Barrierefreie Authentifizierung

Für die Anmeldung zu Websites müssen kognitive Funktionstests vermieden werden

Autor: Jan Hellbusch
Quelle: https://www.hellbusch.de/barrierefreie-authentifizierung/

Zwei neue Erfolgskriterien 3.3.8 und 3.3.9 in den Web Content Accessibility Guidelines (WCAG) 2.2 befassen sich mit der Vermeidung von schwierigen Anmeldeprozessen. Für jeden Schritt in einem Anmeldeprozess sind kognitive Funktionstests durch bestimmte Techniken zu ergänzen oder ersetzen. Während auf Konformitätsstufe AA bestimmte Formen von CAPTCHA erlaubt sind, sind sie auf Konformitätsstufe AAA nicht mehr zulässig.

Anforderungen (WCAG 2.2)

Success Criterion 3.3.8 Accessible Authentication (Minimum)

(Level AA)

A cognitive function test (such as remembering a password or solving a puzzle) is not required for any step in an authentication process unless that step provides at least one of the following:

Alternative

Another authentication method that does not rely on a cognitive function test.

Mechanism

A mechanism is available to assist the user in completing the cognitive function test.

Object Recognition

The cognitive function test is to recognize objects.

Personal Content

The cognitive function test is to identify non-text content the user provided to the Web site.

Note: "Object recognition" and "Personal content" may be represented by images, video, or audio.

Note: Examples of mechanisms that satisfy this criterion include:

- support for password entry by password managers to reduce memory need, and
- copy and paste to reduce the cognitive burden of re-typing.

Success Criterion 3.3.9 Accessible Authentication (Enhanced)

2 (Level AAA)

A cognitive function test (such as remembering a password or solving a puzzle) is not required for any step in an authentication process unless that step provides at least one of the following:

Alternative

> Another authentication method that does not rely on a cognitive function test.

Mechanism

> A mechanism is available to assist the user in completing the cognitive function test.

Übersetzungen

Erfolgskriterium 3.3.8 Barrierefreie Authentifizierung (Minimum)

(Stufe AA)

Ein kognitiver Funktionstest (wie das Merken eines Kennworts oder das Lösen eines Rätsels) ist in keinem Schritt im Prozess der Authentifizierung erforderlich, es sein denn, ein solcher Schritt bietet eines der Folgenden:

Alternative

> eine andere Authentifizierungsmethode, die sich nicht auf einen kognitiven Funktionstest verlässt.

Mechanismus

> Es ist ein Mechanismus verfügbar, um den Benutzer dabei zu unterstützen, den kognitiven Funktionstest durchzuführen.

Objekterkennung

> Beim kognitiven Funktionstest geht es darum, Objekte zu erkennen.

Persönlicher Inhalt

> Beim kognitiven Funktionstest werden Nicht-Text-Inhalte identifiziert, die der Benutzer der Website bereitgestellt hat.

Hinweis: "Objekterkennung" und "persönlicher Inhalt" können durch Bilder, Videos oder Audio dargestellt werden.

Hinweis: Beispiele von Mechanismen, die dieses Kriterium erfüllen, sind unter anderem:

- Unterstützung bei der Eingabe von Kennwörtern durch Passwort-Manager, damit sich der Benutzer weniger merken muss, und
- Kopieren und Einfügen, um die kognitive Belastung des erneuten Tippens zu reduzieren.

Erfolgskriterium 3.3.9 Barrierefreie Authentifizierung (Erweitert)

(Stufe AAA)

Ein kognitiver Funktionstest (wie das Merken eines Kennworts oder das Lösen eines Rätsels) ist in keinem Schritt im Prozess der Authentifizierung erforderlich, es sein denn, ein solcher Schritt bietet eines der Folgenden:

Alternative

> eine andere Authentifizierungsmethode, die sich nicht auf einen kognitiven Funktionstest verlässt.

Mechanismus

> Es ist ein Mechanismus verfügbar, um den Benutzer dabei zu unterstützen, den kognitiven Funktionstest durchzuführen.

Erläuterungen

Anmeldungen zu Webseiten sind ohne Zweifel wichtig. Bei der Verwendung finanzieller, rechtlicher und sonstiger sensibler Daten wäre die Nutzung entsprechender Webseiten ohne Anmeldung undenkbar. Das Problem ist meist, dass Passwörter genutzt werden. Andere Schutzmechanismen wie z.B. eine visuelle CAPTCHA stellen weitere nicht überwindbare Hürden dar.

