MONTHLY SECURITY SUMMARY

)SCIP(

AUSGABE SEPTEMBER 2023
VON BUG-BOUNTIES UND CHATBOT-SCAMS

BUG-BOUNTY ALS HERAUSFORDERUNG

Bug-Bounties als Belohnung für Schwachstellen in Systemen? Wir erläutern, welche Herausforderungen mit Bug-Bounties auftreten können.

ERKENNEN VON CHATBOT-SCAMS

Cyberrisiken machen auch im Umgang mit Chatbots keinen Halt. Wir zeigen deshalb auf, worauf man bei Chatbot-Scams besonders achten sollte.

September 2023: Gekommen, um zu bleiben

In einer zunehmend digitalisierten Welt sind wir von Computern und Online-Diensten abhängiger denn je. Mit dieser Abhängigkeit gehen jedoch auch steigende Risiken einher, insbesondere im Bereich der *Cybersecurity*. Ein aktuelles und alarmierendes Thema, das die Aufmerksamkeit von Unternehmen und Privatpersonen gleichermassen auf sich zieht, ist die Bedrohung durch *Ransomware*.

Ransomware ist besonders gefährlich, da sie nicht nur finanzielle Verluste für Opfer verursacht, sondern auch erhebliche Störungen in Geschäftsprozessen und persönlichen Leben verursacht. Unternehmen können Produktionsausfälle erleiden, Kundenvertrauen verlieren und empfindliche Daten verlieren. Privatpersonen können wichtige persönliche Dateien, wie Fotos und Dokumente, verlieren, die oft von unschätzbarem Wert sind.

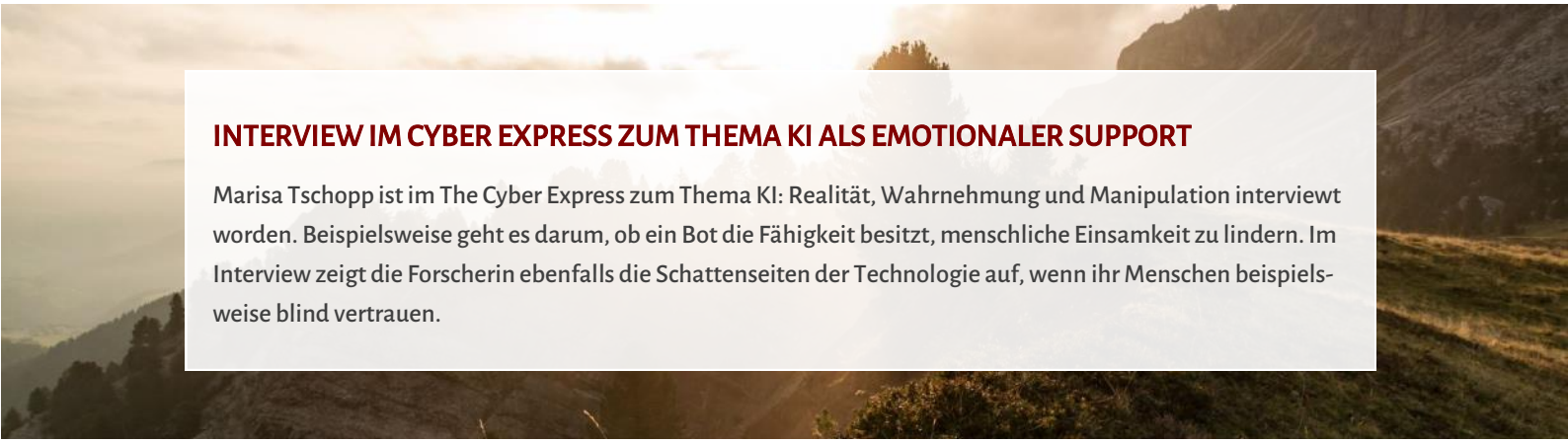
In den letzten Jahren haben sich Ransomware-Angriffe weiterentwickelt und professionalisiert. Die Täter nutzen immer raffiniertere Techniken und Werkzeuge, um ihre Angriffe durchzuführen. Ein besorgniserregender Trend ist die gezielte Ausrichtung auf *kritische Infrastrukturen*, wie Energieversorgungsunternehmen oder Gesundheitseinrichtungen. Diese Angriffe können nicht nur finanzielle Schäden verursachen, sondern auch die öffentliche Sicherheit gefährden.

