SID 19
SAFER INTERNET DAY
Wir sind dabei!

Bayerisches Landesamt für Datenschutzaufsicht

Sicher im Internet –
Digitale Dienste im Datenschutzcheck

1 Cybersicherheit 2 Tracking

Thomas Kranig | Präsident
Bayerisches Landesamt für Datenschutzaufsicht

Ansbach, 5. Februar 2019

Hinweis zur Prüfung

Auf Grund der kurzen Zeitspanne am Safer Internet Day 2019 wurden die beiden Prüfblöcke „Cybersicherheit“ und „Tracking“ im Schnellverfahren durchgeführt. Im Nachgang zur Prüfung findet eine Validierung der Prüfergebnisse statt, sodass das BayLDA mit den gewonnen Erkenntnissen gezielt an die jeweiligen verantwortlichen Unternehmen aus Bayern herantreten kann. Falls bei den übrigen Prüfkandidaten außerhalb Bayerns ein Datenschutzverstoß festgestellt wird, bereitet das BayLDA die Prüfergebnisse auf und leitet sie an die federführende Datenschutzaufsichtsbehörde weiter.

Sicher im Internet -

1 Datenschutzcheck „Cybersicherheit“

Untersuchung von **20** ausgewählten prominenten Websites hinsichtlich datenschutzrechtlicher Anforderungen im sicheren Umgang mit Nutzerdaten (Fokus auf Registrierung & Login – insb. Passwörter)

1 Cybersicherheit

Welche Kategorien von Websites untersucht?

- 2 Streaming-/Videoportale
- 2 E-Mail-Dienste
- 2 Elektronik-Shops
- 2 Fotoservices
- 2 Gesundheit-/Kosmetik-Websites
- 2 Möbel-Shops
- 3 Mode-Shops
- 2 Preisvergleich-/Ticketseiten
- 3 Soziale Netzwerke

1 Cybersicherheit

Wie viele Prüfpunkte wurden hinsichtlich der Sicherheit auf der Website untersucht?

22 Prüfpunkte

Registrierung – Sichere Gestaltung eines Nutzer-Accounts

17 Prüfpunkte

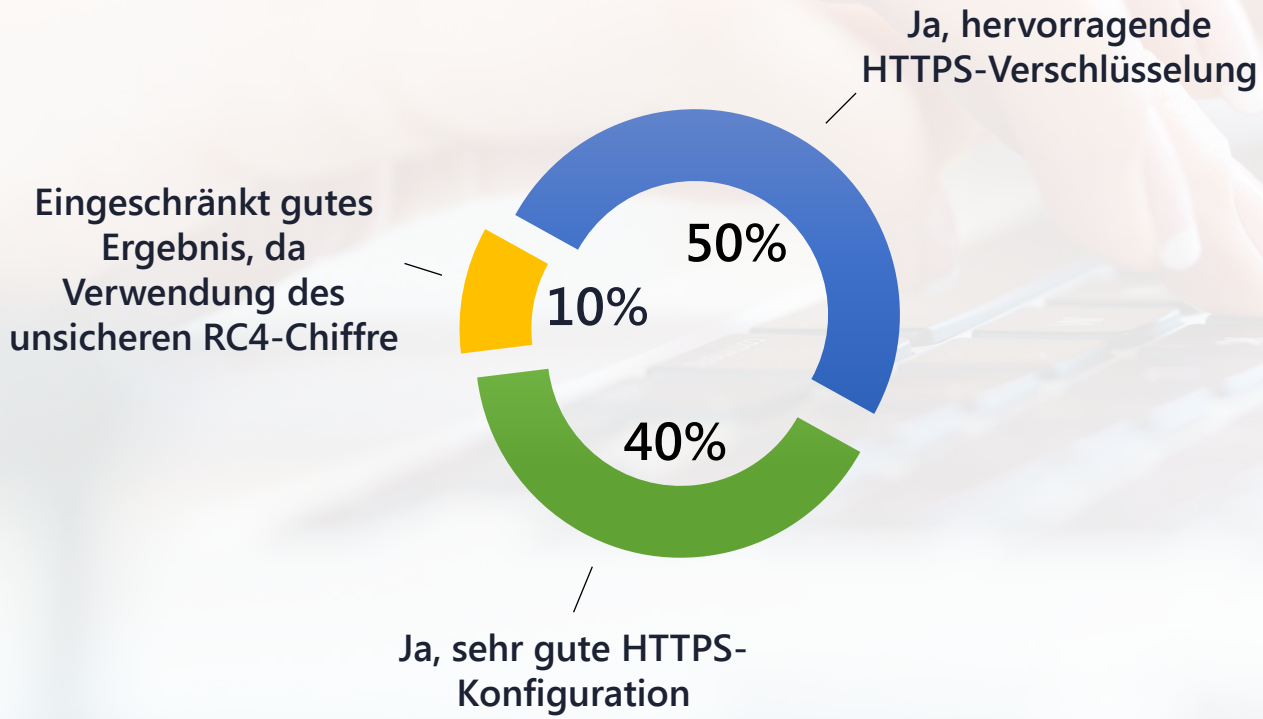
Login – Schutz vor Übernahme eines Nutzer-Accounts durch Cyberkriminelle

Eine Auswahl der wichtigsten Prüfpunkte und Ergebnisse dieses Checks wird nachfolgend dargestellt.

1 Cybersicherheit

HTTPS

Verfügt der Dienst über eine ausreichende HTTPS-Verschlüsselung zum Schutz der eingegebenen personenbezogenen Daten?



