WHITEPAPER

Privacy by Design

So erfüllen die Akamai-Services Bot Manager Premier und Page Integrity Manager die EU-Datenschutzanforderungen

Übersicht

Bei Akamai wissen wir, dass der Schutz personenbezogener Daten und die Einhaltung von Datenschutzauflagen unerlässlich ist, um das Vertrauen der Verbraucher in Technologie und Services zu gewinnen. In diesem Whitepaper erfahren Sie, wie Bot Manager Premier[1] und Page Integrity Manager die Anforderungen der europäischen ePrivacy-Verordnung sowie der Datenschutz-Grundverordnung (DSGVO)[2] erfüllen, damit Sie die Risiken beim Betrieb dieser Services bewerten können.

Bot Manager Premier wurde entwickelt, um automatisierte Anfragen zum Zugriff auf Ihre Webressourcen zu erkennen. Diese Anfragen werden von Bots generiert, die menschliches Verhalten nachahmen, um Anmeldedaten von Endnutzern zu stehlen und auszunutzen. Page Integrity Manager wiederum erkennt JavaScripts, die für kriminelle Zwecke in diese Webressourcen injiziert werden. Nachdem Bots und Skripte erkannt wurden, kategorisiert Akamai sie als schädliche oder legitime Aktivität – gemäß Ihren Anweisungen, öffentlichen Informationen und unserer Threat Intelligence. Nach dieser Kategorisierung wird schädliche Aktivität blockiert, während legitimen Bots und Skripten der Zugriff auf Ihre Ursprungsserver, Infrastrukturen und Daten gewährt wird.

Beide Services schützen von Endnutzern bereitgestellte personenbezogene Daten vor Diebstahl und Missbrauch. Wie wichtig der Schutz vor diesen Bedrohungen ist, zeigen unter anderem die jüngsten Sicherheits- und Datenschutzvorfälle bei British Airways und The North Face.

