Eine Klassifikation sicherheitskritischer UX-Design-Patterns

Laura Buhleier
Sebastian Linsner
Enno Steinbrink
Christian Reuter
reuter@peasec.tu-darmstadt.de
Technische Universität Darmstadt, Wissenschaft und Technik für Frieden und Sicherheit (PEASEC)
Darmstadt, Hessen, Germany

ZUSAMMENFASSUNG

User Experience ist von zunehmender Relevanz für die Entwicklung digitaler Designentscheidungen und hat somit weitgehende Auswirkungen auf das Nutzerverhalten. Dass dies besonders für die Sicherheit und Vertraulichkeit nicht nur von Vorteil sein kann, sondern Nutzer*innen negativ beeinflussen kann, wird in dieser Arbeit ersichtlich. Betrachtet werden dafür die Themengebiete Anti-Patterns, Grey Patterns und Dark-Patterns. Anti-Patterns bezeichnen wiederkehrende Lösungen für ein Konzept eines User Interfaces, die trotz guter Intention ungewünschte Nebeneffekte oder Konsequenzen haben. Dark-Patterns dagegen stellen Designentscheidungen dar, die durch Täuschung oder Ausnutzung psychischen Drucks versuchen Nutzer*innen zu Handlungen zu verleiten, von denen die Ersteller*innen des Dark-Patterns mehr profitieren als die Anwender*innen. Der Begriff Grey Patterns wird in dieser Arbeit für alle Design Patterns genutzt, die sich nicht direkt zuordnen lassen. Da es bisher kaum vergleichende Werke und keinen Konsens zu diesen Themengebieten gibt, ist das Ziel dieser Arbeit ein grundlegendes Modell aufzustellen. Dabei wird durch die Untersuchung bestehender Literatur eine zusammenfassende Taxonomie und ein Vorgehen zur Unterscheidung von Anti-Patterns und Dark-Patterns erarbeitet, die als Grundlage für weitere Arbeiten und zur Entwicklung von Gegenmaßnahmen genutzt werden können.

KEYWORDS

Dark Patterns, Anti Patterns, Grey Patterns, UX Design

1 EINLEITUNG

Im digitalen Alltag kommen Nutzer*innen immer häufiger mit verhaltensbeeinflussenden Designs in Kontakt. So konnte eine Studie feststellen, dass 95 % der untersuchten Apps eines oder mehrere manipulative Designs, sogenannte Dark-Patterns, enthielten [11]. Gray et al. äußern hier auch Befürchtungen, dass sich Designer*innen für manipulative Designs entscheiden könnten, ob bewusst oder unbewusst [14]. Denn Nebenwirkungen verwendeter Designs können auch ungewollt sein: So haben insbesondere Warnmeldungen häufig eine hohe Ablehnungsrate, die vor allem durch die entsprechende User Experience (UX) beeinflusst werden könnte [2]. Daher ist leicht ersichtlich, dass User Experience das Verhalten der Nutzer*innen negativ beeinflussen kann. Eine Gefahr stellen dabei sowohl sogenannte Anti-Patterns dar, bei denen die Designer*innen unbewusst, meist mangels besseren Wissens, Anwender*innen zu sicherheitsgefährdendem Verhalten verleiten [14], als auch Dark-Patterns, die Nutzer*innen absichtlich zu einem für sie nachteiligen Verhalten animieren [7].

Bisherigen Forschungsarbeiten dieser Thematiken fehlt dabei bis auf weiteres ein Konsens bestehender Anti- und Dark-Patterns und auch auf Methoden zur Unterscheidung wurde bislang bis auf eine Gegenüberstellung der Definitionen nicht eingegangen. Außerdem wurde bisher der Begriff Grey Patterns nur als Konzept genannt und eher synonym mit Anti-Patterns verwendet [28]. Diese Arbeit weist der Bezeichnung einen eindeutigen Kontext zu und nennt dieser Kategorie zugehörige Design Patterns. Auch die genaue Unterscheidung zwischen Dark-, Grey- und Anti-Patterns ist noch nicht auf konkreten Patternkategorien ausgeführt worden. Insbesondere in sicherheitskritischen Anwendungsfällen, das heißt wenn das Sicherheits- oder Vertraulichkeitsverhalten der Nutzenden beeinflusst wird, kommt diesem Thema eine besondere Relevanz zu. Um auf diese Problemstellungen einzugehen, beschäftigt sich diese Arbeit mit den Fragen: *Welche UX-Design-Patterns können sich negativ auf das Sicherheits- und Vertraulichkeitsverhalten der Nutzer*innen auswirken und wie lassen sich diese klassifizieren?* Zur Beantwortung dieser Fragen wurde eine systematische Literaturrecherche durchgeführt, um aktuelle Ergebnisse der Themengebiete einzuholen. Dies geschieht unter anderem in Anlehnung an [5, 19, 22, 25], die ebenfalls bestehende Literatur untersuchen und Modelle aufstellen, allerdings in deutlich kleinerem Rahmen als diese Arbeit es vornimmt und es wird nur ein Teil der hier aufgezählten Patterns betrachtet. Aufbauend auf der Literaturrecherche werden eine zusammenfassende Taxonomie, sowie ein Modell zur Unterscheidung Sicherheitskritischer UX-Design Patterns aufgestellt.

2 METHODIK UND GRUNDLAGEN

Da im Folgenden verschiedene Begrifflichkeiten verwendet werden, um auf die Thematiken Anti- und Dark Patterns einzugehen, seien hier formale Definitionen für diese Bezeichnungen gegeben.

User Experience kann nach der ISO 9241-11 [18] definiert werden als "Wahrnehmungen und Reaktionen von Personen, die sich aus der Nutzung und/oder vorraussichtlicher Nutzung eines Produktes, Systems oder einer Dienstleistung ergeben"(Übers. d. Autor*innen). Nach [38] wurde der Begriff *Design Pattern* zunächst in der Architektur eingeführt und würde von Alexander beschrieben werden

Veröffentlicht durch die Gesellschaft für Informatik e.V.
in K. Marky, U. Grünefeld & T. Kosch (Hrsg.):
Mensch und Computer 2022 – Workshopband, 04.-07. September 2022, Darmstadt

https://doi.org/10.18420/muc2022-mci-ws10-275

als "Problem, das in unserer Umgebung immer wieder auftritt und dann den Kern der Lösung so beschreibt, sodass man diese Lösung millionenfach nutzen kann, ohne es jemals zweimal auf dieselbe Weise zu tun"[38] (Übers. d. Autor*innen).

Für die Literaturrecherche ist diese Arbeit systematisch vorgegangen und orientiert sich dabei an den Empfehlungen aus vom Brocke [36]. Ein derartiger Ansatz wurde aufgrund der Zielsetzung dieser Arbeit ein zusammenfassendes Modell zur Erkennung und Unterscheidung von Anti-, Grey- und Dark-Patterns und zur Beantwortung der Forschungsfrage für notwendig eingeschätzt, da dadurch die Erarbeitung des Forschungsstands und bestehender Ansätze zur Erschließung des Modells umgesetzt werden konnte.

