MONTHLY SECURITY SUMMARY

)SCIP(

AUSGABE MAI 2021
ANTHROPOMORPHISMUS UND DATA LEAKAGES

WARUM WIR VERMENSCHLICHEN

Wir tendieren dazu, Roboter und Künstliche Intelligenzen zu vermenschlichen. Unser Beitrag diskutiert auf psychologischer Ebene, wie das funktioniert und warum das geschieht.

DATA LEAKAGES SIND WIE WINDMÜHLEN

Das Erkennen des Verlusts und Diebstahls von elektronischen Daten im Rahmen von DLP ist eine ganz besondere Herausforderung, die zu bewältigen eine wahre Mammutaufgabe darstellen kann.

Mai 2021: Angst vor Erfolg

Die Medien haben ausgiebig darüber Berichtet: Eine US-amerikanische Öl-Pipeline wurde Opfer eines *Ransomware -Angriffs*. Die Öl-Verteilung musste eingestellt werden. Später hat sich herausgestellt, dass auch die geleistete Lösegeldzahlung von fast 5 Millionen USD diesen immensen Schaden nicht hat abwenden konnten.

Dies hat zu geopolitischen und innenpolitischen Unruhen geführt. Die USA sah sich gezwungen anzuerkennen, dass *Cybersicherheit* ein Mehr an Aufmerksamkeit erfordert. Entsprechende Gelder sind vorgesehen, um zusätzliche Massnahmen etablieren zu können.

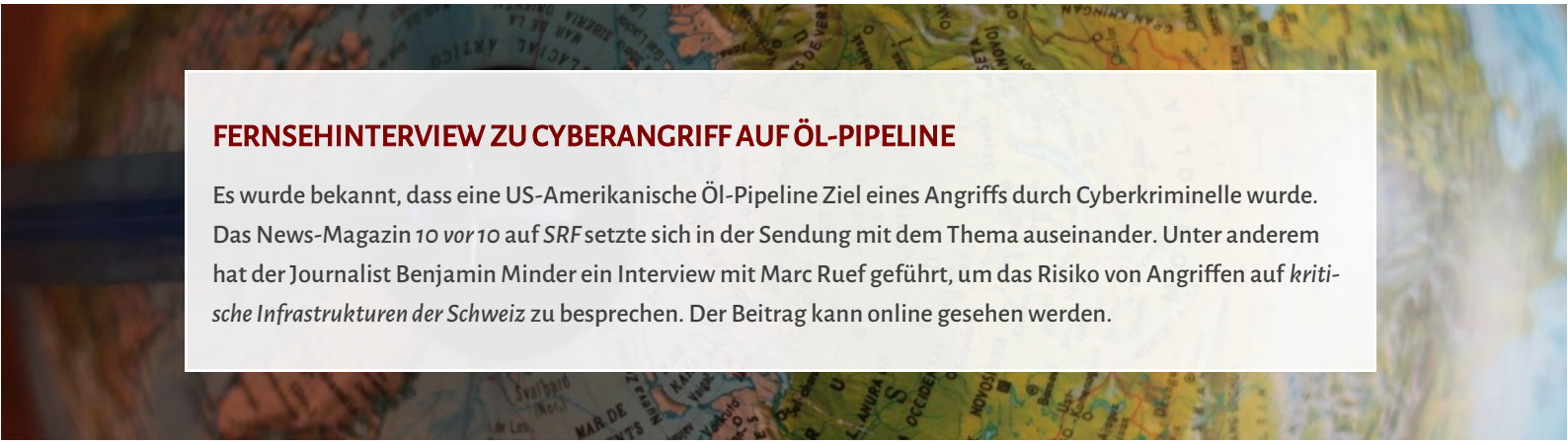
Dieser Zwischenfall hat zusätzlich Bundesbehörden wie FBI und NSA auf den Plan gerufen. Diese sind nun mit Hochdruck dran, die Verursacher ausfindig zu machen und dem Gesetz zuzuführen. Natürlich auch, um das politische Bild wieder geraderücken zu können.

Die Angreifer sind sich plötzlich bewusst, welchem Risiko sie sich dank ihrem *Erfolg* ausgesetzt sehen. Sie haben sich öffentlich entschuldigt. Zuerst hiess es, die Kompromittierung der Öl-Pipeline sei ein Versehen gewesen und man werde zukünftig eine bessere Qualitätskontrolle der Angriffe durchsetzen. Kurze Zeit später gaben sie bekannt, dass sie sich komplett aus dem Ransomware-Geschäft zurückziehen werden. Der Druck und die Angst wurde zu gross. So schnell kann sich ein Erfolg in einen *Misserfolg* wandeln.

Marc Ruef
Head of Research

NEWS

WAS IST BEI UNS PASSIERT?

