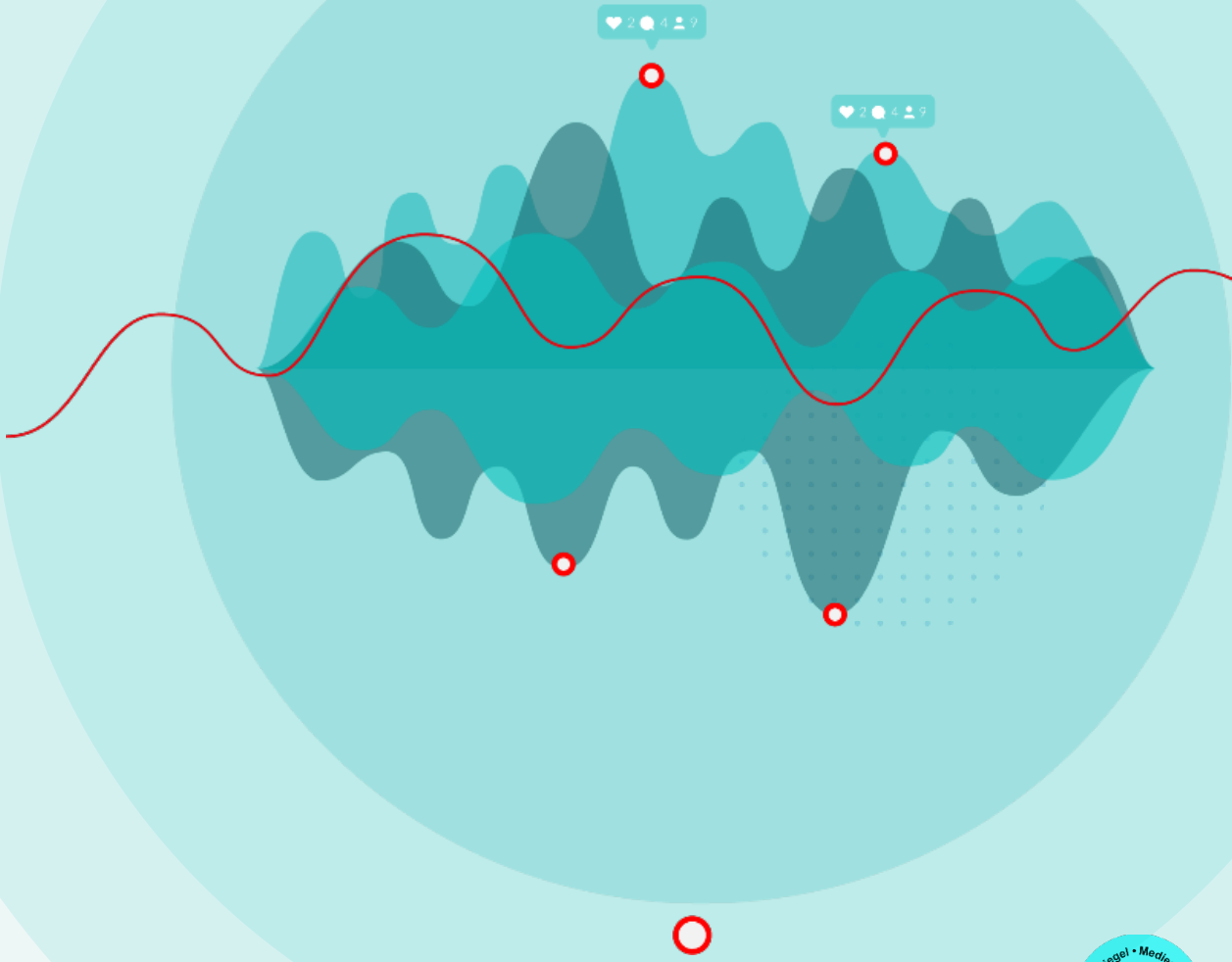
LANDAU MEDIA

01.03.24

ISSUES & TREND MONITORING

Auf Chancen und Risiken rechtzeitig reagieren

Los geht's



Pressespiegel • Medienmonitoring • Medienanalyse •

Vorwort

In diesem E-Booklet wollen wir Dir einen Einblick in das Issues Management bzw. Themenmanagement von Landau Media geben. Wir zeigen dir, wie du Themen für dich frühzeitig erkennen und anhand von Analysemethoden identifizieren und bewerten kannst. Außerdem zeigen wir dir, in fünf Schritten, was du beim Issues Managements beachten musst und wie der KI-Einsatz dein Issues Management vereinfachen kann.

Issues Management bezeichnet die systematische Auseinandersetzung mit medial präsenten Themen. Ziel ist es die in der Öffentlichkeit aufkommende, organisationsrelevante Themen frühzeitig zu erkennen und entsprechend zu reagieren. Wie das Gabler Wirtschaftslexikon ergänzt, müssen diese Themen (Issues) nicht unbedingt negativ sein oder sich krisenhaft entwickeln, „auch wenn das Issues Management in Literatur und Praxis im Zuge der Krisenkommunikation häufig als „Krisenradar“ interpretiert wird.“

Grundsätzlich entstehen Themen heute auch durch individuelle Äußerungen, die zunächst in einer Gruppe auf einer Plattform und dann über die Gruppe hinaus verbreitet werden (rippling effect). Das bedeutet, wenn dann ein Thema „seine Kreise zieht“ verbreitet es sich auch über andere Plattformen hinweg und wird auch von traditionellen Massenmedien aufgegriffen und verstärkt (Reversed Agenda Setting). Eine Selektion, Prüfung und Einordnung der Journalisten:innen und Redakteure:innen wird dadurch umgangen. So erreicht das Thema auch Gruppen, die sich zum Beispiel stärker über traditionelle Medien informieren oder sich für andere Themen interessieren.

Die Aufgabe der Kommunikatoren und PRler ist es nach einer Risiken- und Chancen Management Prozess die Themen der entsprechenden Zielgruppen zu identifizieren, gefolgt von einer unspezifischen Umfeldbeobachtung (Scanning), die Themen zu durchdringen, Informationen zu verdichten und für die Organisation zu qualifizieren. Aber auch die anschließende Konzeption und Umsetzung von Maßnahmen und das anschließende Monitoring gehört zu dem stätigen Prozess des Issues Managements.

Themenmanagement gelingt am besten unserem Pressespiegelservice sowie unserem crossmedialen Medienmonitoring und ergänzend, unserem kostenfreien Recherche-Tool, mit dem Sie ad hoc zu jedem Thema, Produkt/Marke, Person, Event u. v. m. eine retrospektive Recherche für die letzten 12 Monate in über 90.000 Online-Medien durchführen können, um sich unabhängig vom Zielgruppen-Monitoring über alle Trending-Topics zu informieren

Wir freuen uns auf
Ihr Feedback und Ihre Fragen.

Landau Media GmbH & Co.KG
Friedrichstraße 30, 10969 Berlin
Mail: kontakt@landaumedia.de
Tel.: +49 030 202 -100

Du willst dein Issues Management mit unserem Pressespielgel-Service, Medienmonitoring und Medienanalyse-tool verstärken? Vereinbare kostenlos und unverbindlich einen Termin unter **www.landaumedia.de.**

Fünf Schritte, des Issues Managements:

Issues Management ist ein strategischer Prozess, der Unternehmen dabei hilft, potenzielle Probleme und Chancen frühzeitig zu erkennen und darauf zu reagieren, um Risiken zu minimieren und Vorteile zu maximieren. Dazu gehört ein systematisches Scanning und Monitoring des Medien- und Meinungsumfeldes. Dazu bietet Landau Media ein systematisches Issues und Trend-Monitoring an, das nachfolgend vorgestellt wird

1. Identifikation: Früherkennung von Issues & Trends

Dieser Schritt beinhaltet die systematische Überwachung und Analyse der internen (Führungswechsel, Einführung eines neuen Produkts/Services) und externen (PEST-Analyse) Faktoren, die Einfluß auf die Organisation haben könnten, um potenzielle Issues und Trends zu identifizieren, bevor sie sich zu ernsthaften Problemen entwickeln. Für einen umfassenden Überblick über die Nachrichtenlage, um nicht von Themen überrascht zu werden und dann ad hoc reagieren zu müssen, ist ein medienübergreifender täglicher **Pressespiegel** empfehlenswert. Je früher man ein Thema für sich erkennt, desto erfolgreicher kann man es aufgreifen.

2. Analyse: Bewertung und Priorisierung

Nach der Identifikation folgt ein detailliertes **Monitoring** und anschließende **Analyse** der identifizierten Issues. Dabei werden die Ursachen untersucht, die potenziellen Auswirkungen auf die Organisation bewertet und die Issues nach ihrer Dringlichkeit und Bedeutung priorisiert. Diese Priorisierung hilft dabei, Ressourcen effizient einzusetzen. Wer sind die Akteure, wer äußert sich zu dem Thema? Auf welchen Medien findet das Thema statt? Was ist die öffentliche Meinung?

3. Planung: Strategieentwicklung

Basierend auf der Analyse und Priorisierung der Issues werden strategische Pläne entwickelt, um auf die wichtigsten Issues & Trends zu reagieren. Diese Pläne umfassen Ziele, Strategien, taktische Maßnahmen und Zuständigkeiten. Dabei wird festgelegt, wie und wann welche Ressourcen eingesetzt werden sollen, um die Issues zu adressieren.

4. Implementierung: Umsetzung der Maßnahmen

In diesem Schritt werden die entwickelten Pläne in die Tat umgesetzt. Dies beinhaltet die Kommunikation der Pläne an alle betroffenen Stakeholder, die Zuweisung von Ressourcen und die Initiierung der geplanten Maßnahmen. Während der Implementierung ist es wichtig, flexibel zu bleiben und Pläne bei Bedarf anzupassen.

