Interdisziplinäres Bewertungskonzept für Risiken auf Webseiten

Steffen Bartsch, Carina Boos, Gamze Canova, Dominic Dyck,
Birgit Henhapl, Michael Schultheis, Melanie Volkamer

Universität Kassel/provet
Pfannkuchstr. 1, 34109 Kassel
Carina.Boos@uni-kassel.de

usd AG
Robert-Bosch-Straße 25 a, 63225 Langen
Birgit.Henhapl@usd.de

TU Darmstadt/CASED
Hochschulstraße 10, 64289 Darmstadt
Steffen.Bartsch@cased.de, Gamze.Canova@cased.de, D.Dyck@iad.tu-darmstadt.de,
Schultheis@iad.tu-darmstadt.de, Melanie.Volkamer@cased.de

Abstract: Dieser Beitrag beschreibt ein Konzept zur Verbesserung der Sicherheit von Nutzern im Internet: Angepasst auf die jeweilige IT-Sicherheitsexpertise sowie seiner Bereitschaft, Risiken einzugehen, werden dem Nutzer in risikoreichen Situationen unterschiedliche Interventionen geboten. Die Entscheidung, ob und welches Risiko existiert, wird auf rechtlicher und technischer Ebene getroffen: Indikatoren, ob Daten- und Verbraucherschutz eingehalten werden sowie ob grundlegende Maßnahmen der IT-Sicherheit umgesetzt sind, werden automatisiert erkannt und ausgewertet. Auf Grundlage der Risikoeinstufung des jeweiligen Szenarios sowie des antizipierten Risikoverhaltens und der IT-Sicherheitsexpertise des Nutzers wird über die Art der Intervention entschieden: Zusätzlich zu Warnmeldungen, die den Nutzer im Surfverhalten unterbrechen, existieren passive Interventionen, die den Nutzer nicht in seiner Handlung behindern, sowie eine permanente Anzeige über den Sicherheitsstatus einer Seite.

1 Einleitung

Der Einzug des Internets in den Alltag von immer mehr Menschen auch im Privatleben führt neben den großen Chancen für Verbraucher und Anbieter von Waren und Dienstleistungen auch seine Schattenseiten mit. Es entstehen nicht unerhebliche Risiken im Zusammenhang mit der IT-Sicherheit sowie dem Daten- und Verbraucherschutz: Beispiele sind das Ausspähen und Abgreifen von personenbezogenen Daten inklusive der Zugangs- und Kreditkartendaten sowie deren Missbrauch. Ebenso werden häufig verbraucherfeindliche oder unzumutbare Bedingungen nicht klar erkennbar in unübersichtlichen Verträgen formuliert oder sogar auf den Internetseiten versteckt.

Die zum Schutz der Nutzer angebotenen Mechanismen (TLS, Web of Trust, Gütesiegel, etc.) sind oft zeitaufwendig und setzen Expertenwissen voraus.

Das in diesem Beitrag vorgestellte Bewertungstool verspricht eine deutliche Verbesserung des Nutzerschutzes im Internet: Während der Aktionen des Nutzers auf einer Webseite (Surfen, Eingeben persönlicher Daten, Internetbanking, etc.) wird die Seite in Echtzeit auf Sicherheitsmängel sowie erkennbare Verstöße gegen und auf besondere Maßnahmen zum Verbraucher- und Datenschutz untersucht. Angepasst auf ein vorher einmalig erstelltes Risiko- und Expertise-Profil des Nutzers wird dieser bei Bedarf gewarnt und mit ihm verständlichen Handlungsempfehlungen oder -optionen dabei unterstützt zu entscheiden, ob er die Seite weiter verwenden oder verlassen möchte.

2 Analyse der Webseite

Das Bewertungstool untersucht die aktuelle Webseite auf bestimmte Indikatoren, die Aufschlüsse über die Einhaltung des Verbraucher- und des Datenschutzes (s. Abschnitt 2.1) sowie grundlegende Sicherheitsmechanismen (s. Abschnitt 2.2) geben. Ein wichtiger Indikator für beide Analysen ist der Webseitentyp (der mittels Machine Learning Ansätzen ermittelt wird [Ka14]). Das Ergebnis beider Untersuchungen wird anschließend zusammengeführt (s. Abschnitt 2.3). Basierend auf dem antizipierten Risiko und angepasst auf den individuellen Nutzer (s. Abschnitt 3) wird diesem eine Intervention (s. Abschnitt 4) angezeigt. **Fehler! Verweisquelle konnte nicht gefunden werden.** illustriert das Bewertungskonzept im Überblick.