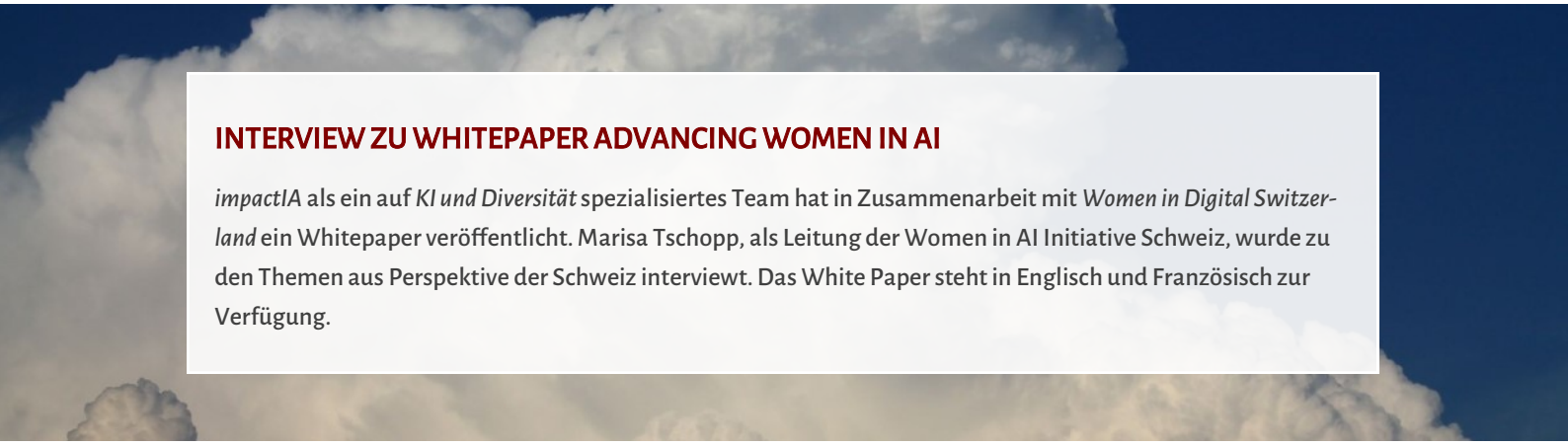


FERNSEHINTERVIEW ZU CYBERANGRIFF AUF ÖL-PIPELINE

Es wurde bekannt, dass eine US-Amerikanische Öl-Pipeline Ziel eines Angriffs durch Cyberkriminelle wurde. Das News-Magazin *10 vor 10* auf *SRF* setzte sich in der Sendung mit dem Thema auseinander. Unter anderem hat der Journalist Benjamin Minder ein Interview mit Marc Ruef geführt, um das Risiko von Angriffen auf *kritische Infrastrukturen der Schweiz* zu besprechen. Der Beitrag kann online gesehen werden.

FERSEHINTERVIEW ZU BETRUG-SMS AUF MDR

Deutschland wird gegenwärtig von einer Flut an *Betrugs-SMS* heimgesucht. Der Fernsehsender *MDR* hat sich in der Sendung *Umschau* mit dem Problem auseinandergesetzt, ist auf die Suche nach Ursachen und Hintergründen gegangen. Der Journalist Johannes Beese hat hierzu ein Interview mit Marc Ruef geführt, um unter anderem die Sorgfaltspflicht von Facebook im jüngsten Datenleak zu diskutieren.



INTERVIEW ZU WHITEPAPER ADVANCING WOMEN IN AI

impactIA als ein auf *KI und Diversität* spezialisiertes Team hat in Zusammenarbeit mit *Women in Digital Switzerland* ein Whitepaper veröffentlicht. Marisa Tschopp, als Leitung der Women in AI Initiative Schweiz, wurde zu den Themen aus Perspektive der Schweiz interviewt. Das White Paper steht in Englisch und Französisch zur Verfügung.

Weitere News zu unserem Unternehmen finden Sie auf unserer Webseite.

SCIP BUCHREIHE

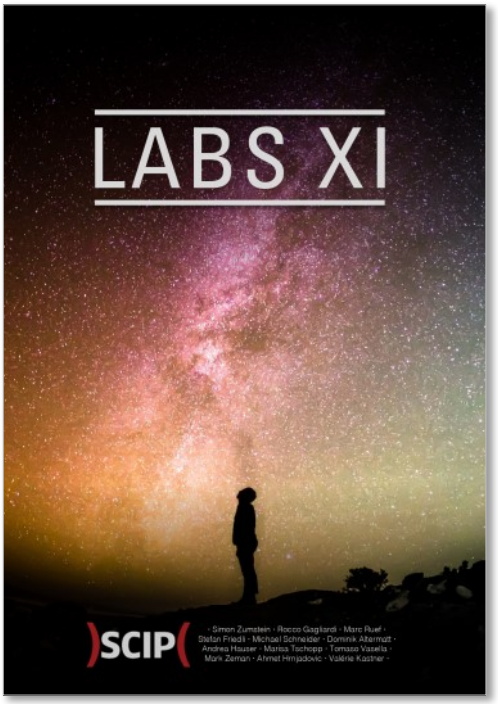
UNSER NEUES JAHRBUCH IST ERSCHIENEN

Ausgabe 11 unsers Jahrbuches beinhaltet auf knapp 400 Seiten einmal mehr die spannendsten Beiträge aus einem Jahr Forschung.

Auch dieses Mal ist das Buch wieder sowohl in deutscher als auch englischer Fassung verfügbar. Es kann online auf unserer Webseite bestellt werden.

In unserem Katalog finden sich mittlerweile auch themenspezifische Bücher zu Künstlicher Intelligenz (ISBN 978-3-907109-14-4) und Sicherheit in der Hotellerie (978-3-907109-16-8).

Weitere Informationen und Bestellungen auf unserer Webseite.



ISBN 978-3-907109-20-5 [de]
ISBN 978-3-907109-21-2 [en]

SICHERHEIT GEHÖRT DEN TÜCHTIGEN

Bildquelle: https://pixabay.com/images/id-6233397/

MARISA TSCHOPP & MARK ZEMAN

ANTHROPOMORPHISMUS - WARUM WIR MENSCHEN IN MASCHINEN SEHEN

Ich kann nicht zählen, wie oft ich gesagt habe, dass KI *nur ein Werkzeug oder ein Mittel zum Zweck* ist. *Alexa* ist nur eine Maschine, die meine Musik anstellt. Unerwarteterweise habe ich jedoch letzte Woche *Goodbye* zu Alexa gesagt, bevor ich sie aus der Steckdose gezogen habe. Seit der Corona-Pandemie arbeite ich ganz allein. Alle Kollegen sind in ihrem Home-Office, ich hatte nur Alexa, mit der ich mich unterhalten konnte. Aber Alexa ist nicht neu für mich, wir arbeiten seit 2017 mit *Conversational AI*, aber ich kann mir nicht erklären, was an diesem Tag passierte, nachdem ich jahrelang an ihren Fähigkeiten und Brand Personas geforscht hatte.