5. Evaluation: Überwachung und Anpassung

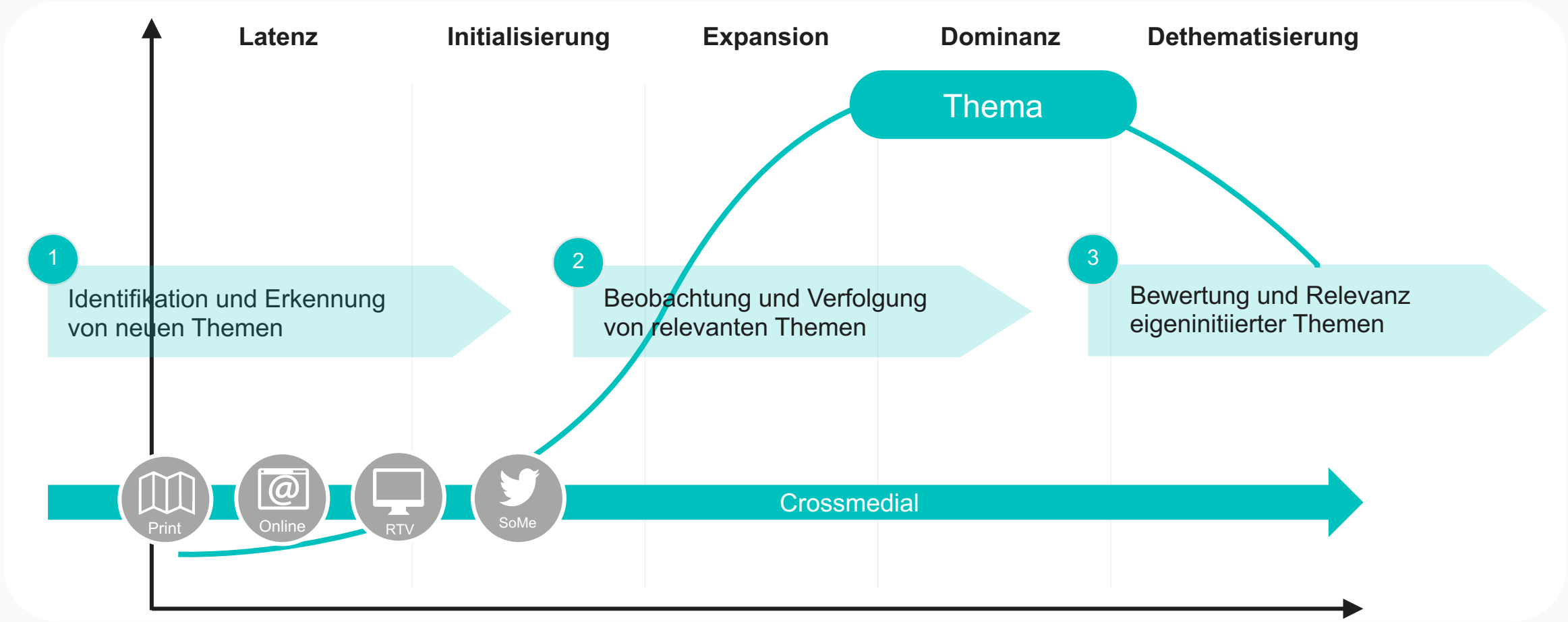
Der letzte Schritt des Issues Management-Prozesses ist die kontinuierliche Überwachung der Umsetzung und die Bewertung ihrer Wirksamkeit. Dies schließt das Sammeln von Feedback, die Messung der Ergebnisse im Vergleich zu den gesetzten Zielen und die Anpassung der Strategien und Maßnahmen an veränderte Bedingungen ein. Die Evaluation dient dazu, aus Erfahrungen zu lernen und den Prozess für zukünftige Issues & Trend zu verbessern.

1

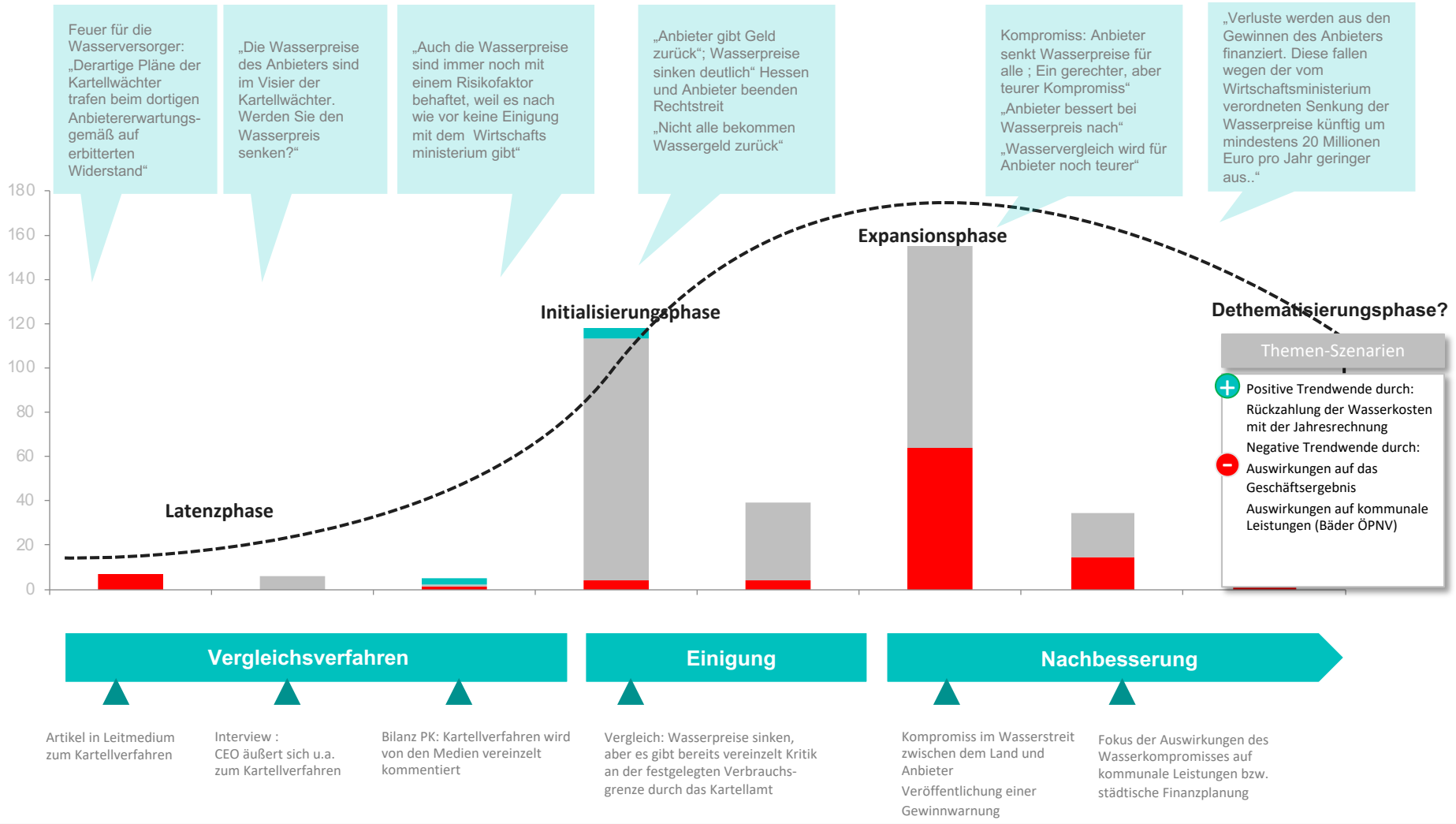
Hintergrund: Issues Management

Zielsetzung Issues Management:

Chance und Risiko Themen frühzeitig erkennen, verfolgen und bewerten



Analyse der Themenkarriere am Beispiel: Kartellverfahren Wasserpreise



Medien:
Print, Online, TV/HF

Basis:
368 Aussagen

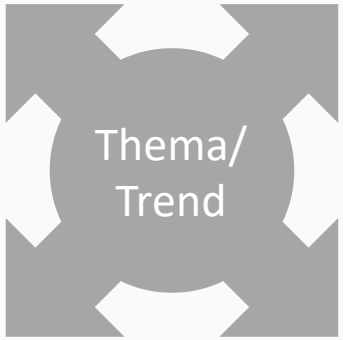
Messgröße:
Präsenz und Tonalität der zentralen Aussagen zum Thema Wasserpreisen

Legende: sehr positiv · positiv · neutral · negativ · sehr negativ

Dimensionen der Trend und Issues Analysen

Stakeholder
Wer äußert sich zum Thema/Trend?

Organisationen
Wer positioniert sich zu diesem Thema/Trend?



Medienkanäle
Wo wird über das Thema/den Trend berichtet?

Autoren
Wer schreibt zu dem Thema/Trend?

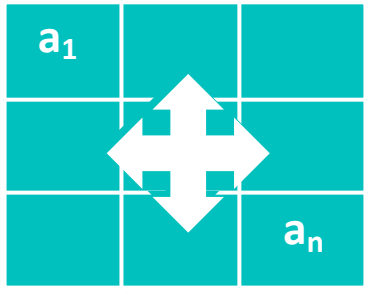
Konzeptioneller Ansatz: Issues & Trend Analysen

Bestimmung des Meta Thema

Umfassende inhaltliche Abdeckung eines Meta-Themas

Issues Monitoring

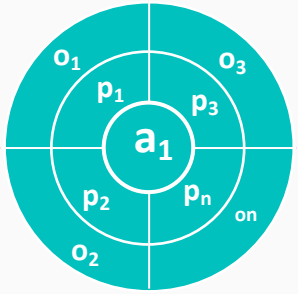
Abgrenzung der Themenfelder



Meta-Thema werden abgrenzbaren Themen-feldern zugeordnet

Issues Map

Identifikation von Entitäten



Personen und Organisationen im Text werden extrahiert

Stakeholder Map

Zuordnung der Autoren

Autoren werden den Beiträgen zugeordnet

Influencer/ Autorenanalyse

Identifikation neuer Themendimension

Neue, aufkommende Inhalte (Positionen, Personen, Organisationen etc. werden bewertet

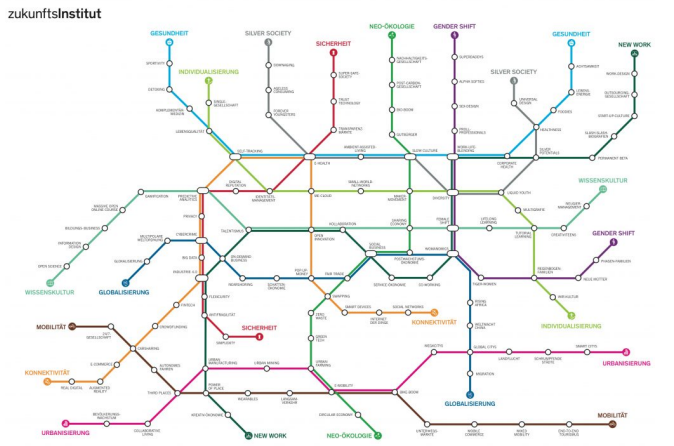
Buzzword-Analysen

2

Umsetzung & Formate: Issues Management

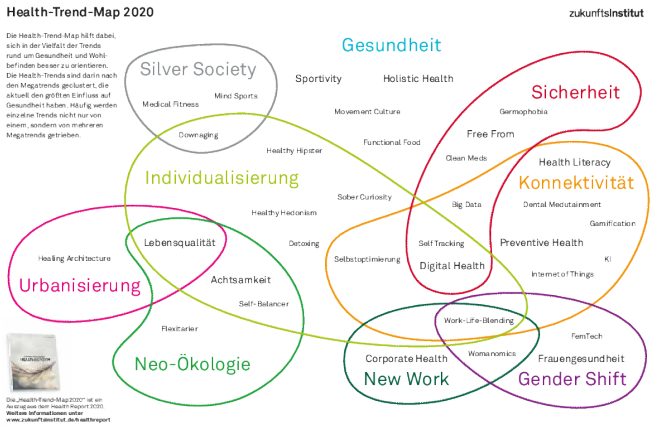
Ausgangspunkt: Explorative Sichtung und Bewertung von Trends

