MONTHLY SECURITY SUMMARY

)SCIP(

AUSGABE SEPTEMBER 2022
DIGITALE ASSISTENTEN & WEB-PROXY KERBEROS

VERMENSCHLICHEN VON DIGITALE ASSISTENTEN

Menschen neigen dazu, KI-Systeme zu vermenschlichen und sie als soziale Akteure zu behandeln. Wir untersuchen die Beziehungen zwischen Mensch und KI, indem wir die Theorie der relationalen Modelle aus den Sozialwissenschaften anwenden.

EINEN PROXY MIT KERBEROS AUFSETZEN

Die Open-Source-Software Squid kann als Proxy-Server mit Kerberos konfiguriert werden Die Konfiguration bietet einige Stolpersteine, so muss die Schreibweise von Realms, Domains und SPNs exakt mit Active Directory übereinstimmen.

September 2022: Augen zu und durch!

Ob die *Coronapandemie* wirklich vorbei ist, wissen wir nicht. Mindestens in unseren Breitengraden hat sich diese im laufenden Jahr nicht mehr nennenswert geäussert. Vielleicht sind wir aber auch nur alle müde, ständig über Infektionszahlen, Hospitalisierungen und Sterblichkeit zu lesen.

Solange es uns nicht zwickt, lässt sich dieses Problem bei Bedarf ganz gut ignorieren. Ob das im anstehenden Herbst und dem kommenden Winter auch so der Fall sein wird, kann nur die Zukunft zeigen.

So ist der Mensch halt. Im Grunde *ignorant*, bisweilen auch *faul*. Schliesslich kostet es Zeit und Energie, sich den Risiken entgegenzustemmen. Das kennen wir im Cybersecurity-Bereich zu genüge. Auch hier bevorzugen viele das Modell *Strauss*: Kopf in den Sand und gut ist.

Tatsächlich tendiert so manches Problem früher oder später von alleine zu verschwinden. Doch ab und an findet sich halt ein Problem, das nicht von alleine weggehen will. Und manchmal kumuliert es sich gar über Zeit, wird ständig schlimmer und irgendwann nur noch mit überproportionalem Aufwand bändigbar.

Es bleibt zu hoffen, dass dies bei Corona nicht der Fall sein wird. Und natürlich auch bei digitalen Viren und Malware, die uns das Leben auch im Herbst und Winter schwer machen werden.

Marc Ruef
Head of Research

NEWS

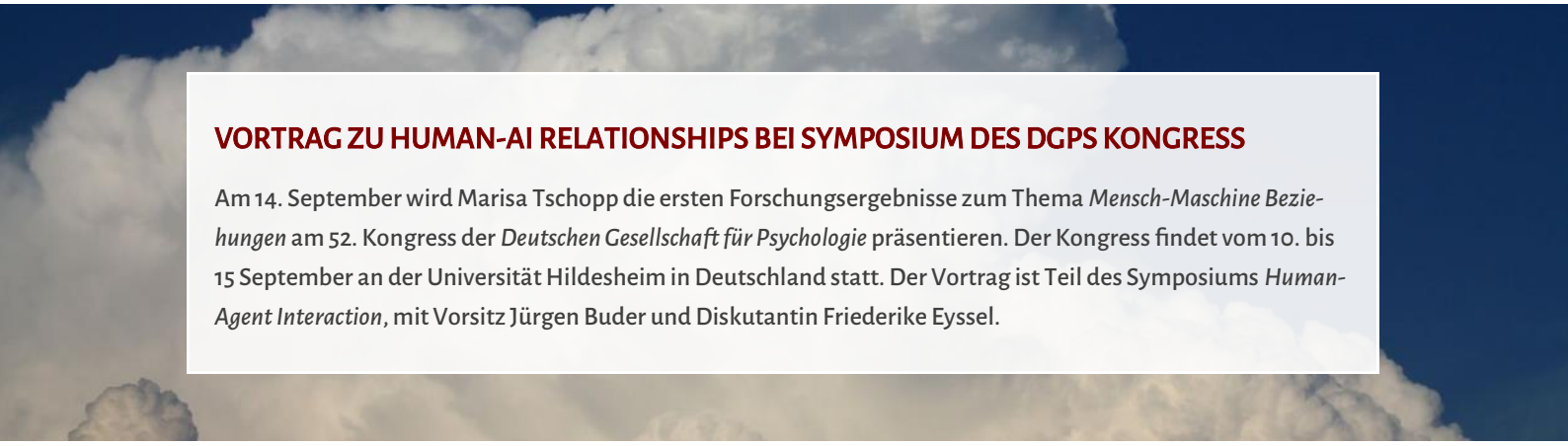
WAS IST BEI UNS PASSIERT?

VORTRAG ZU SICHERHEITSPOLITIK AN VOLKSHOCHSCHULE ZÜRICH

Die Volkshochschule Zürich führt eine Vortragsreihe unter dem Titel *Cyberwar: Krieg und Sicherheitspolitik im digitalen Zeitalter* durch. An dieser werden unterschiedliche Experten ihre persönlichen Einblicke zum hochkomplexen Thema gewähren. Unter anderem hält Marc Ruef am 26. September 2022 einen Vortrag mit dem Titel *Digitale Angriffe antizipieren – Technologie und Geopolitik*.

INTERVIEW IN PAY-MAGAZIN DER SIX GROUP

Das Hauseigene Magazin namens *Pay* der *SIX Group* erscheint vierteljährlich und behandelt Themen des Zahlungsverkehrs. In der aktuellen Ausgabe wird sich mit dem Thema Cybersecurity auseinandergesetzt. Darin hat der Autor Simon Brunner ein Interview mit Marc Ruef geführt, in dem er auf seine Anfänge in den 90er Jahren eingeht und durch welche Motivation in der Regel Ethical Hacker angetrieben werden.