Die Anmeldung zu einer Webseite muss barrierefrei und sicher sein. Um sich einloggen zu können, müssen Nutzende auf den meisten Webseiten mindestens einen Namen oder eine andere Kennung und ein Passwort eingeben. Das Auswendiglernen von Kennungen und Passwörtern bzw. das Abschreiben von Kennungen und Passwörtern macht es manchen Nutzenden mit kognitiven Behinderungen schwer oder unmöglich, sich zu einer Webseite anzumelden, außer sie erhalten Unterstützung beispielsweise durch einen Passwort-Manager.
Wenn sich Nutzende eine webseitenspezifische Kennung merken müssen, handelt es sich bereits um einen kognitiven Funktionstest. Beispiele für kognitive Funktionstests sind:

- Das Merken von Text und Zeichen,
- das Abschreiben von Text oder Zeichen,

- eine korrekte Rechtschreibung,
- das Rechnen oder
- das Lösen von Puzzeln und Rätseln.

Egal ob Nutzende eine zufällige Abfolge von Zeichen eintippen, eine besondere Geste auf dem Touch-Screen ausführen oder eine Frage beantworten müssen – es wird immer Nutzende geben, die solche Aufgaben nicht lösen können. Daher muss es eine Authentifizierungsmethode geben, die keine Aufgabe einschließt, die das Merken, das Verändern oder das Abschreiben voraussetzt.
Hinweis: Persönliche Daten wie Name, Telefon oder E-Mail-Adresse werden im Glossar der WCAG 2.2 von der Anforderung ausgeklammert. Diese Daten verändern sich nicht und das Merken von persönlichen Daten wird für die Nutzung von Webseiten vorausgesetzt.

Generell können wir Authentifizierungsmethoden wie folgt kategorisieren:

- Wissen:
  Nutzende müssen ein auswendig gelerntes Passwort, einen gemerkten Passwort-Satz oder einen eingeprägten Pfad einer Geste eingeben. Die meisten wissensbasierten Authentifizierungsmethoden sind kognitive Funktionstests, so dass mindestens alternative Authentifizierungsmöglichkeiten oder unterstützende Mechanismen verfügbar sein müssen, um sich zur Webseite anmelden zu können.
- Besitz:
  Nutzende erhalten ein Einmal-Passwort auf dem gleichen oder auf einem anderen Gerät oder die Nutzenden müssen ein QR-Code einscannen. Wenn beispielsweise Codes oder Passwörter an ein anderes Gerät geschickt werden, dürfen Nutzende das Passwort nicht abschreiben müssen.
  Wenn im Online-Banking auf einem Desktop-Rechner bei der zweiten Authentifizierung eine TAN

per SMS an ein mobiles Gerät geschickt wird, muss die TAN vom mobilen Gerät abgeschrieben werden, um auf dem Desktop-Rechner eingetippt zu werden. Da das Abschreiben zu den kognitiven Funktionstests gehört, genügt eine solche Methode der Anforderung nicht.

- Biometrie:
  Ein Gerät der Nutzenden scannt einen Fingerabdruck, führt eine Gesichtserkennung durch oder analysiert Tastenschläge. Es ist dabei nicht immer offensichtlich, welche geräteabhängigen Authentifizierungsmöglichkeiten den Nutzenden zur Verfügung stehen. Nutzende werden die Authentifizierungsmethode einrichten, die ihnen am besten passt.

Wenn Webseiten alternative Möglichkeiten der Authentifizierung anbieten, muss eine der Methoden ohne kognitive Funktionstests auskommen. Das gilt auch für die einzelnen Schritte in einer zweifachen Authentifizierung. Jeder Schritt der Anmeldung muss mindestens eine Möglichkeit der Authentifizierung anbieten, die das Bestehen eines kognitiven Funktionstests nicht voraussetzt.
Wenn eine Authentifizierung einen kognitiven Funktionstest voraussetzt, dann muss nach Erfolgskriterium 3.3.8 mindestens eine der folgenden vier Situationen zutreffen:

1. Sie stellen eine alternative Authentifizierungsmethode bereit, die sich nicht auf kognitive Funktionstests verlässt, oder
2. Sie ermöglichen einen Mechanismus, der Nutzende beim Bestehen des kognitiven Funktionstests unterstützt bzw. Sie unterbinden diese nicht, oder
3. der kognitive Funktionstest besteht darin, Objekte in Bildern, Video oder Audio zu identifizieren, oder
4. der kognitive Funktionstest besteht darin, Inhalte in Bildern, Video oder Audio zu identifizieren, die Nutzende selbst zur Webseite hinzugefügt haben.

