Deutsche Stiftung für Recht und Informatik

Gute Bots, schlechte Bots

Betrugsbekämpfung und ihr rechtlicher Rahmen

Joana Becker
Reed Smith LLP

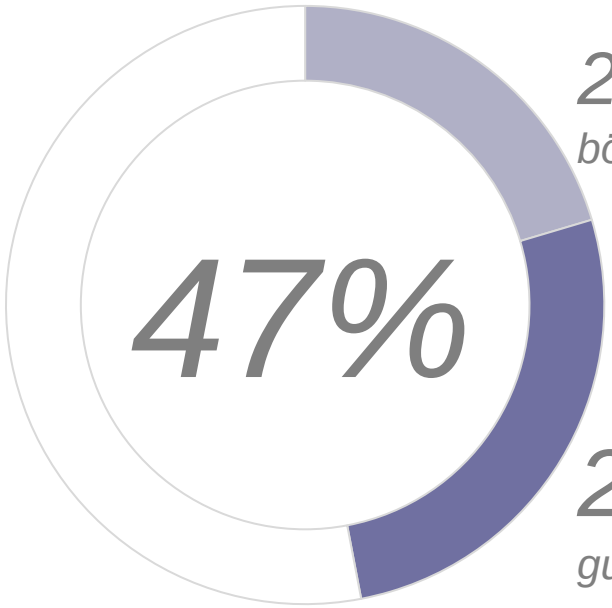
Herbstakademie 2023

Agenda

1. Hintergrund Bot-Traffic im E-Commerce
2. Praktische Auswirkungen von Bot-Angriffen im E-Commerce
3. Lösungen zur Bekämpfung von Bot-Angriffen
4. Datenschutzrechtliche Einordnung von Bot-Bekämpfung
5. Aussicht und Entwicklung

Deutsche Stiftung für Recht und Informatik

Fast die Hälfte des Internetverkehrs entfällt auf Bots; ein signifikanter Anteil davon sind „bösartig“



20%
bösartige Bots

27%
gutartige Bots

des gesamten Internetverkehrs entfällt heute auf Bot-Traffic

- Bereits heute große Relevanz von Bot-Traffic
- Trends wie IoT und KI beschleunigen die Entwicklung von Bot-Technologie weiter
- Bots können in gutartiger als auch in bösartiger Absicht programmiert werden
- Besonders große Vielfalt von Bot-Betrug im E-Commerce

Im E-Commerce gibt es eine besonders große Vielfalt an bösartigen Bots

Beispiele „bösartiger“ Bots

DDoS-Angriffe

- Hohe Anzahl an Serveranfragen durch Bots zur Überlastung des Internetdienstes
- Im E-Commerce besonders relevant, da Verfügbarkeit essenziell für Online-Käufe ist

Account Takeover

- Verschaffen von Zugang zu Nutzerkonten mit betrügerischen Mitteln und autom. Nutzung der Konten durch Bots
- Beim Phishing werden über gefälschte Webseiten oder E-Mails Nutzerdaten ermittelt

Product Scalping

- Bots, die in kürzester Zeit stark nachgefragte Produkte erwerben und zu erhöhten Preisen verkaufen
- Im Ticket-Verkauf bei Veranstaltungen besonders relevant

Advertising Fraud

- Bezeichnet den Betrug bei Werbeanzeigen
- Bots klicken auf Werbeanzeigen, wodurch Werbetreibenden Kosten entstehen aber keine kommerziellen Erfolge erzielt werden

Deutsche Stiftung für Recht und Informatik

Bösartige Bots führen jährlich zu signifikanten Schäden für deutsche Unternehmen

EUR 203 Mrd.

Schaden durch Cyberangriffe auf deutsche Unternehmen

84% *der deutschen Unternehmen von Cyberangriffen betroffen*

- Praktische Auswirkung von Bot-Angriffen als Teil von Cyberangriffen sind vielfältig
- Kosten für betroffene Unternehmen durch fehlinvestierte Werbebudgets sowie mögliche Reputationsschäden
- Zusätzliche rechtliche Konsequenzen, insb. Schadensersatzansprüche gegen betroffene Unternehmen, z.B. aus Datenschutzrecht oder Zivilrecht

E-Commerce Betreiber können auf verschiedene Lösungen zurückgreifen, um sich vor Bot-Angriffen zu schützen

Beispiele technischer Lösungen zur Bekämpfung von Bot-Angriffen

Captcha-Verfahren

- Weit verbreitete Lösung zur Erkennung und Blockierung bösartiger Bots
- Besteht typischerweise aus verzerrten Buchstaben, Zahlen oder Rätseln, die nur von menschlichen Website-Nutzern gelöst werden können
- Neuere und effektivere Lösung aufgrund Weiterentwicklung von Bots: Captcha Cookies