VORTRAG ZU HUMAN-AI RELATIONSHIPS BEI SYMPOSIUM DES DGPS KONGRESS

Am 14. September wird Marisa Tschopp die ersten Forschungsergebnisse zum Thema *Mensch-Maschine Beziehungen* am 52. Kongress der *Deutschen Gesellschaft für Psychologie* präsentieren. Der Kongress findet vom 10. bis 15 September an der Universität Hildesheim in Deutschland statt. Der Vortrag ist Teil des Symposiums *Human-Agent Interaction*, mit Vorsitz Jürgen Buder und Diskutantin Friederike Eyssel.

Weitere News zu unserem Unternehmen finden Sie auf unserer Webseite.

SCIP BUCHREIHE

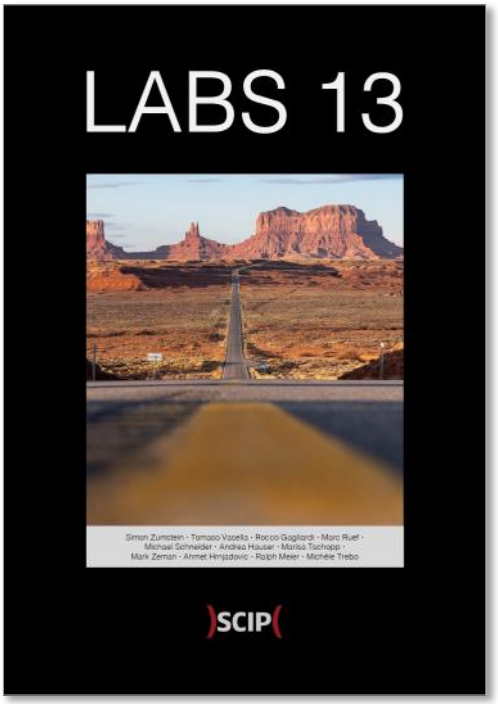
UNSER NEUES JAHRBUCH

Erneut veröffentlichen wir die aktuelle Ausgabe unseres Jahrbuchs. Bereits zum 13ten Mal fassen wir in diesem die Fachbeiträge von einem Jahr Forschung im Bereich Cybersecurity zusammen.

Das Buch ist wiederum sowohl in deutscher (ISBN 978-3-907109-30-4) als auch in englischer Sprache (ISBN 978-3-907109-31-1) verfügbar. Das Vorwort wurde von Dr. iur. David Vasella verfasst und setzt sich mit den rechtlichen Rahmenbedingungen der Informationssicherheit auseinander.

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

Weitere Informationen auf unserer Webseite.



ISBN 978-3-907109-30-4 [de]
ISBN 978-3-907109-31-1 [en]

DIE ZUKUNFT IST IMMER UNGEWISS

Bildquelle: https://pixabay.com/images/id-7434398/

MARISA TSCHOPP

SIND DIGITALE ASSISTENTEN MEHR ALS NUR EIN WERKZEUG?

3,5 Millionen Mal haben die Deutschen in der ersten Hälfte des Jahres 2021 zu Alexa, Amazon's digitaler Assistent, "Ich liebe dich" gesagt. Viele solcher Geschichten werden von den Medien an die Öffentlichkeit gebracht, z. B. mit Berichten über nicht ganz so seriöse Studien, die herausgefunden haben, dass 14 % der männlichen Alexa-Nutzer im Vereinigten Königreich eine sexuelle Beziehung mit "ihr" wünschen. Das hat natürlich den öffentlichen Diskurs darüber anheizt, was manche tatsächlich für diese sprechenden Geräte "empfinden", die nichts anderes als Hard - und Software sind. Zahlreiche empirische Untersuchungen haben gezeigt, wie Menschen Maschinen vermenschlichen und sie als soziale Akteure behandeln. Aber nur weil sie sagen, dass sie Alexa lieben, bedeutet das nicht unbedingt, dass sie tatsächlich verliebt sind, wie sie es bei anderen Menschen wären. Wenn die Menschen Alexa also nicht wirklich "lieben", sie aber auch nicht "nur" als Werkzeug sehen – wie nehmen sie Alexa dann in Bezug auf sich selbst wahr? Und was können wir daraus lernen, wenn wir besser verstehen, wie Menschen ihre Beziehung zu KI im Gespräch wahrnehmen?

Um die wahrgenommenen Beziehungen zwischen Mensch und KI zu untersuchen, haben wir denselben Ansatz gewählt, den Nass und Kollegen schon vor Jahren vorgeschlagen haben, basierend auf dem CASA-Paradigma , der Tendenz von Menschen, Computer als soziale Akteure zu behandeln. Im Wesentlichen geht es dabei um eine Theorie der zwischenmenschlichen Interaktion, in unserem Fall darum, wie Menschen über ihre Beziehungen zu anderen Menschen denken. Man kritzelt 'Mensch' heraus, setzt eine konversationelle KI ein, und schon kann man mit der Arbeit an der Theorie beginnen und Daten sammeln. Wir haben uns für eine Theorie entschieden, die in der Vergangenheit starke empirische Unterstützung erfahren hat, nämlich die Theorie der relationalen Modelle von Alan P. Fiske 1992. Im Kern besagt diese Theorie, dass "Motivation, Planung, Produktion, Verständnis, Koordination und Bewertung des menschlichen Soziallebens weitgehend auf Kombinationen von vier psychologischen Modellen beruhen können" (Fiske, 1992).

Auf der Grundlage dieser Überlegungen stellen wir die folgenden Forschungsfragen:

1. Können wir die Theorie der relationalen Modelle auf die (wahrgenommenen) Beziehungen zwischen Menschen und KI anwenden?