Architektur von Bot Manager Premier

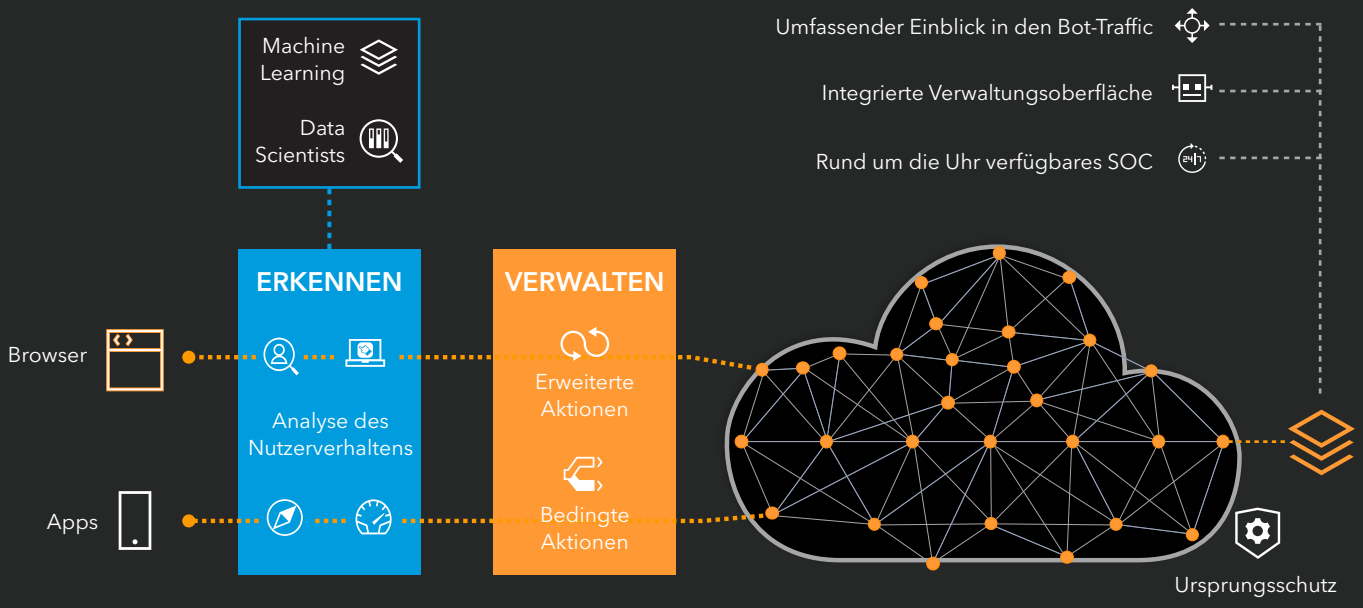


Abb. 1: Architektur von Bot Manager Premier

Architektur von Page Integrity Manager

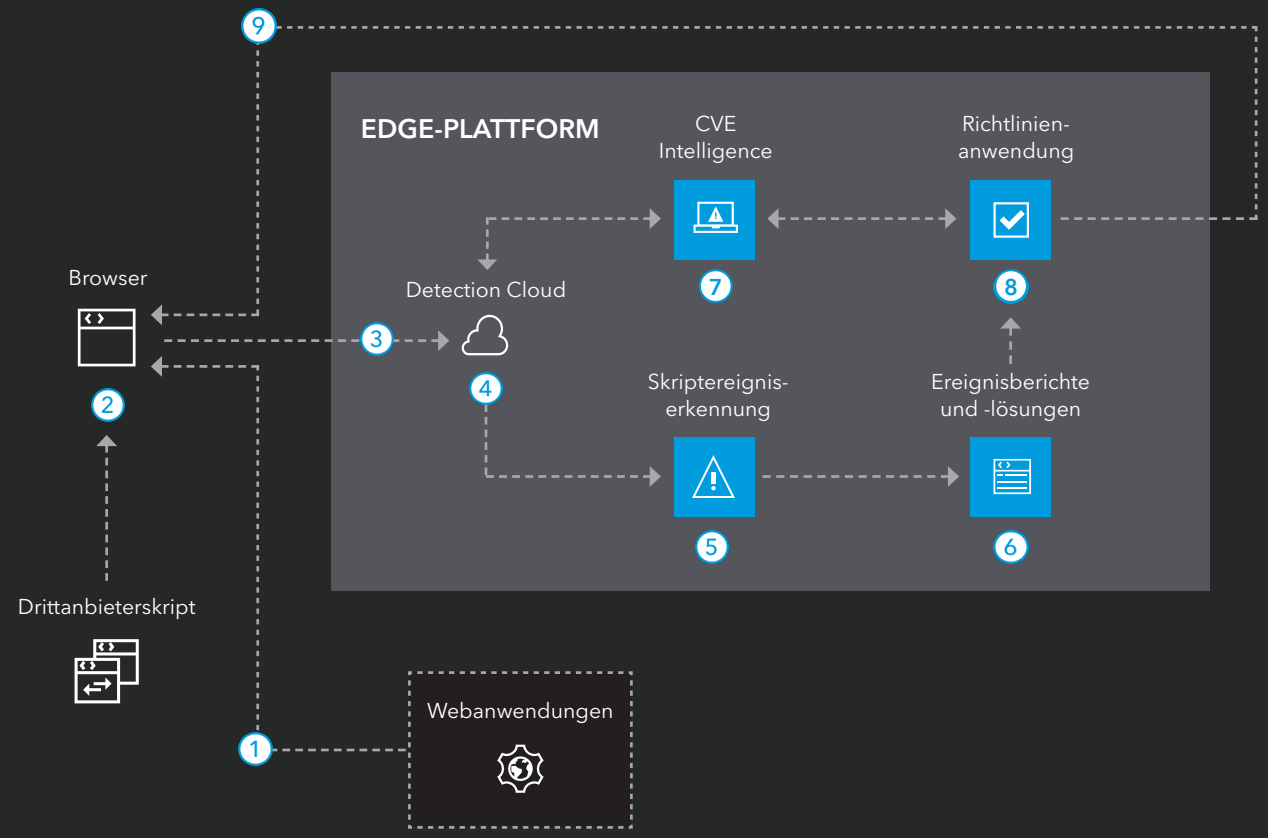


Abb. 2: Architektur von Page Integrity Manager

Die Bot- und Skripterkennung wird per JavaScript Injection oder App-SDK-Integration (Software Development Kit) durchgeführt. Hierbei kommen auch die erfassten Daten aus der Analyse von Netzwerk, Browser und Nutzerverhalten zum Einsatz. Bot Manager Premier analysiert die Daten, um zu bestimmen, ob die Aktivität von einem Bot oder einem Menschen stammt. Gleichzeitig erkennt Page Integrity Manager alle Skripte, die in Webressourcen injiziert werden. Anschließend werden sämtliche Bot- und Skriptaktivitäten als schädlich oder legitim eingestuft und schädliche Aktivität wird blockiert, um Datenextraktion zu verhindern.

JavaScript Injection und SDK-Integration sind in den EU-Gesetzen als „Cookietechnologie" klassifiziert und unterliegen so den ePrivacy-Verordnungen. Darüber hinaus sind einige der erfassten Daten, wie z. B. die IP-Adresse des Endnutzers, als personenbezogene Daten kategorisiert, weshalb hier die DSGVO greift.

Compliance mit europäischer ePrivacy-Verordnung

Bei der Verwendung der Cookietechnologien von Bot Manager Premier und Page Integrity Manager gemäß den EU-Datenschutzgesetzen gelten zwei Ausnahmen von den allgemeinen Regeln: für die Einwilligung und den Opt-out-Mechanismus. Dank dieser Ausnahmen können Sie Bot Manager Premier und Page Integrity Manager in Ihre Webressourcen integrieren und sofort einsetzen.