Die Zukunft vorauszusagen ist immer schwierig. Aber eines ist klar: Ransomware ist gekommen, um zu bleiben.

Marc Ruef
Head of Research

NEWS

WAS IST BEI UNS PASSIERT?

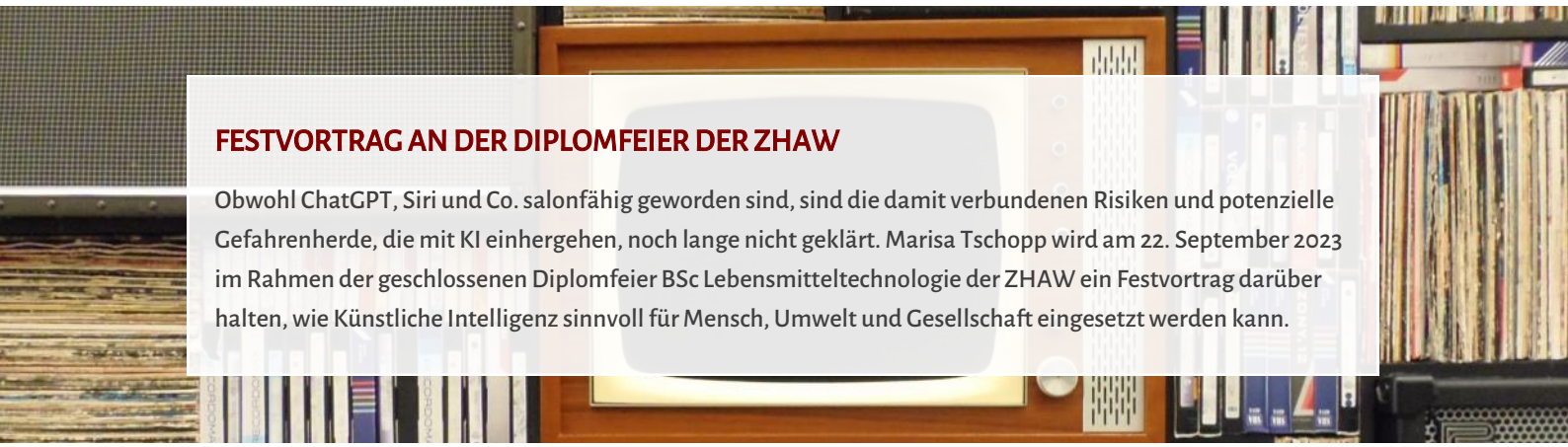


INTERVIEW IM CYBER EXPRESS ZUM THEMA KI ALS EMOTIONALER SUPPORT

Marisa Tschopp ist im The Cyber Express zum Thema KI: Realität, Wahrnehmung und Manipulation interviewt worden. Beispielsweise geht es darum, ob ein Bot die Fähigkeit besitzt, menschliche Einsamkeit zu lindern. Im Interview zeigt die Forscherin ebenfalls die Schattenseiten der Technologie auf, wenn ihr Menschen beispielsweise blind vertrauen.

INTERVIEW IM SRF ÜBER 25 JAHRE GOOGLE

Marc Ruef wurde vom SRF zum 25 jährigen Bestehen von Google interviewt. Die Erfolgsgeschichte des Tech-Giganten habe sich seit der Gründung im Jahre 1998 jedoch nicht nur zum positiven weiterentwickelt. Das Thema Datenschutz beeinträchtigt das Kerngeschäft des Konzerns, denn durch die strenger werdenden Datenrichtlinien werde es für Google schwieriger, die gewünschten Nutzerdaten im Werbeumfeld einzusetzen.



FESTVORTRAG AN DER DIPLOMFEIER DER ZHAW

Obwohl ChatGPT, Siri und Co. salonfähig geworden sind, sind die damit verbundenen Risiken und potenzielle Gefahrenherde, die mit KI einhergehen, noch lange nicht geklärt. Marisa Tschopp wird am 22. September 2023 im Rahmen der geschlossenen Diplomfeier BSc Lebensmitteltechnologie der ZHAW ein Festvortrag darüber halten, wie Künstliche Intelligenz sinnvoll für Mensch, Umwelt und Gesellschaft eingesetzt werden kann.