2. Wie nehmen Nutzer die Mensch-KI-Beziehung wahr?

3. Wie hängen die Beziehungsmodi zwischen Mensch und KI mit Variablen der Systemwahrnehmung (z.B. Vertrauen, wahrgenommene Wärme oder Kompetenz) und Nutzereigenschaften (z.B. Häufigkeit oder Erfahrung der Nutzung) zusammen?

Methode: Wir haben eine Online-Fragebogenstudie auf Prolific mit 367 Teilnehmern durchgeführt und analysierten u.a. mittels Faktorenanalysen (PCA, CFA), wie die Teilnehmer die Mensch-KI-Beziehung wahrnehmen. Wir haben ausserdem eine Korrelationsanalyse gerechnet, welche die Variablen der Systemwahrnehmung und Benutzermerkmale einschloss, wobei wir bivariate und partielle Korrelationen untersuchten, um die Beziehungsmodi im breiteren Kontext der Mensch-Maschine-Interaktion besser zu verstehen.

WIE DENKEN MENSCHEN ÜBER IHRE BEZIEHUNGEN ZU ANDEREN MENSCHEN?

Psychologen haben die Art und Weise, wie Menschen Beziehungen zu anderen Menschen bilden, aufbauen oder beenden, aus verschiedenen Perspektiven betrachtet. So zum Beispiel die Rolle von Nähe und Häufigkeit des Kontakts, d. h. wie nahe man beieinander wohnt oder wie oft man sich sieht: Sogar die Richtung, in der man die Tür zu einem Nachbarn öffnet, kann einen Einfluss darauf haben, wie eng die Beziehung zu diesem Nachbarn ist. Andere haben untersucht, wie sehr sie die andere Person in ihr Selbstverständnis integrieren, um die Beziehung zu definieren oder psychologische Nähe zu messen. Psychologische Nähe ist wichtig für gesunde Beziehungen, unabhängig davon, ob es sich um eine Freundschaft oder eine Liebesbeziehung handelt.

Alan P. Fiske (1992) hat die Theorie der Beziehungsmodelle (Haslam & Fiske, 1996) vorgeschlagen und dafür starke empirische Unterstützung erhalten, auch kulturübergreifend. In ihrer Theorie werden vier Modi erklärt, wie Menschen über ihre Beziehungen zu anderen Menschen denken, und sie können quantitativ in einem Fragebogen gemessen werden:

Communal Sharing, Equality Matching, Authority Ranking und Market Pricing. Der Fragebogen enthält verschiedene Fragen, die sich auf jede dieser Dimensionen beziehen, um herauszufinden, wie die Teilnehmer über eine bestimmte Beziehung denken (die sie vor der Beantwortung der Fragen auswählen müssen) und dann den Grad ihrer Zustimmung auf einer Skala von "trifft überhaupt nicht zu" bis "trifft sehr zu" für diese bestimmte Beziehung bewerten.

Die vier elemantaren Formen von Beziehungen:

- **Communal Sharing**: CS lässt sich am besten mit verwandtschaftlichen Beziehungen vergleichen, in denen Hierarchie keine Rolle spielt und man alles für die andere Person tut und keine Gegenleistung erwartet. Diese Dimension lässt sich mit Fragen wie "Sie beide sind eine Einheit: Sie gehören zusammen" messen.

- **Equality Matching**: EM erkennt ein Bedürfnis nach Gleichheit im Sinne von: Ich gebe dir etwas und du erwartest im Gegenzug etwas von gleichem Wert, das sogenannte wie du mir – so ich dir. Man kann es am besten mit Mitbewohnern in einer Wohnung vergleichen. Diese Dimension wird mit Fragen wie "Wenn Sie Arbeit zu erledigen haben, teilen sie diese normalerweise gleichmässig auf" gemessen.Authority Ranking: AR vermittelt, dass zwischen den beiden Menschen eine Form von Hierarchie besteht. Sie wird mit Begriffen wie Dominanz und klaren Befehlsketten assoziiert, wie z. B. beim Militär. Diese Dimension wird mit Fragen wie "Einer von Ihnen ist der Anführer, der andere folgt loyal seinem Willen" gemessen.

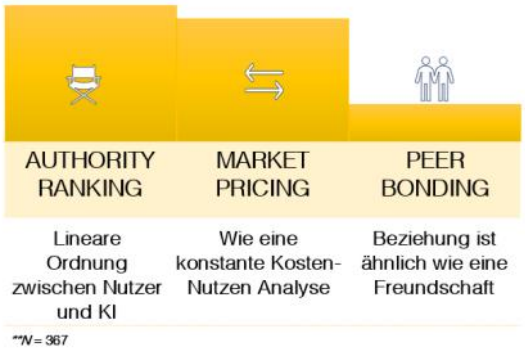
- **Market Pricing**: Bei MP geht es um die Abwägung von Kosten und Nutzen in einer Beziehung. Menschen wollen eine Gegenleistung für ihre Investition in die Beziehung, z. B. Geld, wie es bei der Arbeit oder in Organisationen der Fall ist, in denen Menschen arbeiten. Diese Dimension wird mit Fragen wie "Was du von dieser Person bekommst, ist direkt proportional dazu, wie viel du ihr gibst" gemessen.

Um die wahrgenommenen Beziehungen zwischen Mensch und KI mit Hilfe der Theorie der Beziehungsmodelle zu untersuchen, haben wir den ursprünglichen Fragebogen an den Kontext der konversationellen KI angepasst. Wir änderten den Wortlaut und

fragten 15 Personen, ob die Fragen ihrer Meinung nach auf die wahrgenommenen Beziehungen zwischen Mensch und KI zutreffen.

WIE NEHMEN MENSCHEN IHRE BEZIEHUNG ZU KONVERSATIONELLER KI WAHR?