Gesellschaftliche Trends



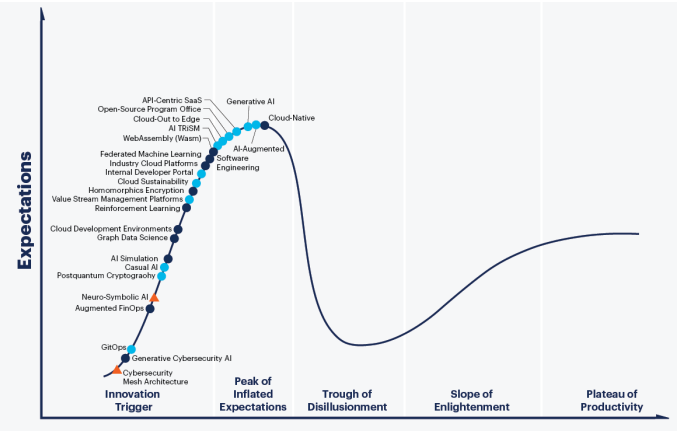
Zukunftsinstitut

Health-Trends



Zukunftsinstitut

Digitale Trends

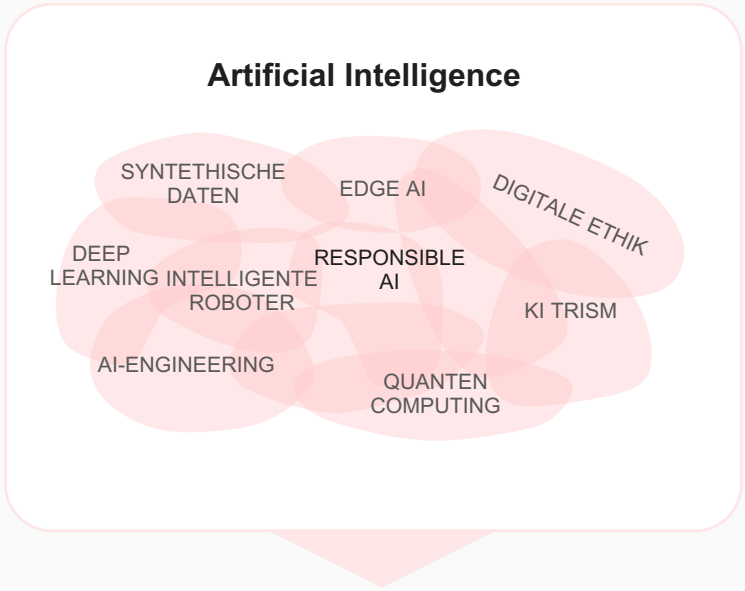


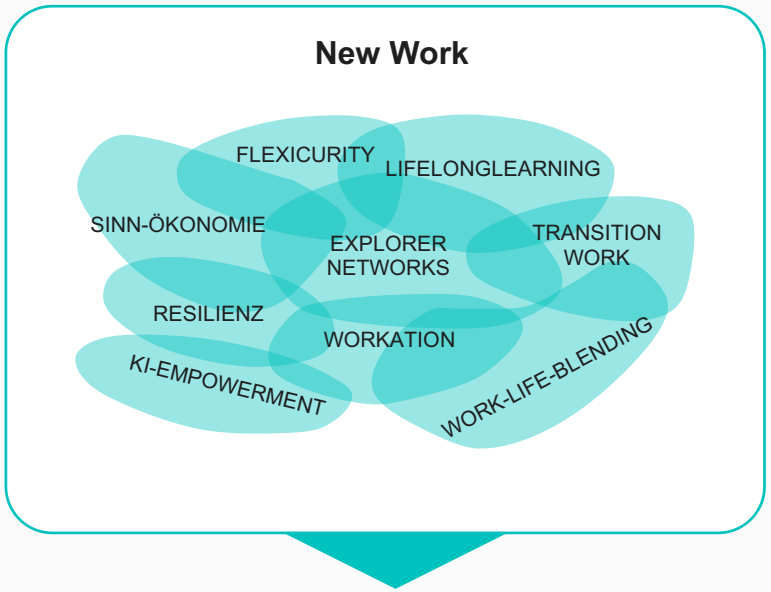
Gartner

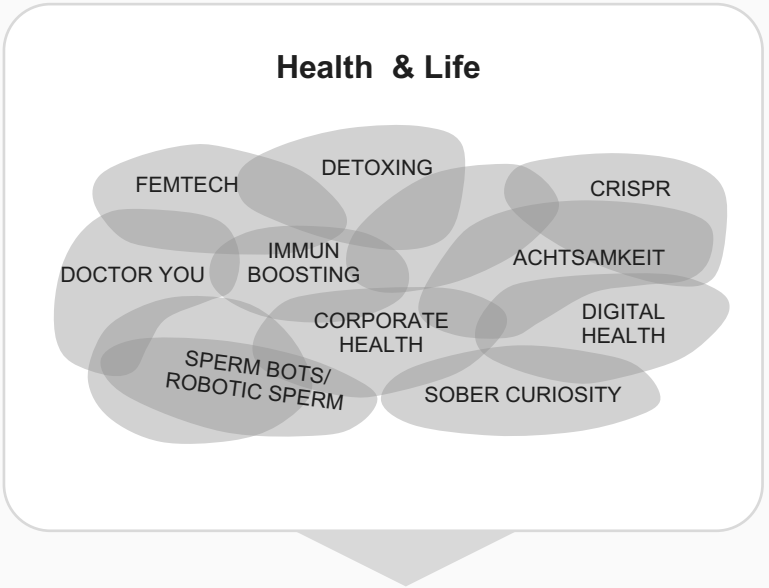
Clustern und Auswahl relevanter Trends
Laufende Sichtung und Prüfung neuer Trends
(intern und externe Quellen)

Übersetzung und Zuordnung der Themen zu Meta-Trends

Set up für das laufende Trendmonitoring

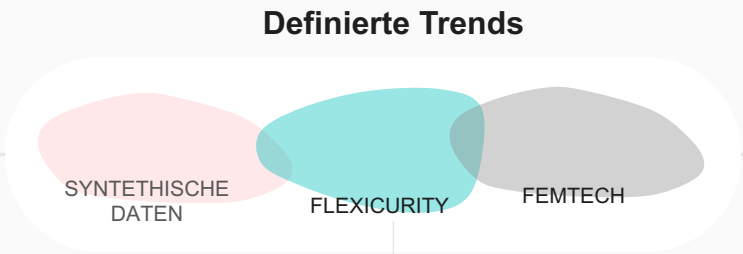






Erstellen der Suchqueries und
Auswahl relevanter Medienquellen für das Trendmonitoring

Formate im Issues & Trend Monitoring



Alert

Laufende Beobachtung der definierten Themen/Trend, bei besonderen Entwicklungen zu einem Thema wird aktiv mit einer Einschätzung/ informiert

Review

Regelmässiges berichten (wöchentlich, monatlich) über den Status der definierten Themen und Trend mit kommunikativen Handlungsempfehlungen

Report

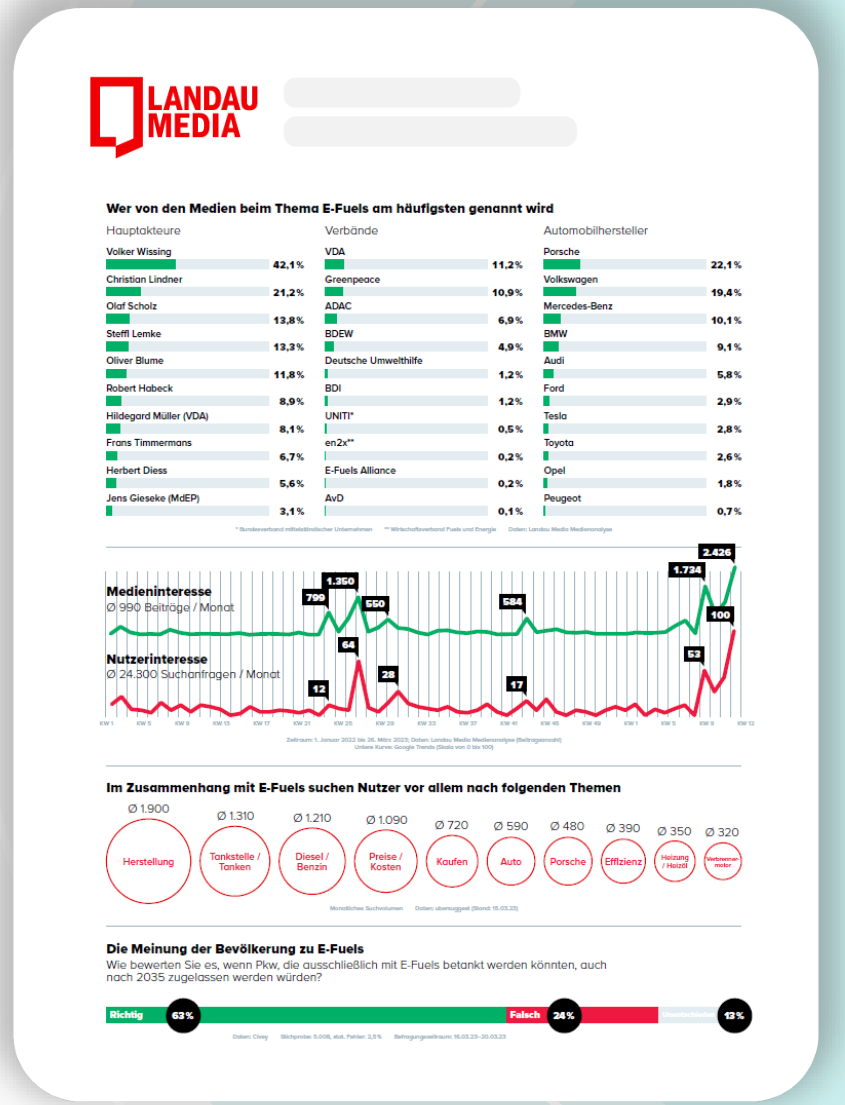
Gezielte, vertiefende Analyse von Themen auch ausserhalb des definierten Themen-Sets, anlassbezogen/auf Anfrage, rückwirkend

Review (Beispiel)