Anwendung der Einwilligungsausnahme

Standardmäßig sieht die ePrivacy-Verordnung vor, dass Unternehmen die Einwilligung des Endnutzers einholen, bevor sie Cookietechnologie einsetzen und zugehörige Daten erfassen. Nur in Fällen, in denen das Cookie zwingend erforderlich ist, um (über Ihre Webressource) einen Dienst der Informationsgesellschaft zu erbringen, den der Endnutzer explizit angefordert hat, ist die Einwilligung für die Cookienutzung nicht erforderlich und die Cookietechnologie kann umgehend verwendet werden.[3]

Die meisten EU-Mitgliedstaaten haben diese Ausnahme in ihre lokalen Umsetzungsgesetze der ePrivacy-Verordnung integriert.

Die Cookietechnologie, die bei Bot Manager Premier und Page Integrity Manager zum Einsatz kommt, ist für den Betrieb der Services zwingend erforderlich. Ohne JavaScript Injection können keine Daten erfasst und analysiert werden. Und ohne Datenanalyse können keine Bots und Skripte erkannt und blockiert werden. Der Zweck der Datenerfassung besteht darin, personenbezogene Daten, die an Ihre Webressourcen übermittelt werden, vor Diebstahl und Missbrauch zu schützen. Die lokalen Datenschutzbehörden haben den Einsatz von Cookietechnologie zur Betrugsbekämpfung bestätigt und auch andere Sicherheitsdienste fallen unter diese Einwilligungsausnahme.[4] Die folgende Tabelle zeigt, unter welchen Bedingungen das Information Commissioner's Office (ICO) im Vereinigten Königreich die Einwilligungsausnahme für Sicherheitsdienste anwendet.[5]