Bewertung des Ergebnisses

Fast jeder geprüfte Dienst verfügt über eine geeignete HTTPS-Verschlüsselung. Bei 50% ist das Ergebnis sogar hervorragend, bei 40% sind kleinere Verbesserungspotentiale erkennbar (z. B. auf Grund schwacher Chiffren oder Unterstützung von veralteten TLS-Protokollen). Zwei kontrollierte Diensten fallen im Schnelltest jedoch negativ durch die Verwendung des unsicheren RC4-Algorithmus auf. Unser Fazit bleibt aber: HTTPS ist für die großen Unternehmen kein Problem.

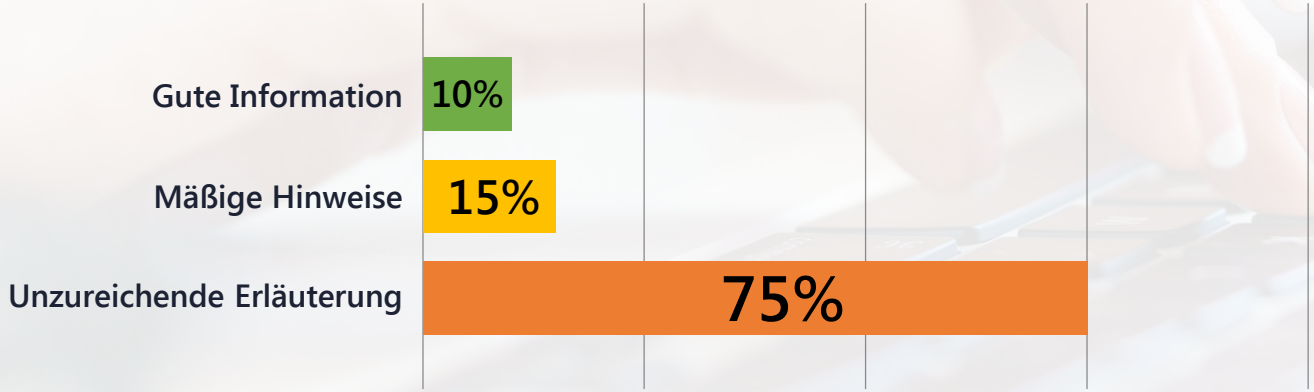
Hintergrund

HTTPS dient als Transportverschlüsselung im Web zur sicheren Übertragung von Daten, z. B. von Passwörtern. HTTPS ist daher eine wesentliche Datenschutzanforderung für Online-Dienste. HTTPS ist aber nicht immer gleich HTTPS – es kommt auf die konkrete Umsetzung an. Websitebetreiber müssen einiges beachten, damit das „grüne Schlosssymbol" im Browser auch tatsächlich für ausreiche Verschlüsselung auf dem Weg durchs Internet steht.

1 Cybersicherheit

Hilfe für ein starkes Passwort

Wird dem Nutzer vom Dienst erklärt, wie ein starkes Passwort gewählt werden kann?



Bewertung des Ergebnisses

Ein Großteil der Websites gibt dem Nutzer bei der Passwortwahl nur unzureichende Hinweise mit an die Hand. In manchen dieser Fälle wird der Nutzer überhaupt nicht unterrichtet, wie sich ein starkes Passwort zusammensetzen soll – der Nutzer ist somit völlig auf sich allein gestellt.

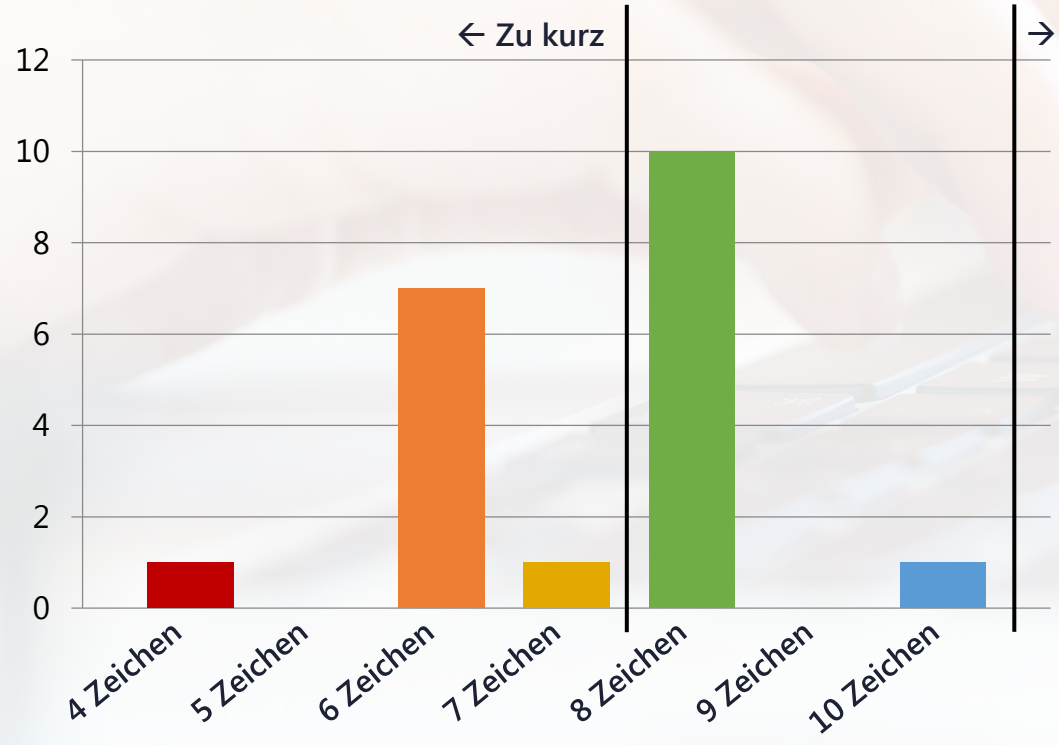
Hintergrund

Ein starkes Passwort ist eine entscheidende Komponente, um die persönlichen Informationen in einem Nutzer-Account vor Fremden zu schützen. Daher ist es wichtig, dass der Nutzer vom Anbieter Hinweise erhält, wie er selbst ein starkes Passwort erzeugen und so seine eigenen Daten schützen kann.

