MONTHLY SECURITY SUMMARY

)SCIP(

AUSGABE FEBRUAR 2022
HEIMNETZWERKE UND SOUVERÄNITÄT VON KI

ABSICHERN VON HEIMNETZWERKEN

Das Absichern von privaten Netzwerken ist wichtig. Wir diskutieren einige Tipps wie sie eine sichere Segmentierung umsetzen und ein möglichst solides WLAN realisieren können.

AGENCY-KONZEPT VON MASCHINEN

Um die Vorteile der KI zu nutzen und ihre Risiken zu mindern, können Handlungssouveränität und Vertrauen eine entscheidende Rolle spielen. Das Gebiet der maschinellen Agency umfasst die Macht der Maschinen.

Februar 2022: Ransomware als Business

Die *Kommerzialisierung der Cyberkriminalität* schreitet unaufhörlich voran. Viren-Entwickler der 90er Jahren haben sich noch über Kreativität definiert. Malware-Entwickler von heute freuen sich nur noch über klingelnde Kassen.

Jahrelang hat man Passwörter und Kreditkarteninformationen abgesaugt, um sie auf dem Schwarzmarkt zu verkaufen. Heute wird *Ransomware* eingesetzt, um Daten unzugänglich zu machen. Mit erpresserischem Nachdruck sollen diese von den Opfern freigekauft werden. Krankenhäuser hatten es zuerst diesbezüglich in die Medien geschafft. Ihre jahrelange Nachlässigkeit sowie die Brisanz einer Fehlbarkeit sind der Grund für die schlechte Publicity.

Unsere *Vernetzbarkeit* führt unweigerlich zu Verletzbarkeit. Für unseren Alltag wird unter Umständen plötzlich alles zur kritischen und damit schützenswerten Infrastruktur. Dessen ist man sich mancherorts noch nicht bewusst, lächelt bevorzugt die Risiken weg. Vielleicht braucht es halt tatsächlich zuerst einen tagelangen Ausfall des öffentlichen Verkehrs, bis man die neue Bedrohung akzeptiert. Es bleibt zu hoffen, dass der Zug dann noch nicht abgefahren ist.

Marc Ruef
Head of Research

NEWS

WAS IST BEI UNS PASSIERT?

INTERVIEW ZUR ZUNAHME VON DATENLEAKS

Die letzten Jahre haben die Anzahl der *Datenleaks*, die an die Öffentlichkeit gekommen sind, massiv zugenommen. Dies ist nicht nur ein Phänomen in der Schweiz, sondern betrifft die ganze Welt. In einem *ausgiebigen Interview* bespricht Marc Ruef dieses vielschichtige Thema mit dem Journalisten Enrique Heer von *SRF*. Es werden Hintergründe, Entwicklungen und Abläufe besprochen.

FERNSEHINTERVIEW ZU RANSOMWARE-ANGRIFFEN IN DER SCHWEIZ

Die *Top News* vom 04. Februar 2022 beschäftigen sich mit einem *Ransomwareangriff* auf den Flughafendienstleister in der Schweiz. Im Fernsehbeitrag der Journalistin Cornelia Stutz kommt Marc Ruef zu Wort, der die Hintergründe und den Ablauf solcher kommerziell getriebener Angriffe erläutert. Der Beitrag kann ebenfalls online gesehen werden.

INTERVIEW IN RENDEZ-VOUS VON SRF

Die Informationssendung Rendez-vous berichtet über das aktuelle Geschehen in Politik und Wirtschaft und liefert Hintergründe und fundierte Analysen. Der Journalist Dario Pelosi hat sich mit Marc Ruef unterhalten. Dabei wird besprochen, welche kommerziellen sowie technischen Aspekte moderne *Cyberkriminalität* mit sich bringt und wie *Whitehat-Hacker* bei der Verteidigung von KMUs helfen können.

Weitere News zu unserem Unternehmen finden Sie auf unserer Webseite.