Aktivität	Wie wahrscheinlich ist die Ausnahme?
Sicherheit	**Abhängig von der Zweckbindung.** Bei Cookies von Erstanbietern, die für Sicherheitszwecke eingesetzt werden, wird die zwingend notwendige Ausnahme angewendet. Hierunter fallen beispielsweise Cookies, die zur Erkennung wiederholt fehlgeschlagener Anmeldeversuche verwendet werden. Sie dürfen darüber hinaus eine längere Lebensdauer aufweisen als ein Sitzungscookie. Cookies, die die Sicherheit anderer Onlinedienste als Ihres eigenen betreffen, erfordern jedoch weiterhin eine Einwilligung. Grund hierfür ist, dass die Funktion, die der Nutzer angefordert hat, Ihren Dienst betrifft und nicht die Dienste Dritter. Auch wenn Sie Fingerabdruckmethoden für einen bestimmten Sicherheitszweck einsetzen, wird die zwingend erforderliche Ausnahme angewendet. Wie bei Cookies gilt jedoch auch hier: Wenn die Informationen für sekundäre Zwecke verarbeitet werden, also z. B. für die Sicherheit von Onlinediensten, die der Nutzer nicht angefordert hat, ist eine Einwilligung erforderlich. Das gilt auch in Fällen, in denen die Informationen zum Zweck der Betrugsbekämpfung verwendet werden – insbesondere in Fällen, in denen mehrere Onlinedienste einen einzigen Dienst zur Betrugsbekämpfung verwenden, der Informationen von Besuchern all dieser Dienste verarbeitet.

Anwendung der Opt-out-Ausnahme

Die ePrivacy-Gesetze sehen vor, dass Unternehmen Endnutzern einen Mechanismus bereitstellen, über den sie die Datenerfassung durch Cookietechnologien deaktivieren können. Diese Anforderung findet sich auch in Artikel 21 der DSGVO zum Recht auf Widerspruch.[6]

Es gibt jedoch einen Ausnahmefall: wenn dieses Recht ausgenutzt wird und der Opt-out-Mechanismus die Ausübung von Datenschutzaktivitäten unmöglich macht. Dieser Ausnahmefall greift also, wenn die Funktionsfähigkeit eines Sicherheitsservice von Cookietechnologie abhängig ist.

Wenn Nutzer die Cookietechnologie deaktivieren, die zur Erkennung schädlicher Bots und Skripte verwendet wird, können Sicherheitsservices den unbefugten Zugriff auf personenbezogene Daten nicht mehr verhindern. Sofern die Cookietechnologie ausschließlich für Sicherheitszwecke eingesetzt wird, stellt die fehlende Kontrolle über die Datenerfassung durch Cookietechnologie keine Beeinträchtigung der Rechte und Freiheiten des Endnutzers dar. Stattdessen gewährleistet diese fehlende Kontrolle den ständigen Betrieb der Cookietechnologie, die personenbezogene Daten vor unbefugtem Zugriff schützt.

Bei dieser Opt-out-Ausnahme sind sich Datenschutzexperten auf der ganzen Welt einig: Wenn die Datenkontrollmechanismen, die Endnutzern bereitgestellt werden, ausgenutzt werden können, um sich unbefugten Zugriff auf Daten zu verschaffen, ist der Mechanismus bedeutungslos und darf nicht implementiert werden. Denn es versteht sich von selbst, dass der reibungslose Betrieb moderner Sicherheitsservices wichtiger ist, als Endnutzern einen Datenkontrollmechanismus (Opt-out) für Cookietechnologie bereitzustellen.[7]

Compliance mit EU-Datensicherheitsgesetzen

Bot Manager Premier und Page Integrity Manager verarbeiten Daten gemäß DSGVO und anderen geltenden Datensicherheits- oder Datenschutzgesetzen. Das umfasst auch die Art der personenbezogenen Daten sowie den Zweck der Erfassung.

Art von personenbezogenen Daten

Bot Manager Premier und Page Integrity Manager erfassen neben Netzwerk- und Browserdaten, wie z. B. TLS-Sitzung, Sitzungs-ID, User-Agent, Anfrageheader, aufgerufene URLs, Zeitstempel, Endnutzer-IP-Adresse, Browsereinstellungen und Standortdaten von Edge-Servern, auch Verhaltensdaten wie Bildschirmberührungen, Mausbewegungen und Tastaturanschläge.