1 Cybersicherheit

Mindestlänge Passwort

Welche Mindestlänge fordert der Dienst bei einem Passwort?



Bewertung des Ergebnisses

Überraschender Weise fordern 9 von 20 Dienste weniger als acht Zeichen bei der Wahl eines Passworts. Besonders negativ fällt ein Dienst mit einer Mindestlänge von nur vier Zeichen auf. Auch sechs Zeichen sind keine Seltenheit.

Einziger Lichtblick ist eine Website, die zehn Zeichen vom Nutzer für das Passwort abverlangt – auch wenn das BayLDA zwölf Zeichen als Mindestlänge für ein Passwort empfiehlt.

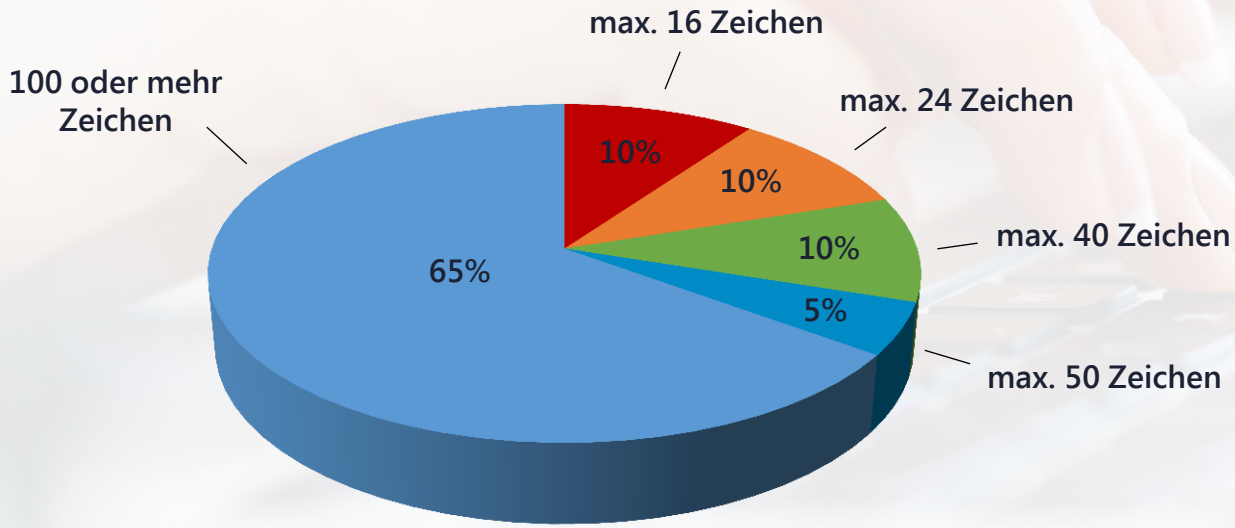
Hintergrund

Die Länge eines Passworts ist zwar nicht das einzige Kriterium, um die Stärke eines Passworts zu bewerten, aber ein sehr wichtiges. Websites, die sehr kurze Passwörter (z. B. sechs Zeichen) zulassen und keine weiteren Sicherheitsmechanismen, wie z. B. einen zweiten Faktor per SMS-Code anbieten, setzen den Nutzer der erhöhten Gefahr einer unbefugten Account-Übernahme durch Kriminelle aus.

1 Cybersicherheit

Maximallänge Passwort

Wie viele Zeichen darf ein Nutzerpasswort maximal haben?



Bewertung des Ergebnisses

Zwei Drittel der Dienste bietet dem Nutzer die Möglichkeit, sehr lange und damit auch potentiell starke Passwörter von 100 Zeichen oder sogar mehr zu verwenden. Vier Dienste schneiden in der Prüfung jedoch weniger gut ab, da dort Passwörter nur mit einer Länge von maximal 16 bzw. 24 Zeichen wählbar sind.

Hintergrund

Websites, die die Länge von Passwörtern mit wenigen Zeichen beschränken, verhindern zum Teil starke Nutzerpasswörter. Der Nutzer sollte daher die Möglichkeit haben, auch sehr lange Passwörter zu verwenden.

1 Cybersicherheit

Starkes Passwort

Wird ein starkes Passwort vom Dienst „erzwungen“ oder kann ein Nutzer auch ein schwaches Passwort verwenden?

Im Test akzeptierte Passwörter:

- 0000
- 123456
- ABC123
- aabbcc1
- Passwort
- abcdefgh
- 12345Aa!
- Aaaaaa1!
- P@sswort
- 12345678
- Passwort12

Bewertung des Ergebnisses

Keiner der Online-Dienste erzwingt ein starkes Passwort. Der einzige Dienst im Prüflauf, der eine Mindestlänge von 10 Zeichen anbietet, fordert keine ausreichende Komplexität, so dass auch dort schwache Passwörter möglich sind. Negativ fällt auf, dass einige Passwortrichtlinien nicht zeitgemäß sind und einfache, unsichere Passwörter nach bekannten Muster gewählt werden können. Erschreckend ist, dass mehrere Websites diese offensichtlich schwachen Passwörter als „sicher“ bewerten.