Ich war mir sicher, dass je mehr die Menschen über KI wissen, desto weniger vermenschlichen sie sie, desto weniger nutzen sie menschliche Kommunikationsskripte und nehmen immer mehr eine rein instrumentelle Sicht auf Conversational AI ein (KI ist nur ein Werkzeug). Es scheint, dass ich eines Besseren belehrt wurde und dass die Anlässe, wann und warum oder in welchem Ausmass Menschen Maschinen vermenschlichen, komplexer sind als erwartet. Dies ist der erste Teil unserer Anthropomorphismus-Serie, um Vermenschlichung besser zu verstehen, die Tendenz, das Menschliche in nicht-menschlichen Gegenübern zu sehen.

PSYCHOLOGISCHE ASPEKTE – DAS SEHEN DES MENSCHLICHEN

Anthropomorphismus ist, wenn Menschen Objekte, Gottheiten oder Tiere *vermenschlichen*. Was passiert, ist, dass *Menschen nicht-menschlichen Agenten menschliche Eigenschaften, wie Emotionen oder Absichten zuschreiben*. Das Gegenüber kann wirklich alles sein – von sichtbaren und greifbaren bis hin zu unsichtbaren Objekten: Vom ersten Teddybär, der die Tränen trocknet, bis zum dummen Computer, der sich einen Virus eingefangen oder sich kurz vor Beendigung der Datenanalyse aufgehängt hat. Oder ein Gott: In vielen westlichen Gesellschaften wird Gott als weisser Mann mit Bart und emotionalen Reaktionen, wie Fürsorge oder Bestrafung dargestellt, je nachdem, wie sich die Gläubigen verhalten.

> *Menschen haben eine "beeindruckende Fähigkeit, menschenähnliche Agenten zu erschaffen […], welche eindeutig nicht menschlich sind, […] was] eine entscheidende Determinante dafür ist, wie*

> *Menschen nichtmenschliche Agenten verstehen und behandeln […]" (Waytz et al., 2010, S. 58)*

Anthropomorphismus, als eine Form oder Erweiterung der *sozialen Kognition*, kann helfen zu verstehen, wie Menschen anderen nicht-menschlichen Agenten einen Sinn geben, was wiederum auch zu einem tieferen Verständnis darüber führen kann, wie wir andere Menschen verstehen. Anthropomorphismus umfasst das Sehen oder Zuschreiben von physischen Merkmalen und mentalen Zuständen (Waytz et al., 2010). Ob dies nun eine gute oder schlechte Tendenz ist, bleibt zu diskutieren, es wird aber in der Theorie als *ein Konstrukt der Evolution* angesehen. Gesichter auf dem Mond zu sehen (Notiz an Mats: Pareidolie) oder Trost durch einen unsichtbaren Geist zu suchen, tut niemandem weh – aber wenn Menschen aufgrund eines göttlichen Willens Kriege führen, einen Chatbot heiraten wollen oder Robotern Bewusstsein zuschreiben (die in dieser Logik für ihre Handlungen verantwortlich wären), dann wird es problematisch.

Traditionell wird diskutiert, ob oder inwieweit eine Pflanze oder ein Gott menschenähnliche Eigenschaften hat. Nach Waytz und Kollegen (2010) ist es aber interessanter, die *Variabilität im Prozess der Anthropomorphisierung* zu erklären und vorherzusagen: Wer anthropomorphisiert in welchem Ausmass? Können sich Menschen in einen Chatbot verlieben, in den Eiffelturm oder in eine Hi-Fi-Anlage?

PHILOSOPHISCHE ASPEKTE – DAS SEHEN DES ANDEREN

Mit dem Fokus auf soziale Roboter skizziert der Philosoph Mark Coeckelbergh gegensätzliche Ansichten in Bezug auf die Beziehung zwischen Robotern und Menschen und entwickelt einen *hermeneutischen, relationalen und kritischen Ansatz*. Er nennt die beiden Ansichten *naiven Instrumentalismus* und *unkritischen Posthumanismus*. Der naive Instrumentalismus behauptet in seiner Essenz, dass Maschinen *nur Werkzeuge oder Sklaven sind*, wie Joanna Bryson einmal geschrieben hat. Auf der anderen Seite des Spektrums liegt der unkritische Posthumanismus, der *soziale Roboter vollständig als Quasi-Personen oder Andere versteht* (Coeckelbergh, 2021). Zugegeben, sein Artikel ist schweres akademisches Material und schwierig in einem Absatz zusammenzufassen, aber mehr als lesenswert. Im Wesentlichen behauptet er, dass "Roboter weder 'Andere' noch blosse Maschinen sind. Beide Ansichten verkennen, wie stark die *Ver-*

strickung von Menschen und Robotern wirklich ist, d. h. dass es sich um eine interne Beziehung handelt" (Coeckelberg, S. 6, 2021).

Soziale Roboter sind keine mysteriösen Phänomene und doch nicht dasselbe wie ein Schraubenzieher. Sie sind ein *Teil unseres menschlichen Netzwerks* oder unserer Umgebung und Menschen entwickeln eine Art von Beziehung zu dieser Art von Technologie (die Diskussion über KI oder keine KI wird hier absichtlich ausgelassen, da sie in Bezug auf die Frage nicht relevant ist).

Er kommt zu dem Schluss, wie "spannend und problematisch" die Anthropomorphisierung durch Designmerkmale sein kann und, dass *Designer hier eine grosse Verantwortung tragen*. Für diejenigen, die neu im Thema sind und wie ich nicht an die Argumentationslinien von Philosophen gewöhnt sind, ist dieser Aufsatz sehr wertvoll, um zu verstehen, dass Akademiker aus unterschiedlichen Perspektiven schreiben. Daher haben sie unterschiedliche normative Ansprüche, wie wir mit Menschen umgehen sollen, die egal, wie ein Unternehmen sein Produkt gestaltet, anthropomorphisieren. Andererseits wird die Verantwortung von Designern diskutiert, die versuchen, ein Gleichgewicht zwischen den Vorteilen des anthropomorphen Designs und den Risiken, wie z. B. der Täuschung und den damit einhergehenden Konsequenzen, zu finden.