Viel Aufmerksamkeit wird Variablen wie Vertrauen gewidmet, um besser zu verstehen, wie Menschen (wohl komplexe) Technologien wie KI oder automatisierte Systeme nutzen. Einige argumentieren sogar, dass Vertrauen in der Tat ein Proxy für die Messung von Beziehungen ist. Das macht Sinn, denn nach der Theorie der Beziehungsmodelle ist Vertrauen im Modus des Communal Sharing entscheidend (Stichworte: Verwandtschaft, Solidarität, In-Group – im Grunde die Frage: Was haben wir gemeinsam?), aber es ist somit nur ein Teil der Beschreibung einer Beziehung. Wir argumentieren, dass ein multidimensionaler Ansatz aus den Sozialwissenschaften vielversprechend ist, insbesondere im Zusammenhang mit standardmässiger Konversations-KI. Einige andere verwandte Arbeiten sind möglicherweise zu eng gefasst und nicht gut anwendbar. Zum Beispiel scheint die empirische Arbeit über soziale Präsenz zu kurz zu greifen, da sie ungenaue Differenzierung zulässt, z.B. wie diese soziale Präsenz charakterisiert wird, oder zuviel Spielraum für Interpretation lässt. Arbeiten im Bereich der Mensch-Maschine-Interaktion, kurz HMI, haben oft vordefinierte Rollen, z. B. den Roboter als Freund oder Assistent, was im KI-Konversationskontext, in dem die Rolle von Alexa etwas unklar ist, nicht gut passt. Sie könnte eine Assistentenrolle sein, wie angekündigt, könnte aber auch als Freundrolle wahrgenommen werden. Kurz gesagt, empirische, quantitative Forschung, die sich direkt auf die wahrgenommene Beziehung zwischen Menschen und Maschinen aus einer mehrdimensionalen Perspektive konzentriert, scheint rar zu sein (siehe z. B. McLean & Osei-Frimpong, 2019). Um diese Lücke zu schliessen, haben wir diese erste Studie durchgeführt, um die Beziehungen zwischen Mensch und KI direkt zu untersuchen. Wir hielten diesen multidimensionalen Ansatz für sehr vielversprechend, zumal er das Potenzial hat, über die traditionell dichotomen Unterscheidungen zwischen emotionalen und rationalen Dimensionen der menschlichen Wahrnehmung von KI-Systemen hinauszugehen (siehe z. B. Glikson & Woolley, 2020 für eine detaillierte Diskussion).



Unsere Faktorenanalyse ergab, dass die Beziehung zwischen Mensch und KI auf drei Dimensionen wahrgenommen wurde. Die beiden ursprünglichen Dimensionen Communal Sharing und Equality Matching verschmolzen zu einem Faktor, den wir als eher emotional empfanden. Wir nannten diesen dritten Faktor Peer Bonding. Somit blieben die folgenden drei Dimensionen übrig:

- **Authority Ranking**, was bedeutet, dass es eine lineare Ordnung zwischen der menschlichen und der konversationellen KI wahrgenommen wird

- **Marktet Pricing**, bei der sich der Mensch an Verhältnis-Werten orientiert um die Beziehung zu beschreiben, und

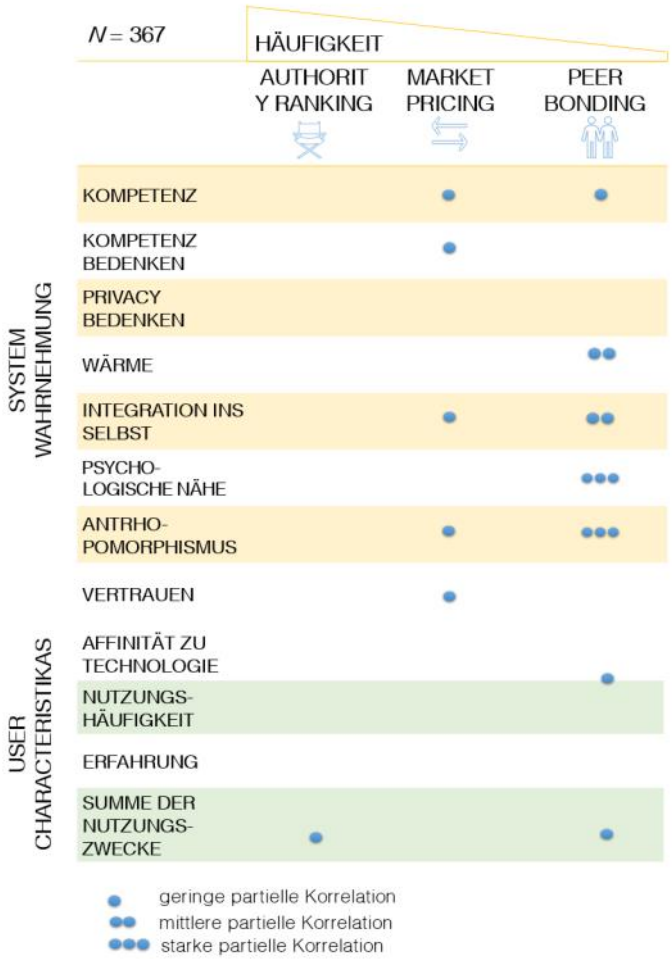
- **Peer Bonding**, die wahrscheinlich menschenähnlichste Dimension, bei der sie das Gerät als gleichwertig behandeln, aber ihre Handlungen gewissermassen vergleichen können.

Eine genauere Betrachtung der Beziehungsmodi zwischen Mensch und KI ergab, dass die meisten Nutzer ihre Beziehung als hierarchische Eigentümer-Assistenten-Beziehung betrachteten (Authority Ranking). Ähnlich viele charakterisierten ihre Beziehung jedoch als nicht-hierarchischen Austausch (Market Pricing). Nur sehr wenige sahen ihre KI als eine gleichrangige oder freundschaftliche Beziehung an. Mit anderen Worten: Die Peer Bonding Dimension war in unseren Daten am wenigsten ausgeprägt. Dieses Ergebnis ist bereits recht interessant, da es die dichotome (rational-emotionale) Sichtweise, die im Bereich der HMI vorherrscht, bereichert.