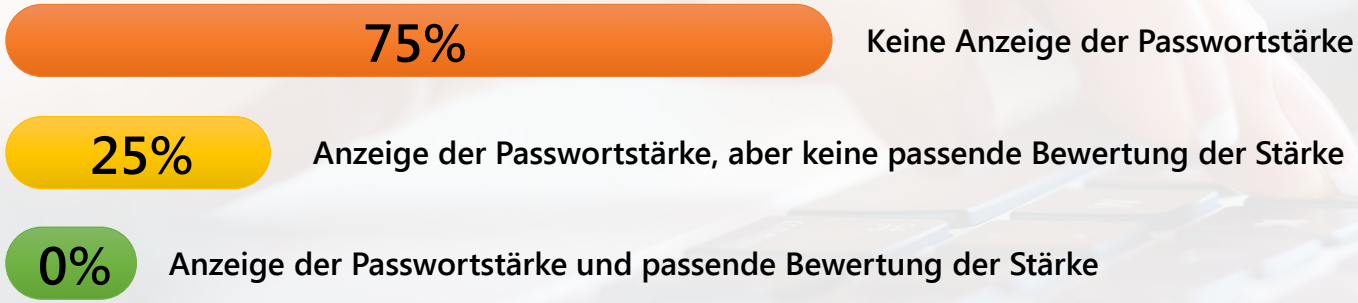
Hintergrund

Gerade für die Websites, die den Login lediglich über Nutzerkennung und Passwort gestalten, ist es essentiell, dass das verwendete Passwort ausreichend sicher ist.

1 Cybersicherheit

Anzeige der Passwortstärke

Wird dem Nutzer die Stärke seines gewählten Passworts angezeigt (z. B. Passwortgütebalken oder Passwortampel)?



Bewertung des Ergebnisses

Drei Viertel der Websites zeigen dem Nutzer bei der Registrierung die Stärke des gewählten Passworts gar nicht an, sondern verweisen höchstens noch auf die eigenen Passwortrichtlinien. Die übrigen Dienste haben mitunter gute Passwortgütebalken oder andere Visualisierungskomponenten – jedoch bewerten diese schwache Passwörter oft irrtümlich als „sicher" oder „stark". Als Randbemerkung fällt auf, dass die Dienste gleiche Passwörter unterschiedlich stark bewerten.

Hintergrund

Viele Nutzer wissen nicht, ab wann ein Passwort stark genug ist, um einen echten Schutz vor unbefugten Zugriffen auf den Account zu gewährleisten. Wenn Dienste den Nutzer hierbei nicht unterstützen oder verwirrende Hinweise mitgeben, neigen manche Nutzer womöglich dazu, Passwörter nur nach den Mindestanforderungen zu wählen. Diese Anforderungen führen dann meist zu sehr schwachen Passwörtern, was man anhand veröffentlichter Passwortlisten aus Datenpannen erkennen kann.

1 Cybersicherheit

Mehr-Faktor-Anmeldung

Wird dem Nutzer auch die Möglichkeit einer Mehr-Faktor-Authentifizierung angeboten (z. B. per SMS-Code oder Geräte-Identifizierung)?

80% Nein,
nur Passwort

Passwort ****

10% Ja,
aber mäßige Information

Passwort ****

SMS-Code ##

10% Ja
und gute Information

Passwort ****

SMS-Code ##

Information

Bewertung des Ergebnisses

Verhältnismäßig wenig Websites bieten dem Nutzer erhöhten Schutz an, in dem neben dem Passwort noch ein weiterer Faktor (z. B. SMS-Code) abgefragt wird, bevor ein Login erfolgreich abgeschlossen werden kann. Bei den Websites, die einen zweiten Faktor anbieten, zeigt sich jedoch noch etwas Luft nach oben, da man als Nutzer zum Teil nur über Umwege im Account-Menü mit mäßigen Informationen an die zusätzliche und sehr sinnvolle Sicherheitsmaßnahme gelangt.

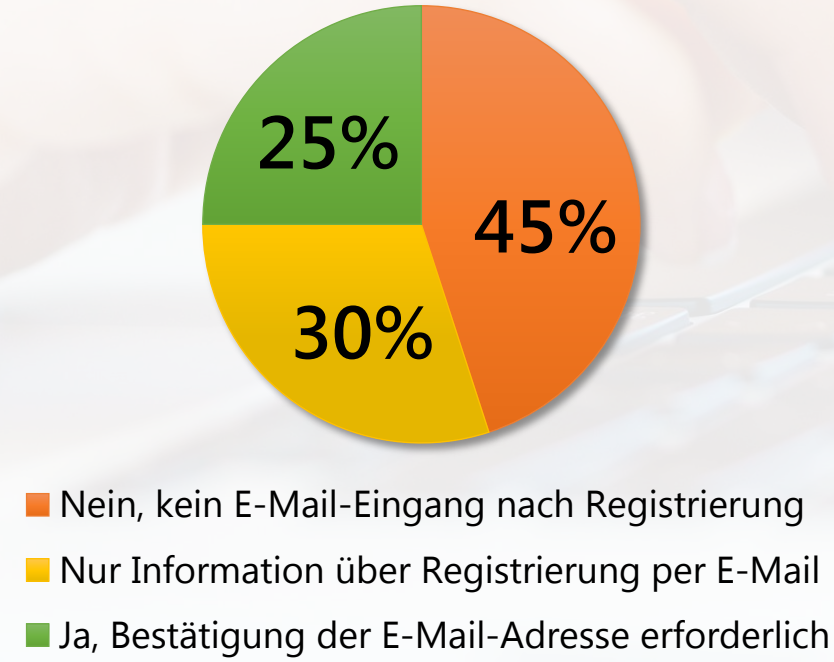
Hintergrund

Mit einer Zwei-Faktor-Authentifizierung hat ein Nutzer die Möglichkeit auf einen deutlichen Sicherheitsgewinn. Zwar nimmt der Login-Vorgang dann etwas mehr Zeit in Anspruch, jedoch beugt man gerade durch den zweiten Faktor (z. B. SMS-Code oder App-Token) vielen klassischen Online-Passwortattacken vor.