Bei den letzten beiden Situationen handelt es sich um CAPTCHA-Verfahren. CAPTCHA steht für „Completely Automated Public Turing-test to tell Computers and Humans Apart“ (vollautomatischer öffentlicher Test, um Computer und Menschen zu unterscheiden) und stellt den Versuch dar, automatisierte Eingaben durch Software von solchen zu unterscheiden, die von Menschen vorgenommen werden. CAPTCHA-Verfahren mit visuellen oder auditiven Inhalten genügen dabei Erfolgskriterium 3.3.9 (Konformitätsstufe AAA) nicht, d.h. Sie sollten diese nicht einsetzen.

Alternative Authentifizierung

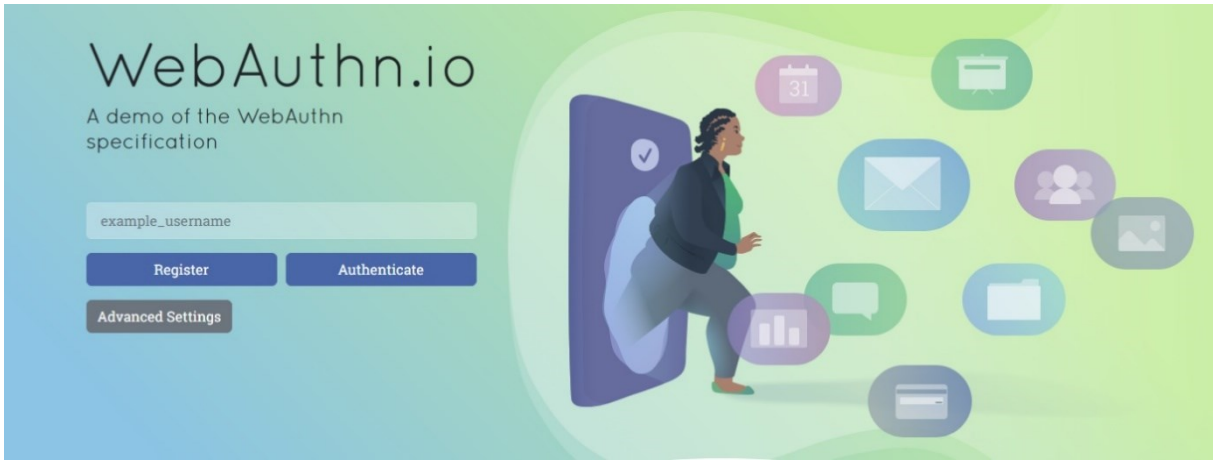
Die Anmeldung zu einer Webseite kann sehr unterschiedlich umgesetzt sein. Damit sich Nutzende Passwort und ggf. Kennung nicht merken oder abschreiben müssen, könnte die Anmeldung auch nur per E-Mail und ohne Passwort erfolgen. Somit kann das Bestehen eines kognitiven Funktionstests vermieden werden.
Die Anmeldung läuft dann folgendermaßen ab: Wenn Nutzende sich mit einer E-Mail-Adresse zu einer Webseite anmelden, wird ein Link für einen einmaligen Login per E-Mail an die E-Mail-Adresse geschickt. Nutzende können den Link in einem E-Mail-Programm direkt aufrufen und die Anmeldung ist abgeschlossen. Nutzende können ihre Aktivitäten im geschützten Bereich der Website aufnehmen.

Freilich genügt eine solche Anmeldung vielen Sicherheitsanforderungen nicht, aber für das Lesen von abonnierten Bezahlinhalten oder für eine Kommentarfunktion, die nur bei Anmeldung zugänglich ist,

kann eine solche Technik Barrieren abbauen. Zumindest soll es für eine Anmeldung zu einer Webseite mindestens eine Technik für die Anmeldung geben, die ohne eine Passworteingabe auskommt.