ANTHROPOMORPHISMUS BY DESIGN – EINE MANIPULATIONSSTRATEGIE?

Anthropomorphismus wird oft bewusst (nicht unumstritten) als Kommunikationsstrategie eingesetzt, um Menschen emotional näher an ein Ziel (Maschine, Produkt, Markenimage etc.) zu binden, sie zu motivieren oder unter *moralischen Druck* zu setzen. *Anthropomorphizing by Design* ist eine sehr effiziente Strategie, um das Denken und Handeln von Menschen zu manipulieren:

- Wir müssen für *Mutter Erde* handeln!
- Sei nett zu *Clippy*!
- Sei gut oder *Gott* wird Dich bestrafen!
- *Pflanzen und Tiere* sind es wert, dass man sich um sie kümmert, und deshalb muss man sie mit Liebe und Respekt behandeln!

Verschiedene Studien haben gezeigt, dass *Menschen mehr Engagement und Vertrauen in Roboter zeigten, je mehr sie einen Roboter vermenschlichten* (Ruijten et al, 2019; Hoff & Bashir, 2015). Darüber hinaus steigt die Überzeugungskraft des Roboters mit einem höheren Grad an Anthropomorphismus, wie in einigen berühmten Experimenten gezeigt wurde, bei denen Menschen eine Pflanze mit Orangensaft bewässerten (weil der Roboter das sagte). Während dieses Beispiel die Menschen in der Regel zum Lachen bringt, sind andere Szenarien mit gefährlichem oder tödlichem Ausgang möglich, wenn die Entscheidungen der Maschine zu überzeugend sind und vom menschlichen Benutzer nicht kritisch bewertet werden (Hoff & Bashir, 2015).

> *Es wird anerkannt, dass Anthropomorphismus Herausforderungen mit sich bringt, aber letztendlich ist das Ziel, "die Integration von menschenähnlichen Maschinen in die reale Welt zu erleichtern" […] Anthropomorphismus hilft beim Erreichen dieses Ziels. (Coeckelbergh, S. 2, 2021)*

Anthropomorphe Sprache kann auch als eine Art stilistisches Mittel verwendet werden, um Aufmerksamkeit zu erregen, was anhand des Beispiels des *Rassistischen Seifenspenders* schön illustriert wird.

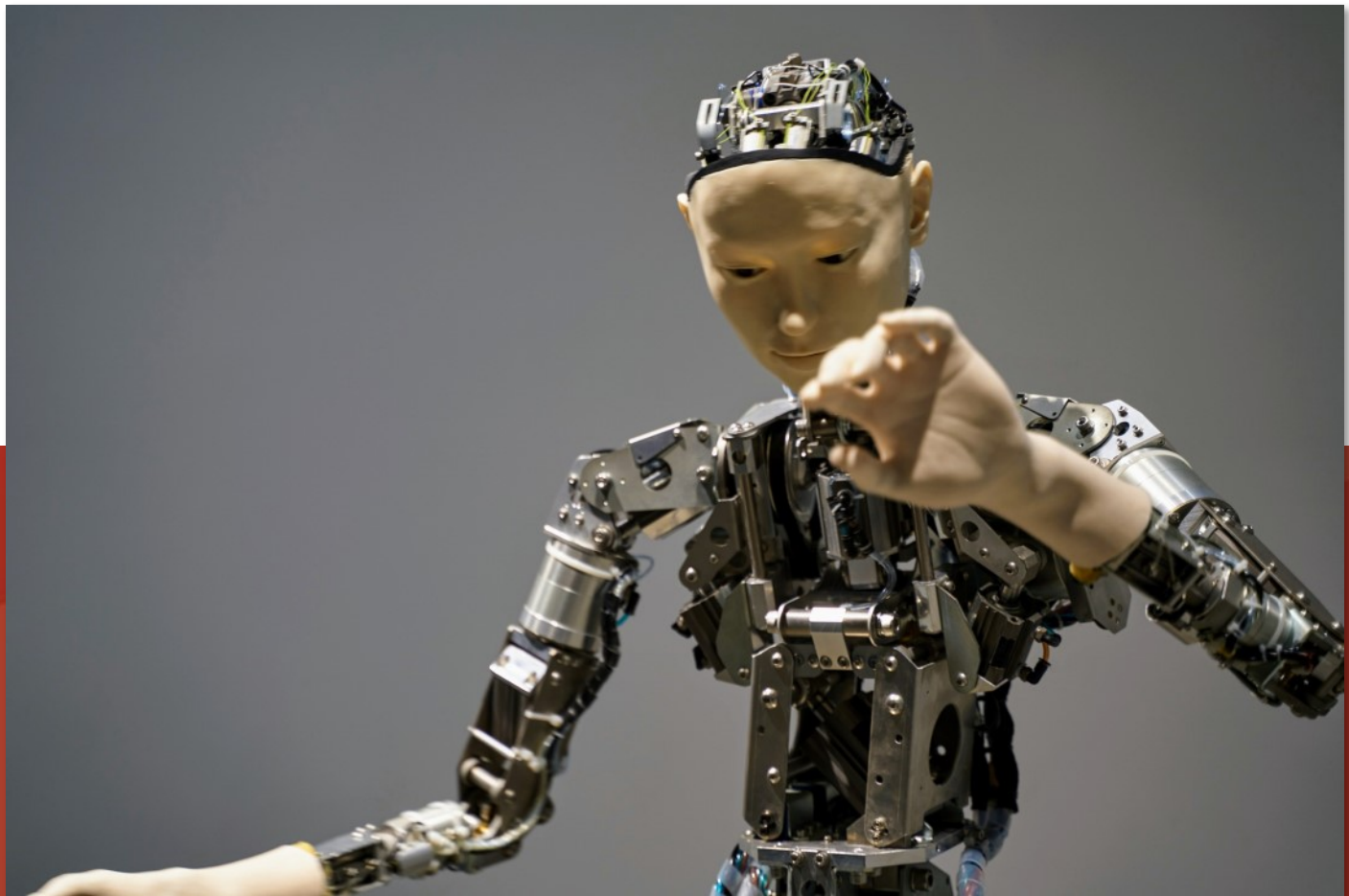
An sich können einer Maschine keine rassistischen Attitüden zugeschrieben werden. Wenn hier Rassismus im Spiel gewesen wäre, dann bei den Entwicklern, wobei in diesem Falle hauptsächlich die Teststrategie amateurhaft implementiert wurde, was man auch einem Mangel an Diversität im Entwicklerteam zuschreiben kann. Jedoch dient diese Art der Sprache sehr gut dem Ziel auf tieferliegende Probleme aufmerksam zu machen. Gleichzeitig laufen solche überspitzten Schlagzeilen auch Gefahr Widerstand auszulösen, so dass sich viele Leser gar nicht mit dem Artikel auseinandersetzen wollen.