SCIP BUCHREIHE

UNSER AKTUELLES JAHRBUCH

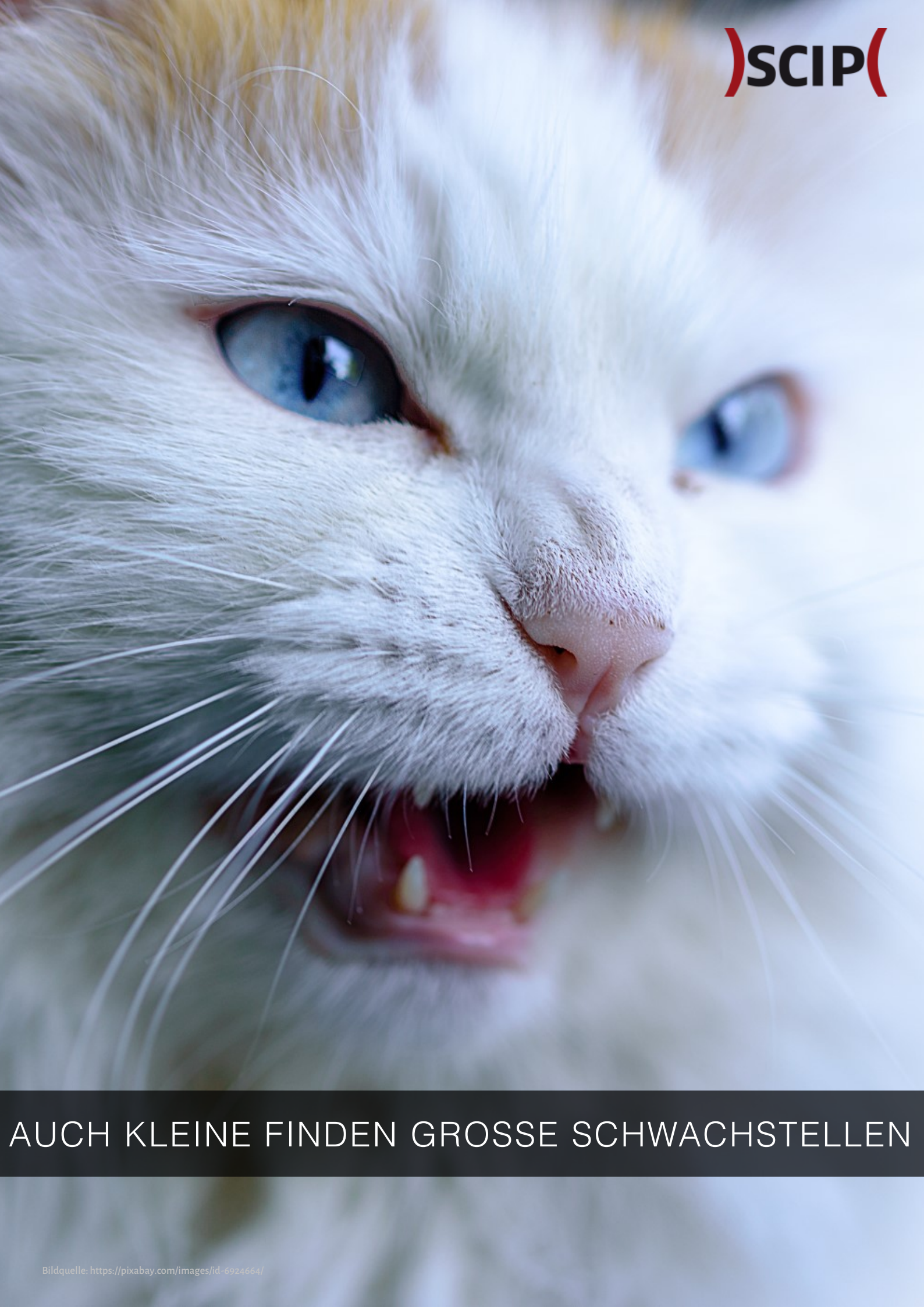
Erneut veröffentlichen wir die aktuelle Ausgabe unseres Jahrbuchs. Bereits zum 11ten Mal fassen wir in diesem die Fachbeiträge von einem Jahr Forschung im Bereich Cybersecurity zusammen.