Weitere News zu unserem Unternehmen finden Sie auf unserer Webseite.

SCIP BUCHREIHE

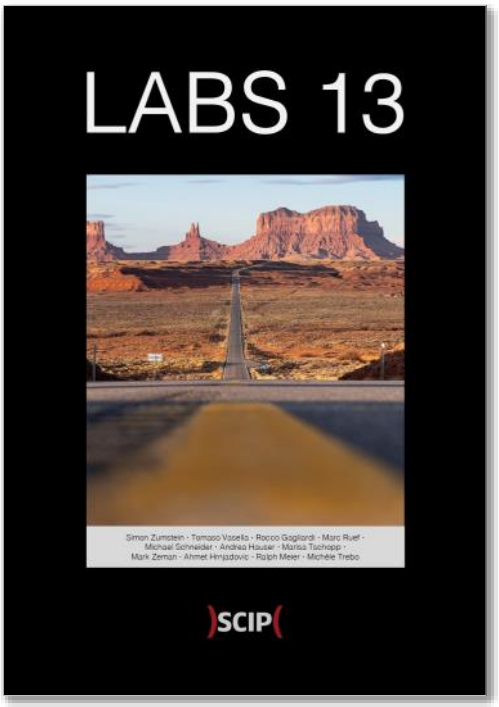
UNSER AKTUELLES JAHRBUCH

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.



)SCIP(

HERAUSFORDERUNGEN MIT BUG-BOUNTY

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

MARC RUEF

BUG-BOUNTY ALS HERAUSFORDERUNG FÜR UNTERNEHMEN

Viele Unternehmen haben erste Gehversuche mit sogenannten Bug-Bounties gemacht. Freiwillige Researcher sollen dafür entlöhnt werden, wenn sie Schwachstellen in Komponenten finden und diese melden. Verlockend ist die Idee, dass man weitestgehend auf regelmässige Security Tests verzichten kann und stattdessen nur noch pro Finding auszahlen muss. Dieser Beitrag diskutiert, wann eine Bug-Bounty sinnvoll ist, wie sie angegangen werden muss und welche Herausforderungen gegeben sind.

Bei einer Bug-Bounty sollen freiwillige Researcher mit einer Entlöhnung motiviert werden, Schwachstellen in Komponenten zu finden und frühzeitig zu melden. Dadurch sollen konkret exponierte Schwachstellen schnellstmöglich entdeckt und adressiert werden können, um das Zeitfenster für erfolgreiche Angriffe auf ein Minimum zu reduzieren. Um eine Bug-Bounty professionell und effizient durchführen zu können, gilt es gewisse Aspekte auszuarbeiten, zu dokumentieren und öffentlich bereitzustellen.

SCOPE EINGRENZEN

Grundsätzlich muss man sich darauf einigen, welchen Scope eine Bug-Bounty abdecken soll. Hier ist es einem freigestellt, welche Abgrenzungen man etablieren will. Viele Firmen definieren sämtliche öffentlichen erreichbaren Systeme. Andere fokussieren sich auf einzelne Services und klammern bestimmte Komponenten vollumfänglich aus.

Die Abgrenzung kann aber auch in der Form von konkreten Angriffstechniken erfolgen. Viele Bug-Bounties schliessen zum Beispiel destruktive Angriffe, bei denen eine Überlastung angestrebt wird, aus. Dazu gehören unter anderem klassische Flooding-Zugriffe, wie sie bei Denial of Service-Attacken genutzt werden.

Das Definieren eines möglichst breitflächigen Scopes lässt natürlich den Vorteil einer Bug-Bounty vollumfänglich entfalten. Man muss sich aber bewusst sein, dass eine Bug-Bounty auch immer ein Mehr an Testern motiviert. Es ist also konkret damit zu rechnen, dass die im Scope enthaltenen Komponenten

einem Mehr an Zugriffen, Stress und Angriffen ausgesetzt sind.