Zweck

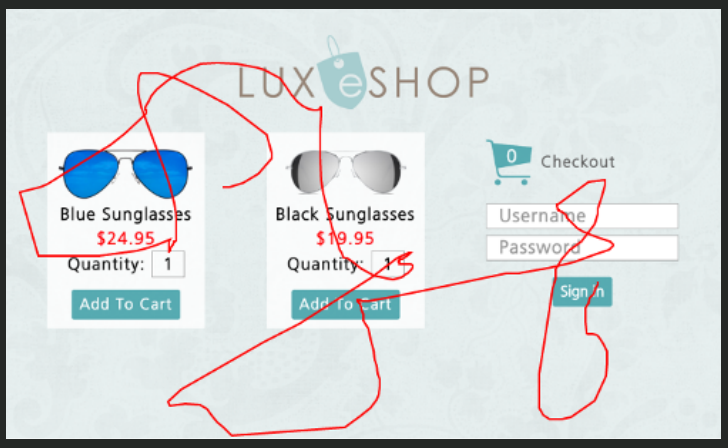
Der Zweck der Datenerfassung und -analyse ist die Erkennung schädlicher Bots und Skripte, die auf Ihren Webressourcen menschliches Verhalten nachahmen, sowie die Verhinderung von Datenextraktion und -missbrauch.

Hierzu muss Akamai analysieren, wie das Gerät beim Zugriff auf Ihre Ressourcen verwendet wird. Weder identifiziert Akamai den Endnutzer bei dieser Analyse, noch werden Profile der Endnutzer erstellt. Darüber hinaus werden die erfassten Verhaltensdaten nicht dazu verwendet, Personen eindeutig zu identifizieren. Die Daten sind deshalb laut DSGVO nicht als biometrische Daten kategorisiert.[8] Daher handelt es sich weder um „sensible Daten" (nach US-Recht) noch um „besondere Datenkategorien" (nach EU-Recht).

Akamai erfasst und analysiert die Verhaltensdaten, um zu bestimmen, ob der Zugriff auf Ihre Webressourcen durch einen Bot oder einen Menschen erfolgt. Wie das funktioniert, zeigen wir Ihnen in den Abbildungen weiter unten.

Mausereignisse

Menschliches Beispiel



Bot-Beispiele

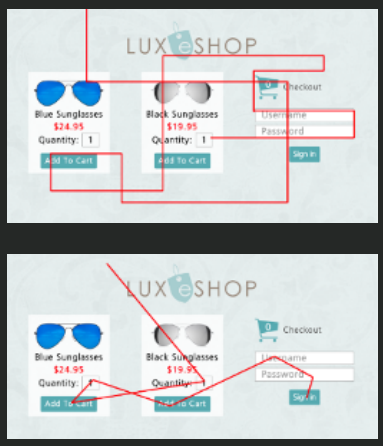
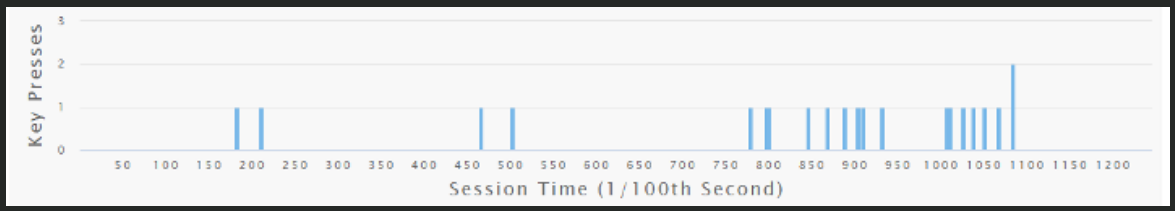


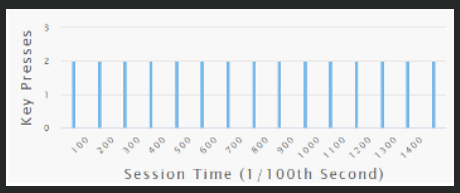
Abb. 3: Fortschrittliche Bots versuchen, auffällige Mausbewegungen zu vermeiden. So wollen sie eine echte Nutzerinteraktion nachahmen. Nach einer bestimmten Anzahl von Versuchen lässt sich jedoch ein Muster feststellen. Akamai kann diese Muster erkennen, um einen Bot zu identifizieren.