Dafür wurden anfangs für die Einarbeitung in die Thematik neun Arbeiten konsultiert, um die Forschungslücke herauszuarbeiten, und aufbauend auf den Erkenntnissen daraus zur Aufstellung von Suchbegriffen weitere elf Paper herausgesucht. Dadurch konnten für die eigentliche methodische Literaturrecherche für die Zielsetzung dieser Arbeit als unabdingbare Suchbegriffe die Stichwörter „Anti Patterns“ und „Dark Patterns“ identifiziert werden. „Anti Patterns“ wurde erweitert zu „UI Anti Patterns“, da aus der anfänglichen Recherche hervorging, dass der Begriff auch in anderen Disziplinen Verwendung findet. Außerdem zeigte sich der Begriff *Nudging* als relevant: Dieser bezeichnet “alle Maßnahmen, mit denen Entscheidungsarchitekten das Verhalten von Menschen in vorhersagbarer Weise verändern können, ohne irgendwelche Optionen auszuschließen oder wirtschaftliche Anreize stark zu verändern"[33], was sich sowohl auf eine positive Beeinflussung als auch eine böswillige Manipulation beziehen kann [5]. Da dies einen zentralen Punkt für Dark-Patterns darstellt, wurden die Suchbegriffe um den Begriff „Digital Nudging“ erweitert. Des Weiteren wurde vermutet, dass Warnmeldungen häufig Gefahr laufen Anti-Patterns darzustellen, und deshalb auch das Stichwort „Security-Warnings“ in die Recherche einbezogen. Dies wird durch zahlreiche Beispiele der anfänglichen Quellen verdeutlicht, wie bspw. die Vermutung, dass Nutzer*innen ein bestimmtes Entscheidungsmuster entwickeln würden und dadurch auch im Ernstfall weniger Aufmerksamkeit für eine Entscheidung aufbringen würden [4].

Das Vorgehen der systematischen Literaturrecherche ist in Abbildung 1 dargestellt. Die verwendeten Litertaturdatenbanken scholar.google.de, link.springer.com, dl.acm.org, hds.hebis.de/ulbda/EBSCO und dl.gi.de wurden aufgrund der großen Menge an Artikeln, bzw. der thematischen Nähe gewählt. Pro Stichwort und Datenbank wurden jeweils die ersten 30 Ergebnisse nach Relevanz und Erscheinungsdatum sortiert betrachtet. Die Reihenfolge und die Anzahl der ausgewählten Artikel richtete sich nach dem Umfang der Datenbank. Daher wurde aus diesen 60 Suchergebnissen (je 30 nach Relevanz und Erscheinungsdatum) pro Stichwort und Datenbank sechs Ergebnisse im Falle von scholar.google.de, springer.link.de und dl.acm.org, fünf Ergebnisse im Falle von hds.hebis.de/ulbda/EBSCO und zwei Ergebnisse im Falle von dl.gi.de ausgewählt, die nach Titel und Kurzbeschreibung für vielversprechend gehalten wurden. Wo möglich wurden Suchoperatoren verwendet und es wurden Artikel ausgeschlossen, die in einer anderen Sprache als der deutschen oder englischen geschrieben waren oder bereits aufgenommen wurden. Da es hier viele Dopplungen unter den Ergebnissen der Literaturdatenbanken gab konnten nur 99 Werke ausgewählt werden, was aber durch die Hinzunahme der Website von Brignull [6] ausgeglichen

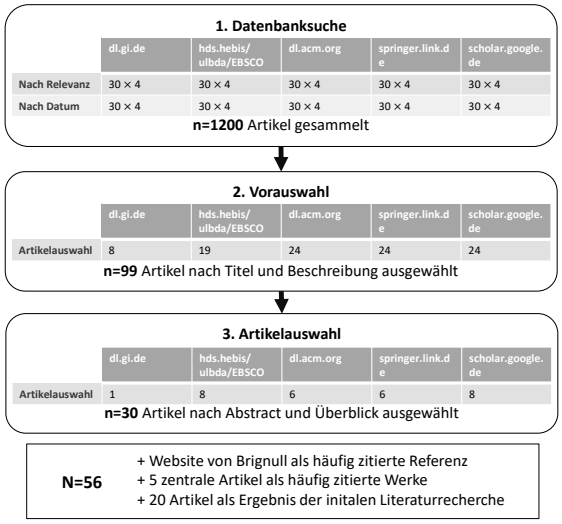

Abbildung 1: Vorgehen der systematischen Literaturrecherche zur Identifikation sicherheitskritischer UX-Patterns

wurde, die in der methodischen Recherche nicht zurückgegeben wurde, aber von vielen Quellen der vorherigen Recherche referenziert wurde. Aus den resultierenden 100 Werken wurden nach kurzer Einsicht in Inhalt, Abstract und Fazit 30 Arbeiten basierend auf der Relevanz für die Forschungsfrage ausgewählt. Fünf weitere zentrale Werke, die aus der Lektüre der Arbeiten hervorgegangen sind wurden anschließend ergänzt. Somit ergibt sich aus den neun Arbeiten der Einarbeitung, den elf Arbeiten der anfänglichen Recherche, den 30 Arbeiten der systematischen Literaturrecherche und den fünf ergänzten Arbeiten ein Literaturkorpus von 55 Werken.

Bei der Recherche wurden auch viele Artikel zurückgegeben, die schon bei der Suche in anderen Datenbanken oder der anfänglichen Recherche aufgenommen wurden, was für eine Angemessenheit des Suchumfangs spricht. Eine Darstellung der Anzahl der in einem Rechercheschritt ausgewählten Ergebnisse geht aus Tabelle 4 im Anhang A hervor.

3 ERGEBNIS

Insgesamt entstand ein Literaturkorpus von 55 Werken, von denen sich fünf mit Anti-Patterns beschäftigen, 17 mit Security-Warnings, 14 mit Dark-Patterns, 15 mit Nudging und vier mit anderen Themen. Diese Artikel wurden zwischen 2007 und 2021 verfasst, davon über die Hälfte in den letzten drei Jahren, was die Aktualität der Thematik unterstreicht. An den Ergebnissen ist ebenfalls ersichtlich, dass der Begriff Anti-Pattern im Gegensatz zu Dark-Pattern in der Disziplin HCI bislang wenig etabliert ist. Auch diesbezüglich trägt diese Arbeit durch die Hervorhebung des Begriffs Anti-Patterns zum Forschungsstand bei. Im Folgenden werden die Begriffe Anti-Patterns und Dark-Patterns zur Abgrenzung auf Basis der Literaturrecherche erläutert. In den Abschnitten danach wird dann die Sammlung bekannter, problematischer UX-Design-Patterns beschrieben sowie das Modell, mit dem diese im Abschnitt 4 klassifiziert wurden.

3.1 Anti-Patterns

Anti-Patterns konnten nach der Zusammenfassung verschiedener Definitionen [5, 10, 12–14, 21, 25, 37] folgendermaßen definiert werden: Ein Anti-Pattern stellt eine Form von Pattern, also eine wiederkehrende Lösung für ein Konzept eines User Interfaces, dar, das trotz guter Intention ungewünschte Konsequenzen oder Nebeneffekte hat. Ein Beispiel hierfür wäre Third Party Authentication, die Nutzer*innen anfälliger für Phishing Attacks machen kann [12]. Hier wird ersichtlich, dass die Nebenwirkungen häufig in Form eines falschen Verständnisses von Sicherheit [12] und Gefühlen von Bedrängung [16], Überforderung [21], Unsicherheit [21] oder Orientierungslosigkeit [21] seitens der Nutzer*innen entstehen. Des Weiteren konnte festgestellt werden, dass es bisher wenig konkrete Ergebnisse zu den Auswirkungen von Anti-Patterns gibt, sodass auch hier die Notwendigkeit weiterer Forschungsarbeiten in diesem Bereich deutlich wird. Auch direkte Lösungsansätze fehlen bisher. Dergleichen ergeben sich jedoch zumindest teilweise daraus, dass Anti-Patterns meist eine Fehleinschätzung der Designer*innen zugrunde liegt, sodass sie nach Erkennen leicht durch andere Patterns ersetzt werden können [21].