Nutzende könnten dazu aufgefordert werden, ein USB-verbundenes Gerät zu nutzen, auf der sie lediglich einen Schalter drücken müssen, um einen Token mit Zeitstempel zu schicken. Andere Mechanismen des Geräts wie das Einscannen eines Fingerabdrucks, eine Gesichtserkennung durchführen oder die Analyse von Tastenschlägen können ebenso genutzt werden. Entscheidend für das Umgehen eines kognitiven Funktionstests ist, dass Nutzende keine Passwörter eintippen oder andere kognitiven Tests bestehen müssen.

Mit der Web Authentication API (WebAuthn) werden Verfahren beschrieben, um Registrierungen, einfache Anmeldungen und Mehrfach-Authentifizierungen auf Webseiten vollständig ohne Passwörter durchzuführen. Eine Einführung mit Code-Beispielen finden Sie auf https://webauthn.guide/



Die Authentifizierung der Nutzenden erfolgt dabei, ohne dass sie etwas merken oder abschreiben müssen. Stattdessen erkennt die Webseite das Gerät, und Nutzende bestätigen dann ihre Identität über Sensoren des Geräts oder mit einem Hardware-Token, den sie mit ihrem Gerät verbinden. Der Browser schickt bei erfolgreicher Legitimation eine Bestätigung der Identität (ein sogenannter Passkey) an den Server.

Bei Passkeys werden Schlüssel unauslesbar in einem speziellen Security-Chip auf einem Gerät gespeichert. Bei der Anmeldung zu einer Webseite wird ein Gerät (statt einer Passworteingabe) mit der Anmeldung verknüpft. Es können verschiedene Geräte für die Anmeldung zu einer Webseite eingerichtet werden. So können Desktop-Rechner und SmartPhones beide als Anmeldeschlüssel Zugang erhalten. Bei der Einrichtung eines neuen Geräts wird z.B. ein QR-Code angezeigt, der von Nutzenden eingescannt werden muss. Danach sind Nutzende über das zweite Gerät ebenfalls authentifiziert.

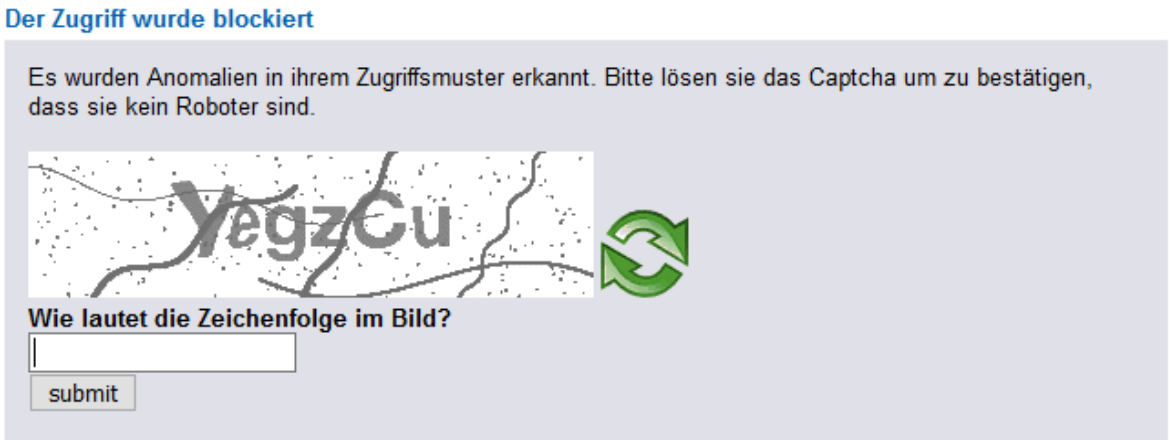
Verfügbare Unterstützungsmechanismen

Authentifizierungen mit einer Kennung oder E-Mail-Adresse und einem Passwort sind WCAG-konform, wenn Browser oder Passwort-Manager die Eingabefelder automatisch ausfüllen können.