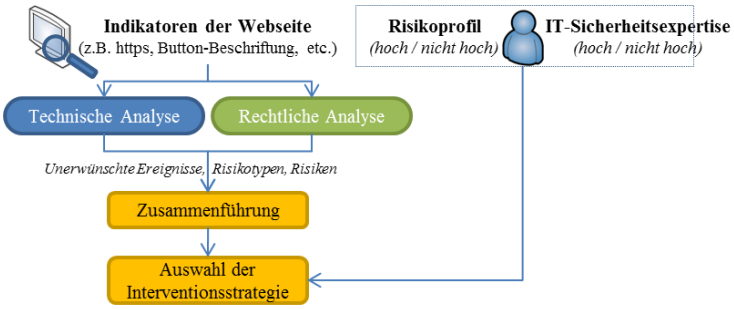


Abbildung 2.1: Bewertungstool im Überblick

2.1 Rechtliche Analyse

Um rechtliche Risiken bei der Nutzung einer Webseite automatisiert einzuschätzen, müssen aus Informationen Rückschlüsse gezogen werden, die automatisiert erhoben werden können. Daher kann und soll nicht die geprüft werden, ob eine Webseite rechtskonform, sondern ob sie vertrauenswürdig ist. Der Nutzer soll darüber informiert werden, ob er dem Anbieter vertrauen kann, nicht dagegen, ob er sein Recht notfalls auch vor Gericht durchsetzen kann.

Es wurde ein Risikomodell entwickelt, das eine Risikoabschätzung für jede Webseite ermöglicht. Dieses basiert auf deutschem Recht und schränkt die Aussagekraft der rechtlichen Risikoanalyse hauptsächlich auf deutsche Webseiten ein. Der Fokus liegt außerdem auf Web-Shops, für die eine Vielzahl einheitlicher Regelungen aus dem Verbraucher- und Datenschutzrecht gelten.

Um ein Schema zur Einschätzung rechtlicher Risiken zu erstellen, wurden nacheinander verschiedene Aspekte zueinander in Beziehung gesetzt: Zum einen wurden Indikatoren bestimmt, die automatisiert von einer Webseite erhoben werden können, um Aussagen über unerwünschte Ereignisse zu treffen, zum anderen abstrakte Risikowerte, die für jede denkbare Webseite eine Risikoabschätzung möglich machen.

Automatisiert auslesbare Indikatoren sind deshalb nötig, weil bei dem hier verfolgten Ansatz kein anbieterseitig eingebundenes System [LBB14] den Verbraucher- und Datenschutz unterstützen, sondern rechtliche Risiken automatisiert eingeschätzt werden. Solche Indikatoren sind bspw. das Vorhandensein, die Position und die Formatierung von Informationen, die rechtlich vorgeschrieben sind. Diese finden sich etwa oft in Datenschutzerklärungen. Aber etwa auch die Allgemeinen Geschäftsbedingungen enthalten automatisiert auslesbare Indikatoren [Bo14].

Anhand dieser Indikatoren können zu vielen unerwünschten Ereignissen bei der Nutzung von Webseiten Aussagen im Bezug auf den Verbraucher- und Datenschutz getroffen werden. Die unerwünschten Ereignisse ergeben sich aus den Gesetzesbegründungen, Rechtsprechung und Literatur. So sollen Verbraucher z. B. in einem Web-Shop davor geschützt werden, aus Versehen einen Vertrag abzuschließen („Abgabe einer übereilten Willenserklärung“). Verschiedene Normen versuchen diese unerwünschten Ereignisse zu verhindern.

Das Abschätzen der Wahrscheinlichkeiten von unerwünschten Ereignissen ist nur auf einem abstrakten Level möglich und muss Einzelfälle außer Acht lassen. Jedem unerwünschten Ereignis wurden deshalb im ersten Schritt alle Normen untergeordnet, die den Eintritt des Ereignisses verhindern sollen. Die Normen sind zueinander danach gewichtet, wie sehr sie vor dem unerwünschten Ereignis schützen.