Über die Definition von Anti-Patterns können auch Anforderungen aufgestellt werden mittels derer überprüft werden kann, wann Security-Warnings Anti-Patterns darstellen können. Demnach handelt es sich bei Security-Warnings natürlicherweise um ein Konzept eines User Interfaces und dieses wurde in der Regel dazu entworfen Nutzer*innen zu schützen und damit in guter Intention implementiert. Bezüglich der Nebenwirkungen, die mit Anti-Patterns einhergehen, kann festgehalten werden, dass auch Security-Warnings häufig ungewünschten Nebeneffekten unterliegen. So konnten mehrere Studien feststellen, dass bei häufiger Konfrontation mit der gleichen Warnmeldung Habituation auftreten kann, d.h. Anwender*innen gewöhnen sich an die Warnmeldung und verarbeiten diese nicht mehr bewusst [1, 3, 4, 34, 35]. Diese Habituation könne auch Generalisierung verursachen, wenn die Habituation auf einen Stimulus auf einen anderen mit ähnlichem Aussehen übergeht [35]. Ein weiteres Problem im Zusammenhang mit Security-Warnings sind schlechte mentale Modelle [32] und mangelndes Verständnis [1], wodurch Nutzer*innen anfälliger für Angriffe werden können [1, 32]. Ein interessanter Ansatz, wie dem entgegengewirkt werden kann, sind polymorphe Warnungen, die bei jedem Auftreten einer Warnmeldung zufällig eines aus mehreren Designs auswählen, um so die Habituation zu umgehen [3, 34]. Durch diese Feststellungen kann geschlussfolgert werden, dass Security-Warnings häufig Anti-Patterns darstellen können, sodass entsprechende Beispiele in die Menge der gesammelten Patterns und das zusammenfassende Modell aufgenommen werden können.

3.2 Dark-Patterns

Auch zu Dark-Patterns konnte eine zusammenfassende Definition aufgestellt werden: Demnach sind Dark-Patterns Designentscheidungen, die durch Täuschung oder Ausnutzung psychischen Drucks versuchen Nutzer*innen zu Handlungen zu verleiten, von denen die Ersteller*innen des Dark-Patterns mehr profitieren als sie selbst [5, 6, 10, 11, 14, 17, 19, 21, 23–25, 27, 29, 30, 38].

Ein Beispiel für ein Dark-Pattern wäre Confirmshaming, das mit emotionsgeladener Sprache eine Entscheidung beeinflussen soll [7]. Dark-Patterns würden durch die Ausnutzung von Heuristiken und Biases häufig nicht bewusst verarbeitet und dadurch ihre täuschende Wirkung erzielen [20, 22]. Auf die Fähigkeit der Nutzer*innen Dark-Patterns zu erkennen, wirke sich vor allem der Bildungsgrad [19] und die Kenntnis des Themas der Nutzer*innen [11] aus, aber auch die Art des Dark-Patterns [20]. Besonders bei Erkennen eines Dark-Patterns könnten sich Nutzer*innen verwirrt oder gestresst fühlen [15, 20, 22] und so auch das Vertrauen zu einer Marke verlieren [20]. Es konnte jedoch festgestellt werden, dass es für die Anwender*innen bzw. Ersteller*innen eines Dark Patterns keine negativen Auswirkungen, wie Verärgerung oder Abschreckung der Nutzer*innen, gibt, wenn das Dark Pattern in seiner Wirkungsweise erfolgreich war [19]. Auch die weit verbreitete Nutzung spricht eindeutig für den Erfolg von Dark-Patterns. Viele Teilnehmer*innen verschiedener Studien sehen unter anderem daher keine direkte Lösung zu Dark-Patterns und halten diese teilweise für unumgänglich [11, 22]. Lösungsvorschläge zum Vorgehen gegen Dark-Patterns sind vor allem die Informierung der Nutzer*innen [15, 17, 20, 22], Designer*innen zur ethischen Überdenkung ihrer Designs anzuregen [21, 27], Plug-Ins und Methoden zur automatischen Erkennung [20] und rechtliche Regulierung [37]. Durch die Rechercheergebnisse zu Nudging, konnte nach Abgleich mit der Dark-Pattern Definition verifiziert werden, dass Digital Nudging häufig ein Designkonzept darstellt [9, 31], aber nicht zwangsläufig zum Nachteil der Anwender*innen designt sein muss [8, 17, 29, 30]. Demnach ist Nudging definiert als „Veränderung der Entscheidungsarchitektur" [8] und nach Einschätzung der Autor*innen als ein mehreren Dark-Patterns zugrundeliegendes Prinzip zu betrachten.

3.3 Übersicht bekannter Design Patterns

Im Rahmen der Literaturrecherche wurden außerdem UX-Design-Patterns gesammelt und mit ihrer Einordnung gemäß der jeweiligen Forschungsarbeit notiert. Eine vollständige Darstellung der in der Recherche gesammelten Patterns findet sich in Tabelle 4 im Anhang A. Einige Patterns wurden dabei von der Literatur hierarchisch kategorisiert, da sie sich als Subtypen anderer Patterns interpretieren lassen. In Abschnitt 4 wird beschrieben, wie diese Patterns klassifiziert wurden. Die spezifische Zuordnung einzelner Patterntypen ist damit ebenfalls in Tabelle 4 dargestellt. Die Pattern-Bezeichnungen wurden den Arbeiten entnommen, die das entsprechende Pattern enthalten, und sind in den Tabellen 1, 3 und 2 näher erläutert. In Tabelle 4 enthalten sind ausschließlich die Arbeiten, die eigene und neue Taxonomien aufstellen und sich nicht lediglich auf die Klassifikation einer anderer Forschungsarbeiten beziehen. Eine Erläuterung des Prozesses zur Aufstellung des Modells zur Klassifikation dieser Arbeit erfolgt im folgenden Abschnitt.

4 MODELL ZUR UNTERSUCHUNG

Nach Abschluss der Literaturrecherche wurde ein Modell erarbeitet, dass zur Differenzierung und Einordnung der verschiedenen Design-Patterns dienen sollte. Dafür wurden eingangs alle in der Recherche erhaltenen Patterns gesammelt und Dopplungen bzw. äquivalent definierte Patterns entfernt, in Tabelle 4 im Anhang A unter „Zu große Ähnlichkeit zu anderen Patterns" aufgelistet. Bspw. sind Friend Spam [7] und Address Book Leeching [5] äquivalent

Tabelle 1: Anti-Patterns mit Beschreibung

Name	Beschreibung
Passwords for Delegated Authentication	Third Party Authentification, für die die Anmeldung bei einem Service über die Anmeldedaten eines anderen Service erfolgt und die Nutzer*innen anfälliger für Phishing-Angriffe machen kann.
Security Images for Site Authentication	Ein Bild oder eine Darstellung wird während der Identifikation angezeigt, um Nutzer*innen bei der Unterscheidung zwischen Phishing-Angriff und vertrauenswürdiger Authentifikation zu unterstützen. Dies kann bei Nutzer*innen schlechte mentale Modelle verursachen.
Malware und Phishing-Warnungen	Sollen Nutzer*innen vor böswilligen Websites schützen bzw. vor Malware und Phishing Angriffen, verursachen aber häufig Habituation, Generalisierung oder schlechte mentale Modelle.
SSL/HTTPS Warnungen	Werden angezeigt, wenn der Browser ein nicht vertrauenswürdiges Zertifikat der Website erkennt, um den Nutzer davor zu schützen Informationen durch unsichere Verbindungen preiszugeben. Verursachen aber häufig Habituation, Generalisierung oder schlechte mentale Modelle.