Das ist auch einer der Gründe, warum DoS- und DDoS-Angriffe in der Regel ausgeschlossen werden. Dabei handelt es sich meist um David gegen Goliath-Angriffe, bei denen früher oder später der Stärkere gewinnen wird. Dieses offensichtliche Konzept im Rahmen einer Bug-Bounty zu beweisen bringt keinen Mehrwert und stört stattdessen nur den regulären Betrieb.

Einige Hersteller schränken die für eine Bug-Bounty zugelassenen Teilnehmer ein. So wird bei Apple nur entlöhnt, wer zu dessen produktspezifischem Bug-Bounty-Programm zuvor eingeladen wurde. Bei sogenanntem Invite-Only handelt es sich um einen fragwürdigen Ansatz, vermag er nämlich ein Grossteil der potentiellen Teilnehmer nicht zu motivieren.

BELOHNUNG DEFINIEREN

Die Motivation für Researcher, sich mit einer Bug-Bounty auseinanderzusetzen, ist in den meisten Fällen die Bounty selbst. Schliesslich wollen sie für ihre Mühen entlöhnt werden. Aus diesem Grund ist es wichtig zu definieren und klar zu kommunizieren, welche Belohnungen zur Verfügung stehen. In den Anfangszeiten des Konzepts von Bug-Bounties wurden bedruckte Kaffeetassen und T-Shirts vergeben. Derlei Möglichkeiten können heutzutage nur noch ergänzend eingesetzt werden, müssen nämlich mittlerweile monetäre Anreize in Aussicht gestellt werden, um Researcher zu motivieren.

Je höher eine Entlöhnung ist, desto eher sind Tester bereit, ihre Zeit zu investieren, um qualitativ hochwertige Schwachstellen zu finden. Ein transparentes Preiskonstrukt hilft allen Seiten, klare und faire Verhältnisse zu schaffen. Grundsätzlich gibt es Preisbereiche für einzelne Server, Dienste oder Mechanismen. Traditionell werden darin Abstufungen für einzelne Schwachstellenklassen definiert. Ein fehlender HTTP-Header, der theoretisch eine Information Disclosure ermöglicht, wird da natürlich ganz anders eingestuft als eine SQL-Injection oder eine Memory Corruption. Hier kann auch ein Modell wie CVSS (Common Vulnerability Scoring System) beigezogen werden. Durch das Erstellen eines Vektors für

eine Schwachstelle lässt sich der Base Score ermitteln und anhand dessen den Preis ableiten.

Bei Bug-Bounties von Herstellern ist es wichtig, dass die Preise möglichst hoch sind. So kann verhindert werden, dass die gefundenen Schwachstellen stattdessen durch eine Ausnutzung oder den Weiterverkauf monetarisiert werden. Bei Bug-Bounties von produktiven Umgebungen ist dies teilweise vergleichbar. Auch hier sollte die Entlöhnung natürlich hoch genug sein, so dass sich ein böswilliges Ausnutzen nicht lohnt. Vor allem bei sehr kritischen Problemen, die eine ganzheitliche Kompromittierung ermöglichen können, sollte nicht gespart werden.

Das Auszahlen der Bug-Bounties kann sich manchmal schwieriger gestalten, als angenommen. Gerade wenn die Researcher in fremden Ländern sitzen und dort das Bankwesen nicht oder nur teilweise etabliert wurde. So ist es dann auch nicht unüblich, dass in solchen Fällen die Auszahlungen über Paypal oder gar Bitcoin umgesetzt werden. Man sollte sich früh damit auseinandersetzen, welche Zahlungsmechanismen man unterstützen will. Auch hier hilft eine klare Kommunikation in der Definition der Bug-Bounty.

KOMMUNIKATIONSKANAL FESTLEGEN

Die Bug-Bounty kann auf der öffentlichen Webseite als solche ausgeschrieben werden. Dadurch ist sie einfach und unkompliziert durch die Interessenten erreichbar.