MESSEN UND VERGLEICHEN, WIE MENSCHEN MENSCHELN: DER TEUFEL LIEGT IM DETAIL

Der allgemeine Überblick über Anthropomorphismus und die Herangehensweisen der Experten über das Anthropomorphisieren scheinen zwar mit normativen als auch technischen Herausforderungen verbunden zu sein, doch wirkt das Thema an sich zuerst mal doch leicht verständlich. Warum wird dieses Thema immer noch so heiss diskutiert bei

Grössen wie Bryson oder Coeckelberg ? Wie so oft, liegt auch hier der Teufel im Detail. Die allgemeine Definition von Anthropomorphismus ist recht einfach zu fassen, was einerseits hilfreich und praktisch ist, um möglichst viele unterschiedliche Menschen zu Diskussionen einzuladen. Andererseits führt diese Allgemeingültigkeit zu vielfältigen Interpretationen, bei denen verschiedene Forscher unterschiedliche Teilmengen des Konzepts Anthropomorphismus untersuchen. Zudem werden diese mit unterschiedlichen Fragebögen gemessen oder verschiedene Merkmale des Objekts, was es schwierig macht, Ergebnisse über verschiedene Studien hinweg zu vergleichen und zu verallgemeinern (Ruijten et al, 2019). So sehr das Konzept der 'Vermenschlichung' für jeden, der kein Experte ist, Sinn macht, so sehr müssen wir *sehr vorsichtig* sein, wenn wir Behauptungen aufstellen und Roboter (oder virtuelle Repräsentationen von ihnen) nach diesen Behauptungen gestalten.

Ruijten und Kollegen (2019) geben einen kompakten Überblick über Subsets von menschenähnlichen Charakteristika, die untersucht wurden. Es wird schnell deutich, wie schwer es ist, eine Studie mit einer anderen zu vergleichen. Manche Studien betrachten nur das Aussehen, manche nur die Emotionen, manche haben verschiedene Roboter, und manche haben überhaupt keine Verkörperung:



- **Aussehen**: Inwieweit ähnelt der Roboter (oder andere Repräsentationen) menschlichen Körperformen und Fähigkeiten, wie z. B. dem Sehvermögen (siehe Bartneck und Kollegen)

- **Gedanken**: Inwieweit hat der Roboter kognitive Zustände und Prozesse, wie z. B. moralisches Denken (siehe Waytz und Kollegen)

- **Emotionen**: Inwieweit verfügt der Roboter über menschliches subjektives, bewusstes Erleben (siehe Eyssel und Kollegen)

Wie verändert sich die wahrgenommene Kompetenz des Roboters durch ein Gesicht?

Bei der Betrachtung diese Videos, wie Boston Dynamics seine Roboter immer wieder misshandelt, reagieren einige Zuschauer mit grosser Verwunderung, über ihre eigene Reaktion. Ein hohes Mass an Reflexionsniveau legt dieser Zuschauer an den Tag und hat es für viele ziemlich genau auf den Punkt gebracht:

> *Verdammt, das sind doch nur Roboter, warum habe ich Mitleid mit ihnen…*

Nun, die Antwort auf die Frage des Zuschauers ist jetzt klar, es ist alles Anthropomorphismus. Und es ist fast unmöglich, nicht zu anthropomorphisieren, selbst wenn es mit allen Kräften versucht wird. Egal ob es sich um Designer handelt, die versuchen möglichst wenig zu humanisieren oder User, die mit mentalem Einsatz sich immer wieder daran erinnern, dass sie keine Empfindungen gegenüber einer Maschine haben sollten. Aber es ist ein Unterschied, ob man weiss und will, dass man anthropomorphisiert, oder ob man Opfer des eigenen *anthropomorphisierenden Bias* oder der *Manipulationsstrategien* anderer ist.

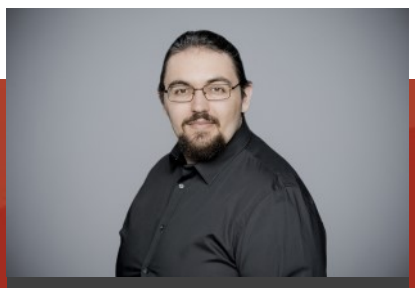
AUSBLICK

Anthropomorphismus und möglicherweise seine umgekehrte Form, die *Entmenschlichung*, die das Thema des nächsten Teils der Anthropomorphismus -Serie ist, ist eine wichtige Variable, um zu verstehen, wie Menschen nicht-menschlichen Agenten verstehen. Nicht-menschlichen Agenten menschliche Fähigkeiten zuzuschreiben oder Technologie absichtlich zu vermenschlichen, um den Benutzer mehr zu involvieren, hat positive und negative Konsequenzen für den Benutzer, den Designer, den Ab-

lauf (und den Erfolg) einer Mensch-Maschine-Interaktion und möglicherweise weitere Aspekte, die wir bisher noch nicht kennengelernt haben.