Tabelle 2: Dark-Patterns mit Beschreibung

Name	Beschreibung
Privacy Zuckering	Nutzer*innen werden zur Freigabe von Daten ausgetrickst oder überredet.
Forced Registration	Der Service erzwingt zu dessen Nutzung die Erstellung eines Nutzerkontos.
Explanation Surveys	Nutzerfeedback wird zur Datensammlung verwendet.
Trick Question	Eine Frage wird unnötig verkompliziert gestellt, sodass, sofern sie nicht genauesten betrachtet und bedacht wird, häufig eine unerwünschte Antwort gegeben wird.
Address Book Leaching	Nutzer*innen werden dazu gedrängt dem Service Zugriff auf ihre Kontaktdaten zu geben, meist unter dem Vorwand dies würde die Serviceleistung verbessern, diese Daten werden aber zur Speicherung und Verarbeitung gesammelt.
Shadow User Profiles	Der Service sammelt über die angegebenen Daten von Nutzer*innen auch Daten über dort nicht registrierte Personen.
Disguised Data Collection	Gesammelte Informationen werden zur Erstellung eines Nutzerprofils missbraucht.

definiert, da sich Address Book Leeching hier aber deutlicher auf die damit einhergehende Datensammlung und Weiterverarbeitung bezieht, wurde dieser Begriff gewählt.

Aufgrund dessen, dass die Forschungsfrage dieser Arbeit auf Designs, die sich auf Sicherheits- und Vertraulichkeitsverhalten auswirken, fokussiert ist, wurden weiterhin alle nicht sicherheitskritischen Patterns ausgeschlossen, ebenfalls aufgelistet in Tabelle 4 im Anhang A. Dabei können nur Patterns als sicherheitskritisch gelten, die das Sicherheits- und Vertraulichkeitsverhalten direkt beeinflussen, indem bspw. Daten in für den Service unverhältnismäßigem Umfang oder für unverhältnismäßige Dauer gespeichert werden, der Zugang zu Vertraulichkeitseinstellungen verweigert oder erschwert wird oder Nutzer*innen dadurch anfälliger für Sicherheitsrisiken werden. Bspw. stellt das Hamburger Menu Pattern [21] vor allem ein Anti-Pattern aufgrund der Unannehmlichkeiten, die es verursacht, dar und wirkt sich nicht nachteilig auf das Sicherheits- und Vertraulichkeitsverhalten aus. Alle Patterns, die nicht mit einer dieser Begründungen ausgeschlossen wurden, fanden damit Einzug in das zusammenfassende Modell.

Im Anschluss wurden Anti-Patterns und Dark-Patterns verglichen und die Sicherheitskritischen Patterns dementsprechend zugeordnet. Dabei liegt der Unterschied vor allem in der Intention der Designer*innen und den Konsequenzen der Patterns. Demnach können als aus technischer Sicht eindeutige Anti-Patterns alle Patterns gewertet werden, bei denen es sich nur um eine gute Intention handeln kann, indem bspw. die Entwickler*innen keinen Vorteil aus den Nebeneffekten schlagen. Ein Vorteil für Entwickler*innen stellt dabei beispielsweise ein Gewinn an Daten oder ein finanzieller Gewinn dar. Als eindeutiges Dark-Pattern können alle Patterns gewertet werden, die absichtlich platziert worden sein müssen, da sie bspw. mit einem Zusatzaufwand verbunden sind oder bewusst verschleiert werden. Als Zusatzaufwand werden alle Maßnahmen gesehen, die über den standardmäßigen Designprozess und Betrieb des Services hinausgehen. Beispielsweise werden bei Shadow User Profiles Daten über Personen gesammelt, die nicht am Service teilnehmen, was einen Mehraufwand für die Betreiber*innen darstellt der für den Betrieb für registrierte Nutzer*innen nicht benötigt wird. Alle Patterns, die nicht eindeutig zugeordnet werden konnten, werden in Anlehnung an die Visibility-Darkness Matrix [28] als

Tabelle 3: Grey-Patterns mit Beschreibung

Name	Beschreibung
Social Pyramid	Nutzer*in muss Bekannte oder Freunde einladen, um Service zu nutzen oder Vorteile zu erhalten.
Forced Dismissal	Nutzer*in wird gezwungen eine Erklärung zu Hintergründen zur Datenverarbeitung abzulehnen, um davon verdeckte Inhalte zu sehen.
Forced Continuity	Eine Serviceleistung oder ein bestehendes Konto kann nicht mit einfachen Mitteln gekündigt werden.
Bait and Switch	Nutzer*innen werden mit dem Angebot einer bestimmten Aktion gelockt, nur damit dann etwas vollkommen anderes passiert.
Preselection	Bei dem Angebot verschiedener Auswahlmöglichkeiten sind bestimmte Defaultwerte ausgewählt.
Nested Details	Details werden hinter mehreren Verlinkungen versteckt.
Roach Motel	Es wird Nutzer*innen sehr leicht gemacht bestimmte Bedingungen zu erfüllen, um zu einer Situation weitergeleitet zu werden, der Ausgang aus dieser wird jedoch unverhältnismäßig erschwert.
Information Overload	Nutzer*innen werden mit Informationen meist in komplizierter Ausdrucksweise überladen, um sie von Inhalten oder Aktionen abzulenken.
Nebulous Prioritization	Nicht alle Informationen werden aufgezählt und die Entscheidung, welche dieser dargestellt werden ist nicht nachvollziehbar.
Hampered Selection	Erschwerte Auswahl gewünschter Information oder Aktionen indem bspw. immer die gleiche Anfrage gestellt werden muss, um Teile dieser zu erhalten.
Confirmshaming	Durch emotionsgeladene Sprache, die Nutzer*innen auf emotionale Ebene beeinflusst, häufig durch die Vermittlung von Schuldgefühlen, sollen diese zu einer bestimmten Aktion überredet werden.
Hidden Information	Bestimmte Informationen sind nur schwer zugänglich oder schwer verständlich, sodass sie regelrecht vor den Nutzer*innen versteckt sind.
Limited View	Durch Überlagerung der gewünschten Informationen werden Nutzer*innen dazu gedrängt den dargestellten Privatheitseinstellungen zuzustimmen.
Competing Elements	Nutzer*innen sollen durch andere visuelle Elemente von Transparenz bietenden Erklärungen abgelenkt werden.
Toying with Emotion	Nutzer*innen werden durch emotionsgeladenen Text oder Design beeinflusst.
False Hierarchy	Visuelle Hervorhebung einer Option, die eigentlich gleichrangig zu anderen dargestellt werden sollte.
Activity Noftifcations	Nutzer*innen werden von Verhalten/Aktionen anderer Nutzer*innen informiert, unter Umständen entsprechen diese Angaben nicht den tatsächlichen Gegebenheiten.
Restricted Dialogue	Es ist Nutzer*innen nicht möglich ein dargestelltes Pop Up dauerhaft zu schließen, indem z.B. nur die Option „nicht jetzt" geboten werden.
Hidden Interaction	Nutzer*innen werden von ihnen unbeabsichtigt zu einer anderen Website umgeleitet.
Making Personal Information Public	Bei einer Proxemic Interaction werden persönliche Informationen öffentlich dargestellt. [1]
We Never Forget	Informationen über eine Proxemic Interaction werden gespeichert, mit der Begründung, dass die Interaktion so nahtlos wieder aufgegriffen werden kann.
The Social Network	Informationen über soziale Interaktionen werden gesammelt, mit der Begründung, dass so ein besserer Service geleistet werden könne.
Privacy Policies/EULAs	Sollen Nutzer*innen alle rechtlichen Informationen zur Datenverarbeitung und Datenspeicherung bzw. zur Nutzung eines Service darstellen, können diese aber überfordern.