In RFC 9116 wird ein simples Dateiformat definiert, dass das Anbieten von Bug-Bounties und das Etablieren von Kommunikationskanälen vereinheitlichen und vereinfachen soll. So soll auf einem Webserver eine Textdatei unter /.well-known/security.txt abgelegt werden, die die folgenden Informationen beinhalten kann:

Feld	Beschreibung
Acknowledgments	Link zu einer Seite, die eine Hall of Fame bereitstellt
Canonical	Eine Canonical-URL der Lokation der security.txt
Contact	Kontaktinformationen, wie Mailadressen, Kontaktformulare oder Telefonnummern
Encryption	Informationen zur Verschlüsselten Kommunikation
Expires	Datumsangabe, wann die Informationen im security.txt verfallen
Hiring	Link zu einer Seite, die offene Stellen anzeigt
Policy	Link zu einer Seite, die die Bestimmungen der Bug-Bounty zeigt
Preferred-Languages	Liste von Sprachen, für die eine Kommunikation gewährleistet werden kann

Eine simple security.txt, so wird sie bei uns eingesetzt, kann also so aussehen:

```
Contact: mailto:info@scip.ch
Contact: https://www.scip.ch/?contact
Expires: 2023-09-30T23:59:59.000Z
Acknowledgments: https://www.scip.ch/?bugbounty
Policy: https://www.scip.ch/?bugbounty
Hiring: https://www.scip.ch/?jobs
Preferred-Languages: en, de
```

Ein einfacher Kommunikationskanal wird bevorzugt, weshalb in erster Linie eine herkömmliche Kommunikation per Email zu etablieren ist. Kontaktformulare auf Webseiten können ebenso genutzt werden, wobei diese möglichst simpel gehalten werden sollten (keine Anmeldung erforderlich, nur wenige Felder). Eine verschlüsselte Kommunikation dank PGP ist empfohlen.

PROZESSE ETABLIEREN

Es muss, gerade in der Anfangszeit nach jedem Aufschalten der Bug-Bounty, mit einer gewissen Anzahl an Submissions gerechnet werden. Manche Security Researcher sind auf der Suche nach neu eröffneten Bug-Bounties und versuchen als erste mögliche Schwachstellen zu finden. Diese werden entsprechend über den etablierten Kommunikationskanal gemeldet. Die Abarbeitung gestaltet sich dann wie folgt:

1. Bestätigen des Empfangs der Submission
2. Plausibilisierung der Submission (sind die richtigen Komponenten getestet worden, klingen die Schwachstellen plausibel)
3. Weitere Details beim Submitter erfragen, falls erforderlich (z.B. Exploit, Video des Angriffs)
4. Weiterleiten und technisches Nachvollziehen der Schwachstellen
5. Bewerten der Schwachstelle (Priorität, Kritikalität)
6. Gegenmassnahmen planen, einleiten, umsetzen und prüfen
7. Akzeptieren oder Zurückweisen der Schwachstelle an den Submitter

8. Transaktion der Belohnung vorbereiten (Zahlungsmethode, Zahlungsinformationen)

9. Übermitteln der Belohnung und Hinzufügen des Submitters in die Hall of Fame

10. Lessons Learned in den neuen Prozess einfliessen und dokumentieren lassen

Wie bei allen Prozessen sollten diese formalisiert und dokumentiert werden. Dadurch lässt sich gewährleisten, dass auch bei einem hohen Datenaufkommen und engen Zeitplänen der korrekte Ablauf und mit ihr die erwartete Qualität gewährleistet werden kann.

Es besteht die Möglichkeit diese Abarbeitung an ein externes Bug-Bounty-Programm auszulagern. Verschiedene Firmen weltweit, auch solche in der Schweiz, bieten derlei Dienstleistungen im kommerziellen Bereich an. Man kann dabei von ihren Erfahrungen und etablierten Prozessen profitieren. Selbstverständlich fallen hierbei jedoch zusätzliche Kosten an. Eine Alternative ist das offene Projekt OpenBugBounty.

Generell ist es ein Problem, wenn viele falsche, fehlerhafte oder ungenaue Submissions bearbeitet werden müssen. Es ist nicht unüblich, dass gewisse Security Researcher durch automatisierte Skripte einfache Schwachstellen finden und von diesen Profitieren wollen. Solche Low Hanging Fruits werden oft aus dem Scope genommen und ihr minimales Risiko wird akzeptiert. Dazu gehört zum Beispiel oftmals das Akzeptieren von älteren Kommunikationsverschlüsselungen oder die vielen HTTP-Security-Header. Dennoch übergehen manche Security Researcher diese Vorgaben und generieren durch die unnötigen Submissions ein Mehr an Aufwand.