In einem zweiten Schritt wurden jeder Norm automatisiert auslesbare Indikatoren zugeordnet, die Aufschluss darüber geben, ob die Normen eingehalten werden. Zu den einzelnen Indikatoren wird entsprechend ihrer Bedeutung für die jeweilige Norm wiederum eine Gewichtung, im Folgenden Indikatorwert genannt, festgelegt. Ein Beispiel: Verschiedene Normen – vor allem Informationspflichten – sollen davor schützen, dass ein Nutzer aus Versehen einen Vertrag abschließt. Besonders wichtig ist dabei die sogenannte Button-Lösung[1]: Um auf der Webseite eines Unternehmers einen Vertrag abzuschließen, durch den ein Verbraucher zur Zahlung verpflichtet wird, muss dies auf dem Button deutlich erkennbar werden, z.B. durch „jetzt kaufen“. Ob diese rechtliche Anforderung eingehalten wurde, kann aufgrund der strengen Vorgaben der Vorschrift weitgehend anhand der Beschriftung, der Formatierung und der Position des Buttons erkannt werden

[1] § 312g Abs. 3 BGB, ab dem 13.6.2014 § 312j Abs. 3 BGB n. F.

[BBV14]. Die Beschriftung ist hierbei am wichtigsten und erhält daher die höchste Gewichtung, d.h. den höchsten Indikatorwert.

Für jede Webseite kann anhand der Gewichtung der jeweiligen Norm sowie der Indikatorwerte die Wahrscheinlichkeit für jedes unerwünschte Ereignis eingeschätzt werden: Dazu werden die sich aus der Webseite ergebenden Indikatorwerte pro relevanter Norm addiert und mit der jeweiligen Normgewichtung multipliziert. Die gewichteten Gesamtwerte ergeben addiert das Risiko für das jeweilige unerwünschte Ereignis.

Als Ergebnis der Berechnung wird für eine konkrete Webseite die Liste der unerwünschten Ereignisse jeweils einem bestimmten quantitativen (z.B. „85 von 100 Punkten“) und qualitativen Wert („hohes Risiko“) zugeordnet.

2.2 Technische Analyse

Die technische Analyse basiert auf den Konzepten der qualitativen Risikoanalyse nach ISO 27005
ISO 27005 [DIVSI12] Deutsches Institut für Vertrauen und Sicherheit im Internet. (2012). DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet. DIVSI.
[II08] und NIST 800-30 [SGF02] und besteht aus den zwei Komponenten, Risikomodell und Risikoabschätzung. Das Modell setzt sich wie folgt zusammen:

Ein Bedrohungsgraph stellt die Zusammenhänge zwischen Nutzeraktionen, technischen Bedrohungen und den daraus resultierenden unerwünschten Ereignissen dar. Zum Beispiel kann das „Senden von persönlichen Daten“ zu den Bedrohungen „Abhören“ und/oder „Phishing“ führen. Dies ermöglicht wiederum „Unautorisiertes Erfassen von Daten“. Dadurch ergeben sich die unerwünschten Ereignisse wie „Unautorisierte Zahlung“, „Unautorisierte Überweisung“ oder „Spam“, welche für den Benutzer von Bedeutung sind.

Aus dem Bedrohungsgraphen lässt sich in Form von Angriffspfaden ableiten, wie bestimmte unerwünschte Ereignisse eintreten können. Von einem unerwünschten Ereignis rückwärts gehend, kommt man zu verschiedenen Schwachstellen. Verschiedene Angriffspfade können daher zu denselben unerwünschten Ereignissen führen. Da sich die Wahrscheinlichkeit des Eintretens einer Bedrohung allerdings je nach Angriffspfad stark unterscheiden kann, werden diese durch sogenannte *Szenarien* unterschieden und die Wahrscheinlichkeiten für alle Angriffspfade getrennt ermittelt.

Im Beispiel von Abbildung 2.2 auf Seite 5 kann sowohl „Abhören“ als auch „Phishing“ zu den unerwünschten Ereignissen „Unautorisierte Zahlung“ und „Unautorisierte Überweisung“ führen. Während beim „Abhören“ das Szenario „Ungeschütztes Senden von Login-Daten“ schon ausreicht, eines der beiden unerwünschten Ereignisse hervorzurufen, ist beim „Phishing“ das „Ungeschützte Senden von Login-Daten an eine nicht vertrauensvolle Webseite“ erforderlich.

