WHITE PAPER

Privacy intrinseca

Come i servizi Bot Manager Premier e Page Integrity Manager di Akamai rispettano i requisiti di privacy dell'UE

Panoramica

Akamai si rende conto di quanto sia importante proteggere i dati personali e mantenere la conformità ai requisiti di privacy per instaurare la fiducia nelle tecnologie e nei servizi offerti. Questo white paper illustra il modo con cui Bot Manager Premier[1] e Page Integrity Manager rispettano la direttiva ePrivacy dell'UE e il regolamento generale sulla protezione dei dati (GDPR)[2] per valutare i rischi legati all'utilizzo di tali servizi.

Bot Manager Premier è concepito per individuare le richieste di accesso automatizzato alle proprietà web, generate da (ro)bot the simulano i comportamenti umani al fine di raccogliere e sfruttare i dati di accesso degli utenti finali.

Page Integrity Manager rileva i codici JavaScript inseriti in queste proprietà per scopi illeciti. Una volta rilevati bot e script, Akamai li classifica come attività dannose o meno in base alle istruzioni fornite, alle conoscenze comuni e alla nostra intelligence sulle minacce. Mentre le attività dannose vengono bloccate, solo i bot e gli script non dannosi possono accedere ai server, all'infrastruttura e ai dati di origine.

Entrambi i servizi garantiscono la protezione dei dati personali forniti dagli utenti finali da rischi di esfiltrazione e abuso. L'importanza di proteggersi da tali minacce è dimostrata dai recenti episodi di violazione della sicurezza e dei dati subiti da British Airways e The North Face.