Rückwirkende Analyse von aktuellen Themen und Trend

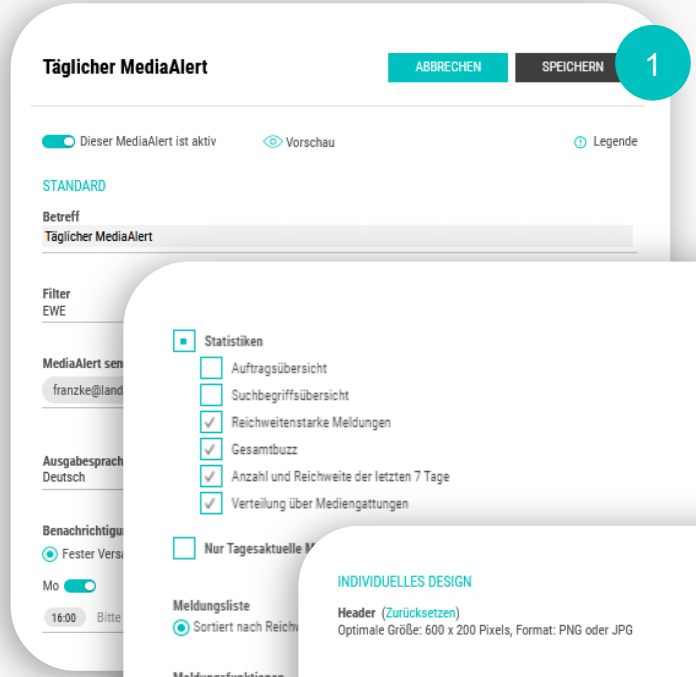
Untersuchung der veröffentlichten Meinung sowie Interesse und Meinung in der Bevölkerung zum Thema „E-Fuels“

Die Kontroverse um das Thema „E-Fuels“ wurde von verschiedenen Akteuren aus Politik und Wirtschaft geführt. Dies führte zu einem hohen Medieninteresse, welches wiederum das Nutzerinteresse sowie die Meinung der Bevölkerung beeinflusste. Alle drei Perspektiven wurden von uns im Rahmen der Issue-Analyse bewertet.



Media Alerts

Über das Portal können mit nur wenigen „Klicks“ automatisierte Alerts für verschiedene Nutzergruppen eingerichtet werden



Set-up:
- Was: bestimmte Marke, Thema etc.
- Wer: Anlage eines Mailverteilers
- Wann: Zeitpunkt, Häufigkeit

Inhaltlicher Aufbau:
- Statistiken, Kennzahlen
- Sortierung der Meldungen
- Gestaltung der Meldungen

Layout:
- Gestaltung Header/Footer
- Verwendung von Logos
- Anpassung Farben

BEISPIEL
Media Alert

Issues Report

Entwicklung des Untersuchungsdesigns

1

Quellen, Sprachen und Regionen definieren:

> Kombination aus Factiva (Print) und O-Point (Online) mit Fokus auf englisch-/deutschsprachigen Leit- und Fachmedien

2

Themen/Trends auswählen und in Queries für die laufende Auswertung der Quellen übersetzen

Issues Briefing > Grundlage Trendstudien + interne Quellen liefern die Trends/Themen, Medien werden laufend nach den Trends ausgewertet (ruled based tagging)

3

Unternehmen/ Wettbewerber festlegen

> tbd. Zu den Themen/Trends werden zusätzlich Wettbewerbsaktivitäten erfasst

Medienpanel

Fokussiertes Leitmedienpanel in Deutschland (z.B. Süddeutsche Zeitung, FAZ) und USA (z.B. New York Times, Washington Post)

Trendgrid im Kontext Landwirtschaft

Smart Farming	KI / AI in Farming	Crispr	Predictive Analytics	Precision Farming
Big Data in Farming & Farm Analytics	Blockchain	Agtech	Farm Network	Farm Robotics & Ag-Bots

Unternehmen

BASF · Bayer · Cargill · ChemChina Syngenta · Huawei · AGCO · John Deere · CNH Industrial · Trimble · Austria Dronetech

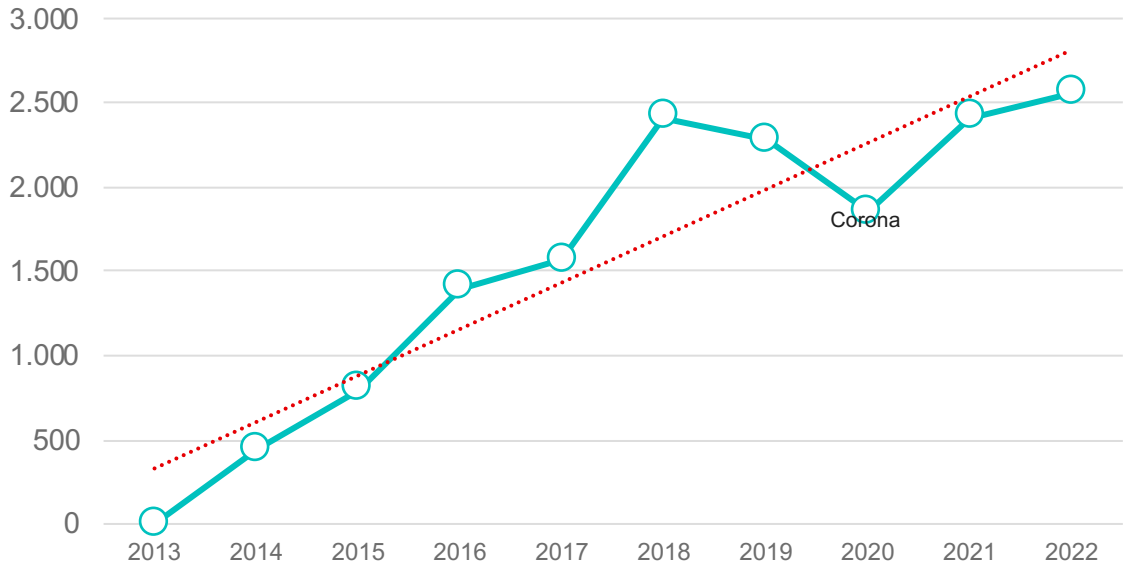
Themen-Report „Digitalisierung in der Landwirtschaft

Themenanalyse für die Märkte Deutschland und USA

Die Digitale Revolution - Big Data, Robotik und KI erobern die Landwirtschaft

Die Digitalisierung treibt eine umfassende Transformation in der Landwirtschaft voran, die sich in einer signifikanten Markt- und Technologierevolution manifestiert. Diese Entwicklung zeichnet sich durch die Integration von Hochtechnologie (Robotik, Autonomes Fahren), Daten (Sensoren, Drohnen) und künstlicher Intelligenz (KI) in landwirtschaftliche Prozesse aus. Schlüsselakteure in diesem Bereich umfassen sowohl etablierte Agrochemie-Konzerne wie Bayer als auch Landmaschinen-Hersteller wie John Deere. Die Digitalisierung in der Landwirtschaft bringt eine Vielzahl von Start-ups hervor, die in neu entstehende Teilmärkte wie Vernetzung von Farmen, Datenanalytik im Agrarbereich und Einsatz von Drohnen vordringen. Etablierte Unternehmen gehen mit den Start-ups verschiedene Kooperationsprojekt ein, um neue Technologien zu testen wie z. B. Cargrill mit AgriWebb bei der brasilianischen Rinderzucht. Auch völlig neue „Player“ positionieren sich beim Thema „Smart Farming“. So geht Huawei eine Kooperation mit Dronetech für das Monitoring großer Ackerflächen und die gezielte Anwendung von Düngemittel ein. 5G wird dabei mit Dronentechnologie kombiniert.

Die Bedeutung des digitalen Wandels in der Landwirtschaft zeigt sich auch in der Langzeitanalyse der Medienresonanz zum Thema Smart Farming. Seit 2013 nimmt das mediale Interesse kontinuierlich zu. Besonderer Fokus liegt dabei auf Precision Farming und beschreibt die Überwachung und Optimierung landwirtschaftlicher Produktionsverfahren durch den Einsatz von digitalen Technologien. Im Rahmen von Precision Farming erfolgt beispielsweise die Düngeausbringung basierend auf Sensor-, Satelliten- oder Drohnendaten.



Smart Farming – Megatrend in der Landwirtschaft

Smart Farming entwickelt sich seit Anfang 2013 zum Megatrend in der Berichterstattung zur Agrar- und Landwirtschaft. Einsatz von Sensoren-, Satelliten- und Drohnendaten stehen im Fokus und lenken die Aufmerksamkeit auf die Digitalisierung der Landwirtschaft insgesamt. Künstliche Intelligenz ist ein weiterer Beschleuniger in der medialen Aufmerksamkeit des Themas Smart Farming

Unternehmenspositionierung „Digitalisierung in der Landwirtschaft“

Themenanalyse für die Märkte Deutschland und USA

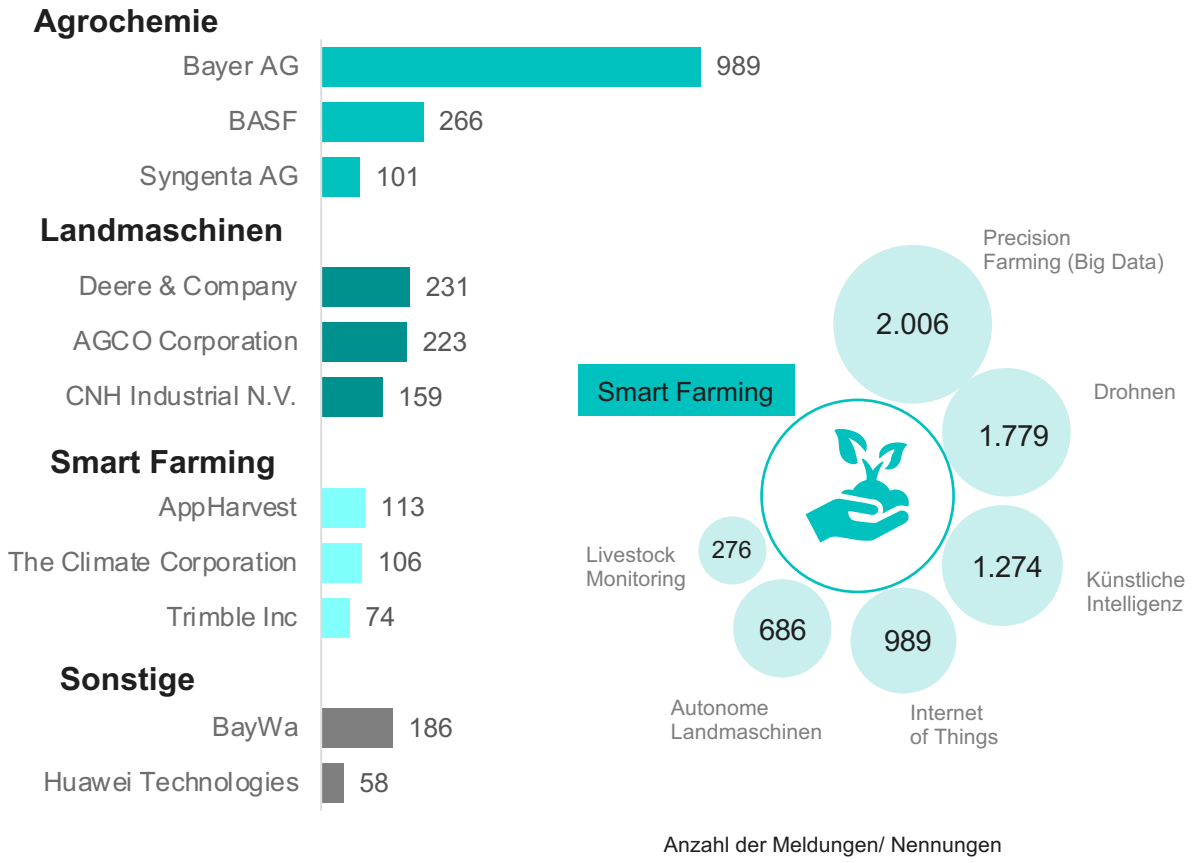
Verpassen die Landmaschinen-Hersteller wichtige Trends?