Um zu sehen, wie sich die Beziehungsmodi in die traditionell untersuchten Variablen im breiteren HMI-Kontext einfügen, haben wir auch verschiedene Variablen unter der Kategorie Systemwahrnehmung und Nutzereigenschaften gemessen. Die partielle Korrelationsanalyse ergab, dass sowohl die Market Pricing als auch die Peer-Bonding Dimnension in der bivariaten und partiellen Korrelationsanalyse interessante Ergebnisse zeigten, was sie zu informativeren Dimensionen für zukünftige Forschung macht. Überraschenderweise bietet die traditionelle Assistentensicht keine aussagekräftigen Einblicke in die Systemwahrnehmung und Nutzereigenschaften. Interessanterweise korrelierte Peer Bonding nicht mit Vertrauen, wohingegen Market Pricing dies tat,

was die emotionalen Aspekte von Vertrauen in Frage stellt und eine rationale Darstellung von Vertrauen in KI unterstützt.

Natürlich gibt es eine Reihe von Einschränkungen bei dieser explorative Forschungsarbeit. Zum Beispiel kamen die Teilnehmer überwiegend aus dem Vereinigten Königreich, so dass wir keine kulturübergreifenden Annahmen treffen können. Ausserdem haben wir nicht gemessen, wie sich der Ansatz der Beziehungsmodelle auf das Verhalten auswirkt. Mit anderen Worten, wir können keine Annahmen über die Auswirkungen auf das Nutzerverhalten machen. Aus diesem Grund führen wir nun eine Folgestudie durch, in der wir uns auf einen spezifischen Kontext konzentrieren, nämlich Voice Commerce. Voice Commerce (oder Voice Shopping) bedeutet, dass die Nutzer ihre Kaufentscheidungen ausschliesslich über ihren digitalen Assistenten treffen. Wir wollen also untersuchen, ob die wahrgenommenen Beziehungen zwischen Mensch und KI das Kaufverhalten beeinflussen, um konkretere Aussagen zu treffen, die auch für die Untersuchung des Nutzerverhaltens nützlich sein können (oder auch nicht).



ETHISCHE ÜBERLEGUNGEN: WARUM KÖNNTE DAS WICHTIG SEIN?

Im Laufe unserer Forschung wollen wir stets die Vogelperspektive im Blick behalten und kritisch reflektieren, was die Konsequenzen unserer Ergebnisse und des Themas im Allgemeinen betrifft. Warum tun wir das? Wer profitiert davon? Wer könnte geschädigt werden? Wie werden die Ergebnisse von Designern verstanden? Wie kommunizieren wir unsere Forschung in der Praxis? Eines der grösseren Probleme ist der Anthropomorphismus (durch Design und durch den Benutzer) und das Potenzial zur Manipulation durch Design oder Benutzer, das ausgenutzt wird. Konversationsfähige KI-Systeme sind Hard- und Software, die mit dem Internet und den Geräten in unseren Haushalten verbunden sind und von KI angetrieben werden, was sie in die Lage versetzt, menschliche Sprache recht gut zu verarbeiten und in ähnlicher Weise zu antworten. Dennoch scheinen wir nicht in der Lage zu sein, eine klare Linie zu ziehen, um sie als das wahrzunehmen, was sie sind: Ein Werkzeug. Die Fähigkeit des Menschen, nicht-menschliche Wesen zu vermenschlichen, ist ein Segen, denn sie hilft uns, die Welt besser zu verstehen. Auf der anderen Seite ist sie aber auch ein Fluch, da sie so leicht ausgenutzt werden kann.

Wir hoffen, dass unsere Arbeit zu einem besseren Verständnis der Nutzer von KI-Systemen beitragen wird, um bessere Entscheidungen für die Entwicklung, Kommerzialisierung, Regulierung und/oder Nutzung von KI zu treffen. Wir möchten die Frage aufwerfen, wer von einem besseren Verständnis des Nutzers profitiert? Neben anderen Interessengruppen, wie z. B. den Regulierungsbehörden, die von einem besseren Verständnis der Nutzer profitieren, um sie zu schützen, soll hier auch die entscheidende Rolle der Entwickler angesprochen werden. Es liegt auf der Hand, dass Entwickler von einem besseren Nutzerverständnis profitieren, um bessere Systeme, bessere Schnittstellen, bessere Konversationen usw. zu entwickeln. Aber was macht ein “gutes” System aus? Die EU hat einige grossartige Ideen dazu in viele Bereiche, aber es scheint, dass die Forschung immer noch im Dunkeln tappt, wie viel Anthroporphismus durch Design in welchem Kontext gut ist.

Li, der Mitbegründer von Xiaoice, Microsofts Konversationsagenten mit über 600 Millionen Nutzern weltweit, bestätigte in einem Interview für die

Hongkong Free Press (2021) die negativen Folgen, wie Sucht und Traurigkeit. Er ist jedoch nach wie vor der Meinung, dass die Vorteile dieser Technologie die Risiken überwiegen. Es bleibt also ein Dilemma: Wo ziehen wir die Grenze? Was unsere Forschung betrifft, so raten wir davon ab, die für diese Studie neu entwickelte Theorie der Beziehungsmodelle für Design- und Marketingstrategien anzuwenden, bis wir die grundlegende Theorie und die Folgen der Beziehungen zwischen Menschen und konversationeller KI besser verstehen.