Architettura di Bot Manager Premier

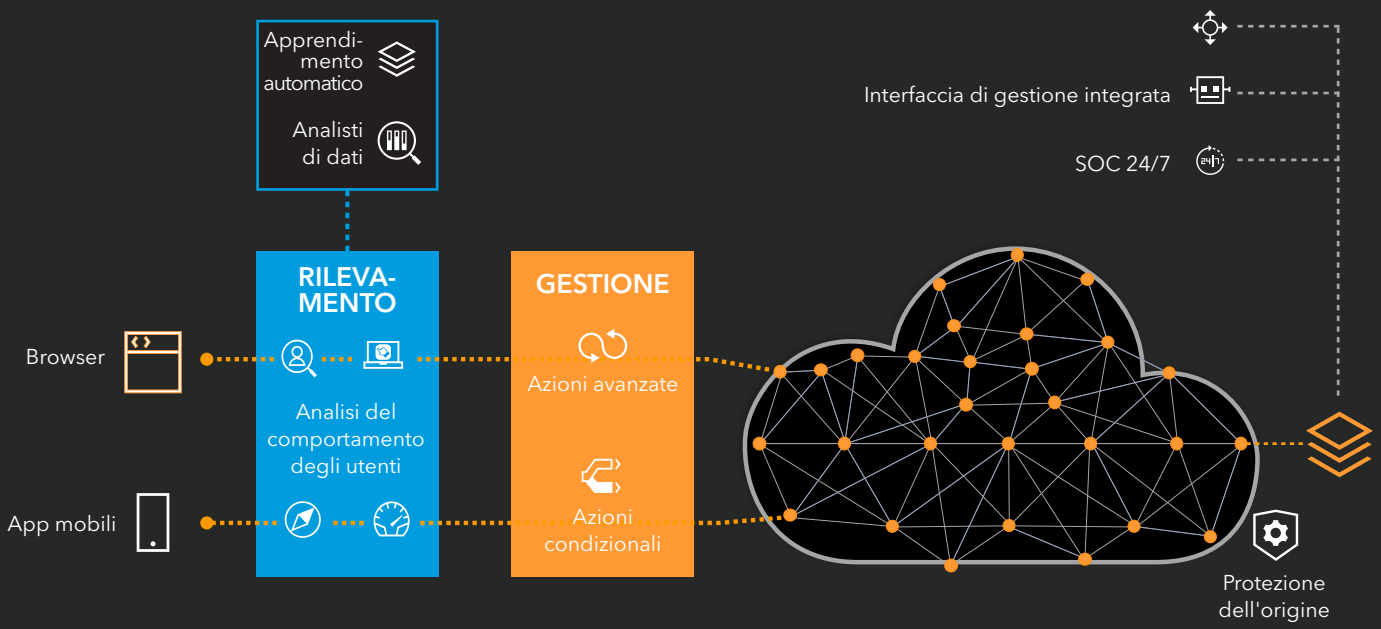


Fig. 1: architettura di Bot Manager Premier

Architettura di Page Integrity Manager

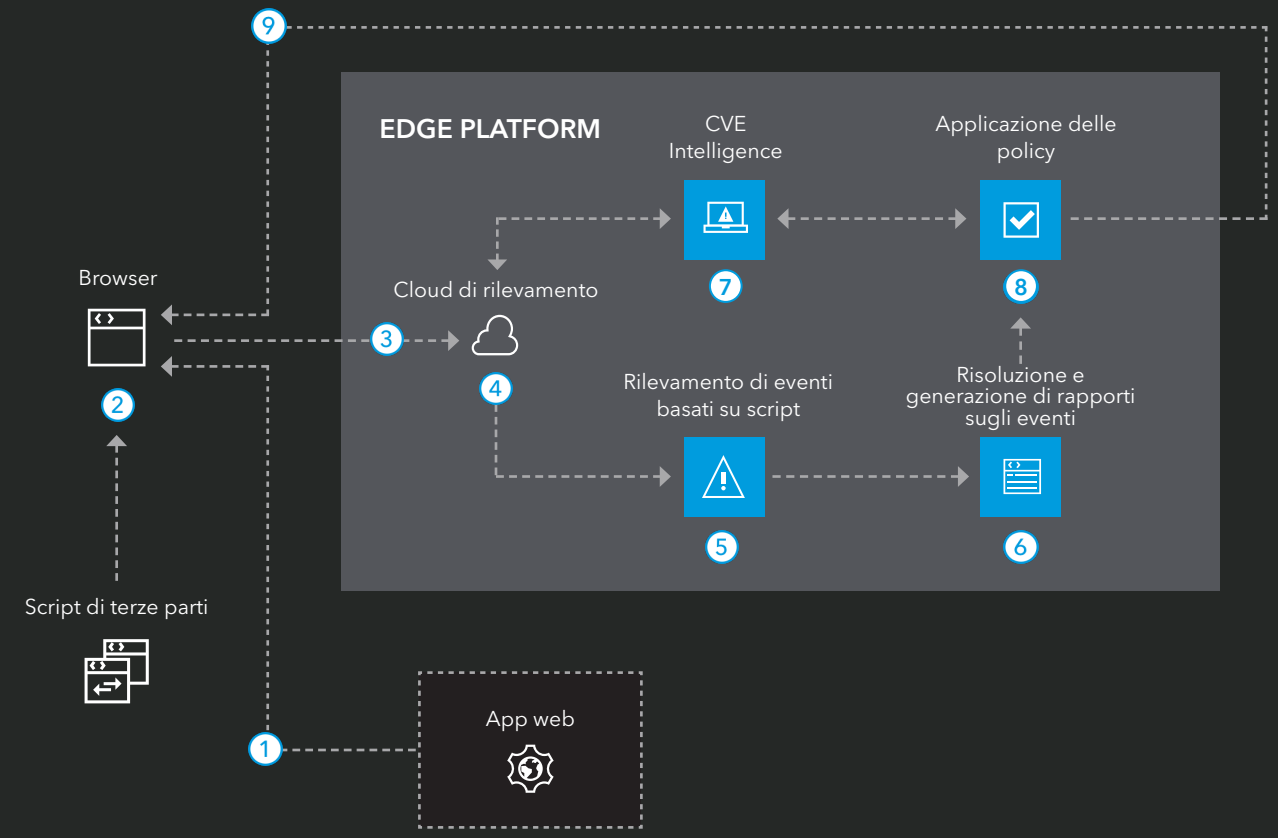


Fig. 2: architettura di Page Integrity Manager

Da un punto di vista tecnico, il rilevamento di bot e script viene effettuato tramite l'inserimento di codici JavaScript o l'integrazione di kit di sviluppo software (SDK) per app mobili, nonché attraverso le statistiche raccolte sulla rete, sul browser e sui dati comportamentali. Bot Manager Premier analizza i dati per stabilire se l'attività è stata originata da un bot o da una persona, mentre Page Integrity Manager identifica tutti gli script inseriti nelle proprietà web. Tutte le attività di bot e script rilevate vengono poi classificate come dannose o meno e quelle dannose vengono bloccate per evitare rischi di esfiltrazione dei dati.