[1] Proxemic Interactions sind Interaktionen, bei denen die physische Distanz zwischem Mensch und System die Reaktion des Systems beeinflusst

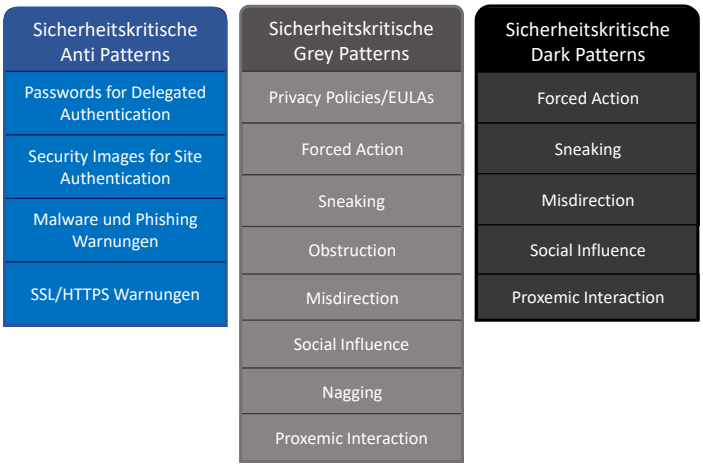

Abbildung 2: Sicherheitskritische Typen von UX-Design-Patterns nach Klassifikation in Anti-, Grey- und Dark-Patterns. Subtypen wurden ausgelassen und finden sich in Tabelle 4 im Anhang A.

Grey-Patterns bezeichnet. So kann bspw. Passwords for Delegated Authentication als eindeutiges Anti-Pattern gewertet werden, da die Nebenwirkungen keine Vorteile für die Entwickler*innen schaffen. Privacy Policies/EULAs können sowohl unbeabsichtigt eine schlechte Usability haben als auch bewusst derart designt sein, um Nutzer*innen von deren Inhalt abzulenken und müssen daher als Grey-Pattern eingeordnet werden und Privacy Zuckering muss aufgrund des zusätzlichen Aufwands der durch die Datenspeicherung und -verarbeitung entsteht und der manipulativen Vorgehensweise zur Erlangung dieser als bewusste Entscheidung und damit als Dark Pattern gelten. Tabellen 1, 3 und 2 enthalten dementsprechend jeweils eine Auflistung der in dieser Arbeit identifizierten Sicherheitskritischen Anti-, Grey- und Dark-Patterns. In Abbildung 2 findet sich eine zusammenfassende Darstellung unter Auslassung einzelner Pattern-Subtypen.

Da sich die Design-Intention aus technischer Sicht für ein bestimmtes Pattern ohne Kontext häufig nicht *eindeutig* ableiten lässt, fallen viele UX-Patterns in die Kategorie der Grey-Patterns. Eine Auflösung der Unschärfe, die sich durch diese Kategorie ergibt, kann für spezifische Implementierungen der UX-Patterns durch die Berücksichtigung kontextueller Faktoren unter Umständen aufgelöst werden, sofern sich die Design-Intention plausibel identifizieren lässt.

Die beschriebenen Kriterien können außerdem in einem Modell zur Identifikation und zur Unterscheidung sicherheitskritischer UX-Patterns umgesetzt werden. Demnach wird zunächst 1. zwischen (aus Nutzersicht) funktionellen Patterns oder Patterns, die sich nachteilig auf das Nutzerverhalten auswirken differenziert, 2. anschließend untersucht, ob diese nachteiligen Patterns sicherheitskritisch sind, daher die IT-Sicherheit, die Privatsphäre der Nutzer*innen oder die Vertraulichkeit betreffen und 3. zuletzt entsprechend der Design-Intention nach Anti-, Grey- oder Dark-Pattern unterschieden. Für die Differenzierung in Schritt 1 werden als Nachteile für Nutzer*innen finanzieller Verlust oder die unbeabsichtigte Freigabe von Daten, sowie andere von den Nutzenden als unangenehm empfunde Erlebnisse, wie bspw. eine schlechte Usability gesehen. Die Unterscheidung in Schritt 2 bezieht sich hier vor allem danach, ob ein Safety-Risiko für die Anwender*innen entsteht, bspw. durch die ungewollte Freigabe von personenbezogenen Daten, nicht auf etwaige Unanehmlichkeiten für den Nutzer. Auch finanzielle Sicherheit, wie sie beispielsweise beim "Sneak into Basket" Pattern gefährdet wird, wurde weitgehend ausgeklammert. Dieses Pattern stellt zwar ein Dark Pattern dar, jedoch liegt in diesem Fall keine Auswirkung auf IT-Sicherheit und Privatsphäre vor. Auch andere entsprechende Patterns können zwar theoretisch je nach Absicht des Designers Anti-, Grey- oder Dark-Patterns darstellen, jedoch wären sie in diesem Falle nicht sicherheitskritisch. Eine Visualisierung dieses Prozesses in Form eines Flussdiagramms ist in Abbildung 3 zu sehen.

5 DISKUSSION UND FAZIT

Durch die Umsetzung einer methodischen Literaturrecherche konnte diese Arbeit damit eingehende Forschungsergebnisse und -ansätze zu den Themen Anti-Patterns und Dark-Patterns sammeln und Kernpunkte dieser darstellen, sowie auf den Zusammenhang von Anti-Patterns und Security-Warnings bzw. Dark-Patterns und Nudging eingehen. Mittels dieser Ergebnisse konnten im Anschluss bestehende Anti- und Dark-Pattern Kategorien in einer Taxonomie zusammengefasst und die vorgenommenen Eingrenzungen zu einem Modell zur Unterscheidung Sicherheitskritischer Anti-, Grey- und Dark-Patterns verarbeitet werden.

