SOP 29

Captchas

Projektleitung | Geschäftsführung | IT | Recht

So schützt du deine Formulare, ohne Menschen auszusperren

Weil Captchas oft mehr Menschen aussperren als Bots. Was als Sicherheitsmaßnahme gedacht ist, kann schnell zur unüberwindbaren Barriere werden – für Menschen mit Seheinschränkung, motorischen Einschränkungen, Legasthenie oder einfach nur Pech. Barrierefreiheit bedeutet hier: Sicherheit ja, aber nicht auf Kosten der Zugänglichkeit.

Wann musst du das machen?

- Immer, wenn du Formulare gegen Spam schützen willst.
- Häufig bei: Kontaktformularen, Login, Registrierung, Kommentarfunktionen, Gästebüchern oder Umfragen.

Welches Gesetz verlangt das?

- EAA/BFSG: Die Interaktion mit deiner Website muss allen Menschen offenstehen – ohne Umwege oder Diskriminierung.
- DSGVO Art. 25: Fordert Sicherheit durch Technikgestaltung, aber diese muss nutzbar sein.
- WCAG 2.1: Insbesondere die Kriterien 1.1.1 (Non-text Content), 1.3.1 (Info and Relationships), 2.1.1 (Keyboard) und 3.3.1 (Error Identification).

Der Prozess im Detail

1. 🟧 **Phase 1: Prüfe die Notwendigkeit – und vermeide Captchas, wenn möglich**

   Die barrierefreiste Lösung ist, gar kein Captcha zu verwenden.

   Ernsthaft.

   Prüfe darum zuerst, ob du wirklich Captchas brauchst oder ob Alternativen ausreichen. Denke dabei an die Faustregel: Je Weniger Barrieren desto mehr Conversions.

   Und, ja es gibt auch jenseits von Captchas Möglichkeiten, dich vor spammigen Bot-Anfragen zu schützen. Beispielsweise diese hier:

   - Honeypot-Feld: Ein für normale Nutzer:innen unsichtbares Formularfeld. Füllen es aber aus, wird der Versand blockiert.
   - Zeitbasierter Schutz: Formulare können erst nach einer kurzen Verzögerung (z. B. 3 Sekunden) abgeschickt werden, was automatisierte Bots ausbremst.
   - Serverseitige Prüfungen: Analyse von IP-Adresse, Verhalten und Frequenz.
   - Double-Opt-In: Bei E-Mail-Formularen oft der beste Schutz, da die Echtheit der Adresse bestätigt wird.

   Auch hier gilt: Wenn das technisch für dich herausfordernd ist (z.B. Honeypot-Feld oder zeitbasierter Schutz), wende dich unbedingt an Profis, die dir dabei weiterhelfen können.

2 🟨 Phase 2: Wähle eine barrierearme Captcha – wenn du schon musst

Es MUSS aber unbedingt ein Captcha für dich sein?

Ok, auch gut.

Falls eine der Alternativen nicht ausreicht, wähle eine Lösung, die immerhin für möglichst viele Menschen zugänglich ist.

Hier ein paar Möglichkeiten inkl. Bewertung, ob sie auch für dich sinnvoll bzw. datenschutzrechtlich ok oder barrierefrei sind:

- Bildbasierte Captchas (z. B. Google reCAPTCHA v2): Sind nicht barrierefrei und sollten vermieden werden.
- Unsichtbare Captchas (z. B. Google reCAPTCHA v3): Sind datenschutzrechtlich bedenklich, da oft keine aktive Einwilligung vor der Datenübertragung erfolgt.
- hCaptcha mit Accessibility-Modus: Eine gute Alternative, da ein barrierefreier Modus explizit aktivierbar ist.
- Einfache Text- oder Mathe-Fragen: Lösungen wie „Welche Farbe hat Gras?“ oder „Was ist 3+5?“ sind oft ausreichend und auch mit Screenreadern gut lösbar.

3 🟩 Phase 3: UX und Hinweisgestaltung optimieren

Hast du dich für eine Alternative entschieden, kommuniziere klar, warum eine Sicherheitsprüfung stattfindet und biete Hilfe an.