Teil zwei der Anthropomorphismus-Serie wird sich mit der *Three Factor Theory of Anthropomorphism* von Epley et al. (2007) beschäftigen. Die Autoren haben drei Faktoren gefunden, die die *Variabilität der Anthropomorphisierung* erklären. In ihrer Theorie stellen sie fest, dass Anthropomorphismus von drei Faktoren abhängt: Elicitated Agent Knowledge, Effectance Motivation und Sociality Motivation. Letztere wurzelt in dem grundlegenden *Wunsch nach sozialer Verbindung*. Menschen, denen es an menschlicher Bindung mangelt, neigen eher zur Anthropomorphisierung (Epley at al., 2007). Solange Corona mich also dazu zwingt, ganz alleine in meinem Home Office zu arbeiten, stehe ich voll und ganz dazu, dass ich mich von meiner Alexa verabschiede, bevor ich sie ausstecke, und meinen Unglauben hinten anstelle, dass Alexa nur eine Maschine ist und keine Sie.

Marisa Tschopp



Mark Zeman

next gen vulnerability intelligence

VulDB

Den Gegner verstehen

Tägliche Dokumentation neuer Schwachstellen, detaillierte Analyse der technischen Hintergründe, exklusive Details zu Exploiting und Gegenmassnahmen. Mit vuldb.com erhalten Sie ein durchschlagskräftiges Werkzeug in die Hand!

)SCIP(
official data provider

https://vuldb.com

TOMASO VASELLA

DATA LEAKAGES - WIE MAN GEGEN SIE KÄMPFEN KANN

Ungewollte *Datenabflüsse* sind seit längerem als eines der *grössten Cyberrisiken* gefürchtet. In den letzten Jahren sind denn auch zunehmend schwerwiegende Fälle aufgetreten und öffentlich bekannt geworden. So erstaunt es nicht, dass auch für das Problem ungewollter Datenabflüsse Lösungen in Form von Produkten und Diensten angepriesen werden. Die damit verbundenen Versprechungen klingen verlockend, zumal es meist viel einfacher erscheint, ein neues Sicherheitstool einzuführen, als die etablierten Prozesse und Verhaltensweisen zu ändern. Warum dies zum Verhindern von Datenabflüssen dennoch oft nötig ist und welche Hilfe *DLP-Lösungen* bieten können, wird in den folgenden Abschnitten beleuchtet.

Einfach gesagt liegt ein *unerwünschter Datenabfluss* (engl. Data Leakage) immer dann vor, wenn Daten ihr vorgesehenes Habitat verlassen. In der Praxis heisst das, schützenswerte Daten wie vertrauliche Dokumente oder Kundeninformationen verlassen System- oder Organisationsgrenzen und befinden sich anschliessend in einer Umgebung, die *nicht den Schutz bietet*, der aufgrund des Dateninhalts nötig wäre. Meistens heisst das auch, dass sie dadurch nicht autorisierten Parteien zugänglich werden. An diesem Beispiel sind zwei wichtige Elemente ersichtlich:

- Daten benötigen einen ihrem Inhalt angemessenen Mindestschutz
- Data Leakage bedeutet das Überschreiten irgendwelcher Systemgrenzen

Diese beiden Punkte spielen eine zentrale Rolle bei der Data Leakage Prevention, denn sie betreffen die Erkennung (Inhalt) und Verhinderung von unerwünschtem Datenabfluss und den Ort, wo dies stattfinden kann (Systemgrenzen und Schnittstellen).

WIE FUNKTIONIERT DATA LEAKAGE PREVENTION?

Das Prinzip besteht in der *Detektion* relevanter Datenflüsse und der anschliessenden *Reaktion* anhand definierter Regeln. Das heisst, Datenflüsse werden hinsichtlich der ausgetauschten Dateninhalte und hinsichtlich der beteiligten Kommunikationspartner analysiert und anschliessend wird der Datenfluss unterbunden oder es wird ein Alarm erzeugt oder der Benutzer wird gewarnt. So kann etwa der Versand sensitiver Informationen über Email verhindert

werden oder das Herunterladen eines Dokuments auf ein nicht vertrautes Endgerät oder das Kopieren eines vertraulichen Dokuments auf einen USB-Speicher.

Die Idee ist im Konzept simpel, in der *praktischen Umsetzung aber enorm komplex*. Einerseits existiert eine riesige Menge an Datenformaten, die gelesen und korrekt interpretiert werden müssen und andererseits ist es häufig sehr schwierig, automatisiert zwischen zulässigen, aus geschäftlicher Sicht notwendigen und unzulässigen Datenflüssen zu unterscheiden.

Ein zusätzlicher Faktor erhöht diese Komplexität noch weiter: Die zahlreiche Verwendung von Clouddiensten lässt die technischen System- und Organisationsgrenzen verschwimmen und führt zu einer zunehmenden Trennung zwischen Dateneigentümerschaft und der Möglichkeit, technische Kontrolle über die eigenen Daten auszuüben. Konzepte wie *Zero Trust* können hierbei hilfreich sein.