Die erhaltenen Ergebnisse beantworten damit insbesondere die Forschungsfrage nach die Sicherheit und Vertraulichkeit beeinflussender User Experience durch entsprechende Designs. Es konnte anschaulich gezeigt werden, dass Sicherheitskritische Anti- und Dark-Patterns, die als solche den Nutzer*innen Transparenz in Hintergrundprozesse bieten sollen, bzw. im Falle von Dark-Patterns diese vortäuschen, sowie die damit einhergehende User Experience sich negativ auf die Sicherheit und Vertraulichkeit der Nutzer*innen und deren Daten auswirken können. Durch die Unterscheidung der entsprechenden Anti-, Grey- und Dark-Patterns wurde dabei

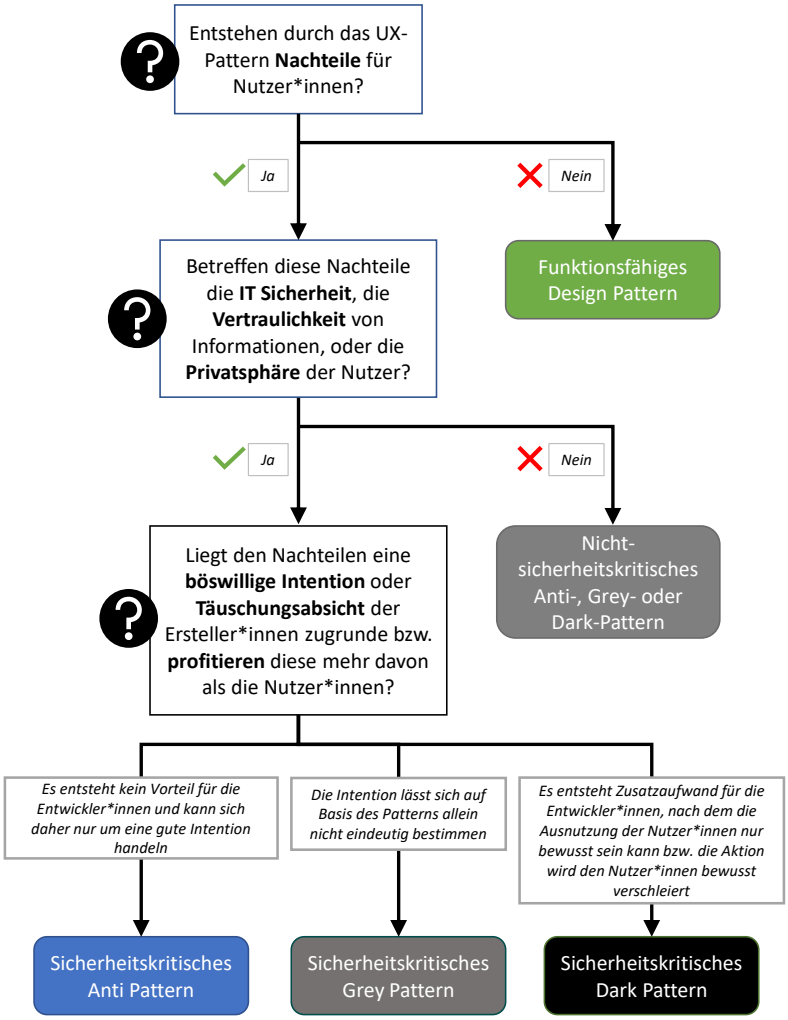

Abbildung 3: Flussdiagramm der notwendigen Schritte um sicherheitskritische Anti-, Grey- und Dark-Patterns zu identifizieren

umfangreich darauf eingegangen, wie dieser Sicherheits- und Vertraulichkeitsverlust entsteht. Arbeiten mit ähnlichem Ansatz beschränken sich bislang auf Fraktionen dieses Themas und häufig fehlt ein Konsens über die Menge bestehender Anti- und Dark-Patterns, auf dem Untersuchungen aufbauen können. Bestehende Arbeiten beschäftigen sich häufig nur mit einem der beiden Themengebiete und der einzige Vergleich von Anti- und Dark-Patterns beruht bisher auf Vergleichen der Definitionen. So beziehen sich bspw. [5] und [24] ausschließlich auf Dark Patterns und [25] vergleichen zwar Anti- und Dark-Patterns, allerdings basierend einzig auf den Definitionen. Somit kann das zusammenfassende Modell auch hier den Forschungsstand erweitern. Dabei wurde die Ergebnismenge natürlich durch die Einschränkung der Suchbegriffe und der Anzahl der untersuchten Artikel limitiert. Auffällig ist auch vor allem die große Menge der nicht eindeutig zuordbaren Grey-Patterns. Hierzu wurde in dieser Arbeit aufgezeigt, dass es kaum möglich ist diese Grauzone aus einer technischen Perspektive weiter einzugrenzen. Weitere Unterscheidungen müssten hier vermutlich basierend auf dem psychologischen Einfluss oder einer juristischen Betrachtungsweise erfolgen. Während sich aus technischer Sicht die Intention der Designer*innen nur anhand des Einsatzes eines bestimmten Patterns häufig nicht eindeutig ableiten lässt, lässt sich im spezifischen Fall einer Implementierung durch kontextuelle Faktoren die unklare Zuordnung zur Anti- und Dark-Patterns dennoch auflösen. Hierbei könnten in künftige Studien empirische Untersuchungen zur Häufigkeit und zum Einsatzgebiet der jeweiligen Patterns oder der Auslegung bestehender Gesetze durchgeführt werden, um eine Auflösung dieser Unschärfe weiter zu unterstützen. Das entstandene Klassifikationsmodell kann nun einerseits zur Anleitung von UX-Designer*innen verwendet werden, um auf entsprechende Gefahren aufmerksam zu machen und andererseits, um darauf aufbauend Maßnahmen gegen die Verwendung dieser

Patterns zu ergreifen, entweder durch juristische Mittel oder durch die Nutzer*innen unterstützende Anwendungen. Zusätzlich kann das einfache Unterscheidungsmodell fachfremde Personen bei der Einschätzung unterstützen, um welchen Typ von Pattern es sich handeln könnte, was im Kontext einer möglichen Regulation von Dark-Patterns einer größere Bedeutung erlangen könnte.

Insgesamt konnte festgestellt werden, dass besonders die Abgrenzung von Anti- und Dark-Patterns in der Literatur noch wenig diskutiert ist und daher weitere Forschung notwendig ist, um ein besseres Verständnis dieser zu erhalten und zu vermitteln. Der wissenschaftliche Beitrag dieser Arbeit in Form der Sammlung verschiedener Patternkategorien und der Aufstellung eines Modells zur Unterscheidung von sicherheitskritischen Anti-, Grey- und Dark-Patterns soll daher als Grundlage dienen, auf die solche ergänzenden Forschungen aufbauen können.

DANKSAGUNG

Diese Arbeit wurde durch die Deutsche Forschungsgemeinschaft (DFG) - SFB 1119 (CROSSING) – 236615297 sowie durch das GRK 2050 (Privacy and Trust for Mobile Users) – 251805230 gefördert.

LITERATUR

[1] N. Agrawal, F. Zhu, and S. Carpenter. Do you see the warning? cybersecurity warnings via nonconscious processing. In M. Chang, D. Lo, and E. Gamess, editors, *Proceedings of the 2020 ACM Southeast Conference*, pages 260–263, New York, NY, USA, 2020. ACM. ISBN 9781450371056. doi: 10.1145/3374135.3385314.

[2] D. Akhawe and A. P. Felt. Alice in warningland: A Large-Scale field study of browser security warning effectiveness. In *22nd USENIX Security Symposium (USENIX Security 13)*, pages 257–272, Washington, D.C., Aug. 2013. USENIX Association. ISBN 978-1-931971-03-4. URL https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/akhawe.

[3] B. B. Anderson, A. Vance, C. B. Kirwan, J. L. Jenkins, and D. Eargle. From warning to wallpaper: Why the brain habituates to security warnings and what can be done about it. *Journal of Management Information Systems*, 33(3):713–743, 2016. ISSN 0742-1222. doi: 10.1080/07421222.2016.1243947.