- Zweck erklären: Ein Hinweis wie „Diese Maßnahme dient dem Spamschutz“ erhöht die Akzeptanz.
- Hilfestellung anbieten: Gib Nutzer:innen eine alternative Kontaktmöglichkeit an, falls sie das Captcha nicht lösen können, z. B. „Probleme beim Ausfüllen? Kontaktieren Sie uns hier.“
- Wechsel ermöglichen: Ein „Captcha nicht lesbar?“-Button, der eine neue Aufgabe oder eine Audio-Alternative anbietet, ist hilfreich.
- Klare Benennung für Screenreader: Verwende ein aria-label=“Spamschutz“, damit der Zweck des Elements klar ist.

4 🟥 Phase 4: Mit Tastatur und Screenreader testen

Überprüfe die technische Umsetzung rigoros bzw. achte darauf, ob sie wirklich barrierefrei ist. Prüfe dabei folgende Punkte:

- Erreichbarkeit: Kann das Captcha-Feld per Tab-Taste erreicht werden?
- Screenreader-Ausgabe: Wird der Zweck des Feldes klar vorgelesen?
- Lösbarkeit: Kann das Captcha sowohl visuell als auch auditiv (falls angeboten) gelöst werden?
- Mobiltauglichkeit: Funktioniert die Lösung auch auf mobilen Geräten einwandfrei?

5 🟦 Phase 5: Datenschutz und DSGVO beachten

Oft wirst du Dienste von Drittanbietern für dein Captcha oder eine Alternative nehmen – und das birgt datenschutzrechtliche Risiken. Prüfe darum:

- Datenübertragung in Drittländer: Wenn der Dienst Daten in die USA überträgt (wie bei Google reCAPTCHA), sind ein klarer Hinweis und eine vorherige, aktive Einwilligung erforderlich. Informiere auch unbedingt deinen Datenschutzbeauftragten darüber(Stichwort: EU Standardvertragsklauseln).
- Ladezeitpunkt: Das Skript des Captcha-Dienstes darf erst geladen werden, nachdem der/die Nutzer:in über das Cookie-Consent-Tool zugestimmt hat. Ein Laden davor ist ein Verstoß gegen Art. 6 DSGVO.
- Keine Kopplung: Nutzer:innen dürfen nicht gezwungen werden, ein Captcha zu akzeptieren, um die Seite an sich zu benutzen.

Ergebnis

Am Ende dieser SOP hast du:

- Ein sicheres, aber gleichzeitig barrierefreies Formular.
- Funktionierende Alternativen zum klassischen, oft frustrierenden Captcha etabliert. Eine Lösung implementiert, die den Anforderungen von DSGVO & EAA gerecht wird.
- Ein Formular, das alle ausfüllen können – auch ohne Maus, Bildschirm oder perfekte Sehkraft.

Wie du gelesen hast, ist es möglichst ideal, gar nicht erst Captcha zu verwenden. Aber was, wenn du das Gefühl hast, dass es nicht geht, weil du regelmäßig von Bots besucht wirst? Mit der nachfolgenden Enscheidungshilfe findest du schnell heraus, welche Entscheidung (für oder gegen Captcha) die sinnvollere für dich ist.

CAPTCHA-Entscheidungshilfe: Kannst du auf ein Captcha verzichten oder nicht?

Entscheidungsbaum: Spamschutz für Formulare

Ziel: Effektiven Spamschutz implementieren, der barrierefrei und datenschutzkonform ist.

Startpunkt: Brauchst du WIRKLICH ein Captcha?

- JA, ich brauche unbedingt ein Captcha.
- Frage 1: Ist Datenschutz oberste Priorität und Datentransfer in Drittländer ein No-Go?
- JA: Wähle hCaptcha mit aktiviertem Accessibility-Modus oder einfache Text-/Mathe-Fragen .
- To-Do: Kommuniziere den Zweck („Spamschutz“), biete Hilfestellung (Kontaktoption) und Wechselfunktion („Captcha nicht lesbar?“). Stelle sicher, dass aria-label="Spamschutz" verwendet wird.
- Technik-Check: Erreichbarkeit per Tab, klare Screenreader-Ausgabe, Lösbarkeit (visuell/auditiv), Mobiltauglichkeit.
- NEIN (Drittanbieter mit US-Transfer ggf. ok, bei klarer Einwilligung):
- To-Do: Implementiere unsichtbares Captcha (z.B. Google reCAPTCHA v3) NUR , wenn du eine aktive, vorherige Einwilligung (via Cookie-Consent-Tool) und eine klare Information über Datentransfer in

Drittländer sicherstellen kannst. Dein Datenschutzbeauftragter muss informiert sein (Stichwort: EU-Standardvertragsklauseln).