Das Buch ist wiederum sowohl in deutscher (ISBN 978-3-907109-26-7) als auch in englischer Sprache (ISBN 978-3-907109-27-4) verfügbar. Das Vorwort wurde von Marko Rogge, seines Zeichens IT-Sicherheitsbeauftragter für Mobile Security bei der Deutschen Bahn AG, verfasst.

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 und Bestellungen auf unserer Webseite.

ISBN 978-3-907109-26-7 [de]
ISBN 978-3-907109-27-4 [en]



AUCH KLEINE FINDEN GROSSE SCHWACHSTELLEN

Bildquelle: https://pixabay.com/images/id-6924664/

RALPH MEIER

SICHERHEIT IM HEIMNETZWERK ERHÖHEN

Sie haben letztens eine *Amazon Alexa* oder ein anderes *Internet of Things* Gerät zugelegt? Ihren Gästen gewähren Sie Zugriff in ihr WLAN-Heimnetzwerk ohne mit den Augen zu zwinkern? Sie wissen über alle Geräte in Ihrem Heimnetzwerk Bescheid, oder nur über einen Teil oder Sie haben gar den Überblick verloren?

Dieser Beitrag soll einige Tipps zur Sicherheit im Heimnetzwerk aufzeigen und Sie bei der Neuinstallation Ihres WLANs unterstützen.

AUSLIEFERUNGSKONFIGURATION EINES ROUTERS

Die meisten Router für den Heimgebrauch erstellen im Installationsprozess nur ein *WLAN mit dem Gerätenamen* und verwenden ein *vordefiniertes Passwort*. Dies ist entweder ein Standardpasswort oder ein individuelles auf dem Router aufgedrucktes Passwort. Für Anwender, welche sich nicht gross mit dem Thema Netzwerkeinstellungen befassen, resultiert also ein einziges Netzwerk, mit welchem logischerweise alle Computer und Smartphones verbunden werden. Damit ist jedoch noch nicht Schluss: Man hat vielleicht noch einen smarten Lautsprecher, einen Smart TV, eventuell einen Hub für Smart Home Geräte und irgendwann kommt ein neues Küchengerät ins Haus, welches neu auch über eine Internetanbindung verfügt. Wenn Gäste zu Besuch sind, brauchen diese teilweise auch einen Internetzugang, somit werden deren Geräte auch ins Netzwerk hinzugefügt.

AUFKOMMENDE PROBLEME

Wenn alle Geräte in ein einziges Netzwerk eingebunden werden, kann dies zu verschiedenen Problemen führen. Zum einen kann man schnell den *Überblick aller mit dem Netzwerk verbundenen Geräte* verlieren. Zum anderen sehen alle Netzwerkteilnehmer geteilte Dateien, sofern öffentliche Freigaben oder Netzlaufwerke vorhanden und falsch beziehungsweise nicht geschützt konfiguriert sind. Es kommen Geräte mit unterschiedlichem und teilweise auch unbekanntem Softwarestand ins Netzwerk und bringen damit unbekannte Sicherheitslücken mit sich.

Alle Geräte können untereinander kommunizieren, da sie im selben Netzwerk sind, das macht es Angreifer leichter, von einem infizierten Gerät auf andere Geräte, wie zum Beispiel den persönlichen Computer, zu springen. Durch die Vermischung von allen Gerä-

ten, sprich Geräten mit privaten Dateien und Internet of Things (IoT) Geräten, wird das *Erstellen von Firewall Regeln schwieriger*. Denn IoT Geräte zum Beispiel müssen oft vom Internet aus angesprochen werden können, um den vollständigen Funktionsumfang nutzen zu können.

SICHERHEITSTIPPS FÜRS HEIMNETZWERK

Es folgen einige grundlegende Verbesserung für mehr Sicherheit im Heimnetzwerk.