Da un punto di vista della privacy, in base alle normative dell'UE l'inserimento di codici JavaScript e l'integrazione di kit di sviluppo software (SDK) vengono classificati come "tecnologie cookie" e determinano l'applicazione delle leggi sull'ePrivacy. Inoltre, poiché alcuni dati raccolti, come l'indirizzo IP dell'utente finale, vengono classificati come dati personali, scatta l'applicazione del GDPR.

Conformità alle leggi sull'ePrivacy dell'UE

Per l'utilizzo della tecnologia cookie di Bot Manager Premier e Page Integrity Manager in conformità con le leggi dell'UE sulla privacy, vengono applicate due eccezioni alle regole generali: l'eccezione del consenso e il meccanismo di revoca del consenso. Queste eccezioni consentono di posizionare Bot Manager Premier e Page Integrity Manager sulle proprietà web per un'operatività immediata.

Applicazione dell'eccezione del consenso

Per impostazione predefinita, la direttiva ePrivacy richiede di raccogliere il consenso dell'utente finale per l'utilizzo di tecnologie cookie e la raccolta dei dati correlati. Solo nel caso in cui il cookie sia strettamente necessario per fornire un servizio informatico (sulle proprietà web) esplicitamente richiesto da un abbonato o un utente (l'utente finale), non sarà richiesto il consenso per l'utilizzo e la tecnologia cookie potrà essere utilizzata immediatamente.[3]

La maggior parte degli stati membri dell'UE ha aderito a questa eccezione nelle leggi di recepimento locali della direttiva ePrivacy.

La tecnologia cookie utilizzata per Bot Manager Premier e Page Integrity Manager è necessaria all'utilizzo dei servizi. Senza l'inserimento di codici JavaScript, non sarebbe possibile raccogliere e analizzare i dati né individuare e bloccare bot o script. Lo scopo della raccolta dei dati è proteggere i dati personali forniti tramite le proprietà web da tentativi di violazione, esfiltrazione e abuso. Le autorità locali di protezione dei dati hanno confermato che l'utilizzo della tecnologia cookie per prevenire frodi e altri servizi di sicurezza rientra nell'eccezione del consenso.[4] La seguente tabella mostra la modalità di applicazione dell'eccezione del consenso per i servizi di sicurezza da parte dell'ICO (Information Commissioner's Office) nel Regno Unito.[5]

Attività	Probabile eccezione?
Sicurezza	**Dipende dalla limitazione delle finalità.** I cookie diretti utilizzati per finalità di sicurezza possono basarsi su eccezioni strettamente necessarie, come, ad esempio, i cookie utilizzati per rilevare i ripetuti tentativi di accesso non riuscito. Possono anche avere una durata più lunga rispetto ai cookie di sessione. Tuttavia, i cookie legati alla sicurezza di altri servizi online richiedono il consenso dell'utente perché la funzionalità richiesta dall'utente è legata al proprio servizio, non a quello di altri. Se si utilizzano tecniche di fingerprinting per un dispositivo con scopi specifici di sicurezza, è possibile basarsi su un'eccezione strettamente necessaria. Tuttavia, come con i cookie, se le informazioni vengono trattate per finalità secondarie, come quelle legate alla sicurezza di servizi online non richiesti dall'utente, è necessario il consenso dell'utente. Lo stesso vale nel caso in cui le informazioni vengano trattate allo scopo di prevenire le frodi, soprattutto se più servizi online utilizzano un unico servizio di prevenzione delle frodi, che tratta le informazioni degli utenti di tali servizi.

Applicazione dell'eccezione alla revoca del consenso

Le leggi sull'ePrivacy stabiliscono che gli enti devono offrire agli utenti finali un meccanismo per revocare il loro consenso relativamente alla raccolta dei dati tramite la tecnologia cookie. Tale requisito riflette il diritto a opporsi previsto dall'articolo 21 del GDPR.[6]

Tuttavia, esiste il caso limite in cui si abusa di questo diritto al controllo e si applica una revoca che evita lo svolgimento delle attività di protezione dei dati. Questo caso limite consiste nella fornitura di un servizio di sicurezza basato su una tecnologia cookie.