- WICHTIG: Das Skript darf erst nach Zustimmung geladen werden. Keine Kopplung der Seitennutzung an Captcha-Akzeptanz.
- Technik-Check: Erreichbarkeit per Tab, klare Screenreader-Ausgabe, Lösbarkeit (visuell/auditiv), Mobiltauglichkeit.
- Frage 2: Kannst du NICHT sicherstellen, dass das Captcha-Skript erst nach Zustimmung geladen wird ODER willst du keine Abhängigkeit von Drittanbietern?
- JA: Wähle einfache Text-/Mathe-Fragen .
- To-Do: Kommuniziere den Zweck („Spamschutz“), biete Hilfestellung (Kontaktoption) und Wechselfunktion („Captcha nicht lesbar?“). Stelle sicher, dass aria-label="Spamschutz" verwendet wird.
- Technik-Check: Erreichbarkeit per Tab, klare Screenreader-Ausgabe, Lösbarkeit (visuell/auditiv), Mobiltauglichkeit.
- NEIN, ich brauche KEIN Captcha (Alternativen genügen).
- Frage 1: Willst du eine unsichtbare, nutzerfreundliche Lösung?
- JA: Implementiere Honeypot-Feld . (Bei technischer Herausforderung: Profis kontaktieren.)
- Frage 2: Möchtest du automatisierte Bots verlangsamen?
- JA: Implementiere Zeitbasierter Schutz (z.B. Formularversand erst nach 3 Sekunden). (Bei technischer Herausforderung: Profis kontaktieren.)
- Frage 3: Ist eine tiefergehende Analyse und Absicherung auf Serverseite möglich?
- JA: Implementiere Serverseitige Prüfungen (IP-Adresse, Verhalten, Frequenz).
- Frage 4: Handelst du mit E-Mail-Adressen und benötigst höchste Sicherheit für die Adress-Echtheit?
- JA: Implementiere Double-Opt-In .

Abschluss-Check (unabhängig von der Wahl):

- Ist der Zweck der Sicherheitsmaßnahme klar kommuniziert („Diese Maßnahme dient dem Spamschutz“)?
- Gibt es eine alternative Kontaktmöglichkeit bei Problemen („Probleme beim Ausfüllen? Kontaktieren Sie uns hier.“)?
- (Falls Captcha gewählt) Gibt es einen „Captcha nicht lesbar?“-Button für neue Aufgaben/Audio-Alternativen?
- (Falls Captcha gewählt) Wird aria-label="Spamschutz" verwendet?
- Wurde der Ladezeitpunkt externer Captcha-Skripte im Cookie-Consent-Tool geprüft (erst nach Zustimmung)?
- Ist die Nutzung der Seite ohne Captcha-Akzeptanz möglich?

Fragen & Antworten

Wir nutzen ein CMS (z.B. WordPress, Typo3). Gibt es hier fertige Plugins/Module für die genannten Alternativen oder Captchas, die ich bedenkenlos nutzen kann?

Ja, für gängige CMS gibt es oft Plugins oder Module, die die Implementierung erleichtern. Für Honeypot-Felder und zeitbasierten Schutz sind diese oft leicht zu finden und relativ unkompliziert. Bei Double-Opt-In bieten viele Newsletter-Tools oder CMS-Erweiterungen bereits integrierte Funktionen. Für hCaptcha gibt es ebenfalls offizielle Plugins. Wichtig ist aber, du, dass du auch bei Plugins die Einstellungen genau prüfst, besonders bezüglich der Barrierefreiheit (ist der Accessibility-Modus standardmäßig aktiviert?) und des Datenschutzes (wann wird das Skript geladen? Wo werden Daten verarbeitet?). Ein Plugin allein garantiert nicht automatisch die volle Konformität mit deiner SOP.

Wie genau funktioniert die %22serverseitige Prüfung%22 praktisch, und brauche ich dafür spezielle Software?