Aktives Fingerprinting

- Ausführen von Programmcode, bspw. JavaScript auf Endgerät, um aus Browser- und Bildschirminformation speziellen Fingerabdruck des Geräts herzuleiten
- Durch Wiedererkennen des Fingerabdrucks kann zwischen menschlichen Nutzern und bösartigen Bots unterschieden werden

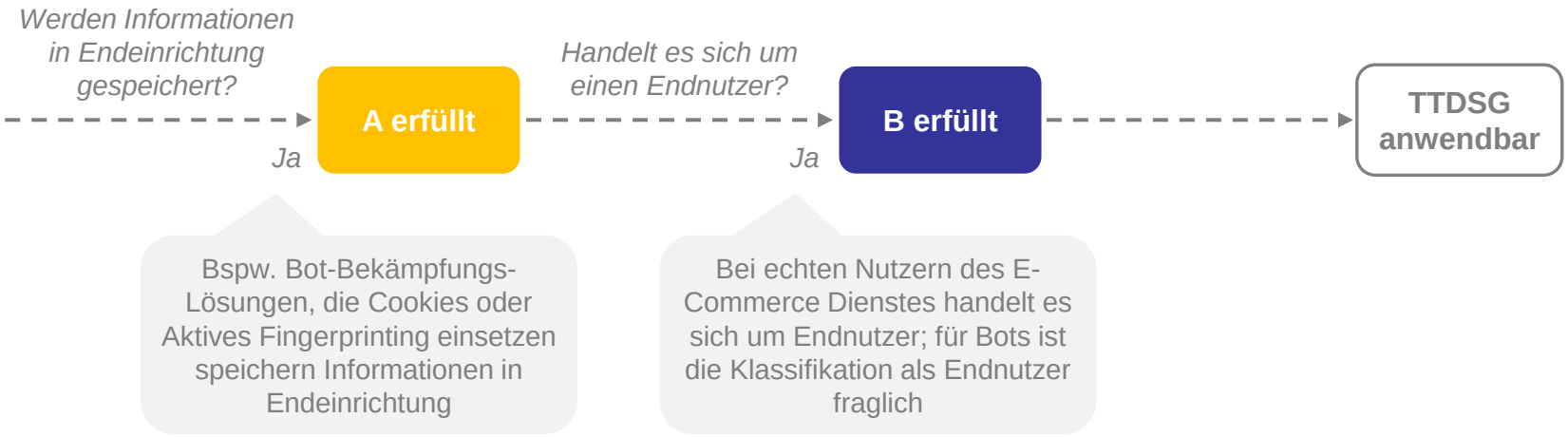
Datenschutzrechtlich kommen das TTDSG und die DSGVO für Bot-Bekämpfungs-Lösungen als Rechtsgrundlage in Frage

Das TTDSG kann bei Bot-Bekämpfung Anwendung finden, bspw. bei Lösungen mit Cookies oder Aktivem Fingerprinting

A

§25 TTDSG: TTDSG anwendbar, wenn durch die Bot-Bekämpfungs-Lösung ***Informationen in Endeinrichtung*** **des Endnutzers gespeichert** werden oder Zugriff auf Informationen erfolgt, die in Endeinrichtung gespeichert sind

B



Bei Anwendung des TTDSG muss grds. eine Einwilligung eingeholt werden; bei Bot-Bekämpfung kann eine Ausnahme greifen

In der Praxis führt die Erforderlichkeit einer Einwilligung zur Wirkungslosigkeit der Bot-Bekämpfungs-Lösung

Grundsätzlich ist eine **Einwilligung des Endnutzers erforderlich**, **wenn Informationen auf seiner Endeinrichtung gespeichert** werden

Ausnahme durch § 25 Abs. 2 Nr. 2 TTDSG

Ausnahme, wenn der Einsatz solcher Lösungen „**unbedingt erforderlich ist**, um den **ausdrücklich vom Endnutzer gewünschten Telemediendienst** zur Verfügung zu stellen“

A

B

A Dienstbetreiber müssen sicherstellen, dass Datenverarbeitung auf ein unbedingt erforderliches Maß beschränkt bleibt

B Entscheidend welche Interessen des Dienstbetreibers hinter dem Einsatz der Bot-Bekämpfungs-Lösung stehen: rein unternehmerische Interessen vs. Nutzerinteressen

Rechtliches Risiko bei Einsatz von Bot-Bekämpfungs-Lösungen für rein unternehmerische bzw. wirtschaftliche Interessen

Datenschutzrechtlich kommen das TTDSG und die DSGVO für Bot-Bekämpfungs-Lösungen als Rechtsgrundlage in Frage

