Whitepaper

DSGVO-konformer Website-Schutz

Mit POWER CAPTCHA schützt du deine Website oder API gegen Bots und gegen den Zugriff durch unberechtigte Personen!

Darum solltest du Captchas verwenden

Gezielte Cyber-Attacken gegen Unternehmen, Verwaltungen oder Internetnutzer:innen sind in den vergangenen Jahren massiv gestiegen. Dabei sind nicht nur der Diebstahl von Informationen und die Schädigung von Infrastrukturen eine Gefahr für Unternehmen, sondern auch der Missbrauch von Online-Funktionen für die Verbreitung von Spam (z.B. über Kontaktformulare) oder zur Schädigung der Reputation. Der Einsatz eines Captchas kann deine Login-Bereiche und Formulare gegen diese Angriffe schützen.

Warum die meisten Captchas für dein Unternehmen nicht geeignet sind

Gemeinsam haben die meisten Captchas den Nachteil, dass sie nur gegen Bots, aber nicht gegen Hacker schützen, da sie direkte, menschliche Interaktionen nicht effektiv einschränken, wie z.B. das Kombinieren von Login-Namen und Passwörtern oder die ungewollte, vielfache Benutzung eines Formulars.

Viele Captchas verfügen über intransparente und nicht steuerbare Wirkungsmechanismen. Es ist meist nicht eindeutig, welche personenbezogenen Daten gespeichert, wo diese gespeichert und wofür diese Daten genutzt werden.

Dazu kommt, dass viele Captchas die Datenschutzbestimmungen gemäß den aktuellen europäischen und deutschen Gesetzen (GDPR / DSGVO) nicht ordnungsgemäß umsetzen. Danach muss für die Nutzung von Captchas, mit einem Datenpool außerhalb der EU oder der Speicherung personenbezogener Daten, vorab aktiv die Zustimmung zur Verwendung durch die Anwender:innen erteilt werden (analog Cookie-Banner).

POWER CAPTCHA schützt gegen Bots und Hacker

Im Gegensatz zu anderen Captchas, unterscheidet POWER CAPTCHA nicht primär, ob ein Mensch oder ein Bot eine Interaktion ausgelöst hat, sondern prüft grundsätzlich, ob der Zugriff berechtigt ist oder nicht. Jede Interaktion mit POWER CAPTCHA erzeugt einen verschlüsselten Code, den die zentrale POWER CAPTCHA-KI bewertet und sich für eine begrenzte Zeit merkt, um anschließend bei weiteren Interaktionen den Schwierigkeitsgrad der Lösung zu erhöhen, die Antwortzeit zu verlängern oder ggf. weitere Interaktionen für eine gewisse Zeit abzulehnen.

Abbildung 1: Sicherheitsabfrage mit POWER CAPTCHA

POWER CAPTCHA ist GDPR- / DSGVO-konform

Wir betreiben POWER CAPTCHA auf gesicherten Servern in zertifizierten Rechenzentren in Deutschland. Die Daten der Anwender:innen bzw. Clients werden über verschlüsselte Kommunikationswege übertragen und in nicht lesbarer Form verarbeitet. Wir speichern diese

Daten nur so lange, bis die Sicherheitsprüfung und der aktuelle Bearbeitungszeitraum abgeschlossen sind. Daher ist POWER CAPTCHA DSGVO-konform, und du benötigst keine vorherige Zustimmung von den Anwender:innen zur Verwendung.

Die maximale Dauer der Speicherung orientiert sich an den Sperrzeiten, die in den POWER CAPTCHA-Tarifen definiert sind. Im Rahmen des Enterprise-Tarifs können wir die Daten maximal für drei Tage speichern (Kundeneinstellung).

Sicherheitslevel, Usability, Barrierefreiheit

Über die gewünschte Balance zwischen Usability und Barrierefreiheit sowie das Sicherheitslevel kannst du selbst entscheiden. Beispiele:

Usability: Nach wie vielen Interaktionen soll ein Captcha angezeigt werden? Möchtest du nur Sicherheitsmechanismen im Hintergrund nutzen, ohne Captcha-Anzeige (No-Captcha-Lösung)?

Security-Level: Welche Komplexität soll das angezeigte Captcha haben, und wann soll die Komplexität erhöht werden?

Lock-Timer: Wie viel Zeit möchtest du User:innen zur Lösung des Captchas geben? Wie lange sollen Clients nach einer Sperre gesperrt bleiben?