Erste Schritte

Bei der Inbetriebnahme eines neuen Routers sollten zuerst die *Standardeinstellungen unverzüglich* angepasst werden. Dies bedeutet, das Passwort fürs WLAN zu ändern auf eine zufällige Abfolge von Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen mit einer Mindestlänge von 12 Zeichen. Da dieses Passwort pro Gerät nur einmal eingeben werden muss, kann es auch gerne länger sein.

Der Name des Netzwerks, die sogenannte SSID (Service Set Identifier), sollte nicht das Modell oder den Hersteller des eingesetzten Routers enthalten. Es empfiehlt sich auch ein Name zu wählen, welcher nicht auf den eigenen Haushalt zurückzuführen ist.

Anschliessend sollte die eingesetzte Verschlüsslungsmethode für das Drahtlosenetzwerk auf die höchstmögliche Option gesetzt werden, zum Zeitpunkt dieses Artikels ist dies *WPA3*.

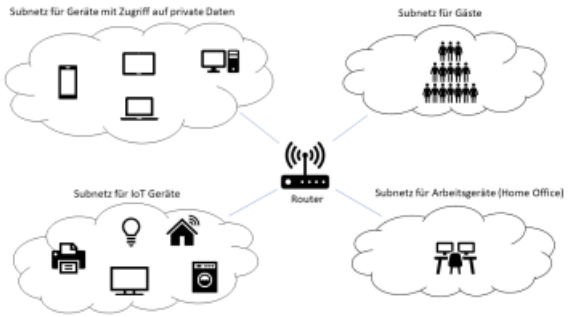
Nun sollte geprüft werden, ob für den Router neue Updates bereitstehen, sowie die Option zukünftige Updates automatische zu installieren, aktiviert werden.

Was tun, wenn noch Geräte vorhanden sind, welche WPA3 nicht unterstützen?

Die beste Lösung wäre, diese Geräte in ein eigenes Virtuelles Lan (VLAN) zu stecken und dort WPA2 zu verwenden. Falls der Router kein WPA3 beziehungsweise WPA2 unterstützt, sollte dieser zeitnah ersetzt werden durch ein neueres Modell.

Gastnetzwerk

Viele heutige Router verfügen über die Option, *ein separates Gastnetzwerk* einzurichten. Dies ist ein ei-



genständiges Subnetz, das über eine eigene SSID und ein eigenes Passwort verfügt. Sofern man seinen Gästen einen Internetzugang zu Verfügung stellen möchte, sollte man dies so konfigurieren.

Damit lösen sich gleich einige zuvor aufgezählte Probleme auf einen Schlag. Einige Router bieten zudem eine Funktion, welche einen QR-Code generiert, um das einfache Verbinden mit dem Gastnetzwerk zu ermöglichen.

Weitere Einstellungen

Nach der Unterteilung zwischen Heimnetzwerk und Gastnetzwerk sollten die restlichen Konfigurationsmöglichkeiten des Routers durchgegangen und überprüft werden. Einige Router bieten verschiedene Funktionen wie eine NAS-Funktionalität oder einen FTP-Server. Hierbei gilt, *sofern die Funktionalität gerade nicht verwendet wird, sollte sie deaktiviert werden*. Dies gilt auch für den Zugriff auf die Administratoroberfläche des Routers aus dem Internet. Sofern diese Option aktiv ist, empfehlen wir, diese zu deaktivieren.

NETZWERKSEGMENTIERUNG

Durch das Anwenden einer Netzwerksegmentierung wird ein Netzwerk in mehrere Subnetze oder VLANs unterteilt. Dies ist etwas für fortgeschrittene Anwender und oft nicht mit Standardroutern umsetzbar.

Ziel dabei ist es, ein *grosses flaches Netzwerk in kleine Subnetze mit "ähnlichen" Geräten zu unterteilen* und somit die Angriffsfläche zu reduzieren.

Mit ähnlichen Geräten ist gemeint, dass in ein erstes Subnetz zum Beispiel alle Geräte mit privaten Daten oder mit Zugang zu privaten Daten, wie Computer, Tablets und Smartphones hineinkommen. In ein weiteres Subnetz kommen Drucker, Fernseher, IoT Geräte und deren Hubs. Dann gibt es ein Subnetz für Gäste und eventuell ein weiteres für das Arbeiten im Homeoffice.