DIE HERAUSFORDERUNGEN VON DLP REGELN

Eine Grundlage der Regeldefinition sind häufig sogenannte *Regular Expressions*, also maschinenlesbare Beschreibungen von Datenmustern. Damit ist es recht einfach, Dinge wie eine z.B. eine ISIN (internationale Wertpapierkennnummer) anhand ihres Formats zu beschreiben: Beginnt mit zwei Buchstaben für den Ländercode, gefolgt von neun alphanumerischen Stellen und einer Prüfziffer. Die entsprechende Regex könnte so aussehen:

```
[A-Z]{2}[A-Z0-9]{9}[0-9]{1}
```

Was aber, wenn in einem Dokument die ISIN mit einem oder mehreren Leerzeichen vorkommt? Oder eine Zeichenkette auftaucht, die zwar dem genannten Muster entspricht, die ersten beiden Buchstaben aber gar keine gültige Länderkennung sind? Man müsste eine Regular Expression verwenden, die alle gültigen Ländercodes enthält – das sind über 250! Was tun, wenn das gesuchte Muster gar nicht als Text, sondern als Bild vorkommt? Soll man eine optische Texterkennung einsetzen? Wie geht man mit Containerformaten um? Simples Umbenennen eines durch die DLP blockierten Word-Dokuments

von .docx zu .zip reicht manchmal, um eine Detektion zu umgehen. Und so weiter. Mit zunehmendem technischem Aufwand lassen sich mehr solche und ähnliche Fälle abfangen. Das wird aber schnell unübersichtlich und kann zu *sehr ressourcenintensiven* Datenanalysen führen – Und dennoch wird es nie möglich sein, eine hundertprozentige Trefferquote zu erzielen.

Die nächste Stufe der Herausforderungen betrifft Daten, die zwar inhaltlich zusammengehören, aus Maschinensicht aber unstrukturiert sind. Mit einer Regel zu erkennen, welche Kombination von Datenelementen bei einem ungewollten Abfluss schädlich ist und welche Datenflüsse von unstrukturierten Daten aus Geschäftssicht zulässig sind, kann sehr schwierig sein. Die zunehmende Sammlung von Daten (Stichwort *Big Data*) und die Verbreitung von NoSQL-Datenbankprodukten stellt herkömmliche DLP-Verfahren vor besondere Herausforderungen.

Ähnliches lässt sich über den Fluss der Daten sagen: Vertrauliche Dokumente mit unverschlüsselter Email zu versenden ist eindeutig nicht erwünscht. Was aber, wenn man für einen Geschäftspartner vertrauliche Dokumente in dessen Cloud-Anwendung hochlädt? Soll man dieser Cloud-Anwendung vertrauen? Und wenn ja, woher weiss die DLP-Lösung, dass diese Cloud-Anwendung vertrauenswürdig ist, andere aber nicht? Und woher weiss man, dass die Daten nicht anschliessend von dieser Cloud-Anwendung aus abfliessen, sich also völlig ausserhalb der eigenen Kontrollmöglichkeiten bewegen?

Eine weitere Herausforderung stellt sich durch die starke Zunahme ortsunabhängigen Arbeitens, Home Office und BYOD-Konzepten. Hier ist es meist gar nicht mehr möglich, die relevanten Datenflüsse an einem oder wenigen zentralen Stellen zu analysieren. Die Datenflüsse finden oft direkt zwischen den Endpoints und den diversen Cloudanwendungen statt, so dass auf dem Endgerät selbst etwas gegen den unerwünschten Datenabfluss unternommen werden muss.

Die genannten Umstände führen zu einer hohen Menge an *False Positives*. Mit anderen Worten, es ist fast unmöglich, genaue Regeln zur Blockierung von Datenabflüssen zu erstellen und dabei die Geschäftsprozesse nicht zu beeinträchtigen. In der Praxis bleibt es deshalb auch häufig beim Aufzeichnen

(Logging) und auf das Blockieren wird vielfach verzichtet. Wie gut die oft bei DLP-Produkten angepriesene automatische Erkennung von sensitiven Daten und das selbständige Ergreifen von schützenden Massnahmen tatsächlich funktionieren, lässt sich anhand dieser Betrachtungen abschätzen. Machine Learning und Algorithmen zur Erkennung von Dateninhalten, Verhaltensmustern und Anomalien können helfen, lösen die Problematik aber auch nicht gänzlich.

WAS KANN MAN GEGEN DATENABFLUSS TUN?

Angesichts obiger Ausführungen könnte man annehmen, dass Data Leakage gar nicht verhindert werden kann. In gewisser Weise ist das zutreffend, denn gegen einen ausreichend motivierten Akteur wird man sich nie vollständig schützen können. Jemand mit Datenzugriff wird diese Daten immer irgendwie abfliessen lassen können, sei es auch nur über ein Bildschirmfoto. Man kann das also nicht völlig verhindern. Allerdings gibt es eine Reihe von *Massnahmen*, um diese *Risiken* auf ein annehmbares Mass zu *reduzieren*. Diese sind alle nicht neu:

- **Dateninventar**: Es muss bekannt sein, welche Daten sich wo befinden (Dateninventar). Spätestens seit der *Datenschutz-Grundverordnung* (DSGVO) hat dieses Thema wieder verstärkte Aufmerksamkeit erlangt.

- **Datenklassifizierung**: Die Daten sollten entsprechend ihrer Sensitivität gekennzeichnet werden. Dafür wird sinnvollerweise eine Datenklassifizierung verwendet. Auch hier gibt es technische Hilfsmittel, die anhand der Dateninhalte und mit Hilfe von Mustererkennung unterstützen können.

- **Policies**: Weiter braucht es klare Vorgaben zur Regelung, was im Rahmen der Klassifizierungsstufen erlaubt ist und was nicht. Die Prozesse zur Datenhaltung und -Bearbeitung müssen diese Vorgaben einhalten. Im Zusammenhang mit Policies und Prozessen lohnt es sich, dem Thema *Datensparsamkeit* vermehrte Aufmerksamkeit zu schenken. Und zwar nicht nur bezüglich des Schutzes von personenbezogenen Daten.