Erkennung der Tastaturanschläge

Tastaturanschläge eines Menschen



Beispiel für Bot-Tastaturanschläge



Beispiel für Bot-Tastaturanschläge

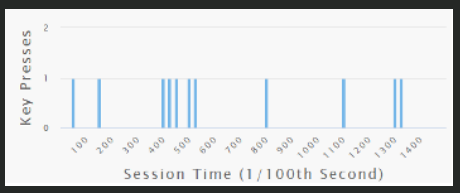


Abb. 4: Menschen drücken Tasten in der Regel so viel ungenauer, dass selbst die fortschrittlichsten Bots nicht mithalten können. Indem wir die Geschwindigkeit und den Rhythmus des vermeintlichen Nutzers analysieren, können wir erkennen, ob es sich um einen Menschen oder einen Bot handelt.

Rechtliche Grundlage

Die rechtliche Grundlage für die Verarbeitung ist unser berechtigtes Interesse daran, Services für Netzwerk- und Informationssicherheit bereitzustellen – in Form der Erkennung und Blockierung schädlicher Bots und Skripte. Berechtigtes Interesse ist eine anerkannte Rechtsgrundlage für die Ausübung von Sicherheitsservices im Rahmen der DSGVO.[9]

Über die Akamai-Systeme werden bis zu 30 Prozent des gesamten Internettraffics bereitgestellt und geschützt. Ohne Services für Bot- und Skriptmanagement würden Datenextraktion und -missbrauch deutlich häufiger auftreten.

Bewertung von Notwendigkeit und Verhältnismäßigkeit

Die Verarbeitung der Daten ist für die Akamai-Services für Netzwerk- und Informationssicherheit, die unter den Datenschutzgesetzen als aktueller „Stand der Technik" gelten, zwingend erforderlich. Indem wir die erfassten Netzwerk-, Browser- und Verhaltensdaten analysieren, kann Akamai Aktionen von Bots und Menschen genau auseinanderhalten und in Webressourcen injizierte Skripte erkennen.

Die Analyse aller erfassten Datenelemente ist angesichts der Raffinesse moderner Bots und Skripte verhältnismäßig. Eine Einschränkung der Datenerfassung beeinträchtigt die Genauigkeit der Analyse und sorgt so für eine weniger effektive Erkennung schädlicher Aktivitäten. Durch bloße Analyse von Endnutzer-IP-Adressen lassen sich Bots nicht erkennen. Zwar lassen auch Netzwerk- und Browserdetails auf die Gerätenutzung schließen, doch sie sind auf passive, signaturbasierte Mechanismen beschränkt und sehr anfällig für False Positives und False Negatives. Damit Sicherheit für Webressourcen dem aktuellen Stand der Technik[10] entspricht, ist eine erweiterte Bot-Erkennung erforderlich. Aktive Bots, die menschliches Verhalten nachahmen, lassen sich nur erkennen, indem Verhaltensdaten analysiert werden.

Die Erfassung zusätzlicher Daten wäre unverhältnismäßig, da sie die Analyse nicht verbessern würden.

Risikobewertung

Das Risiko für die Rechte und Freiheiten von Endnutzern durch die Verarbeitungsaktivitäten von Bot Manager Premier und Page Integrity Manager ist niedrig. Netzwerk-, Browser- und Verhaltensdaten werden nicht als vertraulich, als sensibel oder als besondere Kategorie personenbezogener Daten kategorisiert.[11] Die Verarbeitungsaktivitäten von Akamai für Bot Manager Premier und Page Integrity Manager werden in der Akamai-Datenschutzerklärung beschrieben und sind für Interessierte offen dargelegt. Akamai hält sich an das Prinzip der Datenminimierung und erfasst nur Daten, die für die Bot- und JavaScript-Erkennung zwingend erforderlich sind.

Akamai hat geeignete technische und organisatorische Maßnahmen implementiert, um die verarbeiteten personenbezogenen Daten vor dem unbefugten Zugriff Dritter zu schützen. Auch diese Maßnahmen sind auf unserer Website offen dargelegt: Informationssicherheitsprogramm von Akamai und Technische und organisatorische Maßnahmen von Akamai.