In der Risikoabschätzung folgt die Anwendung des Risikomodells auf eine konkrete Situation in Abhängigkeit von Indikatoren. Das Ergebnis liefert eine Liste von unerwünschten Ereignissen mit entsprechenden Risikowerten für die jeweilige Situation.

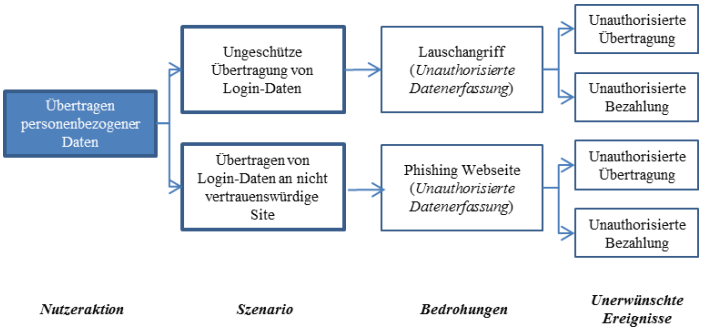


Abbildung 2.2: Beispiel eines Bedrohunggraphs

Zur Abschätzung des Risikos, oder zumindest der Wahrscheinlichkeit, einer bestimmten Situation, beschrieben über Indikatoren, werden Entscheidungsbäume aufgebaut. Die Entscheidungsknoten eines solchen Baumes stellen die Indikatoren dar, ausgehende Kanten jeweils mögliche Zustände der Indikatoren. Die Ergebnisse repräsentieren die Eintrittswahrscheinlichkeiten und je nach Ereignis auch eine zu erwartende Schadenshöhe.

In Abbildung 2.3 auf Seite 5 ist ein Entscheidungsbaum für die Eintrittswahrscheinlichkeit des unerwünschten Ereignisses „Unautorisierte Überweisung“ im Szenario „Ungeschütztes Senden von Login-Daten“ dargestellt.

Jedes Szenario und unerwünschte Ereignis muss einzeln betrachtet werden, da sich die Eintrittswahrscheinlichkeiten unterscheiden. Zusätzlich werden je Szenario die Wahrscheinlichkeiten der jeweiligen Aktion, die zu dem unerwünschten Ereignis führen, ebenfalls über einen Entscheidungsbaum bestimmt. Ist bspw. ein Passwort-Feld angeklickt, so ist die Aktionswahrscheinlichkeit, dass ein Passwort eingegeben wird „hoch“.

Das Risikomodell wird auf die jeweilige Situation angewendet, um das Risiko abzuschätzen. Für jedes einzelne Szenario werden Listen mit unerwünschten Ereignissen und deren Risikoabschätzung bestimmt.

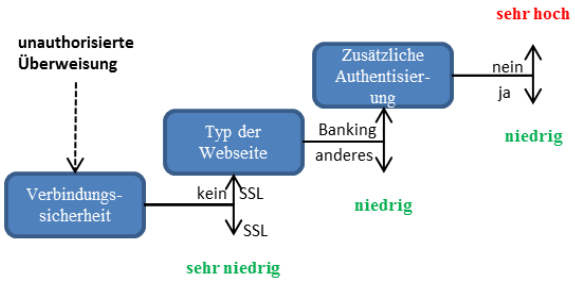


Abbildung 2.3: Beispiel eines Entscheidungsbaums (Ausschnitt)

Die Risikoabschätzung je Situation wird einmalig im Vorfeld in Anlehnung an die Prozess-FMEA [TC02] nach folgender Regel erstellt:

$Risiko_{Ereignis}$ = $Wahrscheinlichkeit_{Ereignis}$ * $Wahrscheinlichkeit_{Aktion}$ * $Schadenshöhe_{Ereignis}$

Dabei werden die Wahrscheinlichkeiten sowie die antizipierten Schadenshöhen den jeweiligen Entscheidungsbäumen entnommen. Ergebnis ist eine Tabelle, der man je Situation und Aktion das antizipierte Risiko entnehmen kann.

Bei der Risikobewertung sind Fehleinschätzungen nicht auszuschließen. Eine vertrauenswürdige Webseite könnte vom Bewertungstool bspw. als nicht vertrauenswürdig eingestuft werden. Zudem ist es nicht möglich alle Risiken automatisiert zu messen. Negative Nutzerbewertungen über die betroffene Webseite auf einer anderen Webseite werden nicht in die Risikomessung einbezogen. Weitere nicht voll-automatisch und mit 100% iger Genauigkeit messbare Risikofaktoren sind z.B. Phishing oder Cross-Site-Scripting.