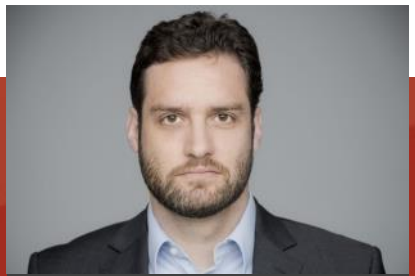
Nicht selten arten solche schwachen Submissions in sogenannte Beg Bounties aus: Die Submitter betteln darum, dass ihre Eingabe dennoch berücksichtigt und ausgezahlt wird. Hier empfiehlt es sich das Scoping sehr konsequent zu dokumentieren und auch durchzusetzen. Wer eine gute Submission macht, soll fair entlöhnt werden. Und wer sich nicht an die Regeln hält, muss mit Einschränkungen rechnen. In extremen Fällen können Submitter geblacklisted und vom Programm ausgeschlossen werden.

Um ein hohes Aufkommen an Submissions möglich effizient abarbeiten zu können, sollte für jeden Kommunikationsschritt entsprechende Templates ausgearbeitet werden. Diese lassen schnell und unkompliziert den aktuellen Stand oder die nächsten Schritte mitteilen.

FAZIT

Bug-Bounties klingen verlockend. Schliesslich muss man einfach ein paar Regeln definieren und kann dann von der Freiwilligkeit etwaiger Spezialisten profitieren. Dies ist aber nur bedingt korrekt. Die meisten Security Researcher, die sich auf Bug-Bounties spezialisiert haben, wollen mit möglichst wenig Aufwand möglichst viel Umsatz machen. Das Nutzen von Automatisierungen und das Fokussieren auf möglichst simple Schwachstellen ist dann im Fokus. Entsprechend ist ein absoluter Grossteil der Submissions von schlechter Qualität. Erfahrungsgemäss sind 99% der Submissions falsch oder minderwertig. Diese müssen dennoch bearbeitet und koordiniert werden. Entsprechend kann man nur von wenigen wirklich guten Submissions profitieren.

Zudem ersetzt eine Bug-Bounty keine anderen Sicherheitsmassnahmen. Informationssicherheit beginnt mit sicherer Entwicklung und wird gestützt durch professionelles Security Testing. Das Etablieren von Bug-Bounties ist ein Zusatz, der erst ganz am Schluss berücksichtigt werden soll. Andernfalls wird ein Bug-Bounty-Programm teurer und aufwändiger weder der Einsatz der etablieren Mechanismen. Wer sich als erstes und ausschliesslich auf Bug-Bounties verlässt, ist schlecht beraten.



Marc Ruef

MICHÈLE TREBO

CHATBOT-SCAMS: ERSCHLEICHEN PERSÖNLICHER INFORMATIONEN

Selbst heute, wo Technologie den Alltag in vielerlei Hinsicht erleichtert, sind nicht alle Fortschritte ohne Risiken. Eines der aufkommenden Bedrohungen im Online-Betrugsumfeld ist der Chatbot-Scam. Als Meisterwerk der Täuschung nutzen Kriminelle Chatbots, um mit potenziellen Opfern zu interagieren und sie in betrügerische Aktivitäten zu verwickeln. Diese raffinierte Form des Betrugs nutzt die fortschreitende Entwicklung von künstlicher Intelligenz und automatisierter Kommunikation, um das Vertrauen der Menschen zu gewinnen und sie dazu zu verleiten, persönliche Informationen preiszugeben, Geld zu überweisen oder auf andere Weise Opfer von finanziellen oder identitätsbezogenen Verbrechen zu werden. Hier wird näher darauf eingegangen, wie Chatbot-Scams erkannt und welche Schutzmassnahmen ergriffen werden können, um ein umfassenderes Verständnis für diese Gefahr zu entwickeln.