TTDSG

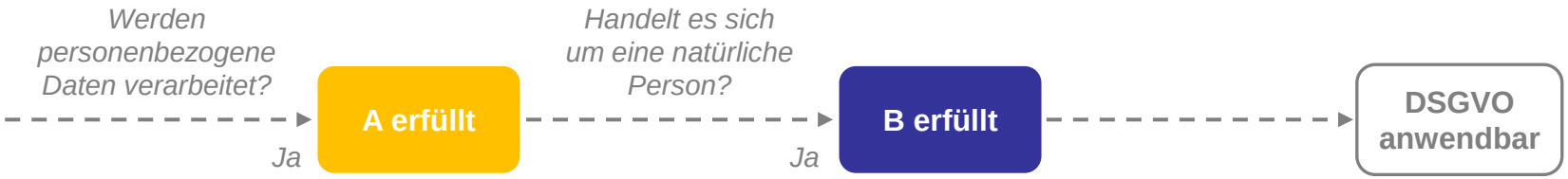
DSGVO

Durch Bot-Bekämpfung werden personenbezogene Daten weiterverarbeitet, sodass auch die DSGVO Anwendung findet

A

DSGVO anwendbar bei Verarbeitung von **Informationen**, die sich auf eine **identifizierte oder identifizierbare natürliche Person** beziehen

B

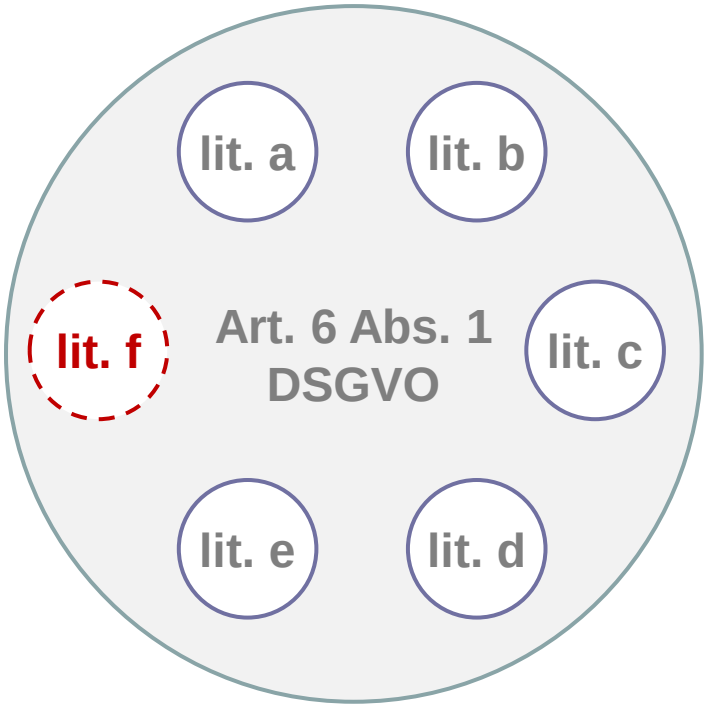


Für die Bot-Bekämpfung werden personenbezogene Daten wie IP-Adresse oder Cookie-ID weiterverarbeitet

Bei echten Nutzern des E-Commerce Dienstes handelt es sich um natürliche Personen; für Bots ist die Klassifikation als natürliche Person fraglich

Der Einsatz von Bot-Bekämpfungs-Lösungen kann durch ein berechtigtes Interesses gerechtfertigt werden

Die Datenverarbeitung ist nur rechtmäßig, wenn:



lit. f

*Die Verarbeitung ist zur Wahrung der **berechtigten Interessen des Verantwortlichen** oder eines Dritten erforderlich, sofern nicht die **Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person**, die den Schutz personenbezogener Daten erfordern, überwiegen.*

- Betrugsprävention und Abwehr von Bots als berechtigtes Interesse des Verantwortlichen rechtlich anerkannt
- Bei Interessenabwägung ist entscheidend, welches Interesse des Dienstbetreibers hinter Einsatz der Bot-Bekämpfungs-Lösung besteht

Rechtliches Risiko bei Einsatz von Bot-Bekämpfungs-Lösungen für rein unternehmerische bzw. wirtschaftliche Interessen

Deutsche Stiftung für Recht und Informatik

Bot-Traffic wird zunehmend relevant; klare rechtliche Grundlagen werden benötigt, um Rechtssicherheit zu schaffen

*Einsatz KI verstärkt **Relevanz** des Themas Bot-Traffic und Cyberangriffe **zunehmend***

***Unternehmen benötigen Rechtssicherheit**, um sich gegen drohende Schäden durch Bot Angriffe effektiv wehren zu können*

*Es bleibt **abzuwarten**, ob durch die **geplante e-Privacy-VO rechtliche Klarheit geschaffen** wird*