2.3 Zusammenführung der Risiken

Nachdem die rechtlichen und technischen Risiken abgeschätzt wurden, müssen die Ergebnisse zusammengeführt werden. Hierzu werden die beiden entstandenen Tabellen zu einer zusammengeführt. Hierbei ist es möglich, dass es zu doppelten Einträgen kommt, d.h. es gibt dasselbe unerwünschte Ereignis im technischen und im rechtlichen Bereich. In diesem Fall wird der Eintrag mit dem höheren Risikowert übernommen und der andere Eintrag wird entfernt.

Szenario	**unerwünschtes Ereignis**	**Risiko**
ungeschützte Übertragung von Login-Daten auf Banking-Seite	unautorisierte Bezahlung	sehr hoch
Übertragung von Login-Daten auf Phishing-Seite	unautorisierte Bezahlung	sehr hoch
Aufrufen einer Seite mit Drittanbietercookies	unerwünschte Profilbildung	mittel

Tabelle 1: Auszug der resultierenden Risikotabelle

3 Individualisierung auf den Nutzer

Um die Unterstützung der Nutzer auf ihr jeweiliges Verhalten im Internet sowie auf ihre IT-Sicherheitsexpertise abzustimmen, wird direkt während der Installation des Bewertungstools ein Risikoprofil des Nutzers erstellt sowie seine IT-Sicherheitsexpertise festgestellt.

3.1 Risikoprofil

Das Risikoprofil erfasst für den individuellen Nutzer die Wahrscheinlichkeit, dass sich diese Person risikoreich verhält. Risikoreiches Verhalten wurde indirekt per Fragebogen gemessen. Die abgefragten Szenarien stammten aus der DOSPERT-G (Johnson et al., 2004) und erfassten jeweils Wahrscheinlichkeit, Risikograd und Nutzen des potenziell risikoreichen Verhaltens. Die u.g. Items zur persönlichen Einstellung entstammen dem Bericht des Deutschen Instituts für Vertrauen und Sicherheit im Internet [DIVSI12] und wurden vom dort verwendeten Interview auf ein Fragebogendesign angepasst. Aufgrund einer Vorerhebung mit insgesamt 386 Probanden fließen folgende Merkmale ein, die mittels linearer Regression als signifikante Prädiktoren ermittelt wurden:

- Alter (16-100)
- Geschlecht (dichotom)
- Internet-Nutzungshäufigkeit (4-fach gestuft zw. „täglich“ und „seltener als monatlich“)
- Internet-Nutzungsdauer (4-fach gestuft zw. „bis zu 3 Jahren“ und „seit über 10 Jahren“)
- Besitz internetfähiger Geräte (0-5)
- Persönliche Einstellung zum Datenschutz (3 Fragen, 5-stufig Likert-skaliert von „stimme garnicht zu“ bis „stimme vollkommen zu“):
    - *„Wir müssen uns an einen freieren Umgang mit Daten im Internet gewöhnen.“*
    - *„Mir persönlich ist es egal, was mit meinen Daten im Internet geschieht.“*
    - *„Neue Angebote und Entwicklungen im Bereich Internet probiere ich immer sofort aus.“*

Die jeweiligen Werte der Nutzer werden in die Regressionsgleichung eingesetzt und diese basierend darauf entweder in die Risikogruppe „hoch“ oder „nicht hoch“ eingeteilt. Die Einteilung in 2 Klassen erfolgte aufgrund projektinterner Überlegungen. Für eine weitere Verwendung kommt aber auch eine Einteilung in mehr Klassen, sowie eine gewichtete Verwertung anhand der Regressionsdaten in Frage. Anhand des Risikoprofils kann prognostiziert werden, ob sich eine Person potenziell eher risikoreich verhält. Es erfasst aber nicht, warum eine Person ein Risiko eingeht und ob sie sich dessen bewusst ist. Dazu wird die IT-Sicherheitsexpertise herangezogen.

3.2 IT-Sicherheitsexpertise

Die IT-Sicherheitsexpertise wird anhand eines weiteren Fragebogens erfasst, der u.a. folgende Fragen beinhaltet:

- Was ist die beste Definition für Cookie?
- Stellen Sie sich eine Internetseite vor, welche normalerweise nur von Ihnen und Ihren Freunden genutzt wird, aber grundsätzlich öffentlich zugänglich ist (z.B. ein Forum mit Fußballfreunden). Welche Gefahren ergeben sich, wenn Ihre E-Mail-Adresse zusammen mit Ihrem Namen auf dieser Seite im Internet veröffentlicht wird?