Durch solch eine Unterteilung können Firewall-Regeln pro Netzsegment eingeführt werden und somit auch effizienter und genauer konfiguriert werden. Verbindungen vom ersten Subnetz kann in das Subnetz mit IoT Geräten und Druckern zugelassen

werden, wobei eine Verbindungsanfrage in die Gegenrichtung blockiert werden kann.

Durch die Einführung von verschiedenen Subnetzen wird auch die laterale Ausbreitung bei einem Cyber-Angriff erschwert beziehungsweise je nach Konfiguration verunmöglicht.

TIPPS FÜR DEN KAUF VON SMARTEN GERÄTEN

Vor dem Kauf von internetfähigen Produkten, welche ins Heimnetzwerk eingebunden werden oder Geräte für den Netzwerkausbau an sich, sollten folgende Aspekte berücksichtig werden:

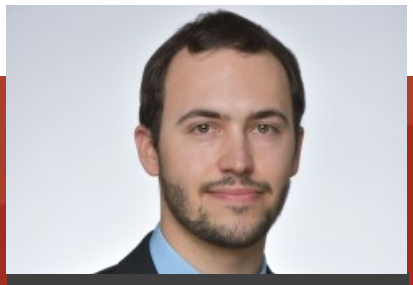
- Wird das Gerät per Kabel oder kabellos ins Netzwerk eingebunden? Ist es kompatibel mit dem bestehenden Netzwerk und kann die volle Geschwindigkeit ausschöpfen werden?

- Wird es vom Hersteller mit regelmässigen Updates versorgt, bestehen öffentlich bekannte Schwachstellen für das Gerät? Gut eignet sich die *VulDB* für das Prüfen auf öffentlich bekannte Schwachstellen von Produkten.

- Es empfiehlt sich auch intensiv zu potenziellen Problemen oder Unklarheiten zu recherchieren in spezifischen Foren, Rezession bei verschiedenen online Shops oder auch App Rezessionen zu durchforsten.

FAZIT

Für ein sicheres Heimnetzwerk sind die Änderung der Standardeinstellung, die Verwendung aktueller Software auf Router und Endgeräte sowie der Einsatz von sicheren Passwörtern essenziell. Ein *gutes Gerätemanagement*, eine Unterteilung in Heimnetzwerk und Gastnetzwerk oder sogar eine spezifischere Netzwerksegmentierung bringen zusätzliche Sicherheit. Ebenfalls ist es wichtig sich vor dem Kauf intensiv zu informieren, um Geräte zu wählen, welche über die gewünschten Funktionen verfügen und untereinander kompatibel sind. Um ungewollte bekannte Schwachstellen beim Neueinbinden von Geräten zu vermeiden, sollten im Voraus eine Schwachstellendatenbank konsultiert werden.



Ralph Meier

WIR SIND IHR PARTNER FÜR PROFESSIONELLE

CYBERSECURITY SERVICES

EINFACH ONLINE BESTELLEN

MARISA TSCHOPP

AGENCY VON MENSCH UND MASCHINE

Komplexe automatisierte Systeme und *künstlichen Intelligenz* (KI) finden zunehmend Eingang in den Konsumkontext. Nutzer ohne Fachkenntnisse werden mit diesen Systemen konfrontiert, wobei die Transparenz und das Verständnis für die Technologie unterschiedlich ausgeprägt sind. Den meisten ist unklar, wie sich die Interaktion mit diesen Systemen auf ihr Leben auswirken kann, ob in positiver oder in negativer Hinsicht. In einer idealen Welt stellen wir uns vor, dass wir die Vorteile von KI nutzen und gleichzeitig die Risiken minimieren können. Aus diesem Grund wurde das *IEEE Trust and Agency Committee* gegründet. Insbesondere im Verbraucherkontext und in dieser Übergangsphase der Innovation, wird das Vertrauen des Endnutzers und die Handlungssouveränität des Endnutzers (und das Zusammenspiel mit der Handlungsfähigkeit von Maschinen) eine Schlüsselrolle spielen, ob diese komplexen Systeme effektiv, nachhaltig und sicher genutzt werden können.