[4] R. Böhme and J. Grossklags. The security cost of cheap user interaction. In *Proceedings of the 2011 New Security Paradigms Workshop*, NSPW '11, page 67–82, New York, NY, USA, 2011. Association for Computing Machinery. ISBN 9781450310789. doi: 10.1145/2073276.2073284.

[5] C. Bösch, B. Erb, F. Kargl, H. Kopp, and S. Pfattheicher. Tales from the dark side: Privacy dark strategies and privacy dark patterns. In *Proceedings on Privacy Enhancing Technologies*, 4, pages 237–254. De Gruyter, 2016. doi: 10.1515/popets-2016-0038.

[6] H. Brignull. Dark patterns, 2021. URL https://www.darkpatterns.org/. (zuletzt geprüft am 20.12.21).

[7] H. Brignull. Dark patterns: Types of dark pattern, 2021. URL https://www.darkpatterns.org/types-of-dark-pattern/. (zuletzt geprüft am 20.12.21).

[8] A. Caraban, E. Karapanos, D. Gonçalves, and P. Campos. 23 ways to nudge: A review of technology-mediated nudging in human-computer interaction. In S. Brewster, G. Fitzpatrick, A. Cox, and V. Kostakos, editors, *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–15, New York, NY, USA, 2019. ACM. ISBN 9781450359702. doi: 10.1145/3290605.3300733.

[9] M. Castmo and R. Persson. The alliance between digital nudging & persuasive design: The complementary nature of the design strategies. Master thesis, Department of Informatics, Lund School of Economics and Management, Sweden, 2018.

[10] M. Chromik, M. Eiband, S. T. Völkel, and D. Buschek. Dark patterns of explainability, transparency, and user control for intelligent systems. In *Joint Proceedings of the ACM IUI 2019 Workshops*, Los Angeles, USA, March 2019.

[11] L. Di Geronimo, L. Braz, E. Fregnan, F. Palomba, and A. Bacchelli. Ui dark patterns and where to find them. In R. Bernhaupt, F. F. Mueller, D. Verweij, J. Andres, J. McGrenere, A. Cockburn, I. Avellino, A. Goguey, P. Bjørn, S. Zhao, B. P. Samson, and R. Kocielnik, editors, *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–14, New York, NY, USA, 2020. ACM. ISBN 9781450367080. doi: 10.1145/3313831.3376600.

[12] N. Doty and M. Gupta. Privacy design patterns and anti-patterns: Patterns misapplied and unintended consequences. In *Trustbusters Workshop at the Symposium on Usable Privacy and Security*, Newcastle, UK, 2013. CyLab Usable Privacy and Security Laboratory (CUPS), PaCT Lab. doi: 10.1145/2207676.2207759.

[13] L. Fritsch. Privacy dark patterns in identity management. In L. Fritsch, H. Roßnagel, and D. Hühnlein, editors, *Open Identity Summit 2017*, pages 93–104, Bonn, Germany, 2017. Gesellschaft für Informatik.

[14] C. M. Gray, Y. Kou, B. Battles, J. Hoggatt, and A. L. Toombs. The dark (patterns) side of ux design. In R. Mandryk, M. Hancock, M. Perry, and A. Cox, editors, *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–14, New York, NY, USA, 2018. ACM. ISBN 9781450356206. doi: 10.1145/3173574.3174108.

[15] C. M. Gray, J. Chen, S. S. Chivukula, and L. Qu. End user accounts of dark patterns as felt manipulation. In *Proceedings of the ACM on Human-Computer Interaction*, volume 5 of *CSCW2*, pages 1–25, New York, NY, USA, October 2021. ACM. doi: 10.1145/3479516.

[16] S. Greenberg, S. Boring, J. Vermeulen, and J. Dostal. Dark patterns in proxemic interactions. In R. Wakkary, S. Harrison, C. Neustaedter, S. Bardzell, and E. Paulos, editors, *Proceedings of the 2014 conference on Designing interactive systems*, pages 523–532, New York, NY, USA, 2014. ACM. ISBN 9781450329026. doi: 10.1145/2598510.2598541.

[17] P. Hausner and M. Gertz. Dark patterns in the interaction with cookie banners. In *Position Paper at the Workshop "What Can CHI Do About Dark Patterns?ät the CHI Conference on Human Factors in Computing Systems*, Yokohama, Japan, May 2021. ACM. doi: 10.1145/3173574.3174108.

[18] International Standards Organization (ISO). ISO 9421-11:2018. Ergonomics of human-system interaction – Part 11: Usability: Definitions and concepts, 2018.

[19] J. Luguri and L. J. Strahilevitz. Shining a light on dark patterns. *Journal of Legal Analysis*, 13(1):43–109, 2021. ISSN 2161-7201. doi: 10.1093/jla/laaa006.

[20] A. M. Bhoot, M. A. Shinde, and W. P. Mishra. Towards the identification of dark patterns: An analysis based on end-user reactions. In *IndiaHCI '20: Proceedings of the 11th Indian Conference on Human-Computer Interaction*, IndiaHCI 2020, page 24–33, New York, NY, USA, 2020. Association for Computing Machinery. ISBN 9781450389440. doi: 10.1145/3429290.3429293.

[21] D. MacDonald. *Practical UI Patterns for Design Systems: Fast-Track Interaction Design for a Seamless User Experience*. Apress, Berkeley, CA, 2019. ISBN 978-1-4842-4937-6. doi: 10.1007/978-1-4842-4938-3.

[22] M. Maier and R. Harr. Dark design patterns: An end-user perspective. *Human Technology*, 16(2):170–199, August 2020. doi: 10.17011/ht/urn.202008245641.

[23] A. Mathur, G. Acar, M. J. Friedman, E. Lucherini, J. Mayer, M. Chetty, and A. Narayanan. Dark patterns at scale: Findings from a crawl of 11k shopping websites. In *Proceedings of the ACM on Human-Computer Interaction*, volume 3 of *CSCW*, pages 1–32. ACM, November 2019. doi: 10.1145/3359183.

[24] A. Mathur, J. Mayer, and M. Kshirsagar. What makes a dark pattern... dark? design attributes, normative considerations, and measurement methods. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA, 2021. Association for Computing Machinery. ISBN 9781450380966. doi: 10.1145/3411764.3445610.

[25] A. G. Mirnig and M. Tscheligi. (Don't) Join the Dark Side: An Initial Analysis and Classification of Regular, Anti-, and Dark Patterns. In *PATTERNS 2017: Proceedings of the 9th International Conference on Pervasive Patterns and Applications*, pages 65–71. IARIA XPS Press, 2017.

[26] H. Molyneaux, E. Stobert, I. Kondratova, and M. Gaudet. Security matters . . . until something else matters more: Security notifications on different form factors. In *International Conference on Human-Computer Interaction (HCII20)*, volume 12210 of *Lecture Notes in Computer Science*, pages 189–205, Copenhagen, Denmark, 2020. Springer International Publishing. ISBN 978-3-030-50308-6. doi: 10.1007/978-3-030-50309-3{_}13.

[27] A. Narayanan, A. Mathur, M. Chetty, and M. Kshirsagar. Dark patterns: Past, present, and future. *Communications of the ACM*, 63(9):42–47, 2020. ISSN 0001-0782. doi: 10.1145/3397884.

[28] T. Nyström and A. Stibe. When persuasive technology gets dark? In M. Themistocleous, M. Papadaki, and M. M. Kamal, editors, *European, Mediterranean, and Middle Eastern Conference on Information Systems (EMCIS20*, volume 402 of *Lecture Notes in Business Information Processing*, pages 331–345. Springer International Publishing, 2020. ISBN 978-3-030-63395-0. doi: 10.1007/978-3-030-63396-7{\textunderscore}22.

