MONTHLY SECURITY SUMMARY

)SCIP(

AUSGABE DEZEMBER 2023
RÜCK– UND AUSBLICK

DAS WAR 2023

Wir lassen das Cybersecurity Jahr 2023 nochmal Revue passieren und fassen die nützlichsten scip-Tipps, Highlights und Geschichten von 2023 zusammen.

DAS WIRD 2024

Was erwartet die Cybersecurity Community im nächsten Jahr? Wir geben einen Ausblick im Rahmen unseres Forecasts für das kommende Jahr 2024.

Dezember 2023: Das war unser Jahr

Das Jahr 2023 neigt sich langsam aber sicher dem Ende zu. Ich weiss nicht, wie es Ihnen geht, aber ich lasse gerne in den letzten Tagen im Dezember mein Jahr nochmals Revue passieren. Wissen Sie noch, was sie so gemacht haben? Sind Sie vielleicht wie ich Fussballunterstützerin, und haben Ihre Lieblingsmannschaft im Stadion bejubelt ? Oder haben Sie sich für einen Studiengang an der Universität Zürich eingeschrieben, um in Ihre Ausbildung zu investieren? Während des Hitzesommers 2023 haben Sie Ihre Ferien irgendwo an einem kühleren Ort verbracht und den Sprung ins kalte Nass gewagt. Sie haben in diesem Jahr mit Spannung Ihre Zeitung gelesen, oder Ihr Zugticket online gekauft. Haben ein Päckli auf die Post gebracht, brav Ihre Steuererklärung ausgefüllt, sich vielleicht die Kinoknüller Barbie oder Oppenheimer angeschaut, aufgrund steigender Prämien noch die Krankenkasse gewechselt und sich arbeitstechnisch entfaltet, und zahlreiche inspirierende Konzepte, Arbeiten und Workshops vorbereitet. Unser Jahr 2023 war gespickt mit wundervollen Erinnerungen, oder?

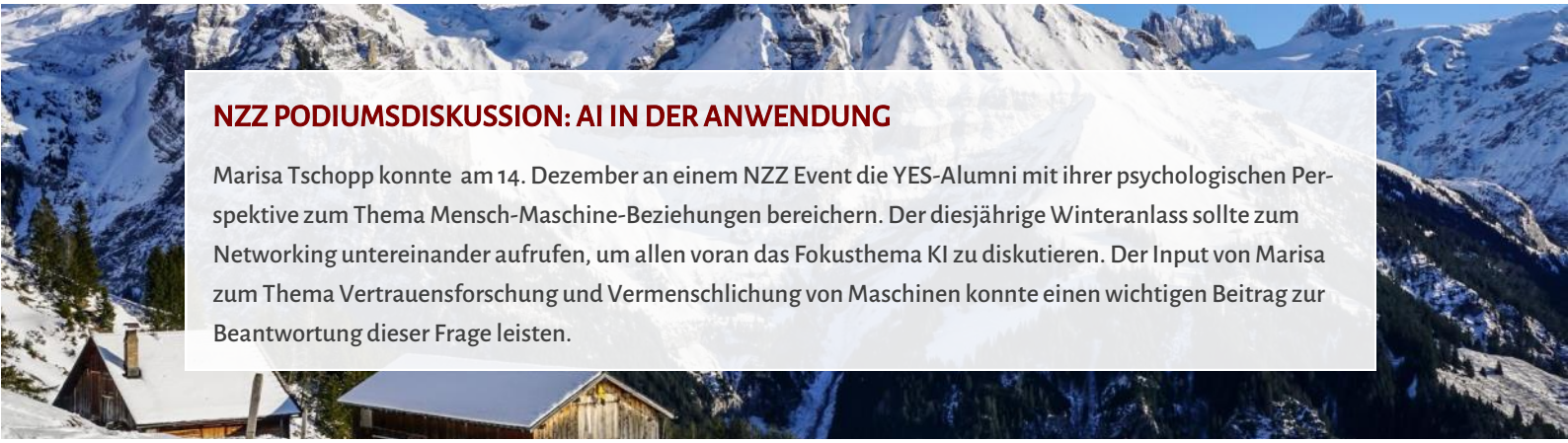
Wenn ich Ihnen unser Jahr 2023 jedoch genauer vor Augen führe, haben alle Aktivitäten, die ich oben beschrieben habe, eine spezifische Gemeinsamkeit: Cyberattacken. Die SBB, Post, E-Booking, Pathé, der Krankenkassenanbieter ÖVV, die Universität Zürich, Tamedia, Microsoft —ja, sogar diverse Ämter der Schweizerischen Bundesverwaltung wurden Opfer von digitalen Angriffen.