Die Antwortmöglichkeiten sind jeweils im Multiple-Choice-Format. Basierend auf den Antworten wird die IT-Sicherheitsexpertise des Nutzers bestimmt. Der Nutzer wird aufgrund dieses Wertes in die Gruppe „hoch“ oder „nicht hoch“ eingeteilt. Eine höherauflösende Einteilung wurde aus Aufwandsgründen vorerst abgelehnt, um die zweistufige Lösung evaluieren zu können.

4 Interventionsstrategien

Aufgrund der berechneten Werte (Gesamtrisiko, Risikoprofil, IT-Expertise) wird die Intervention angepasst an den einzelnen Nutzer selektiert.

4.1 Interventionsarten

Ziel ist es, Nutzer effektiv und gleichzeitig verständlich zu warnen. Dies wird mit einem Konzept aus aktiven und passiven Warnungen plus einer permanenten Statusanzeige für Risiken auf der momentan besuchten Seite verfolgt. *Aktive Warnungen* stoppen den Benutzer in seinem Surfverhalten. Er kann erst nach einem Klickdialog fortfahren. *Passive Warnungen* informieren dagegen den Nutzer über ein etwaiges Risiko (z.B. durch ein im unteren Bildschirmbereich erscheinendes Warnfenster), ohne ihn in seinem Surfverhalten zu stören. Die *permanente Statusanzeige* soll dauerhaft sichtbar sein und einen generellen Zustand der besuchten Seite mithilfe eines Icons (z.B. einer Ampel) darstellen, selbst wenn kein Anlass zu einer höherrangigen Intervention technischer oder rechtlicher Ebene besteht. Dieses Icon ist ortsfest und dient dem Nutzer als Möglichkeit ein schnelles Feedback über den Status der Seite zu erlangen.

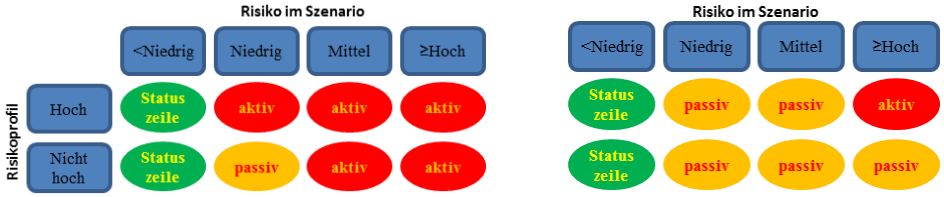
Besonderes Augenmerk wird auf die Verständlichkeit der Nutzerhinweise gelegt. Der Nutzer wird nicht, wie bisher üblich, mit einem für ihn oft unverständlichen Hinweis auf die technischen Mängel (z.B. ungültiges Zertifikat) alleine gelassen. Er bekommt konkrete, von seiner Expertise abhängig formulierte Informationen über die Bedrohung(en), deren mögliche Konsequenzen und Empfehlungen zur weiteren Vorgehensweise. So wird bei Nicht-hoher Expertise z.B. bei Auffinden von Tracking-Cookies in der Warnmeldung darauf hingewiesen, dass auf dieser Site das Nutzerverhalten verfolgt wird. Bei

Nicht-hoher Expertise findet immer ein Trade-off zwischen Verständlichkeit und Informationsgehalt statt, die exakte Information (d.h. die, die auch der Nutzer mit hoher Expertise erhalten würde) ist aber jederzeit umschaltbar.

4.2 Entscheidungsalgorithmus zur Intervention

Die jeweilige Entscheidung zu den Interventionsarten *Statuszeile*, *passive Intervention* und *aktive Intervention* wird in der Abbildung 4.1 auf Seite 9 für Nutzer mit nicht hoher und in **Fehler! Verweisquelle konnte nicht gefunden werden.** für Nutzer mit hoher IT-Sicherheitsexpertise dargestellt.