Die Analyse zur Bot- und Skripterkennung wird auf Akamai-Systemen durchgeführt, die in den USA bereitgestellt werden. Wenn also Endnutzer aus der EU auf Webressourcen zugreifen, die durch Bot Manager Premier und Page Integrity Manager geschützt sind, erfordert die Analyse die Verarbeitung europäischer personenbezogener Daten in den USA. Um die Datensicherheit bei der Verarbeitung in den USA zu gewährleisten, wendet Akamai nicht nur in der Akamai-Unternehmensgruppe selbst, sondern auch bei unseren Kunden und Auftragsverarbeitern die EU-Standardvertragsklauseln an. Darüber hinaus haben wir zusätzliche Sicherheitsmaßnahmen implementiert, um personenbezogene Daten bei der Verarbeitung in den USA vor dem Zugriff Dritter zu schützen.

Bei Akamai gelten in allen Konzerngesellschaften dieselben Datenschutzanforderungen, unabhängig vom Standort des jeweiligen Akamai-Unternehmens. Wir haben ergänzende Maßnahmen implementiert, um Daten auch während der Übertragung vor dem Zugriff Dritter zu schützen. Darüber hinaus handelt es sich bei den Daten, die Akamai über Bot Manager Premier und Page Integrity Manager in die USA überträgt, unserer Meinung nach nicht um die Art von Daten, an denen Geheimdienste (in den USA) bei ihrer Arbeit interessiert sind.[12] Die meisten Daten sind frei verfügbar, da sie erforderlich sind, um eine Internetverbindung aufzubauen. Dementsprechend müssen Dritte nicht an Akamai herantreten, um diese Daten zu erheben, sondern können auf deutlich einfachere Weise darauf zugreifen. Entsprechend stuft Akamai das Risiko, dass Dritte auf die in die USA übertragenen Daten zugreifen, bei Bot Manager Premier und Page Integrity Manager als minimal ein. Details finden Sie in der Akamai-Erklärung zu Datenübertragungen im Akamai Privacy Trust Center.

Akamai hält sich an das Prinzip der Datenminimierung und -sicherheit und bewahrt Daten deshalb nur 90 Tage lang auf. Dieser Zeitraum ist verhältnismäßig, da wir die Netzwerk-, Browser- und Verhaltensdaten über einen bestimmten Zeitraum und verschiedene Regionen hinweg analysieren müssen, um eine möglichst effektive Bot- und Skripterkennung zu gewährleisten.

Die Akamai-Services für Bot-/Skripterkennung und -management schützen nicht nur Ihre Webressourcen, sondern verbessern auch das Internet im Allgemeinen. Denn indem die Akamai Intelligent Edge Platform Bots und Skripte erkennt und blockiert, verhindern wir nicht nur den Diebstahl und Missbrauch der personenbezogenen Daten Ihrer Endnutzer, sondern gewinnen auch Bedrohungsinformationen, die wir in Netzwerk- und Sicherheitsservices einspeisen können. So profitieren Millionen von Endnutzern von den gewonnenen Daten.

Maßnahmen zur Risikominimierung

In Bereichen, bei denen Akamai davon ausgeht, dass Bot Manager Premier und Page Integrity Manager ein Risiko für die Rechte und Freiheiten betroffener Personen darstellen, haben wir diese Risiken minimiert. So werden zum Beispiel Endnutzer bei der Erfassung von Verhaltensdaten nicht identifiziert. Darüber hinaus schützt Akamai personenbezogene Daten auf angemessene Weise und hat zusätzliche Maßnahmen implementiert, um auch übertragene Daten vor dem Zugriff Dritter zu schützen.

Zusammenfassung

Akamai Bot Manager Premier und Page Integrity Manager entsprechen den EU-Datenschutzgesetzen. Die Cookietechnologien, die für den Betrieb der Services zum Einsatz kommen, sind zwingend erforderlich und ermöglichen den Schutz der personenbezogenen Daten des Endnutzers. Deshalb greifen hier die Ausnahmen für Einwilligung und Opt-out-Mechanismus.