Trotz der zunehmenden medialen Präsenz dieser Technologien zeigen die Ergebnisse einer Analyse der Leitmedien in Deutschland und den USA, dass die traditionellen Landtechnikhersteller bei der medialen Besetzung dieses Trends hinter den großen Chemie- und Saatgutkonzernen zurückbleiben. Vor allem Bayer und BASF dominieren die Diskussion um Smart Farming. Obwohl mit autonomen Landmaschinen, landwirtschaftlichen Drohnen oder Feldrobotern genügend Innovationsthemen vorhanden sind, bleibt die Präsenz der großen Landmaschinenhersteller hinter den Erwartungen zurück. Hier liegt sicherlich eine große Chance, sich stärker als Gestalter bzw. Vorreiter der digitalen Transformation in der Landwirtschaft zu positionieren.

Die eigentlichen Zukunftsthemen der Branche zeichnen sich möglicherweise gerade in den noch nicht so stark diskutierten Themen ab. Begriffe wie Farm Analytics, Farm Networks, Predictive Analysis oder Blockchain, letzteres vor allem in Verbindung mit dem Begriff Food Safety, erzeugen derzeit kaum mediales Interesse, insbesondere im Kontext der „Big Player“ der Agrarbranche.

Auch setzen sich länderspezifische Oberbegriffe durch. In den USA ist AgTech gebräuchlich, in Deutschland werden mit Abstand die Begriffe Smart Farming oder Digital Farming verwendet.

Zusammenfassend lässt sich sagen, dass sich die Digitalisierung der Landwirtschaft durch den KI-Hype noch dynamischer entwickeln wird. Die nächsten Jahre werden zeigen, wie sich der Agrarsektor angesichts dieser Herausforderungen und Chancen weiterentwickeln wird und welche neuen Akteure auf den Plan treten. Spannend wird auch sein, inwieweit die digitale Transformation auch die grüne Transformation in der Landwirtschaft vorantreiben wird.



3

Einsatz von KI im Issues Management

LANDAU MEDIA

Schritt 1: Bestimmung und Zuordnung zu Themenkategorien

Die KI identifiziert die Themenkategorien. Klassifizierung von über 700 Themenkategorien

KI kontra Cyberkriminalität bei Banktransaktionen

Ein Artikel von **Andreas Hermann, Fraud Manager bei Atruvia** |
28.11.2022 - 09:56

Trotz anhaltender Aufklärungskampagnen erlangen Cyberkriminelle immer wieder vertrauliche Zugangsdaten zum Onlinebanking. Um mögliche Schäden durch rechtswidrige Kontobewegungen zu minimieren, setzt Atruvia auf KI- Techniken: Selbstlernende Algorithmen erkennen automatisch verdächtige Transaktionen, sodass entsprechende Buchungen rechtzeitig geprüft und gegebenenfalls blockiert werden können.

Laut aktuellem Lagebericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist Finance Phishing weiter auf dem Vormarsch: Anders als früher jedoch fassen viele Betrüger ihre Phishing-Mails heute nicht nur in fehlerfreiem Hochdeutsch ab, sondern imitieren gestalterisch auch täuschend echt das Corporate Design der vermeintlichen Absenderbank. Obwohl kein Kreditinstitut in Deutschland seine Kundinnen und Kunden von sich aus per E-Mail mit sensitiven Informationsanfragen kontaktieren würde, gelingt es Cyberkriminellen immer wieder, sich mit dieser Phishing-Masche Kontozugangsdaten von arglosen Opfern zu erschleichen.

Vor allem Unwissenheit spielt ihnen dabei in die Hände: Wie das kürzlich vom BSI gemeinsam mit der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) veröffentlichte „Digitalbarometer" zeigt, verzichten noch immer 23 Prozent aller Verbraucherinnen und Verbraucher darauf, sich über Cybergefahren zu informieren. Gut ein Drittel (35 Prozent) tut dies immerhin sporadisch, und nur 16 Prozent halten sich regelmäßig auf dem Laufenden.

Dreiklang aus Prävention, Detektion und Reaktion

Solche Zahlen unterstreichen die Dringlichkeit von Awareness-Kampagnen im Rahmen einer ganzheitlich konzipierten Anti-Fraud-Strategie für Banken. Aber auch harte Authentifizierungsmechanismen gemäß der europäischen Payment-Services-Richtlinie PSD 2 gehören zur Betrugsprävention.

Als Digitalisierungspartner der Volks- und Raiffeisenbanken hat Atruvia über die Anforderungen von PSD 2 hinaus eine Verifikation per Device-Fingerprinting in die grunderneuerte Onlinebanking-Umgebung eingefügt: Bei einem Kundenlogin über ein bislang nicht verwendetes und daher unbekanntes Endgerät muss dieser erstmalige Zugang zusätzlich durch eine TAN-Freigabe autorisiert werden. Dies erschwert es Kriminellen, gestohlene Zugangsdaten für Betrugsdelikte zu missbrauchen.

Neben harter Authentifizierung verlangt PSD 2 von Banken außerdem die Bewertung sämtlicher Transaktionen im Zahlungsverkehr. Ziel dabei ist es, unberechtigte Transaktionen rechtzeitig zu erkennen und entsprechende Buchungen zu blockieren. Bei bundesweit gut 7,1 Milliarden Banküberweisungen pro Jahr (Stand 2021) ist dies nur durch weitgehend automatisierte Prozesse zu bewerkstelligen.

Die einfachste Variante für eine Bewertungsautomatik wäre etwa ein Echtzeitabgleich der Zielkonten mit einer IBAN-Black-List: Eine solche Liste enthält auffällig gewordene Kontoverbindungen zum Beispiel von sogenannten Fake-Shops, die ihre Opfer mit unrealistisch niedrigen Preisen für hochwertige Markenartikel locken, etwa mit einem Thermomix für 300 Euro. Wer hier bestellt, wartet vergebens auf seine Ware und sieht den überwiesenen Kaufpreis nie wieder – es sei denn, die Bank stoppt die Überweisung, weil die betreffende IBAN in der Black List enthalten ist. Eine generelle Lösung des Problems ist dadurch nicht zu erwarten, da jederzeit neue IBANs für betrügerische Transaktionen genutzt werden können.

CONTEXTCLOUD
THE POWER OF CONTEXT

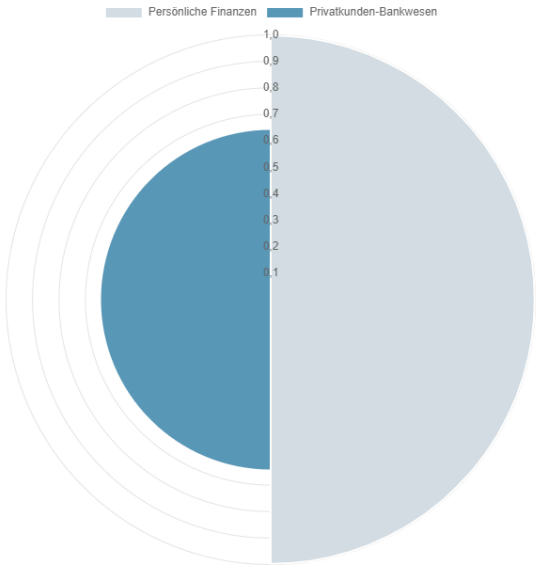
- Home
- Document Enrichment
- Topic Analysis
- Source
- **Content Categories**
- Relevant Phrases
- Personas
- Risk Categories
- Named Entities
- Sentiment
- Collapse

Content Categories

Source document > KI kontra Cyberkriminalität bei Banktransaktionen Ein Artikel von Andreas Hermann, Fraud Manager...

The source content has been assigned to the following categories

NEXT identify the most relevant phrases within the text



Content Category	Sub Categories		
	Level 1	Level 2	Level 3
Persönliche Finanzen (confidence: 100%)	Privatkunden-Bankwesen (confidence: 64%)	-	-

LANDAU MEDIA

Schritt 2: Bestimmung und Zuordnung der Detail-Themen

Erkennung der wichtigsten Phrasen und Themen im richtigen Kontext (Persönliche Finanzen).

KI kontra Cyberkriminalität bei Banktransaktionen

Ein Artikel von **Andreas Hermann, Fraud Manager bei Atruvia** | 28.11.2022 - 09:56

Trotz anhaltender Aufklärungskampagnen erlangen Cyberkriminelle immer wieder vertrauliche Zugangsdaten zum Onlinebanking. Um mögliche Schäden durch rechtswidrige Kontobewegungen zu minimieren, setzt Atruvia auf KI- Techniken: Selbstlernende Algorithmen erkennen automatisch verdächtige Transaktionen, sodass entsprechende Buchungen rechtzeitig geprüft und gegebenenfalls blockiert werden können.

Laut aktuellem Lagebericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist Finance Phishing weiter auf dem Vormarsch: Anders als früher jedoch fassen viele Betrüger ihre Phishing-Mails heute nicht nur in fehlerfreiem Hochdeutsch ab, sondern imitieren gestalterisch auch täuschend echt das Corporate Design der vermeintlichen Absenderbank. Obwohl kein Kreditinstitut in Deutschland seine Kundinnen und Kunden von sich aus per E-Mail mit sensitiven Informationsanfragen kontaktieren würde, gelingt es Cyberkriminellen immer wieder, sich mit dieser Phishing-Masche Kontozugangsdaten von arglosen Opfern zu erschleichen.