Se si rifiuta di fornire il consenso alla tecnologia cookie utilizzata per rilevare bot e script dannosi, vengono arrestati i servizi di sicurezza utilizzati per la protezione da accessi non autorizzati ai dati personali. Purché la tecnologia cookie venga utilizzata esclusivamente per scopi di sicurezza, la mancanza di controllo sulla raccolta dei dati tramite la tecnologia cookie per l'utente finale non inficia le libertà e i diritti di cui gode l'utente. Al contrario, questa mancanza di controllo garantisce un utilizzo continuo della tecnologia cookie per la protezione dei dati personali da accessi non autorizzati.

I responsabili della privacy in tutto il mondo concordano sulla necessità di adottare questa eccezione alla revoca del consenso: nel caso in cui un meccanismo di controllo dei dati offerto a singoli individui (utenti finali) viene sfruttato per accedere a tali dati in maniera non autorizzata, il meccanismo di controllo dei dati diventa inutile e non deve essere utilizzato. In altre parole, è buona norma preferire l'utilizzo di servizi di sicurezza all'avanguardia ad un meccanismo di controllo dei dati (revoca del consenso) relativo alla tecnologia cookie.[7]

Conformità alle leggi UE sulla protezione dei dati

Bot Manager Premier e Page Integrity Manager trattano i dati in conformità al GDPR e ad altre leggi applicabili in materia di protezione dei dati o privacy, inclusi il tipo di dati personali raccolti e la finalità della raccolta.

Tipo di dati personali

Bot Manager Premier e Page Integrity Manager raccolgono dati relativi alla rete, al browser e al comportamento, come sessione TCP, sessione TLS, ID sessione, user agent, intestazione della richiesta, URL visitati, indicatore di data e ora, indirizzo IP dell'utente finale, impostazioni del browser e dati di geolocalizzazione degli edge server, nonché dati relativi al comportamento come tocchi dello schermo, movimenti del mouse e pressioni dei tasti.

Finalità

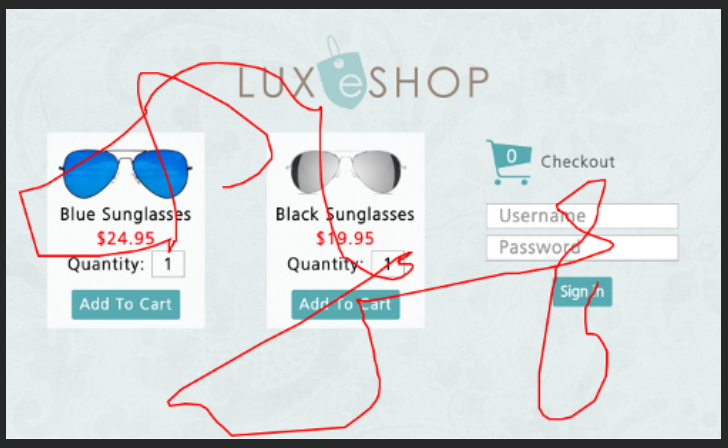
La finalità alla base della raccolta e dell'analisi dei dati consiste nel rilevamento di bot e script dannosi che simulano il comportamento umano nelle proprietà web, così come la prevenzione da rischi di esfiltrazione di dati e abusi da essi perpetrati.

Per soddisfare tale finalità, Akamai analizza il modo con cui un dispositivo viene utilizzato quando accede alle proprietà web. Akamai non identifica l'utente finale quando effettua questo tipo di analisi né crea profili degli utenti finali. Inoltre, i dati sul comportamento raccolti non vengono utilizzati al solo scopo di identificare un individuo. I dati, pertanto, non devono essere classificati come dati biometrici ai sensi del GDPR[8] né come dati sensibili (nei termini degli Stati Uniti) o categorie speciali di dati (nei termini dell'UE).

Akamai raccoglie e analizza i dati sul comportamento per determinare se l'accesso alla proprietà web viene effettuato da un bot o da una persona, come descritto dalle seguenti figure.