Das ist beispielsweise der Fall, wenn Sie das autocomplete-Attribut gemäß Erfolgskriterium 1.3.5 einsetzen.
Damit können Browser und Passwort-Manager den Eingabezweck für die Eingabefelder ermitteln und entsprechende Vorschläge anbieten oder gleich die korrekten Angaben einsetzen. Wenn die Webseite aber das automatische Ausfüllen verhindert, dann ist dieser Unterstützungsmechanismus nicht verfügbar.
Ein alternativer Unterstützungsmechanismus ist die Möglichkeit, Texte in die Eingabefelder per Copy-und-Paste einzufügen. Die Webseite darf die Copy-und-Paste-Funktionalität nicht blockieren. Nutzende können dann ihren Passwort-Manager aufrufen, die Anmeldedaten für eine Webseite nacheinander kopieren und in das Anmeldeformular der Webseite einfügen.
Bei zweifacher Authentifizierung kommen oft weitere Authentifizierungsmethoden zum Tragen. Ob die Authentifizierung durch Drittanbieter (auf der Webseite oder per App) genutzt werden kann, hängt davon ab, ob ein Passwort eingegeben werden muss. Wenn die Anmeldung über einen Drittanbieter lediglich durch eine Bestätigung vorgenommen werden kann, dann handelt es sich um eine alternative Authentifizierung ohne kognitiven Funktionstest. Natürlich setzt diese Methode voraus, dass Nutzende über solche Konten bei Drittanbietern verfügen.

CAPTCHA

Bei einem CAPTCHA handelt es sich um einen automatisierten Test, der feststellen soll, ob ein Mensch oder ein Roboter beispielsweise eine Eingabe in einem Eingabefeld vornimmt. Auf Webseiten gibt es verschiedene Arten von CAPTCHA. Die gängigste Form ist ein visuelles CAPTCHA mit einer Grafik, die eine Folge zufällig ausgewählter Buchstaben oder Ziffern zeigt. Die Buchstaben und Ziffern werden durch Verzerrung oder durch die Darstellung vor einem komplizierten Hintergrund absichtlich schwer leserlich gemacht. Nutzende müssen die Zeichen erkennen und in ein Eingabefeld abtippen.



Erfolgskriterium 1.1.1 gibt vor, dass ein visuelles CAPTCHA durch eine andere Form von CAPTCHA für Nutzende, die die Grafik visuell nicht erfassen können, ergänzt werden muss. Auf Webseiten können vor allem folgende Formen von alternativen CAPTCHAs von Nutzende gelöst werden müssen:

- Audio-CAPTCHAs, die gesprochenen Inhalte verzerrt wiedergeben, und
- Logische CAPTCHAs, die eine verhältnismäßig einfache Aufgabe wie „Was ist das Ergebnis von 4 + 2“ oder „Welche Farbe hat die Sonne?“ stellen. Schon bei der Frage nach der Farbe der Sonne

sollte klar sein, dass die Beantwortung solcher Fragen nicht immer eindeutig sein kann, denn die Sonne kann auch rot sein.

Die eben beschriebenen CAPTCHAs dürfen nicht eingesetzt werden:

- Die visuellen und auditiven CAPTCHAs stellen kognitive Funktionstests dar, weil Nutzende ein Text abschreiben müssen.
- Logische CAPTCHAs setzen immer eine kognitive Leistung voraus und sind daher ebenfalls nicht WCAG-konform.

Sie dürfen CAPTCHAs nach Erfolgskriterium 3.3.8 nur dann in Anmeldeprozessen einsetzen, wenn nutzende in dem CAPTCHA Gegenstände identifizieren und auswählen müssen. Meist sind solche CAPTCHAs mit einer Frage verbunden. Ein solcher Test könnte aus 16 Bildern und der Frage „Welche der Bilder zeigen eine Ampel?“ bestehen.

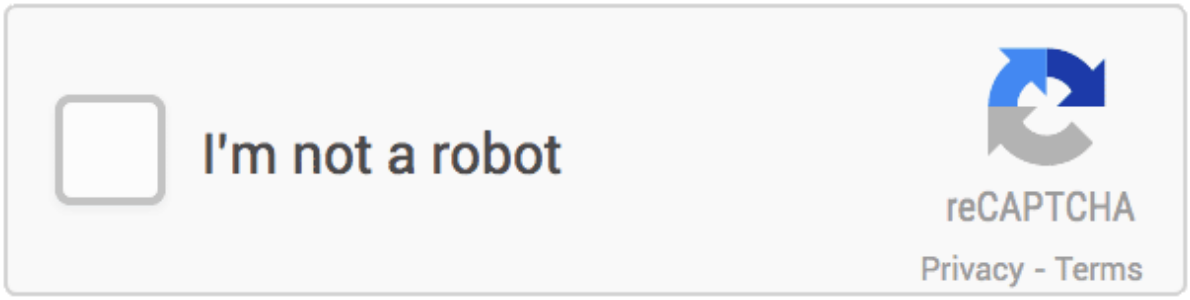
Solange die Frage einfach gehalten wird und die Bilder Alltagsgegenstände zeigen und gut unterscheidbar sind, stellt diese Art von CAPTCHA keinen kognitiven Funktionstest dar. Die zugelassenen Verfahren können wie folgt beschrieben werden:

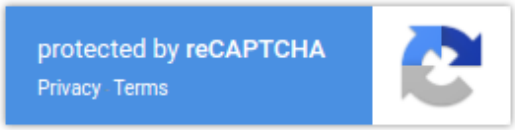
- Es wird eine Auswahl an Bildern angezeigt und Nutzende müssen ein bestimmtes Bild identifizieren (z.B. ein Auto unter anderen Gegenständen erkennen oder ein Taxi unter mehreren Autos) oder

- es wird eine Auswahl an Bildern angezeigt und Nutzende müssen das Bild identifizieren, das sie selbst bereitgestellt haben oder
- es wird eine Auswahl von Gegenständen in Textform angezeigt und Nutzende müssen den Gegenstand identifizieren, den sie selbst bereitgestellt haben.

Ein häufig genutzter Dienst zur Einbindung von CAPTCHAs ist ReCAPTCHA. Es bestehen mit „No CAPTCHA reCAPTCHA“ oder reCAPTCHA V3 unterschiedliche Verfahren. Die Barrierefreiheit muss unterschiedlich bewertet werden:

- Mit „No CAPTCHA reCAPTCHA“ können Nutzende ein Kontrollkästchen „Ich bin kein Roboter“ aktivieren. Bei der Aktivierung verwendet Google die verfügbaren Informationen, unter anderem die Bewegung des Mauszeigers, um zu bestimmen, ob die/der BesucherIn ein Roboter ist oder nicht. Wird ein Mensch vermutet, erscheint ein grünes Häkchen. Wenn Zweifel bestehen, wird ein visuelles CAPTCHA mit Auswahlmöglichkeiten eingeblendet. Dieses Verfahren erkennt Menschen aber nicht, wenn ein Screenreader aktiviert ist.
- reCAPTCHA V3 ist ein punktebasiertes Verfahren und für Nutzende unsichtbar. Es wird ein Wert zwischen 0 und 1 ermittelt, abhängig vom Verhalten der Nutzenden, und das Entwicklerteam muss in der Konfiguration festlegen, was mit niedrigen Bewertungen geschehen soll (z.B. zusätzliche Authentifizierung durch eine E-Mail mit einem Bestätigungslink).





CAPTCHAs können aber auch vollständig ohne Interaktion angeboten werden. Ein Beispiel für ein solches Verfahren finden Sie auf
https://friendlycaptcha.com/#demo
Auf Konformitätsstufe AAA wird die Ausnahme, dass visuelle CAPTCHAs in Anmeldeprozessen genutzt werden dürfen solange sie nur eine Auswahl bieten, aufgehoben. Nach Erfolgskriterium 3.3.9 sollen visuelle oder auditive CAPTCHAs während der Authentifizierung nicht verwendet werden. Das W3C bietet ein eigenes Dokument zum Umgang mit CAPTCHAs und beschreibt Honeypot-Verfahren und Heuristiken als Alternativen:
https://www.w3.org/TR/turingtest/

Weiterführende Links

- Erläuterungen zu Erfolgskriterium 3.3.8 beim W3C: https://www.w3.org/WAI/WCAG22/Understanding/accessible-authentication-minimum
- Erläuterungen zu Erfolgskriterium 3.3.9 beim W3C: https://www.w3.org/WAI/WCAG22/Understanding/accessible-authentication-enhanced
- Neun neue Kriterien, eine Übersicht der Änderungen in den WCAG 2.2 gegenüber WCAG 2.1: https://www.hellbusch.de/neun-neue-kriterien/

Hellbusch Accessibility Consulting

- Tests und Gutachten zur Konformität Ihrer Webseiten, Apps und Software zu den Barrierefreiheitsrichtlinien.
- Überarbeitung Ihrer nicht barrierefreien PDF-Dokumente und -Formulare in PDF/UA-Qualität.
- Schulungen für die barrierefreie Gestaltung von Webseiten und PDF-Dokumenten.

HELLBUSCH
ACCESSIBILITY CONSULTING

Schauen Sie vorbei auf https://www.barrierefreies-webdesign.de.

Nehmen Sie Kontakt auf: jan@hellbusch.de oder +49 (163) 3369925