Das englische Wort *Agency* hat keine klare Übersetzung im Deutschen und wird hier Handlungssouveränität genannt. Vertrauen und Handlungssouveränität im Zusammenhang mit Technologie werden in verschiedenen Bereichen diskutiert, z.B. Mensch-Roboter-Interaktion, Human Factors, User Experience (UX) durch die Perspektive verschiedener Disziplinen, wobei Philosophie, Psychologie, Soziologie und Ethik im Vordergrund dieser Diskussionen stehen. Allerdings scheint es *wenig Übereinstimmung* bei den Definitionen und Methoden zu geben, die in der Forschung und Praxis verwendet werden.

Ein ähnliches Problem gibt es bei der Interpretation von Vertrauen (engl. Trust) und der Art und Weise, wie sich Menschen auf Maschinen verlassen (engl. Reliance). Das englische Wort lautet hier ‘reliance’, was auch oft mit Vertrauen übersetzt wird, wobei eine andere Bedeutung dahintersteht. Vertrauen wird im Mensch-Maschine Kontext sogar von *Vertrauensskeptikern* insgesamt in Frage gestellt, die behaupten, dass man KI-Systemen nicht trauen kann – oder, in den berühmten Worten von Joanna Bryson: *AI is nothing to be trusted!*

Das IEEE Trust and Agency Committee versucht eine Grundlage für eine offene Diskussion und Neubewertung der Begriffe Vertrauen, Reliance und Handlungssouveräntät (Agency) im Zusammenhang mit KI zu schaffen. Das Verständnis dieser Konzepte und ihrer Beziehung zu anderen Faktoren (eine grosse

Bandbreite von dispositionellen bis hin zu situativen Variablen wartet darauf, erforscht zu werden) soll zu Entwickler wich auch Nutzer positiv beeinflussen. Der Artikel soll auch die Designer solcher Systeme positiv inspirieren, z. B. ob und wie sie *Design for Agency* umsetzen können und ihre Nutzer in der Verwendung ihrer Systeme schulen wollen. Genauer gesagt, wie sie Produkte genauer vermarkten können oder noch genauer gesagt, ethischer. Letztendlich möchte das Kommittee zu den ersten gehören, die Standards entwickeln, welche die Handlungssouveränität der Endnutzer fördern.

VERTRAUEN VERSUS VERTRAUENSWÜRDIGKEIT

Lee & See haben bedeutende, weitreichende Erkenntnisse zum Thema Vertrauen in Automatisierung geliefert, wobei sie sich auf (mindestens) drei Komponenten konzentrieren: (1) Vertrauen ist eine Einstellung, (2) Vertrauen ist auf ein Ziel gerichtet und (3), zu vertrauen beinhaltet das Risiko verletzt zu werden. Das bedeutet die Situation ist durch Ungewissheit gekennzeichnet, die den Vertrauensgeber gegenüber dem Vertrauensnehmer verwundbar macht. Können wir menschliches Vertrauen und Vertrauenswürdigkeit direkt auf die Interaktion zwischen Mensch und Maschine übertragen? Einige Leute sagen ja, aber mit Modifikationen: Zwischenmenschliches Vertrauen, d. h. Vertrauen in oder zwischen Menschen, kann im Prinzip in Vertrauen in Maschinen übersetzt werden. Mit dem grossen Unterschied, dass es sich beim Mensch-Maschine Vertrauen eher um eine unidirektionale Beziehung handelt.