Ein Nutzer mit nicht hoher Expertise und hohem Wert im Risikoprofil erhält derzeit bei Benutzung des Tools selbst bei niedrigem Risiko aktive Warnungen. Nutzer mit hoher IT-Sicherheitsexpertise werden dagegen nur selten aktiv gewarnt und so seltener unnötig „behelligt“. Es ist jedoch in Planung diesen Algorithmus in Benutzerstudien noch weiter zu erproben und die gewonnenen Einsichten in den Algorithmus zu integrieren sowie die Ergebnisse zu publizieren.



a) bei nicht hoher IT-Sicherheitsexpertise *b) bei hoher IT-Sicherheitsexpertise*

Abbildung 4.1: Interventionswahl

Die Grenze, wann ein Nutzer eine aktive oder passive Warnung erhält, kann sich, abhängig von der auftretenden Dichte der Warnungen im Feldversuch, noch verschieben. Ebenfalls in Iteration befindet sich eine Variante des Algorithmus, bei der die Anzahl der Risiken, die selbst eine Intervention hervorrufen würden, in den Inhalt der gezeigten Intervention einfließt, sodass eine Website, die z.B. 5 niedrige und ein mittleres Risiko hat, einen höheren Risikowert erhält, als eine Seite mit nur einem mittlerem Risiko.

5 Anwendungsfallbeispiele

Im Folgenden werden zwei Fallbeispiele zur Verdeutlichung der Entstehung der verschiedenen Warnungen gegeben.

5.1 Aufrufen eines Webshops oder eines Forums ohne HTTPS

Situation: Ein Verbraucher klickt auf einen Link zu einem Webshop oder Forum

Bedrohungshintergrund: Technisches Problem mit der Verbindungsverschlüsselung, z.B. die Webseite verwendet kein HTTPS

Unerwünschtes Ereignis: Abhören des Passwortes (im Fall eines Logins), daraus resultierend: Bestellung (Webshop) bzw. Beiträge (Forum) im Namen des Verbrauchers

Indikatoren: Verbindungssicherheit: *kein HTTPS*, Typ der Webseite: *Webshop/Forum*

Resultierendes Risiko: Medium

Nutzer: hohes Risikoprofil, hohe IT-Sicherheitsexpertise

Resultierende Warnung: passiv (siehe Abbildung 5.1)

Abbildung 5.1: Anwendungsfall 1, Nutzer: hohe Expertise, hohes Risikoprofil

5.2 Aufrufen einer Seite mit Drittanbietercookies

Situation: Ein Verbraucher gibt eine URL zu einem Webshop ein. Der Benutzer führt auf der Webseite weitere Aktionen aus (bspw. Klicks)

Bedrohungshintergrund: Verwendung von Drittanbieter-Cookies mit langer Speicherzeit ohne den Verbraucher zu informieren

Unerwünschtes Ereignis: Profilbildung

Indikatoren: Typ der Webseite: *Webshop*, Web-of-Trust Bewertung: *negativ (Datenschutz)*, Drittanbieter-Cookies: *vorhanden (Speicherzeit: 5 Jahre)*, Datenschutzerklärung: *vorhanden (Hinweis auf eigene Cookies, aber nicht auf die von Drittanbieter)*

Resultierendes Risiko: Mittel

Nutzer: nicht hohes Risikoprofil, nicht hohe IT-Sicherheitsexpertise

Resultierende Warnung: aktiv (siehe Abbildung 5.2 unten)

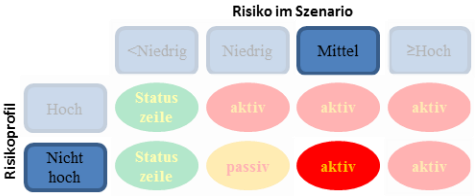


Abbildung 5.2: Anwendungsfall 2, Nutzer: nicht hohe Expertise, nicht hohes Risikoprofil

6 Fazit und Ausblick

Das vorgestellte Bewertungstool[2] basiert zunächst auf einer Einschätzung des tatsächlichen Risikos für unerwünschte Ereignisse aus dem Bereich der IT-Sicherheit sowie des Verbraucher- und Datenschutzes auf einer bestimmten Webseite. Zusätzlich wird die Interventionsart an den einzelnen Nutzer angepasst, indem diese von seinem antizipierten Verhalten in risikoreichen Situationen (Risikoprofil) und seinem Verständnis von Risiken (IT-Sicherheitsexpertise) abhängig gemacht wird. Er wird genau soweit unterstützt, wie er es aufgrund seines Risikoprofils, seiner Einstellung zu Gefahren sowie seiner Expertise benötigt. Das hinlänglich bekannte „genervte Wegklicken“ von Sicherheitshinweisen, die zu häufig oder zu unverständlich sind, soll so vermieden werden.

