query di qualsiasi risorsa presente nella rete che ha ricevuto l'aggiornamento corrotto. L'applicazione granulare inclusa consente, inoltre, di isolare le risorse interessate finché non viene fornita una correzione.
- **Enterprise Threat Protector** rileva gli attacchi di phishing, che possono avvicinare amministratori e utenti con privilegi avanzati delle applicazioni a ambienti ostili o fonti non affidabili.
- L'applicazione di patch virtuali con regole personalizzate permette di gestire rapidamente nuovi difetti di deserializzazione, finché non sarà possibile applicare le patch.
- **Page Integrity Manager** rileva script di terze parti, li monitora alla ricerca di cambiamenti e agisce sugli script che sono stati compromessi.

A09: errori di registrazione e monitoraggio della sicurezza

"La registrazione, il rilevamento, il monitoraggio e la risposta attiva insufficienti si verificano in qualsiasi momento:

- Eventi verificabili, quali accessi, accessi non riusciti e transazioni ad alto valore, non vengono registrati.
- Avvisi ed errori generano messaggi di registro inadeguati o non chiari o non li generano affatto.
- I registri delle applicazioni e le API non vengono monitorati alla ricerca di attività sospette.
- I registri vengono memorizzati localmente.
- Soglie di avvisi e processi di escalation delle risposte non sono in atto o sono inefficaci.
- I test e l'analisi di penetrazione tramite strumenti di test della sicurezza delle applicazioni dinamici (DAST) non attivano avvisi.

Le applicazioni non possono individuare, inoltrare o avvisare riguardo ad attacchi attivi in tempo reale o quasi."

- Fonte: owasp.org

Il contributo di Akamai

Gli errori di registrazione e monitoraggio della sicurezza rappresentano una falla nella capacità di un'organizzazione di individuare le vulnerabilità e i tentativi di sfruttarle. Akamai include molteplici funzionalità per fornire alle organizzazioni una maggiore visibilità sugli attacchi:

- Akamai offre dashboard e strumenti per la creazione di report all'interno dell'interfaccia utente grafica Akamai Control Center.
- I prodotti di sicurezza delle applicazioni di Akamai si integrano nell'infrastruttura SIEM esistente di un'organizzazione per correlare gli eventi rilevati da Akamai con quelli di altri fornitori di servizi di sicurezza.
- **Managed Security Service** offre funzionalità di analisi e risposta agli attacchi 24 ore su 24/7 giorni su 7.
- **App & API Protector** include una funzionalità Penalty Box che consente una maggiore registrazione degli IP che mostrano attività dannose o sospette per un'analisi più approfondita.
- **Enterprise Application Access** offre una soluzione di gestione delle identità integrata per autenticare e controllare l'accesso a tutte le applicazioni aziendali. Combinando tutto ciò con le funzionalità proxy basate sull'identità, le organizzazioni possono avere una visibilità dettagliata sulle azioni degli utenti, inclusa la visibilità su ogni azione GET/POST.
- **Enterprise Threat Protector** assicura una piena visibilità su tutte le richieste DNS esterne da parte di un'azienda, sia dannose che legittime.
- **Akamai Guardicore Segmentation** offre la visibilità approfondita nei flussi di comunicazione all'interno della vostra rete, in modo da attivare degli avvisi quando si verificano comunicazioni non autorizzate o non previste e di applicare le policy di sicurezza a livello di singolo processo o servizio per limitarle. Con il modulo di rilevamento delle violazioni aggiuntivo, è possibile individuare e risolvere rapidamente le potenziali minacce.

A10: falsificazione richieste lato server

> "Gli attacchi SSRF si verificano quando un'applicazione web recupera una risorsa remota senza convalidare l'URL fornito dall'utente. Ciò consente all'autore di un attacco di forzare l'applicazione a inviare una richiesta creata a una destinazione inattesa, anche quando è protetta da un firewall, una VPN o un altro tipo di elenco di controllo degli accessi alla rete (ACL)".
>
> - Fonte: owasp.org

Il contributo di Akamai

Akamai WAAP include regole che cercano attacchi injection negli URL. Questa funzionalità può impedire agli autori di attacchi di indurre il server a inviare una richiesta che potrebbe essere interpretata come valida dai vostri analisti della sicurezza.

- Le regole di **App & API Protector** aiutano a impedire in primo luogo che queste richieste di exploit raggiungano il server vulnerabile.
- **Akamai Guardicore Segmentation** può monitorare e bloccare il traffico in uscita non previsto a livello di server.

Conclusione

Per sviluppare la migliore difesa contro le vulnerabilità indicate nell'elenco OWASP Top 10, le organizzazioni e i loro fornitori di soluzioni di sicurezza devono collaborare per portare alla luce queste vulnerabilità il prima possibile e implementare soluzioni per mitigarle. Scoprite maggiori informazioni relative ai prodotti per la sicurezza sull'edge di Akamai. Se desiderate discutere ed esplorare il modo in cui possiamo collaborare per creare la migliore protezione per la vostra azienda, contattate il vostro rappresentante vendite Akamai.

A sostegno e protezione della vita online c'è sempre Akamai. Le principali aziende al mondo scelgono Akamai per creare, offrire e proteggere le loro experience digitali, aiutando miliardi di persone a vivere, lavorare e giocare ogni giorno. Con la piattaforma di computing più distribuita al mondo, dal cloud all'edge, siamo in grado di semplificare lo sviluppo e l'esecuzione di applicazioni per i nostri clienti, avvicinando le experience agli utenti e allontanando le minacce. Per ulteriori informazioni sulle soluzioni per la sicurezza, il computing e la delivery di Akamai, visitate il sito akamai.com e akamai.com/blog o seguite Akamai Technologies su Twitter e LinkedIn. Data di pubblicazione: 10/22.