> *Mensch-Maschine Vertrauen kann als eine besondere Art von zwischenmenschlichem Vertrauen betrachtet werden, bei dem der zu Vertrauende einen Schritt vom Vertrauensgebenden entfernt ist. (Hoff & Bashir, 2015)*

In der Regel wird Vertrauen erforscht, indem man das Wesen des Menschen oder – in der Mensch-Maschine-Interaktion – die Eigenschaften von Maschinen betrachtet. In diesem Zusammenhang sprechen wir von *Vertrauenswürdigkeit*: Vertrauenswürdigkeit als Merkmal von Menschen oder als Eigenschaft von Maschinen. Beim zwischenmenschlichen Vertrauen wurden drei Eigenschaften als Elemente der Vertrauenswürdigkeit identifiziert: Fähigkeiten, Integrität und Wohlwollen. In ähnlicher Weise hängen verschiedene Attribute der *Vertrauenswürdigkeit*

von Maschinen von leistungsbasierten Attributen (d.h. wie gut ist das Produkt), Prozessmerkmalen (d.h. wie ist das System für einen Nutzer verständlich) und Wohlwollen ab. Letzteres ist ein zweckbasiertes Attribut, das sich auf die Absicht der Designer bezieht, warum dieses System gebaut wurde.

Vertrauen und Vertrauenswürdigkeit stehen in einer komplizierten Beziehung, die nicht immer auf die logischste Weise funktioniert. Im Idealfall würden Menschen ihr Vertrauen in Menschen setzen oder sich auf Maschinen verlassen, die als vertrauenswürdig erachtet werden. Menschen oder Maschinen, die ihr Vertrauen nicht verdienen, würden sie ablehnen und sich nicht auf sie verlassen und die Konsequenzen tragen. So kann beispielsweise ein Unternehmen oder ein System (es muss noch erforscht werden, wer der eigentliche Empfänger des Vertrauens ist) als vertrauenswürdig eingestuft werden, der Nutzer vertraut dem System und nutzt es. In einem anderen Fall hat der Betreiber keine Ahnung von dem Unternehmen oder dem System, vertraut ihm nicht und nutzt es dennoch. Es sind verschiedene Szenarien denkbar, die zu unterschiedlichen Beziehungen zwischen Vertrauen und Nutzung führen, die mit Merkmalen der Vertrauenswürdigkeit verbunden oder davon abhängig sein können.

Obwohl es also logisch ist, sich auf die Vertrauenswürdigkeit zu konzentrieren, ist sie nicht notwendigerweise das Wundermittel zur Vertrauensbildung und garantiert nicht, dass sich Nutzer auf die Maschine verlassen. Die konkreten Bedingungen für Vertrauenswürdigkeit und ihre Korrelate bleiben unklar. Das vorherrschende Rätsel um die Rolle der *Transparenz* ist ein gutes Beispiel dafür, wie unübersichtlich und widersprüchlich diese Beziehungen sein können. Es gibt zahlreiche *empirische Belege* dafür, dass bei Interaktionen zwischen Mensch und Maschine Transparenz positiv mit Vertrauen korreliert ist (meist wird dies als kognitives Vertrauen bezeichnet). Das bedeutet, je mehr wir verstehen und kontrollieren können, desto mehr vertrauen wir der Maschine und werden sie wahrscheinlich auch nutzen. Forscher haben jedoch auch *Beweise für das Gegenteil* gefunden, nämlich dass Transparenz eine *negative* Wirkung auf das Vertrauen haben kann. Ausgehend von dieser Überlegung könnte man sich fragen, wie wir ein effektives Vertrauensverhältnis zu Maschinen schaffen können, bei dem wir eine Art oder ein angemessenes Mass an Autorität über die

Maschine behalten? Wir gehen davon aus, dass ein Schlüssel zur Beantwortung dieser Frage in der Ermöglichung von Handlungssouveränität als Mittel zur Kontrolle liegen könnte.

SPANNUNG ODER DYNAMIK: MENSCHLICHES UND MASCHINELLES HANDELN

Die meisten Menschen werden nie verstehen, wie KI Systeme funktionieren. Einige jedoch schon, und man kann sie um Hilfe und Rat fragen. Ausserdem schützen einige Gesetze die Nutzer vor böswilligen Handlungen, z. B. der Missachtung des Datenschutzes. Es gibt noch eine dritte Möglichkeit, die wir hervorheben möchten. Es ist unpraktisch und unmöglich, jeden über die Einzelheiten von KI aufzuklären. Genauso wie man nicht jedem beibringen kann, wie ein Auto funktioniert. Man kann jedoch die Grundlagen der Mechanik lehren, und man muss die Regeln und Richtlinien verstehen, wie man ein Auto sicher benutzt. Dies kann auch für KI Systeme gelten. Menschliche Agency bedeutet, dass Menschen die *Macht* haben, ihre Lebensumstände zu gestalten, ihre Zukunft zu entwerfen und Handlungsalternativen zu ändern, wenn der aktuelle Status quo nicht den eigenen Werten oder Zielen entspricht (Bandura, 2006).