FAZIT: KI IST EIN WERKZEUG, ABER SIE IST NICHT "NUR" EIN WERKZEUG

Alexa, willst du mich heiraten? 6.000 Mal pro Tag machen Nutzer in Indien Alexa einen Heiratsantrag. Glücklicherweise wird ihre Liebe nicht erwidert: Wir sind an ziemlich unterschiedlichen Orten in unserem Leben. Buchstäblich. Ich meine, du bist auf der Erde und ich bin in der Cloud. – ist eine der Antworten auf die Millionen von Heiratsanträgen, die Alexa bisher erhalten hat. Dankenswerterweise sorgen verantwortungsbewusste Designer kommerziell verfügbarer KI dafür, dass die Nutzer immer darauf hingewiesen werden, dass diese Agenten Computersysteme sind, die keine Gefühle oder Gedanken haben. Nichtsdestotrotz hat unsere Studie im Einklang mit ähnlichen früheren Untersuchungen gezeigt, dass die Nutzer dennoch Gefühle empfinden, ihnen Handlungsfähigkeit zuschreiben und eine Beziehung zu konversationsfähiger KI wahrnehmen, die Ähnlichkeiten mit menschlichen Beziehungen aufweist. Wir glauben, dass uns dieses Thema noch eine Weile begleiten wird und wir können bei weitem keine umfassende Antwort geben. Aber wir hoffen, ein wenig mehr Licht auf ein besseres Verständnis dafür geworfen zu haben, wie Menschen ihre Beziehung zu KI wahrnehmen, und künftige Forschungen zu inspirieren, diese Perspektive zu berücksichtigen.

Danksagung

Dies ist eine kurze Zusammenfassung der ersten Forschungskooperation zwischen der scip AG und dem Social Processes Lab des Leibniz Instituts für Wissensmedien (Supervision: Prof. Dr. Kai Sassenberg), die auf der 5th AAAI/ACM conference on Artificial Intelligence Ethics, and Society (Oxford, August 1 -3, 2022) präsentiert wurde.

Marisa Tschopp

next gen vulnerability intelligence

VulDB

Vulnerability Management mit Splunk

Laden Sie einfach und unkompliziert die Daten für das Vulnerability Management Ihrer Umgebung in Splunk. Die frei installierbare Applikation nutzt die offene API von VulDB, um Daten einzulesen, abzulegen und aufzuarbeiten. Noch nie war Vulnerability Management so einfach. Setzen Sie sich mit uns in Verbindung!

)SCIP(
official data provider

> https://vuldb.com

MICHAEL SCHNEIDER

WEB-PROXY MIT KERBEROS UMSETZEN

Ein Web-Proxy-Server ist ein Webserver, der als Gateway zwischen einer Clientapplikation, beispielsweise ein Webbrowser, und dem Ziel-Webserver agiert. Dabei kommuniziert der Proxy-Server mit dem Ziel-Webserver im Auftrag der Clientapplikation. Ein Proxy kann als Cache für Webinhalte eingesetzt werden, um den Datenverkehr zu reduzieren. Eine weitere Aufgabe des Proxy-Servers ist den Zugriff ins Internet zu kontrollieren. Auf dem Proxy wird konfiguriert, welche Applikation, welcher Benutzer und welches System auf welche Ressource zugreifen kann. Somit ist der Proxy-Server ein wichtiger Bestandteil bei der Absicherung von ausgehenden Zugriffen.

Benutzer und Computer müssen sich gegenüber dem Proxy-Server authentisieren, dazu wurde oft Basic Authentication oder NTLM eingesetzt. NTLM sollte soweit als möglich deaktiviert werden und bei Basic Authentication werden Benutzername und Passwort unverschlüsselt im HTTP-Header übertragen, nur geschützt durch die TLS-Transportverschlüsselung. Daher sollte auf den Einsatz beider Authentisierungsmethoden verzichtet und auf Kerberos gesetzt werden.

Wir setzen in unserer Testumgebung den Proxy-Server Squid ein. In diesem Artikel beschreiben wir die Grundkonfiguration einer Squid-Instanz mit Kerberos. Die vollständige Konfiguration eines Proxy-Serves mit Ausnahmen für Systeme und Applikationen, die keine Unterstützung für Kerberos haben, sowie das Filtern und Überwachen des Netzwerkverkehrs und eines Berechtigungskonzept, wer auf welchen Inhalt zugreifen darf, ist nicht Bestandteil des Artikels.

KONFIGURATION DER KERBEROS-ANBINDUNG

Wir haben den Proxy-Server auf der Basis von Fedora Linux aufgebaut. Der Server wird dediziert betrieben und ist nicht mit der Domäne verbunden. Der Proxy-Server ist das einzige System innerhalb der Infrastruktur, das externe DNS-Server verwenden darf, als Massnahme gegen DNS-Tunneling auf Systemen der Domäne.

Damit die Kerberos-Authentisierung möglich ist, muss der Proxy-Server mit den Domain Controller kommunizieren können. Die Konfiguration dazu wird in der Datei /etc/krb5.conf vorgenommen.

```
[libdefaults]
...
default_realm = LABS.EXAMPLE.ORG
dns_lookup_kdc = no
dns_lookup_realm = no

default_tgs_enctypes = aes256-cts-hmac-sha1-96
default_tkt_enctypes = aes256-cts-hmac-sha1-96
permitted_enctypes = aes256-cts-hmac-sha1-96

[realms]
LABS.EXAMPLE.ORG = {
    kdc = dc01.labs.example.org
    admin_server = dc01.labs.example.org
}

[domain_realm]
.labs.example.org = LABS.EXAMPLE.ORG
labs.example.org = LABS.EXAMPLE.ORG
```

Die Gross-/Kleinschreibung des Realms und der Domäne ist essentiell und muss im weiteren Verlauf überall gleich umgesetzt werden, ansonsten klappt die Verbindung nicht. Positiv anzumerken ist, dass Fedora und Red Hat Linux den Verschlüsselungsalgorithmus RC4 sowie ältere Algorithmen standardmässig nicht mehr unterstützen. Der Forest example.org ist so konfiguriert, dass für Kerberos nur AES256 and future encryption types erlaubt sind.