Gefahren im Cyberraum sind also zu einem festen Bestandteil unseres Lebens geworden. Deshalb unser Rat zum Jahresende: Cybersicherheit ist und bleibt wichtig, allen voran in unserer volldigitalisierten Gesellschaft. Lassen wir uns im 2024 deshalb vermehrt zusammenarbeiten, gemeinsam forschen und uns dafür einsetzen, die digitale Welt sicherer für uns alle zu machen. Wir wünschen Ihnen frohe Festtage und alles Gute fürs kommende Jahr!

Serena Bolt, Business Analystin

NEWS

WAS IST BEI UNS PASSIERT?



NZZ PODIUMSDISKUSSION: AI IN DER ANWENDUNG

Marisa Tschopp konnte am 14. Dezember an einem NZZ Event die YES-Alumni mit ihrer psychologischen Perspektive zum Thema Mensch-Maschine-Beziehungen bereichern. Der diesjährige Winteranlass sollte zum Networking untereinander aufrufen, um allen voran das Fokusthema KI zu diskutieren. Der Input von Marisa zum Thema Vertrauensforschung und Vermenschlichung von Maschinen konnte einen wichtigen Beitrag zur Beantwortung dieser Frage leisten.

VORSICHT VOR BETRÜGERN AUF TEMU: EXPERTENKOMMENTAR AUF BLICK.CH

Auf der beliebten chinesischen Shopping-App Temu häuften sich in der letzten Zeit gefälschte Lieferbenachrichtigungen. Betrüger wollten dadurch persönliche Informationen ihrer Nutzerinnen und Nutzer erschleichen. Marc Ruef hat das Risiko zur aktuellen Situation auf blick.ch eingeschätzt und warnte vor der problematischen Applikation. Geopolitisch motivierte Faktoren spielen eine wichtige Rolle, die damit einhergehende Risiken sind jedoch weder neu noch speziell, sagt Marc Ruef.

WAS TUN, WENN PERSÖNLICHE DATEN IM NETZ LANDEN: INTERVIEW

Was tun, wenn persönliche Daten im Netz landen? Marc Ruef hat sich anlässlich dieser Frage mit Tobias Bolzern von blick.ch zu dieser Thematik ausgetauscht. Darin bestätigte Ruef, dass Unternehmen Cybersicherheit lange nicht ernst genommen haben. Mit der Digitalisierungskampagne vieler Unternehmen steige eben die Angriffsfläche für Cyberkriminelle, die mittlerweile ihr Geschäftsmodell professionalisiert haben. Cybersicherheit sollte in jedem Fall integral in die digitale Transformation betrachtet werden.

Weitere News zu unserem Unternehmen finden Sie auf unserer Webseite.