Serverseitige Prüfungen sind fortgeschrittener und setzen oft technisches Know-how voraus oder spezielle Lösungen. Sie analysieren im Hintergrund Muster, die auf Bots hinweisen:

- IP-Blacklisting: Bekannte Spammer-IPs werden blockiert.
- Verhaltensanalyse: Ungewöhnlich schnelle Formularausfüllzeiten (ohne Zeitverzögerung), wiederholte Anfragen von derselben IP oder ungewöhnliche User-Agent-Strings (Browser-Kennungen) können als Indikatoren dienen.
- Frequenzbegrenzung (Rate Limiting): Beschränkt die Anzahl der Anfragen von einer IP-Adresse innerhalb eines bestimmten Zeitraums, um Brute-Force-Angriffe zu verhindern. Du brauchst dafür nicht zwingend spezielle Software, aber oft sind dafür Anpassungen im Backend-Code oder der Einsatz von Web Application Firewalls (WAFs) nötig, die solche Funktionen bereitstellen. Hier ist der Rat eines versierten Entwicklers oder Sicherheitsexperten oft unerlässlich.

Die SOP erwähnt, dass bei Google reCAPTCHA v3 oft keine aktive Einwilligung vor der Datenübertragung erfolgt. Gibt es Wege, dies datenschutzkonform zu gestalten?

Die Herausforderung bei reCAPTCHA v3 liegt darin, dass es Daten sammelt, bevor der Nutzer eine Interaktion hat oder explizit zugestimmt hat (da es „unsichtbar“ ist). Um es datenschutzkonform zu nutzen, müsstest du, du, folgende Maßnahmen ergreifen, was technisch aufwendig sein kann:

- Zustimmung vor dem Laden: Das reCAPTCHA-Skript darf erst geladen werden, nachdem der Nutzer über ein Cookie-Consent-Tool explizit in die Datenverarbeitung durch reCAPTCHA eingewilligt hat. Das bedeutet, der Ladezeitpunkt muss kontrolliert werden.
- Transparenz: Klare Information in deiner Datenschutzerklärung über die Nutzung von reCAPTCHA, die Art der gesammelten Daten, den Zweck der Verarbeitung und den Transfer in Drittländer (USA).
- Alternative anbieten: Wenn der Nutzer nicht zustimmt, muss das Formular trotzdem nutzbar sein, eventuell mit einer weniger komfortablen, aber datenschutzfreundlichen Alternative (z.B. einer einfachen Mathe-Frage als Fallback). Aufgrund dieser Komplexität und der fortwährenden Diskussion um den Datentransfer in die USA (Stichwort Schrems II und EU-US Data Privacy Framework) wird von reCAPTCHA v3 oft abgeraten, wenn Datenschutz höchste Priorität hat.

Meine Zielgruppe ist sehr technisch versiert. Könnte ich nicht auch %22richtige%22 Programmier-Aufgaben oder Code-Puzzles als Captcha verwenden?

Theoretisch ja, du könntest komplexere Aufgaben stellen. Aber die SOP betont „barrierefreiste Lösung“ und „für möglichst viele Menschen zugänglich“. Auch wenn deine Zielgruppe technisch versiert ist, können solche Puzzles schnell zu unnötigen Barrieren werden:

- Zeitaufwand: Selbst für Profis können solche Aufgaben im Kontext eines Formulars frustrierend sein.
- Fehleranfälligkeit: Tippfehler oder Syntaxfehler könnten zu unnötigen Problemen führen.
- Barrierefreiheit: Für Nutzer mit Screenreadern oder motorischen Einschränkungen wären solche Puzzles extrem schwierig oder unlösbar. Bleibe lieber bei den empfohlenen, einfacheren Methoden wie Mathe-Fragen oder hCaptcha, die eine breite Zugänglichkeit gewährleisten und gleichzeitig den Großteil der Bots abwehren.

Was ist, wenn trotz aller Maßnahmen immer noch Spam durchkommt?

Kein Spamschutz ist 100% sicher. Wenn trotz sorgfältiger Implementierung immer noch Spam durchkommt, solltest du:

- Maßnahmen kombinieren: Oft ist eine Kombination von Maßnahmen am effektivsten (z.B. Honeypot + Zeitverzögerung + serverseitige Prüfung).
- Analysieren und Anpassen: Versuche herauszufinden, wie der Spam durchkommt. Ist es ein Mensch, der den Spam manuell eingibt (dann hilft ein Captcha nicht), oder ein Bot, der eine bestimmte Schutzmaßnahme umgeht? Passe deine Strategie entsprechend an.
- Regelmäßige Überprüfung: Spam-Bots entwickeln sich ständig weiter. Überprüfe deine Schutzmaßnahmen regelmäßig auf ihre Wirksamkeit und informiere dich über neue Angriffsmethoden und Gegenmaßnahmen. Manchmal sind kleine Anpassungen der Parameter (z.B. eine längere Zeitverzögerung) bereits hilfreich.