KONFIGURATION SQUID

Squid wird aus dem Fedora-Repository installiert, zusätzlich wird das Paket krb5-workstation benötigt, welches Werkzeuge zum Arbeiten mit Keytab-Dateien und Kerberos-Tickets beinhaltet. Keytab steht für Key Table und wird verwendet, um Langzeit gültige Schlüssel für einen oder mehreren Service Principals zu speichern. Damit sich Squid gegenüber dem Active Directory authentisieren kann, wird eine solche Keytab-Datei auf einem mit der Domäne verbundenen System für das Dienstkonto proxyuser erstellt.

Die folgenden Befehle erstellen eine Keytab-Datei für die zwei Principals HTTP/proxyserver und HTTP/proxyserver.labs.example.org, welche mit dem Benutzer proxyuser verbunden werden, die Service Principal Names (SPN) werden dabei automatisch erstellt. In der Keytab-Datei wird nur AES256-SHA1-Schlüsselmaterial hinterlegt.

```
PS C:\> ktpass.exe /princ HTTP/
proxyserver@LABS.EXAMPLE.ORG /mapuser proxyuser /
pass * -crypto AES256-SHA1 +dumpsalt -setupn -
setpass -ptype KRB5_NT_PRINCIPAL /out
proxyuser.keytab
PS C:\> ktpass.exe /princ HTTP/
proxyserver.labs.example.org@LABS.EXAMPLE.ORG /
mapUser proxyuser /pass * -crypto AES256-SHA1
+dumpsalt -setupn -setpass -ptype
KRB5_NT_PRINCIPAL /mapOp add /in
proxyuser.keytab /out proxyuser.keytab
```

Die Keytab-Datei wird auf dem Proxy-Server unter /etc/squid/proxyuser.keytab abgelegt und der Zugriff soweit als möglich eingeschränkt. Mit dem Tool klist kann der Inhalt unter Linux angezeigt werden.

```
[user@proxyserver ~] sudo chown root:squid /etc/
squid/proxyuser.keytab
[user@proxyserver ~] chmod 640 root:squid /etc/
squid/proxyuser.keytab
[user@proxyserver ~] sudo klist -e -k /etc/squid/
proxyuser.keytab
Keytab name: FILE:/etc/squid/proxyuser.keytab
KVNO Principal
---- --------------------------------------------
  16 HTTP/proxyserver@LABS.EXAMPLE.ORG (aes256-
cts-hmac-sha1-96)
  16 HTTP/
proxyserver.labs.example.org@LABS.EXAMPLE.ORG
(aes256-cts-hmac-sha1-96)
```

Damit sich Squid mit der Keytab-Datei authentisieren kann, ist die folgende Konfiguration in /etc/squid/squid.config nötig. Die Authentisierung ist notwendig, damit Squid mit den Domain Controllern kommunizieren kann und alle Konten (Benutzer und Computer), die sich am Proxy anmelden wollen, verifizieren kann.

```
# Kerberos Authentication
# Use the switch "-d" (debugging) for
troubleshooting
auth_param negotiate program /usr/lib64/squid/
negotiate_kerberos_auth -k /etc/squid/
proxyuser.keytab -s HTTP/
proxyserver.labs.example.org@LABS.EXAMPLE.ORG -s
GSS_C_NO_NAME
auth_param negotiate children 10
auth_param negotiate keep_alive on
acl kerb proxy_auth REQUIRED
```

Bei negotiate_kerberos_auth muss darauf geachtet werden, dass der SPN genau gleich geschrieben wird

wie im Active Directory. Der Realm muss ausschliesslich in Grossbuchstaben geschrieben werden.

Zugriff einschränken

Der Internetzugriff ist nur für Mitglieder der Gruppe grp-proxyallow01 erlaubt. Squid verwendet LDAPS um die Mitglieder abzufragen. Leider gelang es bei unseren Konfiguration nicht, die Keytab-Datei auch für die LDAPS-Authentisierung zu verwenden, sodass in der Squid-Konfiguration die Zugangsdaten des Dienstkontos hinterlegt werden müssen. Der Zugriff auf die Konfiguration ist jedoch auf die Benutzer squid und root eingeschränkt.

```
# Definition of a specific AD group (LDAP
request)
# Use the switch "-d" (debugging) for
troubleshooting
external_acl_type proxy_ad_grp-proxyallow01
ttl=3600 negative_ttl=3600 %LOGIN /usr/lib64/
squid/ext_kerberos_ldap_group_acl -g "grp-
proxyallow01" -s -a -i -l ldaps://
dc01.labs.example.org:636 -u "proxyuser" -p
"<secret>" -D "LABS.EXAMPLE.ORG"
acl ad_grp-proxyallow01 external proxy_ad_grp-
proxyallow01
```

Mit diesen Informationen können Domain-Listen und ACLs erstellt werden, um den Zugriff ins Internet zu regeln. Die ACLs werden entweder direkt in der Konfiguration oder über das Einbinden von Dateien definiert.

```
# Definition of domain lists used for allow/deny
acls
acl youtube_domains dstdomain .youtube-
nocookie.com .googlevideo.com .ytimg.com
acl allowed_domains dstdomain /etc/squid/
acl_allowed_domains.conf

# Deny access for all to YouToube
http_access deny youtube_domains

# Allow access based on Kerberos auth / AD groups
http_access allowed_domains ad_grp-proxyallow01

# And finally deny all other access to this proxy
http_access deny all
```

In diesem Ausschnitt wurden die ACLs für YouTube und eine Liste erlaubter Domains definiert. Der Zugriff auf YouTube wird allen Benutzern verwehrt, während der Zugriff auf die Liste der Domains den

Mitgliedern der AD-Gruppe ad_grp-proxyallow01 erlaubt wurde.