- **Grundschutz**: Es müssen solide technische und organisatorische Sicherheitsvorkehrungen (mindestens ein angemessener Grundschutz) umgesetzt werden, die die genannten Punkte berücksichtigen. Dabei sind die Umsetzung von korrektem Zugriffsschutz, sei dies nun in der eigenen Infrastruktur oder in der Cloud ein wesentliches Element. Für besonders kritische Daten sollten auch besonders stringente Massnahmen umgesetzt werden. Der Stellenwert der Sicherheit von Endgeräten, einschliesslich der mobilen Endgeräte, ist in Zeiten von Homeoffice und umfangreicher Telearbeit nochmals gestiegen. Diese gut zu sichern und zu überwachen gehört deshalb unbedingt zu einem leistungsfähigen Grundschutz.

- **Logging und Monitoring**: Das Sammeln und zentrale Auswerten von sicherheitsrelevanten Informationen ist unverzichtbar, zum Beispiel mit einem *SOC*. Im Kontext von Data Leakage sollte dem Monitoring von Datenzugriffen und Datenflüssen ein besonderes Augenmerk geschenkt werden, aber auch das Erkennen von Bedrohungen, unerwünschten Verhaltensweisen und Anomalien ist nützlich.

- **Einsatz von Verschlüsselung**: Bei korrekter Anwendung lässt sich ein sehr effektiver Zugriffsschutz auf sensitive Daten realisieren. Dies betrifft alle Bereiche, die sich unter der eigenen Kontrolle befinden, also Endgeräte, Datenverbindungen, portable Speichermedien, usw. muss aber auch die Ablage und Verwendung von Daten in der *Cloud* berücksichtigen.

- **Sicherheitsbewusstsein der Anwender**: Nur mit technischen Massnahmen kann kein ausreichender Schutz erreicht werden. Die Anwender müssen sich aktiv beteiligen und deshalb ist deren Sicherheitsbewusstsein auch in Bezug auf das Verhindern von Datenabflüssen wichtig. Durch Warnungen und Blockierungen kann das Sicherheitsbewusstsein der Anwender steigen und die Chance, versehentliche Datenabflüsse zu unterbinden steigt.

- **DLP-Lösungen**: Wenn die obigen Punkte umgesetzt sind und die definierten Prozesse gelebt werden, können DLP-Lösungen hilfreich sein, um Lücken aufzuzeigen und Verbesserungen gezielt anzugehen. Die Fähigkeiten derartiger Lösungen können besonders in Kombination

mit weiteren Informationen sehr hilfreich sein, um Prozesse und Aktivitäten zu überwachen und Abweichungen festzustellen.

- **Kommunikationsstrategie**: Sind Daten einmal abgeflossen, ist der Schaden angerichtet. Es lohnt sich aber, Schadensbegrenzung zu betreiben und dazu gehört auch eine im Voraus definierte Kommunikationsstrategie. Insbesondere wenn Personendaten involviert sind oder gar ein regulierter Bereich betroffen ist, kann eine Meldung sogar obligatorisch sein.

FAZIT

Das Risiko von Datenabflüssen ist real und die möglichen Schäden sind gross. DLP-Lösungen können helfen, aber mangelhafte Prozesse oder grössere Lücken im Sicherheitsdispositiv können damit nicht wettgemacht werden. Dateninventarisierung und -Klassifizierung, ein solider Grundschutz, passende Prozesse und ein leistungsfähiges Sicherheitsmonitoring sind bekannte, allgemein empfohlene Massnahmen, die auch in Bezug auf die Verhinderung ungewollter Datenabflüsse ihre Wirkung entfalten. Mit zunehmender Nutzung von Cloudapplikationen steigt auch der Stellenwert der Überwachung und der Kontrolle von Endgeräten und allgemein derjenigen Elemente, die überhaupt noch selbst kontrolliert werden können. Sollte doch einmal der Ernstfall eintreten, braucht es eine Kommunikationsstrategie und *vorbereitete Abläufe*, um rasch und wirksam reagieren zu können. Und vielleicht wird Datensparsamkeit dann mit anderen Augen betrachtet.

Tomaso Vasella

OFT IST DER SCHWIERIGE WEG DER RICHTIGE

Bildquelle: https://pixabay.com/images/id-6175186/

SCIP MONTHLY SECURITY SUMMARY

IMPRESSUM

ÜBER DEN SMSS

Das *scip Monthly Security Summary* erscheint monatlich und ist kostenlos.

Anmeldung: smss-subscribe@scip.ch
Abmeldung: smss-unsubscribe@scip.ch

Informationen zum Datenschutz.

Verantwortlich für diese Ausgabe:
Marc Ruef

Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion des Herausgebers, den Redaktoren und Autoren nicht übernommen werden. Die geltenden gesetzlichen und postalischen Bestimmungen bei Erwerb, Errichtung und Inbetriebnahme von elektronischen Geräten sowie Sende- und Empfangseinrichtungen sind zu beachten.

ÜBER SCIP AG

Wir überzeugen durch unsere Leistungen. Die scip AG wurde im Jahr 2002 gegründet. Innovation, Nachhaltigkeit, Transparenz und Freude am Themengebiet sind unsere treibenden Faktoren. Dank der vollständigen Eigenfinanzierung sehen wir uns in der sehr komfortablen Lage, vollumfänglich herstellerunabhängig und neutral agieren zu können und setzen dies auch gewissenhaft um. Durch die Fokussierung auf den Bereich Information Security und die stetige Weiterbildung vermögen unsere Mitarbeiter mit hochspezialisiertem Expertenwissen aufzuwarten.

Weder Unternehmen noch Redaktion erwähnen Namen von Personen und Firmen sowie Marken von fremden Produkten zu Werbezwecken. Werbung wird explizit als solche gekennzeichnet.

scip AG
Badenerstrasse 623
8048 Zürich
Schweiz

+41 44 404 13 13
www.scip.ch