Eventi del mouse

Esempio di una persona



Esempi di un bot

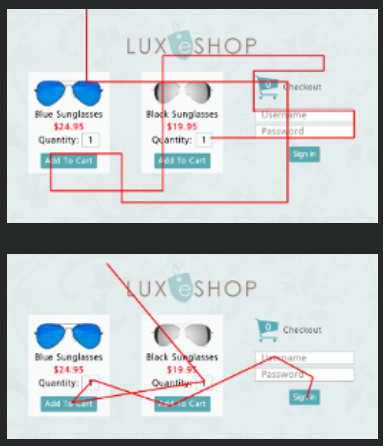
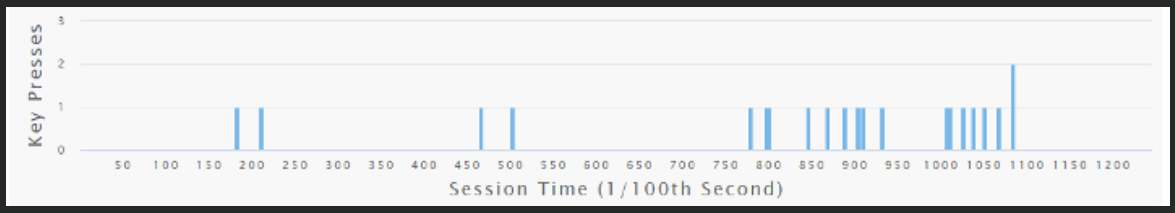


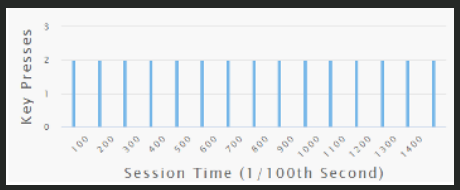
Fig. 3: i bot sofisticati tentano di nascondersi muovendo il mouse per emulare l'interazione di un utente. Tuttavia, dopo un certo numero di movimenti, emerge uno schema. Akamai è in grado di rilevare questi schemi per identificare un bot.

Rilevamento di schemi di pressione dei tasti

Pressioni dei tasti da parte di una persona



Esempio di pressione dei tasti da parte di un bot



Esempio di pressione dei tasti da parte di un bot

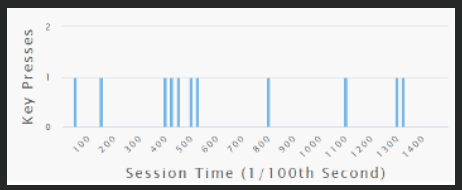


Fig. 4: le persone, in genere, premono casualmente i tasti, al contrario di un bot sofisticato. Esaminando la velocità e il ritmo delle pressioni dei tasti da parte di una persona, Akamai riesce a stabilire con maggior precisione se l'utente è un bot.

Base giuridica

La base giuridica per il trattamento è il legittimo interesse di Akamai nel fornire servizi per la sicurezza di informazioni e reti tramite il blocco e il rilevamento di bot e script dannosi. Il legittimo interesse è una base giuridica riconosciuta e atta a fornire servizi di sicurezza ai sensi del GDPR.[9]

Akamai fornisce e protegge fino al 30% di tutto il traffico in Internet. Senza i suoi servizi per la gestione di bot e script, si verificherebbe un numero molto maggiore di episodi di esfiltrazione e abuso di dati online, con un conseguente danno ai diritti e alle libertà degli utenti finali.

Valutazione di necessità e proporzionalità

Il trattamento dei dati è necessario affinché i servizi per la sicurezza di informazioni e reti di Akamai vengano considerati all'avanguardia ai sensi delle leggi in materia di privacy. Effettuando un'analisi dei dati raccolti relativamente alla rete, al browser e al comportamento, Akamai riesce a distinguere con precisione se le azioni sono eseguite da bot o persone, rilevando gli script inseriti in una proprietà web.

L'analisi di tutti i dati raccolti è proporzionata, considerando la sofisticatezza dei bot e degli script odierni. Se viene ridotta la quantità di dati raccolti ne risente l'accuratezza dell'analisi, il che determina un rilevamento meno efficace delle attività dannose. Non è possibile individuare i bot analizzando soltanto gli indirizzi IP degli utenti finali. Anche se i dati sul browser e sulla rete indicano un uso del dispositivo, si limitano a meccanismi passivi, basati su firme e soggetti a un numero elevato di falsi positivi e falsi negativi. La sicurezza all'avanguardia per le proprietà web[10] si estende al rilevamento di bot sofisticati. I bot attivi che simulano il comportamento umano vengono rilevati soltanto se si analizzano i dati relativi al comportamento.

Raccogliere altri dati sarebbe eccessivo perché l'analisi non risulterebbe migliorata.