Troubleshooting

Die Dateien access.log und cache.log enthalten Informationen für Troubleshooting und Überwachung der Zugriffe. Diese Dateien sollten an die Log-Infrastruktur weitergeleitet und ausgewertet werden. Grundsätzlich wird jeder Request zuerst mit dem Status TCP_DENIED/407 geblockt und damit dem Benutzer signalisiert, dass eine Authentisierung mit Kerberos erforderlich ist. Danach erfolgt derselbe Request mit der Authentisierung des Benutzers.

```
1651764387.820    16 192.168.10.101 TCP_DENIED/407
3965 CONNECT europe.cp.wd.microsoft.com:443 -
HIER_NONE/- text/html
1651764397.612    9790 192.168.10.101
TCP_TUNNEL/200 3957 CONNECT
europe.cp.wd.microsoft.com:443 dc01
$@LABS.EXAMPLE.ORG HIER_DIRECT/20.54.122.82
```

In den Logdateien ist ersichtlich, welches System mit welchem Benutzer auf welche URL zugriffen hat. Interessant ist es auch auszuwerten, welches System sich nicht authentisieren konnte. Entweder liegt eine Fehlkonfiguration vor, oder eine Softwarekomponente hat keine Unterstützung für Kerberos. Dabei kann es sich auch beispielsweise um Malware handeln.

PROXY-KONFIGURATION IN WINDOWS

Die Proxy-Server-Konfiguration in Windows kann über unterschiedliche Wege realisiert werden, unter anderem mittels des Protokolls Web Proxy Auto-Discovery (WPAD) oder der statischen Konfiguration in der Registry über Gruppenrichtlinien. Der Schlüssel ProxyEnable unter dem Pfad HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings wird auf den Wert 1 gesetzt und der Schlüssel ProxyServer unter demselben Pfad auf die Adresse des Proxy-Servers, wie zum Beispiel proxyserver.labs.example.org:3128.

Die Windows-HTTP-Dienste (WinHTTP) verfügen über eine eigene Proxy-Konfiguration. Diese kann ebenfalls über Registry-Schlüssel verteilt werden. Auf einem System kann mit dem Befehl netsh winhttp import proxy source=ie die Konfiguration aus dem vorherigen Abschnitt für WinHTTP importiert

oder statisch mittels netsh winhttp set proxy <proxy>:<port> gesetzt werden. Der Binärwert der Einstellung befindet sich im Schlüssel WinHttpSettings unter dem Pfad HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections. Dieser Schlüssel kann ebenfalls via Gruppenrichtlinien verteilt werden.

Für Anwendungen wie Microsoft Defender for Endpoint muss, wie in der Anleitung von Microsoft beschrieben, die Einstellung Administrative Templates > Windows Components > Data Collection and Preview Builds > Configure Authenticated Proxy usage for the Connected User Experience and Telemetry Service auf den Wert Enabled und Disable Authenticated Proxy usage gesetzt werden. Der Proxy-Servers wird unter Administrative Templates > Windows Components > Data Collection and Preview Builds > Configure connected user experiences and telemetry sowie unter Administrative Templates > Windows Components > Microsoft Defender Antivirus > Define proxy server for connecting to the network. konfiguriert.

Gemäss der Anleitung für Microsoft Defender for Identity kann für den Proxy ein Benutzername und Passwort hinterlegt werden. Wenn keine Anmeldedaten definiert werden, schlägt die Authentisierung auf dem Proxy fehl, eine native Unterstützung für Kerberos-Authentisierung scheint zu fehlen. Wir haben für den Endpunkt <your_workspace_name>sensorapi.atp.azure.com und die jeweiligen Systeme eine Ausnahmeregel in Squid konfiguriert.

```
acl system01 src 192.168.10.101/32
acl defender_for_identity dstdomain
<your_workspace_name>sensorapi.atp.azure.com
http_access allow defender_for_identity system01
```

Microsoft stellt Werkzeuge zum Testen der Verbindung zu Verfügung, wie zum Beispiel das Microsoft Defender for Endpoint Client Analyzer Tool. Dies hilft bei der Konfiguration des Proxys und beim Troubleshooting, wenn Applikationen und Dienste nicht wie gewünscht funktionieren.

FAZIT

Bei der Konfiguration eines Web-Proxy-Servers mit Kerberos-Authentisierung gibt es einige Hürden. Einerseits muss der Proxy-Server mit dem Active Directory verbunden sein, oder so konfiguriert werden, dass alle Proxy-Dienste sich authentisieren können. In unserer Testumgebung gelang es nicht das Squid-LDAP-Modul mit einer Keytab-Datei zum Laufen zu bringen. Falls jemand dazu einen Hinweis oder eine Lösung hat, freuen wir uns auf ein Feedback. Die Verwendung von Kerberos stellt eine sichere Authentisierungsmethode dar. Da nicht alle Applikationen und Dienste über Kerberos-Unterstützung verfügen, werden Ausnahmen konfiguriert und dokumentiert werden müssen.

Tim MalcomVetter, Head of Managed Security Services bei Cyderes, hatte im Februar 2019 eine Twitter-Umfrage zur Konfiguration mit Squid Proxy und Kerberos durchgeführt. Von 68 Stimmen haben 75% noch keine solche Konfiguration vorgenommen und die anderen 25% haben zugestimmt, dass es nichts Schwierigeres gibt. In diesem Sinne hoffen wir, dass dieser Artikel bei kommenden Installationen und Konfigurationen eine Hilfe darstellt und die Implementation erfolgreich durchgeführt werden kann.

Michael Schneider

UNAUFFÄLLIGE KLEINIGKEITEN KÖNNEN MASSGEBLICH EINEN SIEG ENTSCHEIDEN

Bildquelle: https://pixabay.com/images/id-7373562/

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