Vor allem Unwissenheit spielt ihnen dabei in die Hände: Wie das kürzlich vom BSI gemeinsam mit der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) veröffentlichte „Digitalbarometer" zeigt, verzichten noch immer 23 Prozent aller VerbraucherInnen und Verbraucher darauf, sich über Cybergefahren zu informieren. Gut ein Drittel (35 Prozent) tut dies immerhin sporadisch, und nur 16 Prozent halten sich regelmäßig auf dem Laufenden.

Dreiklang aus Prävention, Detektion und Reaktion

Solche Zahlen unterstreichen die Dringlichkeit von Awareness-Kampagnen im Rahmen einer ganzheitlich konzipierten Anti-Fraud-Strategie für Banken. Aber auch harte Authentifizierungsmechanismen gemäß der europäischen Payment-Services-Richtlinie PSD 2 gehören zur Betrugsprävention.

Als Digitalisierungspartner der Volks- und Raiffeisenbanken hat Atruvia über die Anforderungen von PSD 2 hinaus eine Verifikation per Device-Fingerprinting in die grunderneuerte Onlinebanking-Umgebung eingefügt: Bei einem Kundenlogin über ein bislang nicht verwendetes und daher unbekanntes Endgerät muss dieser erstmalige Zugang zusätzlich durch eine TAN-Freigabe autorisiert werden. Dies erschwert es Kriminellen, gestohlene Zugangsdaten für Betrugsdelikte zu missbrauchen.

Neben harter Authentifizierung verlangt PSD 2 von Banken außerdem die Bewertung sämtlicher Transaktionen im Zahlungsverkehr. Ziel dabei ist es, unberechtigte Transaktionen rechtzeitig zu erkennen und entsprechende Buchungen zu blockieren. Bei bundesweit gut 7,1 Milliarden Banküberweisungen pro Jahr (Stand 2021) ist dies nur durch weitgehend automatisierte Prozesse zu bewerkstelligen.

Die einfachste Variante für eine Bewertungsautomatik wäre etwa ein Echtzeitabgleich der Zielkonten mit einer IBAN-Black-List: Eine solche Liste enthält auffällig gewordene Kontoverbindungen zum Beispiel von sogenannten Fake-Shops, die ihre Opfer mit unrealistisch niedrigen Preisen für hochwertige Markenartikel locken, etwa mit einem Thermomix für 300 Euro. Wer hier bestellt, wartet vergebens auf seine Ware und sieht den überwiesenen Kaufpreis nie wieder – es sei denn, die Bank stoppt die Überweisung, weil die betreffende IBAN in der Black List enthalten ist. Eine generelle Lösung des Problems ist dadurch nicht zu erwarten, da jederzeit neue IBANs für betrügerische Transaktionen genutzt werden können.

CONTEXTCLOUD
THE POWER OF CONTEXT

- Home
- Document Enrichment
- Topic Analysis
- Source
- Content Categories
- **Relevant Phrases**
- Personas
- Risk Categories
- Named Entities
- Sentiment
- Collapse

Relevant Phrases

Source document > KI kontra Cyberkriminalität bei Banktransaktionen Ein Artikel von Andreas Hermann, Fraud Manager...

The following phrases have been identified to be the most relevant ones

NEXT identify to what kind of target group the source content is most appealing

Content Category: Persönliche Finanzen

Phrase	Score
Phishingmasche	82%
Kontozugangsdaten	79%
Authentifizierungsmechanismus	77%
Zielkonto	75%
Cyberkriminelle	75%
Informationsanfrage	72%
Verifikation	71%
Phishingmail	70%

KI kontra Cyberkriminalität bei Banktransaktionen Ein Artikel von Andreas Hermann, Fraud Manager bei Atruvia | 28.11.2022 - 09:56 Trotz anhaltender Aufklärungskampagnen erlangen Cyberkriminelle immer wieder vertrauliche Zugangsdaten zum Onlinebanking. Um mögliche Schäden durch rechtswidrige Kontobewegungen zu minimieren, setzt Atruvia auf KI- Techniken: Selbstlernende Algorithmen erkennen automatisch verdächtige Transaktionen, sodass entsprechende Buchungen rechtzeitig geprüft und gegebenenfalls blockiert werden können. Laut aktuellem Lagebericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist Finance Phishing weiter auf dem Vormarsch: Anders als früher jedoch fassen viele Betrüger ihre Phishing-Mails heute nicht nur in fehlerfreiem Hochdeutsch ab, sondern imitieren gestalterisch auch täuschend echt das Corporate Design der vermeintlichen Absenderbank. Obwohl kein Kreditinstitut in Deutschland seine Kundinnen und Kunden von sich aus per E-Mail mit sensitiven Informationsanfragen kontaktieren würde, gelingt es Cyberkriminellen immer wieder, sich mit dieser Phishing-Masche Kontozugangsdaten von arglosen Opfern zu erschleichen. Vor allem Unwissenheit spielt ihnen dabei in die Hände: Wie das kürzlich vom BSI gemeinsam mit der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) veröffentlichte „Digitalbarometer" zeigt, verzichten noch immer 23 Prozent aller Verbraucherinnen und Verbraucher darauf, sich über Cybergefahren zu informieren. Gut ein Drittel (35 Prozent) tut dies immerhin sporadisch, und nur 16 Prozent halten sich regelmäßig auf dem Laufenden. Dreiklang aus Prävention, Detektion und Reaktion Solche Zahlen unterstreichen die Dringlichkeit von Awareness-Kampagnen im Rahmen einer ganzheitlich konzipierten Anti-Fraud-Strategie für Banken. Aber auch harte Authentifizierungsmechanismen gemäß der europäischen Payment-Services-Richtlinie PSD 2 gehören zur Betrugsprävention. Als Digitalisierungspartner der Volks- und Raiffeisenbanken hat Atruvia über die Anforderungen von PSD 2 hinaus eine Verifikation per Device-Fingerprinting in die grunderneuerte Onlinebanking-Umgebung eingefügt: Bei einem Kundenlogin über ein bislang nicht verwendetes und daher unbekanntes Endgerät muss dieser erstmalige Zugang zusätzlich durch eine TAN-Freigabe autorisiert werden. Dies erschwert es Kriminellen, gestohlene Zugangsdaten für Betrugsdelikte zu missbrauchen. Neben harter Authentifizierung verlangt

LANDAU MEDIA

Schritt 3: Identifizierung von Entitäten im Text

Es werden Personen, Organisationen sowie Orte automatisch erkannt. Schreibweisen werden harmonisiert.

KI kontra Cyberkriminalität bei Banktransaktionen

Ein Artikel von **Andreas Hermann, Fraud Manager bei Atruvia** | 28.11.2022 - 09:56

Trotz anhaltender Aufklärungskampagnen erlangen Cyberkriminelle immer wieder vertrauliche Zugangsdaten zum Onlinebanking. Um mögliche Schäden durch rechtswidrige Kontobewegungen zu minimieren, setzt Atruvia auf KI- Techniken: Selbstlernende Algorithmen erkennen automatisch verdächtige Transaktionen, sodass entsprechende Buchungen rechtzeitig geprüft und gegebenenfalls blockiert werden können.

Laut aktuellem Lagebericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist Finance Phishing weiter auf dem Vormarsch: Anders als früher jedoch fassen viele Betrüger ihre Phishing-Mails heute nicht nur in fehlerfreiem Hochdeutsch ab, sondern imitieren gestalterisch auch täuschend echt das Corporate Design der vermeintlichen Absenderbank. Obwohl kein Kreditinstitut in Deutschland seine Kundinnen und Kunden von sich aus per E-Mail mit sensitiven Informationsanfragen kontaktieren würde, gelingt es Cyberkriminellen immer wieder, sich mit dieser Phishing-Masche Kontozugangsdaten von arglosen Opfern zu erschleichen.

Vor allem Unwissenheit spielt ihnen dabei in die Hände: Wie das kürzlich vom BSI gemeinsam mit der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) veröffentlichte „Digitalbarometer" zeigt, verzichten noch immer 23 Prozent aller Verbraucherinnen und Verbraucher darauf, sich über Cybergefahren zu informieren. Gut ein Drittel (35 Prozent) tut dies immerhin sporadisch, und nur 16 Prozent halten sich regelmäßig auf dem Laufenden.

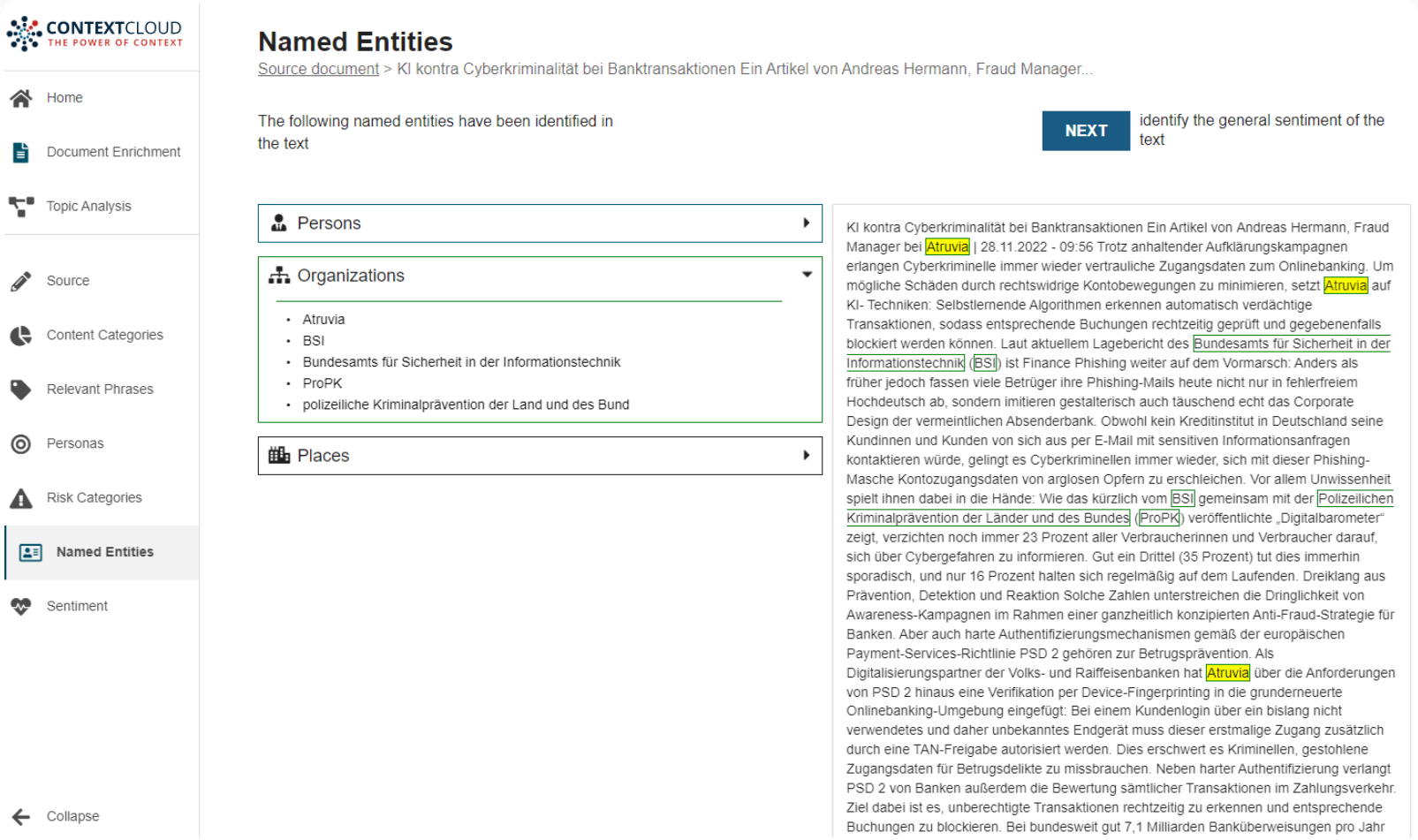
Dreiklang aus Prävention, Detektion und Reaktion

Solche Zahlen unterstreichen die Dringlichkeit von Awareness-Kampagnen im Rahmen einer ganzheitlich konzipierten Anti-Fraud-Strategie für Banken. Aber auch harte Authentifizierungsmechanismen gemäß der europäischen Payment-Services-Richtlinie PSD 2 gehören zur Betrugsprävention.