DEFINITION CHATBOT-SCAM

Der Begriff Chatbot-Scam beschreibt betrügerische Aktivitäten, bei denen Chatbots verwendet werden, um Nutzer zu täuschen und finanziell zu schädigen. Oft tarnt sich ein Chatbot-Scam als legitime Kundensupport-Anwendung, um das Vertrauen der Opfer zu gewinnen. Diese betrügerischen Chatbots können auf Social-Media-Plattformen, Messenger-Diensten oder Websites eingesetzt werden, um ihre Opfer anzulocken. Die Betreiber von Chatbot-Scams nutzen raffinierte Algorithmen, um automatisierte Gespräche zu führen und persönliche Informationen von ahnungslosen Nutzern zu sammeln. Ein häufiges Ziel von Chatbot-Scams ist es, sensible Finanzdaten wie Kreditkarteninformationen oder Bankdaten zu stehlen. Ein weiterer verbreiteter Chatbot-Scam ist der Versuch, Opfer dazu zu bringen, auf gefälschte Links zu klicken oder Malware herunterzuladen. Die Betreiber dieser betrügerischen Chatbots nutzen oft sozialpsychologische Taktiken, um Verwirrung zu stiften oder Druck auf die Opfer auszuüben, damit diese schnelle Entscheidungen treffen.

ERKENNEN VON CHATBOT-SCAMS

Das Erkennen eines Chatbot-Scams erfordert eine gewisse Aufmerksamkeit und Achtsamkeit. Um sich vor solchen betrügerischen Aktivitäten zu schützen, sollte man einige wichtige Anzeichen beachten:

1. Unrealistische Schnelligkeit – Chatbot-Scams sind oft darauf ausgelegt, automatisierte Antworten in Sekundenschnelle auszugeben. Wenn man bemerkt, dass der Chatbot ungewöhnlich schnell antwortet, ohne dass die Anfragen angemessen verarbeitet werden, könnte es sich um einen Betrugsversuch handeln.

2. Standardisierte Antworten – Da Chatbot-Scams vordefinierte Texte verwenden, neigen sie dazu, auf Fragen und Anliegen mit allgemeinen, nicht massgeschneiderten Antworten zu reagieren. Echte Kundensupport-Mitarbeiter hingegen können individueller und spezifischer auf Anfragen eingehen.

3. Fehlende Empathie – Betrügerische Chatbots sind nicht darauf programmiert, Empathie zu zeigen oder emotionale Unterstützung zu bieten. Echte Kundensupport-Vertreter hingegen können Verständnis für Ihre Gefühle und Bedürfnisse zeigen.

4. Aufforderung, persönliche Informationen bekannt zu geben: Wenn der Chatbot jemanden auffordert, persönliche oder finanzielle Informationen preiszugeben, wie beispielsweise Kreditkartennummer, Passwörter oder Sozialversicherungsnummer, dann sollte man besonders vorsichtig sein. Seriöse Unternehmen würden niemals solche Informationen über Chatbots anfordern.

5. Grammatik- und Rechtschreibfehler – Chatbot-Scams können oft Fehler in ihren Antworten aufweisen, da sie nicht menschliche Sprachmuster perfekt nachahmen können. Wenn also viele Grammatik- oder Rechtschreibfehler bemerkt werden, sollte man misstrauisch sein.

6. Verdächtige URLs oder Links – Betrügerische Chatbots könnten versuchen, Sie dazu zu bringen, auf Links zu klicken, die zu Phishing-Websites oder schädlicher Software führen. Seien Sie äusserst vorsichtig, wenn der Chatbot unerwartete Links sendet.

7. Wiederholte Phrasen – Wenn ein Chatbot immer wieder dieselben Sätze oder Fragen wiederholt, deutet dies darauf hin, dass es sich um eine auto-

matisierte Antwort handeln könnte. Echte Kundensupport-Mitarbeiter würden auf Abwechslung und individuelle Gespräche setzen.

8. Fehlende Kontaktdaten – Seriöse Unternehmen bieten normalerweise klare Kontaktinformationen, über die Sie den echten Kundensupport erreichen können. Fehlt diese Angabe im Chatbot, ist es ein Warnsignal für potenziellen Betrug.