1 Cybersicherheit

Bestätigung der E-Mail-Adresse nach Registrierung

Erhält der Nutzer eine E-Mail, um die im Account hinterlegte E-Mail-Adresse erfolgreich zu bestätigen (evtl. mit URL-Token) und die Registrierung abzuschließen?



Bewertung des Ergebnisses

In nur 25% der Fälle muss der Nutzer die Registrierung auf der Website mit einem Klick auf einen Link in einer E-Mail bestätigen.

In fast jedem zweiten Fall ist eine Registrierung mit einer E-Mail-Adresse möglich, ohne dass der Besitzer der E-Mail-Adresse den Registrierungsvorgang überhaupt mitbekommt, da keinerlei Information an die angegebene E-Mail-Adresse stattfindet.

Hintergrund

Vollständige Adressdatensätze zu Millionen verschiedener Menschen kursieren schon lange im Internet. Um Identitätsdiebstahl zu erschweren, ist es wichtig, dass Websites bei Registrierungen Maßnahmen ergreifen, um Anmeldungen von Betrügern zu erkennen. Die Bestätigung des Accounts per E-Mail ist eine wichtige Komponente hierfür, wenngleich der Dienst dafür sorgen muss, dass dadurch keine „Spam-Schleuder“ entsteht.

1 Cybersicherheit

Warnung vor Phishing

Wird der Nutzer während oder kurz nach der Registrierung über die Gefahren möglicher Phishing-Angriffe informiert?

Nein

Drei Beispiele „gescheiterter" Information:

- Die Information befindet sich irgendwo auf der Website versteckt in den FAQ

  → Schlecht auffindbar – die FAQ lesen schließlich die wenigsten Nutzer nach der Registrierung

- In einer E-Mail des Dienstes wird erwähnt, dass man als Nutzer die Echtheit von E-Mails des Dienstes daran erkennt, dass Links mit „https" beginnen und den Name des Dienstes enthalten

  → Phishing-Mails können diese Kriterien spielerisch erfüllen, somit ist diese Information trügerisch

- Eine Website informiert zwar auf einer Unterseite kurz darüber, dass es eine aktuelle Phishing-Welle gibt, bietet aber dann keine konkreten Hilfemaßnahmen zum Erkennen dieser Nachrichten an

  → Ausbaufähig

Bewertung des Ergebnisses

Die Verantwortung beim Thema Phishing sehen viele Websitebetreiber scheinbar alleine beim Nutzer, da sie keine oder nur verstecke Hilfe hinsichtlich Phishing-Nachrichten anbieten.

Hintergrund

Gerade unter Vortäuschung, ein „großer" Anbieter zu sein, versuchen Cyberkriminelle mit Phishing-Nachrichten an die Zugangsdaten des Nutzers zu gelangen. Es wäre daher wichtig, den Nutzer hinsichtlich bekannter und aktuell laufender Angriffsarten zu informieren, so dass die Wahrscheinlichkeit sinkt, dass der Nutzer auf die Betrugsmasche hereinfällt.

1 Cybersicherheit

Fehlgeschlagene Logins und fremde Sitzungen

Wird der Nutzer darüber informiert, ob es fehlgeschlagene Logins gab und ob fremde Geräte eingeloggt (d. h. weitere Sitzungen aktiv) sind?

Nur 1 der geprüften Websites

informiert über fehlgeschlagene Logins

25%

zeigen aktive Sitzungen aller Geräte

Bewertung des Ergebnisses

Eine Website zeigt im Test bereits im Account-Menü sofort Information über fehlgeschlagene Logins. Bei den anderen Websites kann zumindest im Schnellverfahren nicht erkannt werden, an welcher Stelle man diese Information erhält.
Ein Viertel der Dienste bietet zudem das Feature an, zu sehen, welche Geräte mit welcher IP-Adresse im Account eingeloggt sind. Nutzer können so merkwürdige Aktivitäten leichter erkennen und diese beenden.

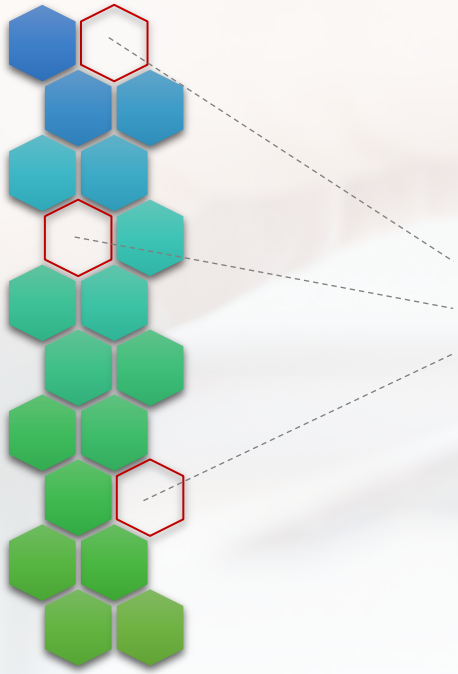
Hintergrund

Ob eine Information über fehlgeschlagene Logins für den Nutzer hilfreich oder eher abschreckend ist, sei dahingestellt. Fest steht jedoch, dass ein Nutzer grundsätzlich wissen sollte, wenn seine „digitale Identität" in Gefahr ist. Dann jedoch wäre eine Unterstützung in Form von geeigneten Tipps und Tools vom Dienst erforderlich. Ein solches Werkzeug ist bspw. das Verwalten von aktiven Sitzungen.

1 Cybersicherheit

Passwortabfrage bei Passwortänderung

Wird bei Passwortänderung das bestehende (alte) Passwort vom Nutzer erneut abgefragt?