Als Digitalisierungspartner der Volks- und Raiffeisenbanken hat Atruvia über die Anforderungen von PSD 2 hinaus eine Verifikation per Device-Fingerprinting in die grunderneuerte Onlinebanking-Umgebung eingefügt: Bei einem Kundenlogin über ein bislang nicht verwendetes und daher unbekanntes Endgerät muss dieser erstmalige Zugang zusätzlich durch eine TAN-Freigabe autorisiert werden. Dies erschwert es Kriminellen, gestohlene Zugangsdaten für Betrugsdelikte zu missbrauchen.

Neben harter Authentifizierung verlangt PSD 2 von Banken außerdem die Bewertung sämtlicher Transaktionen im Zahlungsverkehr. Ziel dabei ist es, unberechtigte Transaktionen rechtzeitig zu erkennen und entsprechende Buchungen zu blockieren. Bei bundesweit gut 7,1 Milliarden Banküberweisungen pro Jahr (Stand 2021) ist dies nur durch weitgehend automatisierte Prozesse zu bewerkstelligen.

Die einfachste Variante für eine Bewertungsautomatik wäre etwa ein Echtzeitabgleich der Zielkonten mit einer IBAN-Black-List: Eine solche Liste enthält auffällig gewordene Kontoverbindungen zum Beispiel von sogenannten Fake-Shops, die ihre Opfer mit unrealistisch niedrigen Preisen für hochwertige Markenartikel locken, etwa mit einem Thermomix für 300 Euro. Wer hier bestellt, wartet vergebens auf seine Ware und sieht den überwiesenen Kaufpreis nie wieder – es sei denn, die Bank stoppt die Überweisung, weil die betreffende IBAN in der Black List enthalten ist. Eine generelle Lösung des Problems ist dadurch nicht zu erwarten, da jederzeit neue IBANs für betrügerische Transaktionen genutzt werden können.



LANDAU MEDIA

Schritt 4: Bestimmung des Sentiments

Auf Basis der identifizierten Textpassagen sowie bestimmten Wortkombinationen wird ein Sentiment des Gesamtartikels bestimmt

KI kontra Cyberkriminalität bei Banktransaktionen

Ein Artikel von **Andreas Hermann, Fraud Manager bei Atruvia** | 28.11.2022 - 09:56

Trotz anhaltender Aufklärungskampagnen erlangen Cyberkriminelle immer wieder vertrauliche Zugangsdaten zum Onlinebanking. Um mögliche Schäden durch rechtswidrige Kontobewegungen zu minimieren, setzt Atruvia auf KI- Techniken: Selbstlernende Algorithmen erkennen automatisch verdächtige Transaktionen, sodass entsprechende Buchungen rechtzeitig geprüft und gegebenenfalls blockiert werden können.

Laut aktuellem Lagebericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist Finance Phishing weiter auf dem Vormarsch: Anders als früher jedoch fassen viele Betrüger ihre Phishing-Mails heute nicht nur in fehlerfreiem Hochdeutsch ab, sondern imitieren gestalterisch auch täuschend echt das Corporate Design der vermeintlichen Absenderbank. Obwohl kein Kreditinstitut in Deutschland seine Kundinnen und Kunden von sich aus per E-Mail mit sensitiven Informationsanfragen kontaktieren würde, gelingt es Cyberkriminellen immer wieder, sich mit dieser Phishing-Masche Kontozugangsdaten von arglosen Opfern zu erschleichen.

Vor allem Unwissenheit spielt ihnen dabei in die Hände: Wie das kürzlich vom BSI gemeinsam mit der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) veröffentlichte „Digitalbarometer" zeigt, verzichten noch immer 23 Prozent aller Verbraucherinnen und Verbraucher darauf, sich über Cybergefahren zu informieren. Gut ein Drittel (35 Prozent) tut dies immerhin sporadisch, und nur 16 Prozent halten sich regelmäßig auf dem Laufenden.

Dreiklang aus Prävention, Detektion und Reaktion

Solche Zahlen unterstreichen die Dringlichkeit von Awareness-Kampagnen im Rahmen einer ganzheitlich konzipierten Anti-Fraud-Strategie für Banken. Aber auch harte Authentifizierungsmechanismen gemäß der europäischen Payment-Services-Richtlinie PSD 2 gehören zur Betrugsprävention.

Als Digitalisierungspartner der Volks- und Raiffeisenbanken hat Atruvia über die Anforderungen von PSD 2 hinaus eine Verifikation per Device-Fingerprinting in die grunderneuerte Onlinebanking-Umgebung eingefügt: Bei einem Kundenlogin über ein bislang nicht verwendetes und daher unbekanntes Endgerät muss dieser erstmalige Zugang zusätzlich durch eine TAN-Freigabe autorisiert werden. Dies erschwert es Kriminellen, gestohlene Zugangsdaten für Betrugsdelikte zu missbrauchen.

Neben harter Authentifizierung verlangt PSD 2 von Banken außerdem die Bewertung sämtlicher Transaktionen im Zahlungsverkehr. Ziel dabei ist es, unberechtigte Transaktionen rechtzeitig zu erkennen und entsprechende Buchungen zu blockieren. Bei bundesweit gut 7,1 Milliarden Banküberweisungen pro Jahr (Stand 2021) ist dies nur durch weitgehend automatisierte Prozesse zu bewerkstelligen.

Die einfachste Variante für eine Bewertungsautomatik wäre etwa ein Echtzeitabgleich der Zielkonten mit einer IBAN-Black-List: Eine solche Liste enthält auffällig gewordene Kontoverbindungen zum Beispiel von sogenannten Fake-Shops, die ihre Opfer mit unrealistisch niedrigen Preisen für hochwertige Markenartikel locken, etwa mit einem Thermomix für 300 Euro. Wer hier bestellt, wartet vergebens auf seine Ware und sieht den überwiesenen Kaufpreis nie wieder – es sei denn, die Bank stoppt die Überweisung, weil die betreffende IBAN in der Black List enthalten ist. Eine generelle Lösung des Problems ist dadurch nicht zu erwarten, da jederzeit neue IBANs für betrügerische Transaktionen genutzt werden können.

CONTEXTCLOUD
THE POWER OF CONTEXT

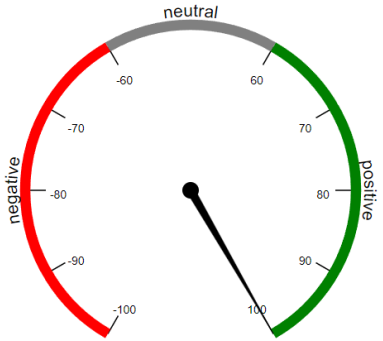
- Home
- Document Enrichment
- Topic Analysis
- Source
- Content Categories
- Relevant Phrases
- Personas
- Risk Categories
- Named Entities
- Sentiment

Collapse

Sentiment

Source document > Atruvia favorisiert künftig Plattformarchitektur über API und Webservices – Daniela Bücker,...

The sentiment of the source text is as follows



WHAT MEANS SENTIMENT?

Text can carry a certain sentiment (or mood), based on usage and combination of certain words.

CONTEXTCLOUD assigns a sentiment value between +1 (very positive) and -1 (very negative).

CONTEXT API

For easy integration **CONTEXT**CLOUD provides a standard REST API for document enrichment

Documentation
programmatic interface

LANDAU MEDIA

Optional Schritt 5: Definierte Reputationsrisiken bestimmen

Auf werden automatisch risikobehaftete Themenfelder erkannt. Es gibt über 18 verschiedene Kategorien, darunter z.B. Nachhaltigkeit (Green Washing), Cyber Security, Waffen, Alkohol, Hate Speech etc.

KI kontra Cyberkriminalität bei Banktransaktionen

Ein Artikel von **Andreas Hermann, Fraud Manager bei Atruvia** | 28.11.2022 - 09:56

Trotz anhaltender Aufklärungskampagnen erlangen Cyberkriminelle immer wieder vertrauliche Zugangsdaten zum Onlinebanking. Um mögliche Schäden durch rechtswidrige Kontobewegungen zu minimieren, setzt Atruvia auf KI- Techniken: Selbstlernende Algorithmen erkennen automatisch verdächtige Transaktionen, sodass entsprechende Buchungen rechtzeitig geprüft und gegebenenfalls blockiert werden können.

Laut aktuellem Lagebericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist Finance Phishing weiter auf dem Vormarsch: Anders als früher jedoch fassen viele Betrüger ihre Phishing-Mails heute nicht nur in fehlerfreiem Hochdeutsch ab, sondern imitieren gestalterisch auch täuschend echt das Corporate Design der vermeintlichen Absenderbank. Obwohl kein Kreditinstitut in Deutschland seine Kundinnen und Kunden von sich aus per E-Mail mit sensitiven Informationsanfragen kontaktieren würde, gelingt es Cyberkriminellen immer wieder, sich mit dieser Phishing-Masche Kontozugangsdaten von arglosen Opfern zu erschleichen.

Vor allem Unwissenheit spielt ihnen dabei in die Hände: Wie das kürzlich vom BSI gemeinsam mit der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) veröffentlichte „Digitalbarometer" zeigt, verzichten noch immer 23 Prozent aller Verbraucherinnen und Verbraucher darauf, sich über Cybergefahren zu informieren. Gut ein Drittel (35 Prozent) tut dies immerhin sporadisch, und nur 16 Prozent halten sich regelmäßig auf dem Laufenden.