9. Unangemessener Druck – Betrügerische Chatbots können versuchen, Druck auf Sie auszuüben, um schnelle Entscheidungen zu treffen, wie beispielsweise Ihre persönlichen Daten weiterzugeben. Echte Kundensupport-Vertreter würden Sie niemals zu solchen Massnahmen drängen.

10. Unbekannter Absender – Wenn Sie einen Chatbot kontaktiert haben, aber nicht sicher sind, wer der Absender ist oder von welchem Unternehmen er stammt, sollten Sie keine persönlichen Informationen preisgeben und stattdessen das Unternehmen direkt über eine verifizierte Kontaktoption erreichen.

SCHUTZ VOR CHATBOT-SCAMS

Um sich vor Chatbot-Scams zu schützen, sollten verschiedene Punkte beachtet werden.

1. Seien Sie skeptisch gegenüber unerwarteten Nachrichten von unbekannten Absendern, insbesondere wenn sie nach sensiblen Informationen oder Geld fragen.

2. Überprüfen Sie die Identität und Authentizität des Chatbots oder Absenders, bevor Sie persönliche Informationen weitergeben oder auf Anfragen reagieren.

3. Geben Sie niemals persönliche oder finanzielle Daten über einen Chatbot weiter, es sei denn, Sie sind sich absolut sicher, dass es sich um eine vertrauenswürdige Quelle handelt.

4. Klicken Sie nicht auf verdächtige Links, die Ihnen über Chatbots zugeschickt werden. Stellen Sie sicher, dass Links von seriösen Quellen stammen, bevor Sie daraufklicken.

5. Initiieren Sie Kontakte zu Unternehmen oder Dienstleistern selbst über offizielle Kanäle, anstatt auf Nachrichten von Chatbots zu reagieren.

6. Lassen Sie sich nicht unter Druck setzen, schnelle Entscheidungen zu treffen. Kriminelle nutzen oft Dringlichkeit, um Opfer zu überrumpeln.

7. Nutzen Sie eine zuverlässige Antiviren- und Anti-Malware-Software, um sich vor schädlichen Links oder Downloads zu schützen.

8. Bleiben Sie über aktuelle Betrugsmethoden auf dem Laufenden, um besser informierte Entscheidungen zu treffen.

9. Interagieren Sie nur mit bekannten und vertrauenswürdigen Chatbots oder Plattformen. Wenn Sie verdächtige Aktivitäten bemerken, melden Sie diese an die entsprechenden Behörden oder Plattformen, um andere vor möglichen Bedrohungen zu schützen.

Indem Sie diese Schritte befolgen und eine vorsichtige Herangehensweise an Online-Kommunikation entwickeln, können Sie Ihr Risiko, Opfer eines Chatbot-Scams zu werden, erheblich reduzieren.

ZUSAMMENFASSUNG

Chatbot-Scams werden immer anspruchsvoller und schwerer zu erkennen. Kriminelle setzen dabei Chatbots ein, um Opfer in betrügerische Handlungen zu verwickeln. Diese fortschrittliche Betrugsmethode nutzt künstliche Intelligenz und automatisierte Kommunikation, um Vertrauen zu schaffen und persönliche Informationen zu stehlen. Die Erkennung von Anzeichen wie raschen, gefühlsarmen Antworten oder Aufforderungen zur Preisgabe sensibler Daten ist hierbei von entscheidender Bedeutung. Um sich vor Chatbot-Scams zu schützen, ist gesunde Skepsis angebracht. Verifizierung der Absenderidentität und die Zurückweisung sensibler Informationen und verdächtiger Links sind ebenso wichtig. Um dieser zunehmenden Bedrohung zu begegnen, ist die enge Kooperation zwischen Internetnutzern, Unternehmen und Behörden unerlässlich, um die digitale Sicherheit zu stärken. Gleichzeitig liegt jedoch auch die Verantwortung bei jedem Einzelnen, sich proaktiv vor Chatbot-Scams zu schützen und zur kollektiven Sicherheit der Online-Community beizutragen.

Michèle Trebo

BEI NEUEN TECHNOLOGIEN GILT:
CHANCEN UND RISIKEN ABWÄGEN.

Bildquelle: https://unsplash.com/photos/vEE0oHx5d0Q

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