Release-Timer: Wann sollen die bisherigen Ereignisse der Clients wieder zurückgesetzt werden?

Barrierefreiheit: Im Rahmen des Enterprise-Tarifs enthält POWER CAPTCHA eine 2-Faktor-Authentifizierung für einen barrierefreien Zugriff.

Custom Actions: Was soll z.B. im Falle einer Sperrung geschehen? Standardmäßig wird ein entsprechender Hinweis eingeblendet. Hast du einen anderen Bedarf, kontaktiere gerne unseren Vertrieb.

Überwachung von Schlüsselwerten

Damit Hacker oder Bots nicht mehrere IP-Adressen verwenden können, um eine Sperre zu umgehen, kannst du u.a. einstellen, wie oft ein Benutzername oder eine E-Mail-Adresse verwendet werden darf. Benutzernamen und E-Mail-Adresse sind lediglich Beispiele für Werte, die du schützen kannst.

Grundsätzlich kannst du jeden Wert an POWER CAPTCHA übergeben und vor missbräuchlicher oder ungewünschter Anwendung schützen. Beispiele für mögliche Einsatzszenarien sind Limitierungen von Downloads, Online-Services oder der Aufruf von Websites oder App-Funktionen, oft auch ohne die sichtbare Anzeige eines Captcha (No-Captcha Einstellung).

Abbildung 2: Auszug POWER CAPTCHA-Einstellungen (Screenshot)

Systembeschreibung

Rufen Benutzer:innen einen der mit POWER CAPTCHA geschützten Bereiche deiner Website auf oder senden ein geschütztes Formular ab (Abbildung 3, Step 1), wird zunächst überprüft, ob gemäß deinen Voreinstellungen im Kunden-Center ein POWER CAPTCHA Pop-up angezeigt werden soll (Abbildung 3, Step 2). Wird diese Anfrage vom POWER CAPTCHA-Server mit „ja“ bestätigt, wird ein Captcha angezeigt und ein Lösungswert muss eingegeben werden (Abbildung 3, Step 3).

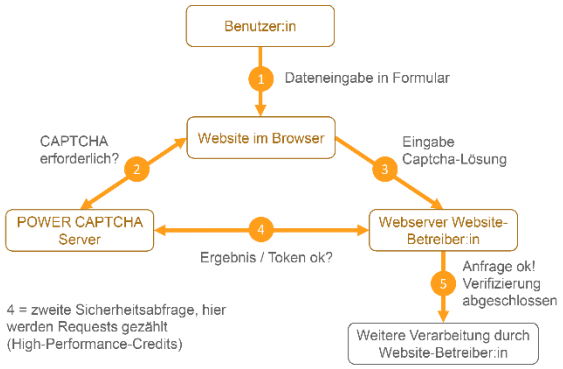

Abbildung 3: Skizze Systemarchitektur POWER CAPTCHA

Bis zu dem Zeitpunkt, an dem eine Captcha-Lösung abgesendet wird, findet die Kommunikation zwischen dem POWER CAPTCHA-Server und dem Browser statt, der deine Website aufgerufen hat. Auf deinem Webserver entsteht kein zusätzlicher Traffic, wenn vom Browser neue Captchas angefordert werden. Erst wenn ein korrekter Captcha-Lösungswert angeklickt wird, erfolgt die Weitergabe an deinen Webserver (Abbildung 3, Step 3).

Für einen barrierefreien Zugang können Benutzer:innen alternativ einen Zugangscode per E-Mail anfordern, welcher vom POWER CAPTCHA-Server versendet wird.

Dein Webserver nimmt die Lösungsanfrage entgegen und prüft, ob das Captcha richtig gelöst wurde und der Zugriff zulässig ist. Hierfür wird von deinem Webserver eine Verifizierungsanfrage an den POWER CAPTCHA-Server gestellt (Abbildung 3, Step 4). Diese Anfrage enthält das Token der Captcha-Lösung, den Benutzernamen, die E-Mail-Adresse oder einen anderen zu schützenden Wert, sowie die IP-Adresse der Browseranfrage. Zudem bescheinigt mit deinem persönlichen Secret-Key gleichzeitig die Berechtigung der Anfrage (Server-Authentisierung).

So verhindern wir, dass die Lösungsanfrage durch Dritte abgefangen und missbraucht werden kann. Außerdem hast du damit die Kontrolle über die Anzahl der verbrauchten Highspeed Security Checks pro Monat *, denn nur Anfragen von deinem Webserver-Backend werden dem Verbrauch von Highspeed Security Checks hinzugerechnet.