3 von 20 Websites erlauben eine Passwortänderung in der Session ohne Eingabe des alten Passworts

Bewertung des Ergebnisses

Bei fast allen Diensten wird bei einer Änderung des Passworts das bestehende Passwort vom Nutzer abgefragt. Bei drei Websites reicht es jedoch aus, eingeloggt zu sein – dann kann mühelos ein neues Passwort vergeben werden.

Hintergrund

Aus Sicherheitsgründen sollten Dienste bei der Durchführung eines Passwortwechsels vom Nutzer Nachweise erhalten, dass dieser tatsächlich der Nutzer ist, für den er sich ausgibt.

Nicht selten gelingt es ansonsten Angreifern, die Sitzung (Session) eines eingeloggten Nutzers zu übernehmen (z. B. durch fehlerhaftes Sessions Management des Dienstes).

1 Cybersicherheit

Information über Passwortänderung

Wird der Nutzer über einer Passwortänderung per E-Mail informiert?

Nur

50%

der Websites informieren den Nutzer über die Änderung seines Passworts per E-Mail an die hinterlegte E-Mail-Adresse

Bewertung des Ergebnisses

Nur bei jeder zweiten Website wird der Nutzer darüber informiert, dass das Passwort seines Accounts geändert wurde – unabhängig davon, wer tatsächlich die Passwortänderung durchgeführt hat.

Hintergrund

Übernimmt ein Cyberkrimineller einen Nutzer-Account, weil er das bisher verwendete Passwort erraten, geknackt, „gefunden" oder eine Schwachstelle im Dienst ausgenutzt hat, so beginnt meist ein Wettlauf gegen die Zeit. Sollte der Unbefugte das Passwort des Nutzers ändern und den Nutzer aussperren, so ist die Information an die hinterlegte E-Mail-Adresse ein wichtiger Hinweis für den Nutzer, dass er sich unverzüglich an den Website-Betreiber wenden sollte.

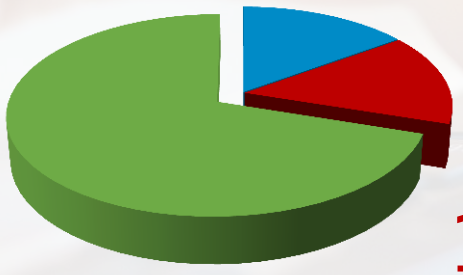
1 Cybersicherheit

Passwort-Vergessen

Wird bei der Passwort-Vergessen-Funktion eine E-Mail mit zeitlich begrenzt gültiger URL an die hinterlegte E-Mail-Adresse des Nutzers versendet?

15%
Ein anderes sicheres Verfahren wird verwendet (z. B. SMS-Code)

70%
Ja, Passwort kann über Link per E-Mail zurückgesetzt werden



15%
Nein, das neue Passwort wird per E-Mail mitgeteilt (im Klartext versendet)

Bewertung des Ergebnisses

Die allermeisten Websites bieten den Nutzer geeignete Verfahren an, um Passwörter zurückzusetzen bzw. neu zu vergeben. Drei Dienste fallen jedoch negativ auf, weil sie Passwörter direkt an die E-Mail-Adresse des Nutzers senden – dies birgt viele Sicherheitsrisiken.

Hintergrund

Damit ein Passwort eine geheime Information bleibt, die der Nutzer für die Anmeldung bei einem Dienst verwenden kann, darf diese Information mit niemanden geteilt werden. Wird ein Passwort vollständig in einer E-Mail genannt, bestehen mehrere unterschiedliche Gefahren, wie Unbefugte an das Passwort gelangen könnten.

1 Cybersicherheit

Support bei Sicherheitsfragen und Hacking

Stellt die Website Informationen zu Fragen rund um die Account-Sicherheit bereit, wenn z. B. der Account des Nutzers von einem Unbefugten übernommen wurde?

6 von 20 Websites

bieten Support an, wenn ein Nutzer befürchtet oder feststellt, dass der eigene Account von Fremden übernommen wurde

Bewertung des Ergebnisses

Bei deutlich mehr als der Hälfte der geprüften Websites sind keine oder nur dürftige Support-Informationen vorzufinden. Sechs Dienste machen es dagegen besser und zeigen dem Nutzer Schritt für Schritt, was er tun kann, wenn der eigene Account von Fremden übernommen wurde.