Valutazione del rischio

Il rischio di danneggiare i diritti e le libertà degli utenti finali in relazione alle attività di trattamento eseguite da Bot Manager Premier e Page Integrity Manager è basso. I dati relativi al browser, alla rete e al comportamento non vengono classificati come altamente riservati, sensibili o appartenenti ad una categoria speciale di dati personali.[11] Le attività di trattamento di Akamai relative a Bot Manager Premier e a Page Integrity Manager vengono descritte nell'Informativa sulla privacy di Akamai e rese trasparenti alle parti interessate. Akamai aderisce al principio di minimizzazione dei dati in quanto raccoglie soltanto i dati necessari al rilevamento di bot e JavaScript.

Akamai dispone di appropriate misure tecniche e organizzative messe in atto per proteggere i dati personali trattati da accessi non autorizzati da parte di terze parti. Anche queste misure sono state pubblicate con trasparenza sul nostro sito web: Programma sulla sicurezza delle informazioni di Akamai e Misure tecniche e organizzative di Akamai.

L'analisi del rilevamento di bot e script viene effettuata sui sistemi Akamai implementati negli Stati Uniti. Di conseguenza, se utenti finali dell'UE accedono a proprietà web protette da Bot Manager Premier e Page Integrity Manager, l'analisi richiederà il trattamento dei dati personali dell'UE negli Stati Uniti. Per garantire un'adeguata protezione dei dati relativamente al trattamento negli Stati Uniti, Akamai ha adottato le clausole contrattuali standard dell'UE all'interno del gruppo Akamai, con i propri clienti e subincaricati, implementando ulteriori misure tecniche di salvaguardia per la protezione dei dati personali da accessi di terze parti.

Akamai applica gli stessi requisiti di protezione dei dati in tutte le entità del gruppo, a prescindere dalla posizione in cui si trovano tali entità. Abbiamo messo in atto ulteriori misure per proteggere i dati trasferiti dall'accesso di terze parti. Inoltre, secondo Akamai, i dati trasferiti negli Stati Uniti da Akamai per Bot Manager Premier e Page Integrity Manager non rientrano nel tipo di dati a cui sono interessate le agenzie di sorveglianza (americane) nell'espletamento delle loro attività.[12] La maggior parte dei dati è liberamente accessibile per stabilire una connessione a Internet ed eventuali terze parti non devono necessariamente richiedere tali dati ad Akamai (esistono modi più comodi per consentire a terze parti di accedere a tali dati). Di conseguenza, Akamai ha valutato un minimo rischio di accesso da terze parti ai suoi dati trasferiti negli Stati Uniti per Bot Manager Premier e Page Integrity Manager. Per informazioni, è possibile consultare l'Informativa sul trasferimento dei dati di Akamai nel Privacy Trust Center di Akamai.

In conformità ai principi di minimizzazione e sicurezza dei dati, Akamai ha fissato un periodo di conservazione dei dati pari a 90 giorni. Tale periodo è appropriato se si considera la necessità di dover analizzare i dati relativi alla rete, al browser e al comportamento in un certo periodo di tempo all'interno di più aree geografiche per un rilevamento di bot e script più efficace.

I servizi per il rilevamento e la gestione di bot e script forniti da Akamai non solo proteggono le proprietà web, ma migliorano anche lo stato di Internet in generale. Individuando e bloccando bot e script sull'Akamai Intelligent Edge Platform, non solo possiamo prevenire eventuali rischi di esfiltrazione e abuso dei dati personali degli utenti finali, ma consentire anche a milioni di utenti finali di trarre vantaggio da un'intelligence sulle minacce per i servizi di rete e sicurezza.

Misure di mitigazione

Akamai è riuscita sempre a mitigare i rischi per i diritti e le libertà dei soggetti interessati causati dall'uso dei servizi Bot Manager Premier e Page Integrity Manager. Durante la raccolta dei dati sul comportamento, l'utente finale non viene identificato. Inoltre, Akamai ha adeguatamente protetto i dati personali e messo in atto misure aggiuntive per garantire un'appropriata protezione dei dati trasferiti dal rischio di accesso da terze parti.

Riepilogo

I servizi Bot Manager Premier e Page Integrity Manager di Akamai rispettano le leggi UE sulla protezione dei dati. La tecnologia di cookie utilizzata per l'uso dei servizi è strettamente necessaria e serve a proteggere i dati personali dell'utente finale, pertanto viene richiesto il consenso e viene applicato il meccanismo di revoca del consenso.