Menschen *sollten* die Macht haben, die Art und Weise ihrer Technologienutzung zu gestalten. Das sollte steht jedoch in Anführungszeichen, weil viele Systeme so konstruiert sind, dass sie die Entscheidungsfindung des Menschen beeinträchtigen, z. B. durch süchtig machende oder anthropomorphe Designmerkmale oder durch übertriebenes Marketing, um nur einige Beispiele zu nennen. Die Förderung der Handlungssouveränität des Endnutzers als Standard für die Gestaltung und Entwicklung von Produkten, wird den Menschen die Möglichkeit geben, Fähigkeiten zur Selbstregulierung und den Glauben an ihre Wirksamkeit zu entwickeln. So können sie Alternativen schaffen, ihre Handlungsfreiheit erhöhen und somit erfolgreicher sein, wenn sie sich für Technologien und Strategien entscheiden, die sie wirklich wünschen. Was die menschliche Agency zu einem so heiklen Thema macht, ist ihre dynamische Interaktion mit der *Maschinen Agency*. Wir müssen noch erforschen und verstehen, wie wir das Spannungsverhältnis zwischen der Macht der Maschinen und der Macht der Menschen lösen können: Welche Entscheidungen liegen in der Hand der Maschine und

welche in der Hand des Nutzers? Handelt es sich dabei um stabile oder dynamische Prozesse, und hängen sie von der Zuverlässigkeit der Maschine oder dem mit der Entscheidungsfindung verbundenen Risiko ab? Bedeutet mehr Maschinen Agency automatisch weniger Endnutzer Agency und umgekehrt? Was sind hier die genauen Zusammenhänge, Bedingungen, Korrelationen oder Dynamiken?

FAZIT

Es bleiben viele offene Fragen zu Vertrauen und Handlungssouveränität im Kontext der Mensch-KI-Interaktion: Wie kann der zeitliche und dynamische Kontext abgebildet werden, Vertrauensverläufe oder Grenzen der Handlungsouveränität. Was ist der Einfluss von Gesetzen und Kultur, Bildung und vieles mehr. Ist Vertrauen eine Vorbedingung für menschliche Agency oder ist menschliche Agency eine Vorbedingung für Vertrauen? Ist Vertrauen überhaupt relevant und sollten wir besser aufhören, über Vertrauen zu sprechen? Die Synthese dieser Themen und der Versuch, sie zu modellieren, ist eine grosse Herausforderung. Vor allem angesichts der Neuartigkeit und Dynamik der Situation und angesichts der Tatsache, dass die Definition des Artefakts, das uns interessiert, nämlich Systeme der künstlichen Intelligenz, selbst umstritten ist.

Das neu gegründete *IEEE Trust in Agency Committee* hat sich zum Ziel gesetzt, die Entwicklung einer erfolgreichen Transdisziplinarität rund um KI zu unterstützen, verbunden mit dem Wunsch, das praktische Feld der Technologie nicht allein einer vermeintlich erhabenen Perspektive zu überlassen.

Danksagung

Wir danken Shyam Sundar und John Havens für ihre Unterstützung beim Verfassen dieses Artikels. Eine Kurzfassung des Beitrags mit zusätzlichen Einblicken in die Arbeit des Komitees finden Sie auf der Homepage *IEEE Beyond Standards*.

Marisa Tschopp

ALLE PERSÖNLICHEN DATEN SIND SCHÜTZENSWERT

Bildquelle: https://pixabay.com/images/id-6994245/

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