[29] Ş. Özdemir. Digital nudges and dark patterns: The angels and the archfiends of digital communication. *Digital Scholarship in the Humanities*, 35(2):417–428, 2020. ISSN 2055-7671. doi: 10.1093/llc/fqz014.

[30] L. A. Reisch. Nudging hell und dunkel: Regeln für digitales Nudging. *Wirtschaftsdienst: Zeitschrift für Wirtschaftspolitik*, 100(2):87–91, 2020. ISSN 0043-6275. doi: 10.1007/s10273-020-2573-y.

[31] C. Schneider, M. Weinmann, and J. vom Brocke. Digital nudging: Guiding online user choices through interface design. *Communications of the ACM*, 61(7):67–73, 2018. ISSN 0001-0782. doi: 10.1145/3213765.

[32] E. Spero and R. Biddle. Out of sight, out of mind: Ui design and the inhibition of mental models of security. In *New Security Paradigms Workshop 2020*, pages 127–143, New York, NY, USA, 2020. ACM. ISBN 9781450389952. doi: 10.1145/3442167.3442174.

[33] R. H. Thaler and C. R. Sunstein. *Nudge: Wie man kluge Entscheidungen anstößt*. Ullstein Buchverlage, Berlin, 1 edition, 2011.

[34] A. Vance, J. L. Jenkins, B. B. Anderson, D. K. Bjornn, and C. B. Kirwan. Tuning Out Security Warnings: A Longitudinal Examination of Habituation Through fMRI, Eye Tracking, and Field Experiments. *MIS Quarterly*, 42(2):355–380, 2018. ISSN 02767783. doi: 10.25300/MISQ/2018/14124.

[35] A. Vance, D. Eargle, J. L. Jenkins, C. B. Kirwan, and B. B. Anderson. The fog of warnings: How non-essential notifications blur with security warnings. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 407–420, Santa Clara, CA, Aug. 2019. USENIX Association. ISBN 978-1-939133-05-2. URL https://www.usenix.org/conference/soups2019/presentation/vance.

[36] J. vom Brocke, A. Simons, K. Riemer, B. Niehaves, R. Plattfaut, and A. Cleven. Standing on the shoulders of giants: Challenges and recommendations of literature search in information systems research. *Communications of the Association for Information Systems*, 37(9):205–224, 2015. doi: 10.17705/1CAIS.03709.

[37] F. Westin and S. Chiasson. Opt out of privacy or "go home": understanding reluctant privacy behaviours through the fomo-centric design paradigm. In M. Carvalho, W. Pieters, and E. Stobert, editors, *Proceedings of the New Security Paradigms Workshop*, pages 57–67, New York, NY, USA, 2019. ACM. ISBN 9781450376471. doi: 10.1145/3368860.3368865.

[38] K. Widdicks, D. Pargman, and S. Bjork. Backfiring and favouring: How design processes in hci lead to anti-patterns and repentant designers. In D. Lamas, H. Sarapuu, I. Šmorgun, and G. Berget, editors, *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*, pages 1–12, New York, NY, USA, October 2020. ACM. ISBN 9781450375795. doi: 10.1145/3419249.3420175.

A ANHANG

Tabelle 4: Aufzählung aller in der Literaturrecherche gesammelter Anti-, Gray- und Dark-Patterns mit den Forschungsarbeiten, die sie beschreiben und welcher Überkategorie die Pattern in der jeweiligen Arbeit untergeordnet werden (FA = Forced Action, Sn = Sneaking, O = Obstruction, M = Misdirection, I = Interface Interference, AM = Aesthetic Manipulations, Sc = Scarcity, SP = Social Proof).

	[7]	[16]	[5]	[13]	[14]	[10]	[23]	[21]	[12]	[2]	[4]	[26]
Sicherheitskritische Anti-Patterns												
Passwords for Delegated Authentication									•			
Security Images for Site Authentication									•			
Malware und Phishing Warnungen										•		
SSL/HTTPS Warnungen										•		
Sicherheitskritische Grey-Patterns												
Privacy Policies/EULAs									•		•	•
Forced Action					•	•	•					
- Social Pyramid					FA							
- Forced Dismissal						FA						
Sneaking					•	•	•					
- Forced Continuity	•				Sn							
- Bait and Switch	•	•			Sn							
Obstruction					•	•						
- Roach Motel	•				○							
- Information Overload						○						
- Nebulous Prioritization						○						
- Nested Details						○						
- Hampered Selection						○						
Misdirection							•					
- Confirmshaming	•						M	•				
- Interface Interference					•	•						
– *Hidden Information*					I							
– *Preselection*					I							
– *Limited View*						I						
– *Competing Elements*						I						
– *Aesthetic Manipulations*					I							
— *Toying with Emotion*					AM							
— *False Hierarchy*					AM							
Social Influence												
- Activity Notifications							SP					
Nagging					•	•						
- Restricted Dialogue						N						
- Hidden Interaction						N						
Proxemic Interaction												
- Making Personal Information Public		•										
- We Never Forget		•										
- The Social Network		•										

Tabelle 4: Aufzählung aller in der Literaturrecherche gesammelter Anti-, Gray- und Dark-Patterns mit den Forschungsarbeiten, die sie beschreiben und welcher Überkategorie die Pattern in der jeweiligen Arbeit untergeordnet werden (FA = Forced Action, Sn = Sneaking, O = Obstruction, M = Misdirection, I = Interface Interference, AM = Aesthetic Manipulations, Sc = Scarcity, SP = Social Proof).

	[7]	[16]	[5]	[13]	[14]	[10]	[23]	[21]	[12]	[2]	[4]	[26]
Sicherheitskritische Dark-Patterns												
Forced Action					•		•					
- Privacy Zuckering	•				FA							
- Forced Registration			•									
Sneaking					•		•					
- Explanation Surveys						Sn						
Misdirection	•						•					
- Forced Action					•	•	•					
– Aesthetic Manipulations					•							
— Trick Question	•				AM		M					
Social Influence												
- Address Book Leaching			•									
- Shadow User Profiles			•									
Proxemic Interaction												
- Disguised Data Collection		•										
Friend Spam	•											
Immortal Accounts			•									
Hidden Legalese Stipulations			•									
Bad Defaults			•									
Fogging Identification with Security				•								
Zu große Ähnlichkeit zu anderen Patterns												
Sweet Seduction				•								
You can run but you can't hide				•								
Forced Data Exposure						FA						
Hidden Access						○						
Unfavorable Default						I						
Forced Enrollment							FA					
Hard to Cancel							○					
Visual Interference							M					
Testimonials							SP					
Nicht sicherheitskritisch												
Hamburger Menu								•				
Overflow Menu								•				
Pop-Ups								•				
Too Much Information								•				
The Captive Audience		•										
The Attention Grabber		•										
The Milk Factor		•										
Hidden Costs	•				Sn		Sn					
Sneak into Basket	•				Sn		Sn					
Price Comparison Prevention	•				○							
Disguised Ad	•											
Gamification					FA							
Intermediate Currency					○							
Explanation Marketing						Sn						
Low-Stock Message							Sc					
High-Demand Message							Sc					
Countdown Timer							U					
Limited-Time Message							U					
Hidden Subscription							Sn					
Pressured Selling							M					