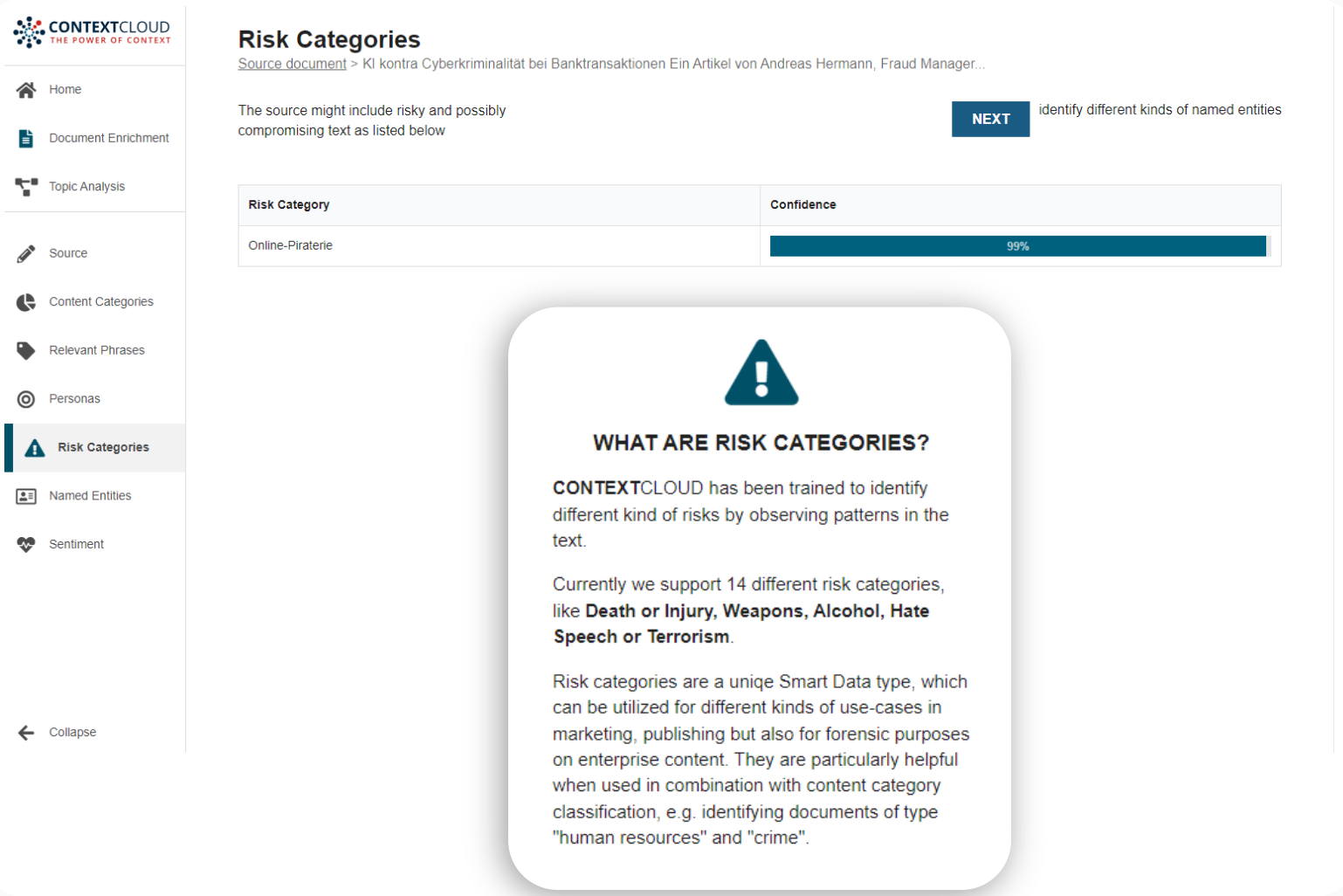
Dreiklang aus Prävention, Detektion und Reaktion

Solche Zahlen unterstreichen die Dringlichkeit von Awareness-Kampagnen im Rahmen einer ganzheitlich konzipierten Anti-Fraud-Strategie für Banken. Aber auch harte Authentifizierungsmechanismen gemäß der europäischen Payment-Services-Richtlinie PSD 2 gehören zur Betrugsprävention.

Als Digitalisierungspartner der Volks- und Raiffeisenbanken hat Atruvia über die Anforderungen von PSD 2 hinaus eine Verifikation per Device-Fingerprinting in die grunderneuerte Onlinebanking-Umgebung eingefügt: Bei einem Kundenlogin über ein bislang nicht verwendetes und daher unbekanntes Endgerät muss dieser erstmalige Zugang zusätzlich durch eine TAN-Freigabe autorisiert werden. Dies erschwert es Kriminellen, gestohlene Zugangsdaten für Betrugsdelikte zu missbrauchen.

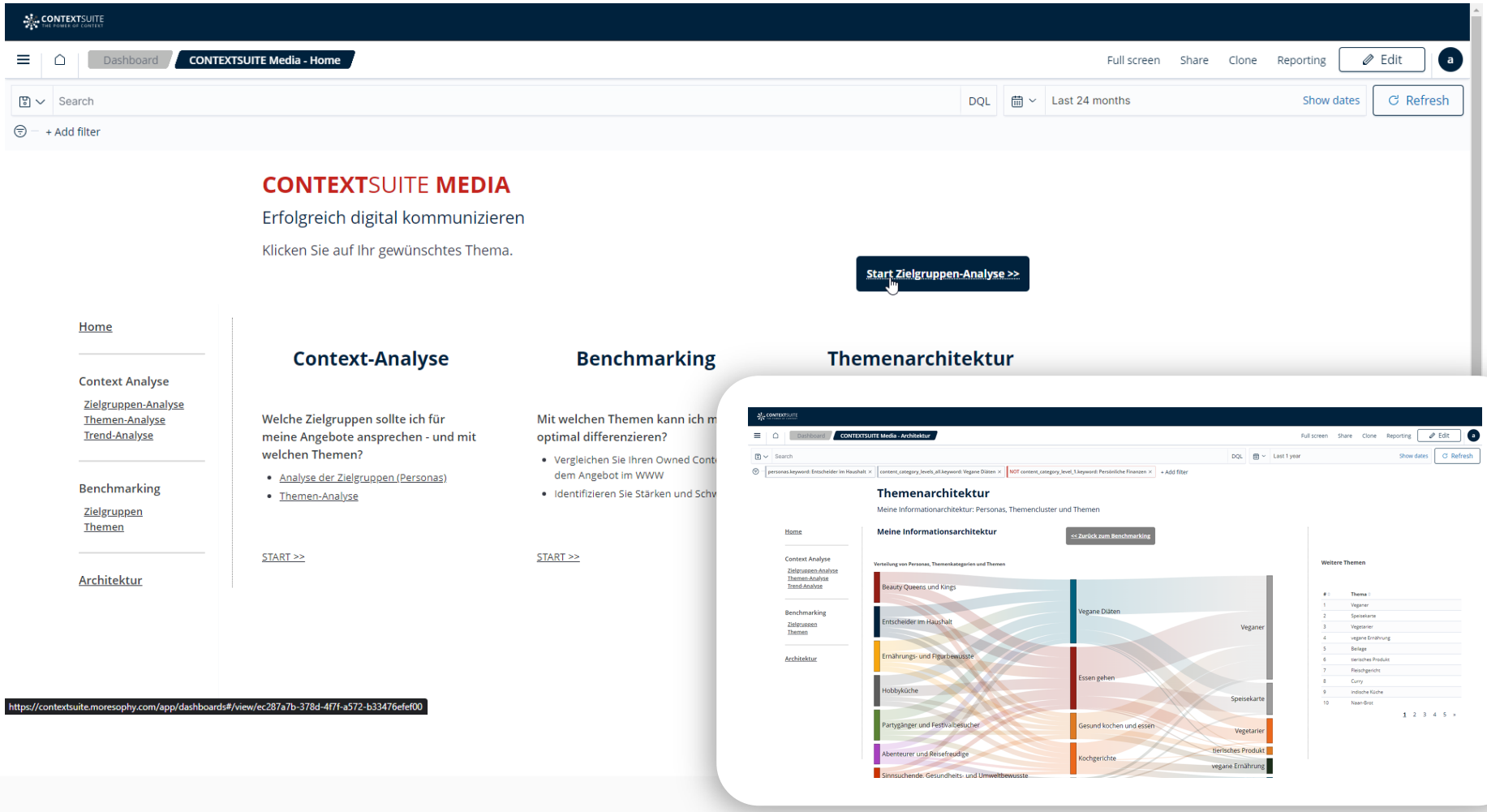
Neben harter Authentifizierung verlangt PSD 2 von Banken außerdem die Bewertung sämtlicher Transaktionen im Zahlungsverkehr. Ziel dabei ist es, unberechtigte Transaktionen rechtzeitig zu erkennen und entsprechende Buchungen zu blockieren. Bei bundesweit gut 7,1 Milliarden Banküberweisungen pro Jahr (Stand 2021) ist dies nur durch weitgehend automatisierte Prozesse zu bewerkstelligen.

Die einfachste Variante für eine Bewertungsautomatik wäre etwa ein Echtzeitabgleich der Zielkonten mit einer IBAN-Black-List: Eine solche Liste enthält auffällig gewordene Kontoverbindungen zum Beispiel von sogenannten Fake-Shops, die ihre Opfer mit unrealistisch niedrigen Preisen für hochwertige Markenartikel locken, etwa mit einem Thermomix für 300 Euro. Wer hier bestellt, wartet vergebens auf seine Ware und sieht den überwiesenen Kaufpreis nie wieder – es sei denn, die Bank stoppt die Überweisung, weil die betreffende IBAN in der Black List enthalten ist. Eine generelle Lösung des Problems ist dadurch nicht zu erwarten, da jederzeit neue IBANs für betrügerische Transaktionen genutzt werden können.



Perspektive: Einrichtung einer Context Suite

Auf Basis eines bereits bestehenden Sprachmodells von Moresophy trainiert Landau Media ein individuelles Sprachmodell zur Identifizierung und Verfolgung von Themen und Stakeholdern



Behalten Sie den Überblick

Landau Media GmbH & CO. KG

Friedrichstrasse 30
10969 Berlin

T.: +49 (0) 30 20 242 - 100
F.: +49 (0) 30 20 242 - 101

info@landaumedia.de
landaumedia.de
facebook.com/landaumedia
twitter.com/landaumedia
youtube.com/LandauMediaAG

Oliver Plauschinat
RESEARCH & INSIGHTS