Die interdisziplinäre Webseitenanalyse bezüglich IT-Sicherheit sowie Verbraucher- und Datenschutz (beschränkt auf den deutschen Raum) erweitert die bisherigen Angebote zur Nutzerunterstützung: Durch die Disziplinen übergreifend gleichförmige Bewertung sind die Ergebnisse der technischen und rechtlichen Analyse vergleichbar und der Nutzer wird über die technischen Problematiken hinaus auch im Daten- und Verbraucherschutz unterstützt. Da sowohl der rechtliche als auch technische Algorithmus auf Annahmen und Wahrscheinlichkeiten basiert, kann nicht sichergestellt werden, dass die Ergebnisse in jedem Einzelfall korrekt sind. Im weiteren Verlauf sind deshalb haftungsrechtliche Fragen und Möglichkeiten von Haftungsausschlüssen zu untersuchen.

Das Bewertungstool befindet sich derzeit sowohl in der Entwicklungs- als auch in der Evaluationsphase. Das Feedback von vielen Nutzern wird sicherlich sowohl weitere Verbesserungen in den Nutzerhinweisen als auch in den Einstufungen der Interventionskategorie bringen.

Weitere, hier nicht beschriebene, Arbeiten können auf der Projektseite www.secuso.informatik.tu-darmstadt.de/de/research/projects/projekt-inuse/[3] nachgelesen werden.

[2] Das Bewertungstool kann auch auf einem abgesicherten Medium installiert werden. Dies wurde bereits in Zusammenarbeit mit der Firma KOBIL Systems GmbH prototypisch entwickelt. In diesem Paper steht das Bewertungstool im Vordergrund.
[3] Zugriffsdatum: 17.06.2014

7 Acknowledgement

Der Beitrag entstand im Rahmen des Forschungsprojekts „Benutzerunterstützung zur Bewertung der Vertrauenswürdigkeit von Webseiten und Webshops (Internet Usage Support: InUse)“. Die Förderung des Vorhabens erfolgt aus Mitteln des BMEL auf Grund eines Beschlusses des Deutschen Bundestags. Die Projektträgerschaft erfolgt über die Bundesanstalt für Landwirtschaft und Ernährung (BLE).

8 Literaturverzeichnis

[BBV14] Boos, C.; Bartsch, S.; Volkamer, M.: Rechtliche und technische Nutzerunterstützung bei der Button-Lösung – Ein Lösungsvorschlag zur Erkennbarkeit von Kostenfallen als dem immer noch ungelösten Kernproblem. In: Computer und Recht (2014), S. 119-127

[Bo14] Boos, C., Nutzerunterstützung durch automatisierte Auswertung einzelner standardisierter Vertragsbedingungen, AGB: Was habe ich verpasst?. In: Verbraucher und Recht (2014), S. 47-52

[DIVSI12] Deutsches Institut für Vertrauen und Sicherheit im Internet. (2012). DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet. DIVSI.

[II08] ISO/IEC 27005:2008: Information Technology – Security techniques – Information security risk management. ISO, Geneva, Switzerland (2008)

[Ka14] Karpf, A.-C.: Web Genre Classification for Context-Specific Security Warnings. Technische Universität Darmstadt, Master Thesis in Informatik (2014)

[LBB14] Luhn, S.; Bruns, I.; Böhme, R., Consumer Participation in Online Contracts, Exploring Cross-Out Clauses, Proceedings GI-SICHERHEIT (2014), S. 255-266

[SGF02] Stoneburger, G.; Goguen, A.; Feringa, A.: Risk Management Guide for Information Technology Systems – NIST Special Publication 800-30. Tech. Rep., National Institute of Standards and Technology (2002)

[TC02] Theden, P; Colsman, H.: Fehlermöglichkeits- und -einflussanalyse (FMEA). In: Qualitätstechniken. Werkzeuge zur Problemlösung und ständigen Verbesserung (Pocket Power). 3. Auflage, Hanser 2002. S. 78-89.

[WBB02] Weber, E. U., Blais, A. R., & Betz, N. E. (2002). A domain-specific risk-attitude scale: Measuring risk perceptions and risk behaviors. Journal of behavioral decision making, *15*(4), 263–290.