Hintergrund

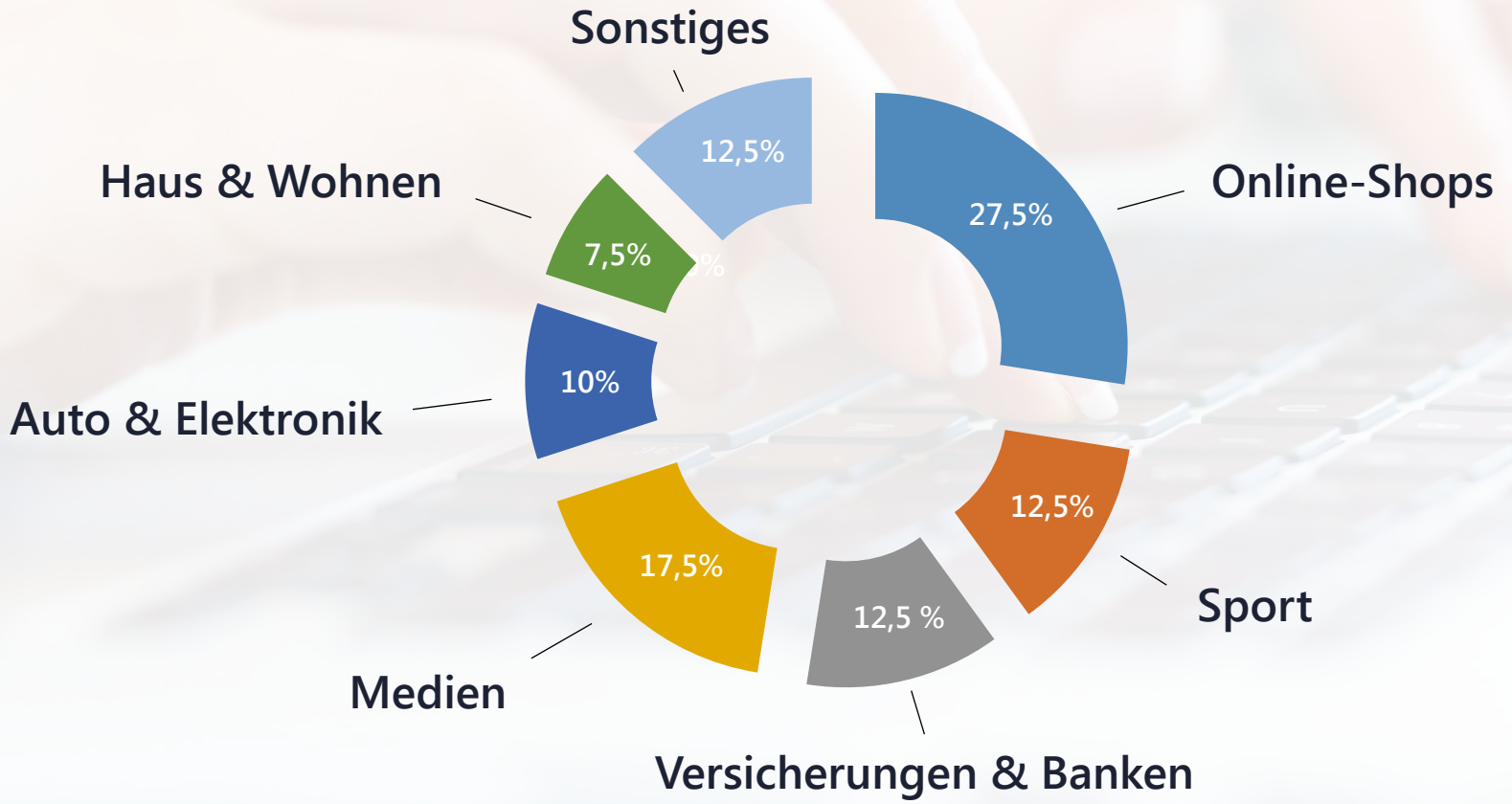
Ob ein Dienst den Schutz der Daten des Nutzers wirklich ernst nimmt oder eher nicht, kann man auch daran erkennen, welche Hilfestellung dem Nutzer bei Sicherheitsnotfällen aktiv auf der Website mit an die Hand gegeben werden.

Sicher im Internet -

2 Datenschutzcheck „Tracking“

Untersuchung von **40** ausgewählten bayerischen Websites hinsichtlich datenschutzkonformer Einbindung von Tracking-Tools (u. a. Information und Einwilligung)

Welche Kategorien von Websites wurden untersucht?



2 Tracking

Tracking-Tools auf Websites

Sind auf der Website Tracking-Tools eingebunden, die umfangreiche Profile der Nutzer anlegen?

Von 40 geprüften Websites

binden 40 Websites Tracking-Tools ein

Bewertung des Ergebnisses

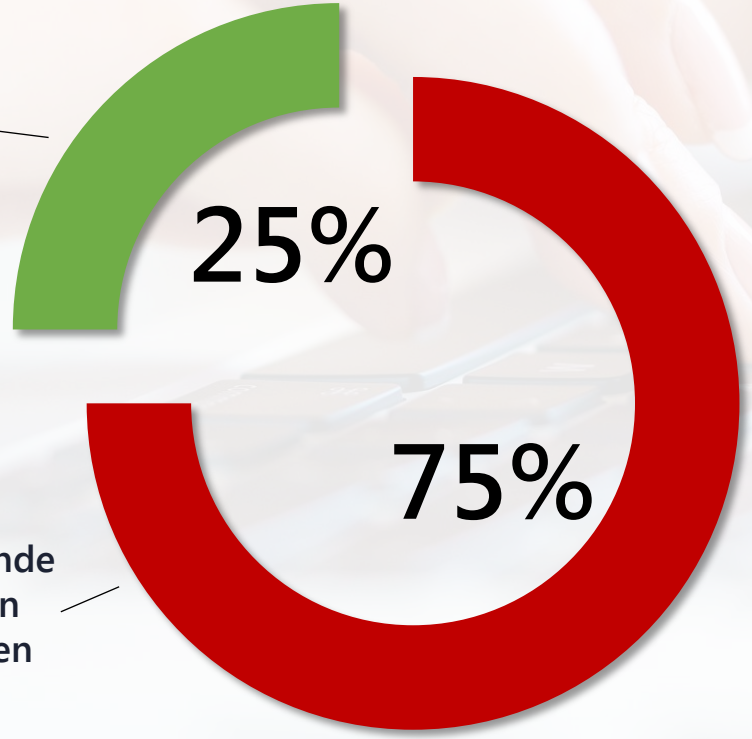
Alle geprüften Websites binden Tracking-Tools von Drittanbietern ein und veranlassen somit eine Datenverarbeitung durch fremde Dienste. Besucht ein Nutzer die Website, so werden automatisch Daten des Nutzers im Hintergrund an Drittanbieter gesendet, ohne dass es der Nutzer erfährt.

Hintergrund

Tracking-Tools werden auf Websites zu unterschiedlichen Zwecken, z. B. zur Werbefinanzierung, Optimierung der Inhalte oder aus Sicherheitsgründen eingebunden. Häufig werden umfangreiche Profile des Nutzers erstellt. Zusätzlich werden den Nutzungsprofilen oftmals auch Merkmale und Interessen zugeordnet, die auf dem Surfverhalten des Nutzers beruhen – z. B. Rückschlüsse auf politische Einstellung, Gesundheit oder sexuelle Präferenz.