Der POWER CAPTCHA-Server prüft nun ob die Lösung des Captchas korrekt erfolgt ist. Wird das Token vom POWER CAPTCHA-Server als gültig bestätigt, ist die Verifizierung durch POWER CAPTCHA abgeschlossen. Die weitere Verarbeitung der Anfrage, wie z.B. die Prüfung der Login-Daten, geschieht anschließend durch dich als Website-Betreiber:in (Abbildung 3, Step 5).

Wenn du den Modus „No-Captcha“ eingestellt hast, wird Benutzer:innen kein Captcha angezeigt und die Sicherung deiner Website erfolgt durch andere von dir freigegebene Maßnahmen, wie die Begrenzung der Login-Versuche innerhalb eines Zeitlimits. Die No-Captcha-Einstellung entspricht einer korrekten Captcha-Lösung, und Step 3 aus Abbildung 3 wird übersprungen.

*** Ergänzung zu Highspeed Security Checks:** Die Bereitstellung von Captchas im Rahmen von Highspeed Security Checks erfolgt mit höchster Priorität (meist wenige Millisekunden). Wenn dein Volumen an Highspeed Security Checks pro Monat aufgebraucht ist, verringert sich die Geschwindigkeit der Bereitstellung. Die Anzahl der in deinem POWER CAPTCHA-Tarif enthaltenen Highspeed Security Checks pro Monat findest du in der Tabelle unter „Tarife“.

Einfache Integration

Mit deiner Registrierung erhältst du automatisch einen Kundenschlüssel für die Installation. In deinen Account-Einstellungen kannst du anschließend die gewünschten Einstellungen für POWER CAPTCHA vornehmen oder mit unseren Voreinstellungen starten. Die Einbindung in deine Website oder App erfolgt mit JavaScript oder verfügbaren Plugins (z.B. WordPress-Plugin). Das Token kannst du auf deinem Server mit PHP oder einer anderen Programmiersprache verifizieren. Auf unserer Website findest du dafür Vorlagen und Anwendungsbeispiele, die du direkt verwenden oder nach Bedarf anpassen kannst.

Tarife

Tarif	Starter	Professional	Enterprise
Gewerblicher Einsatz	✓	✓	✓
Schutz für Formulare, Buttons und Login-Bereiche	✓	✓	✓
Unbegrenzte POWER CAPTCHA-Einsätze	✓	✓	✓
Einstellbares Limit für Lösungsversuche	✓	✓	✓
Highspeed Security Checks / Monat	300	1.000	2.000
Erhöhung der Schwierigkeit	automatisch	einstellbar	einstellbar
Überwachungs-zeitraum	30 Minuten	1-120 Minuten	1 Minute bis 3 Tage
Sperrzeit bei nicht gelösten Captcha	5 / 15 Minuten	1-120 Minuten	1 Minute bis 3 Tage
Service-Kanäle	FAQ, E-Mail mit Standard-Prio	FAQ, E-Mail mit erhöhter Prio, Ticket-System (ab 3 Lizenzen)	FAQ, E-Mail mit hoher Prio, Ticket-System mit hoher Prio (gem. SLA)
Captcha-Anzeige verzögern	-	✓	✓
Barrierefrei (2-Faktor-Authentisierung)	-	-	✓
Individ. Absender-kennzeichnung der 2-Faktor-Authentisierung	-	-	✓
Zusätzlicher Schutz von Login-Namen, E-Mailadressen, etc.	-	-	✓
Captcha-Editor (auf Anfrage)	-	-	✓

On-Premises-Version

Für Szenarien mit besonders hohen Anforderungen in Bezug auf die Integration von 3rd-Party Lösungen, ist POWER CAPTCHA auch als On-Premises-Version für die lokale Installation auf eurer Infrastruktur verfügbar. Fragen dazu beantwortet dir gerne unser Vertrieb: sales@power-captcha.com.

Über POWER CAPTCHA

POWER CAPTCHA ist eine Marke und Entwicklung der Uniique Information Intelligence AG. Die Uniique AG ist ein Hamburger Software-Unternehmen, welches seit 2010 u.a. eine mehrfach ausgezeichnete Software für die Automatisierung und Personalisierung im Kommunikations-, Marketing- und Service-Umfeld anbietet.