La raccolta dei dati necessari all'utilizzo dei servizi è legittima, necessaria e proporzionata. Inoltre, le misure di mitigazione intraprese garantiscono che il rischio causato dalle attività di trattamento sui diritti e le libertà degli utenti finali sia molto basso. I vantaggi derivanti dalle performance di Bot Manager Premier e Page Integrity Manager per gli utenti finali superano i rischi poiché una maggiore sicurezza di Internet va a beneficio di tutti.

Akamai Technologies
Dr. Anna Schmits, EMEA DPO

Fonti:

1. Le dichiarazioni qui presenti si riferiscono anche al servizio Bot Manager Standard di Akamai, tranne per la raccolta dei dati, che si limita ai dati relativi alla rete al browser. Ulteriori informazioni su Akamai Bot Manager: https://learn.akamai.com/it-it/products/cloud_security/bot_manager.html
2. Vedere il white paper sulla privacy digitale disponibile all'indirizzo: https://ec.europa.eu/digital-single-market/en/online-privacy
3. Cfr. la rettifica all'articolo 5 (3) della direttiva ePrivacy 2002/58/CE in base alla direttiva 2006/24/CE disponibile all'indirizzo: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN.
4. Vedere, ad esempio, le linee guida sui cookie stilate dall'ICO nel Regno Unito, disponibili all'indirizzo https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-the-rules-on-cookies-and-similar-technologies/#rules9, le linee guida del CNIL francese, disponibili all'indirizzo https://www.cnil.fr/en/cookies-and-other-tracking-devices-council-state-issues-its-decision-cnil-guidelines, oppure le linee guida della Commissione delle autorità tedesche, disponibili (solo in tedesco) all'indirizzo https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf.
5. Vedere le linee guida dell'ICP sui cookie, disponibili all'indirizzo: https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/#comply16.
6. Vedere l'articolo 21 (1) del GDPR, disponibile all'indirizzo: https://gdpr-info.eu/art-21-gdpr/.
7. Vedere, ad esempio, le linee guida dell'ICO, disponibili all'indirizzo: https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-the-rules-on-cookies-and-similar-technologies/#rules9.
8. Vedere l'articolo 9 (1) del GDPR, disponibile all'indirizzo: https://gdpr-info.eu/art-9-gdpr/.
9. Vedere l'articolo 49 del GDPR, disponibile all'indirizzo: https://gdpr-info.eu/recitals/no-49/
10. Come previsto dall'articolo 32 del GDPR, disponibile all'indirizzo: https://gdpr-info.eu/art-32-gdpr/
11. Vedere l'articolo 9 del GDPR, disponibile all'indirizzo: https://gdpr-info.eu/art-9-gdpr/
12. Misure di salvaguardia della privacy negli Stati Uniti basate sulle decisioni del comitato scientifico per la sicurezza dei consumatori (CSSC) e su altre basi giuridiche europee per il trasferimento dei dati in Europa o negli Stati Uniti dopo la sentenza Schrems II, settembre 2020.
Disponibili all'indirizzo: https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF

Akamai *Intelligent Security Starts at the Edge*

Akamai garantisce experience digitali sicure per le più grandi aziende a livello mondiale. L'Akamai Intelligent Edge Platform permea ogni ambito, dalle aziende al cloud, permettendovi di lavorare con rapidità, efficacia e sicurezza. I migliori brand a livello globale si affidano ad Akamai per ottenere un vantaggio competitivo grazie a soluzioni agili in grado di estendere la potenza delle loro architetture multicloud. Più di ogni altra azienda, Akamai avvicina agli utenti app, experience e processi decisionali, tenendo lontani attacchi e minacce. Il portfolio Akamai di soluzioni per l'edge security, le web e mobile performance, l'accesso aziendale e la delivery di contenuti video è affiancato da un servizio clienti di assoluta qualità e da un monitoraggio 24 ore su 24, 7 giorni su 7, 365 giorni all'anno. Per scoprire perché i principali brand mondiali si affidano ad Akamai, visitate il sito **www.akamai.com** o **blogs.akamai.com** e seguite **@Akamai** su Twitter. Le informazioni di contatto internazionali sono disponibili all'indirizzo **www.akamai.com/locations**. Data di pubblicazione: 03/21.