Transparenz

Wird der Nutzer transparent über den Einsatz von Tracking-Tools informiert?



Bewertung des Ergebnisses

Nur wenige Datenschutzbestimmungen erfüllen die Anforderungen zur Transparenz. Viele Website-Betreiber verschweigen den Einsatz von Tracking-Tools; andere hingegen informieren pauschal über verschiedenste Tools, die zum Teil gar nicht auf der Website eingebunden sind. Im Ergebnis wird der Nutzer nur selten transparent darüber informiert, ob und welche seiner Daten für welche Zwecke verarbeitet werden.

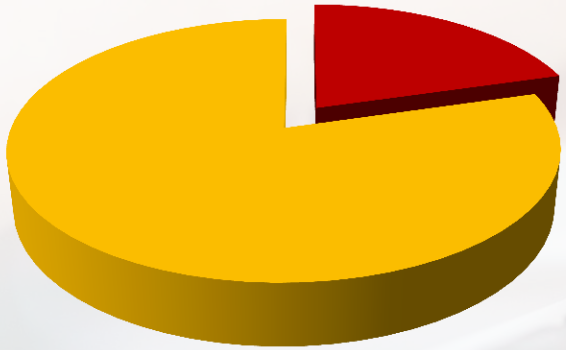
Hintergrund

Die DS-GVO verpflichtet die Website-Betreiber, den Nutzer in einfacher und verständlicher Sprache über die Daten-verarbeitung zu informieren. Hierzu gehört es auch, alle Inhalte von Drittanbietern und eingebundene Tracking-Tools zu benennen. Außerdem muss der Nutzer darüber informiert werden, welche Daten von ihm erhoben werden, für welche Zwecke dies erfolgt und wie lang diese Daten gespeichert werden.

2 Tracking

Einwilligung

Wie viele Websites fragen nach der Einwilligung des Nutzers über einen „Cookie-Banner“?



20% Holen keine Einwilligung des Nutzers ein

80% Holen eine Einwilligung ein, die jedoch nicht datenschutzkonform ist

Bewertung des Ergebnisses

Von den geprüften Websites setzen 30 sog. „Cookie-Banner“ ein. Über den Cookie-Banner soll der Nutzer eine Einwilligung für die Verarbeitung seiner Daten abgeben. Die Prüfung ergab, dass alle Einwilligungen, die über Cookie-Banner eingeholt wurden, unwirksam sind.

Hintergrund

Website-Betreiber, die Cookie-Banner einsetzen, gehen davon aus, dass sie für eine rechtmäßige Datenverarbeitung eine Einwilligung des Nutzer benötigen. Das stellen die Website-Betreiber auch in der Datenschutzbestimmung klar. Ist die Einwilligung unwirksam, ist unter Umständen der Einsatz von Tracking-Tools rechtswidrig.

2 Tracking

Einwilligung

Werden die Anforderungen an eine wirksame Einwilligung von den Websites erfüllt?

0 von 40 haben alle Anforderungen erfüllt

Keine der Einwilligungen ist wirksam

Bewertung des Ergebnisses

Keine der eingeholten Einwilligungen ist wirksam. Das beutet im Ergebnis, dass die Datenverarbeitung durch einwilligungsbedürftige Tracking-Tools rechtswidrig ist.

Hintergrund

Eine Einwilligung ist nur wirksam, wenn sie vorab erteilt wird, d. h. wenn alle Tracking-Skripte blockiert sind, solange bis der Nutzer aktiv zugestimmt hat. Außerdem muss die Einwilligung freiwillig sein und der Nutzer vorab über die Datenverarbeitung informiert werden. Ist auch nur eine dieser Voraussetzungen nicht berücksichtigt, so ist die Einwilligung rechtswidrig.

2 Tracking

Keine Datenverarbeitung durch Tracking-Tools

Kann der Nutzer die Profilbildung durch Tracking-Tools auf der Website selbst durch eigene Einstellungen im Browser verhindern?

Lediglich auf

1 Website

kann der Nutzer eine Profilbildung selbst verhindern

Bewertung des Ergebnisses

Nur auf einer Website hat der Nutzer beim Aufruf der Website eine echte Wahl und kann festlegen, ob seine Daten von Tracking-Tools verarbeitet werden oder nicht. Auf allen anderen geprüften Websites findet ein Tracking statt, bevor der Nutzer überhaupt entscheiden kann, ob er diese Datenverarbeitung zulässt oder nicht. Selbst die Browser-Einstellung „do not track" wurde nur von einem Website-Betreiber beachtet.

Hintergrund

Unabhängig davon, ob eine Einwilligung eingeholt wird oder nicht, wird der Nutzer beim Aufruf der Website getrackt. Nur eine Website akzeptierte die Einstellung „do not track" und blockierte die Ausführung von Tracking-Skripten. Bei allen anderen Websites hat der Nutzer keine Möglichkeit beim Aufruf der Website das Tracking zu verhindern.

Fragen oder Anmerkungen?

presse@lda.bayern.de

Bayerisches Landesamt für Datenschutzaufsicht
Promenade 27 (Schloss)
91522 Ansbach

Telefon: 0981 53 1473

Das Bayerische Landesamt für Datenschutzaufsicht mit Dienstsitz Ansbach überwacht die Einhaltung des Datenschutzrechts im nicht-öffentlichen Bereich in ganz Bayern, das heißt in den privaten Wirtschaftsunternehmen, bei den freiberuflich Tätigen, in Vereinen und Verbänden sowie im Internet.