Die Datenerfassung, die für den Betrieb der Services erforderlich ist, ist rechtmäßig, erforderlich und verhältnismäßig. Des Weiteren gewährleisten die implementierten Maßnahmen, dass die Verarbeitungsaktivitäten nur ein sehr geringes Risiko für die Rechte und Freiheiten der Endnutzer darstellen. Die Vorteile von Bot Manager Premier und Page Integrity Manager für Ihre Kunden und andere Onlinenutzer überwiegen bei Weitem die Risiken – schließlich profitieren wir alle von einem sicheren Internet.

Akamai Technologies
Dr. Anna Schmits, EMEA DPO

Quellen:

1. Die in diesem Dokument getroffenen Aussagen gelten auch für Akamai Service Bot Manager Standard, mit Ausnahme des Umfangs der Datenerfassung, die hier auf Netzwerk- und Browserdaten beschränkt ist. Weitere Informationen zu Akamai Bot Manager erhalten Sie hier: https://learn.akamai.com/en-us/products/cloud_security/bot_manager.html
2. Siehe „Digitale Privatsphäre", verfügbar unter: https://ec.europa.eu/digital-single-market/en/online-privacy
3. Siehe Änderung von Artikel 5 (3) der ePrivacy-Verordnung 2002/58/EC durch Verordnung 2006/24/EC, verfügbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32002L0058&from=DE.
4. Siehe z. B. die Cookierichtlinien des ICO im Vereinigten Königreich (unter 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), die Richtlinien der französischen CNIL (unter https://www.cnil.fr/en/cookies-and-other-tracking-devices-council-state-issues-its-decision-cnil-guidelines) oder die Richtlinien der deutschen Datenschutzkonferenz (unter https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf).
5. Siehe den ICP-Cookieleitfaden, verfügbar unter: 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. Siehe Artikel 21 (1) der DSGVO, verfügbar unter: https://dsgvo-gesetz.de/art-21-dsgvo/.
7. Siehe z. B. den ICP-Leitfaden, verfügbar unter: 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. Siehe Artikel 9 (1) der DSGVO, verfügbar unter: https://dsgvo-gesetz.de/art-9-dsgvo/.
9. Siehe Erwägungsgrund 49 der DSGVO, verfügbar unter: https://dsgvo-gesetz.de/erwaegungsgruende/nr-49/
10. Wie erforderlich gemäß Artikel 32 der DSGVO, verfügbar unter: https://dsgvo-gesetz.de/art-32-dsgvo/
11. Siehe Artikel 9 der DSGVO, verfügbar unter: https://dsgvo-gesetz.de/art-9-dsgvo/
12. US-Datenschutzmaßnahmen, die für SCCs relevant sind, und andere EU-Rechtsgrundlagen für die Datenübertragung von der EU in die USA nach Schrems II, Sept. 2020. Verfügbar unter: https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF

Akamai stellt sichere digitale Erlebnisse für die größten Unternehmen der Welt bereit. Die Intelligent Edge Platform umgibt alles – vom Unternehmen bis zur Cloud –, damit unsere Kunden und ihre Unternehmen schnell, intelligent und sicher agieren können. Führende Marken weltweit setzen auf die agilen Lösungen von Akamai, um die Performance ihrer Multi-Cloud-Architekturen zu optimieren. Akamai bietet Schutz vor Angriffen und Bedrohungen, beschleunigt Entscheidungen und Anwendungen und liefert herausragende Online-Erlebnisse. Das Akamai-Portfolio für Website- und Anwendungsperformance, Cloudsicherheit, Unternehmenszugriff und Videobereitstellung wird durch einen herausragenden Kundenservice, Analysen und Rund-um-die-Uhr-Überwachung ergänzt. Warum weltweit führende Unternehmen auf Akamai vertrauen, erfahren Sie unter **www.akamai.com**, im Blog **blogs.akamai.com** oder auf Twitter unter **@Akamai**. Unsere globalen Standorte finden Sie unter **www.akamai.com/locations**. Veröffentlicht: März 2021.