SCIP BUCHREIHE

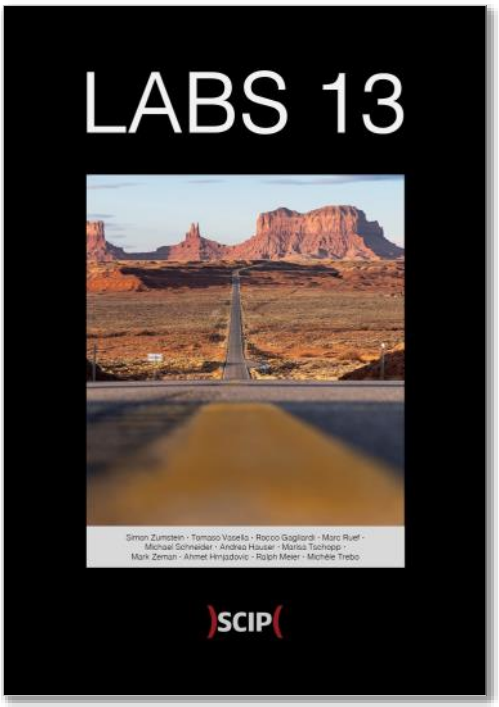
UNSER AKTUELLES JAHRBUCH

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.



DAS WAR 2023

Bildquelle: https://unsplash.com/de/fotos/flachfokusfotografie-der-grunfichte-S9miGKjxmb4

SERENA BOLT

DAS WAR 2023: UNSER JAHRESRÜCKBLICK

UNSERE WICHTIGSTEN SCIP TIPPS 2023

Aus einem Jahr Forschung und Recherche haben wir als Basis unsere LABs von 2023 wieder herausgenommen und folgende Tipps zusammengestellt:

- ChatGPT ist aus unserer Sicht ein nützliches Tool zur Ergänzung unseres Arbeitsalltags, wird uns aber kaum ersetzen.
- Bei verdächtigen Anfragen nach persönlichen Informationen steckt womöglich ein Phishing-Versuch dahinter.
- Eines der Hauptproblematiken mit neuen Technologien sind oftmals deren unreflektierte Vermarktung. Datenschutz, ethische Faktoren oder soziale Folgen werden oftmals nicht diskutiert.
- Bei JavaScript Prototype Pollution können Entwicklerinnen und Entwickler innerhalb von Burp auf ein gutes Tooling zur Identifizierung dieser Schwachstellentyps zurückgreifen.
- Flipper Zero eignet sich gut für Angriffe mit notwendiger physischer Nähe, um per Funk ein gewünschtes Ziel anzugreifen.
- Transparenz und Rechenschaftspflicht bei der Entwicklung und Bereitstellung von Chatbots gilt es zu wahren, um die ethischen Aspekte zu gewährleisten.
- Die Implementierung von Security Frameworks hängen von verschiedenen Kriterien ab: Fokus, Abdeckung, Stärken und Einschränkungen können bei der Wahl helfen.
- IT Bedrohungen nehmen zu: Verteidiger sollten wachsam bleiben, ihre Verteidigungsmassnahmen regelmässig testen und proaktive Massnahmen ergreifen, um potenzielle Angriffe zu mindern.
- Die Toolunterstützung im Bereich Websocket Fuzzing ist unvollständig. Unser entwickeltes Skript kann dabei helfen.

- Ransomware-Zwischenfälle haben sich in der letzten Zeit gehäuft. Ein fehlendes Verständnis für das Thema Cybersicherheit begünstigt diese.
- Burp Makros können das Testen viel effizienter gestalten.
- Allgemein betrachtet sind die Empfehlungen für den Schutz vor nicht-volumenbasierten DDoS-Angriffen dieselben wie auch sonst in der IT-Sicherheit: Stets für vollständig aktuelle und sicher konfigurierte Systeme und Anwendungen sorgen; geeignete Schutzsysteme verwenden, regelmässige Sicherheitstests durchführen und Überwachen und Alarmieren.
- Eine klare Definition und Ankündigung des Bug-Bounty-Programms ist unerlässlich, um eine professionelle Umsetzung zu ermöglichen.
- Überprüfen Sie die Identität und Authentizität des Chatbots oder Absenders, bevor Sie persönliche Informationen weitergeben oder auf Anfragen reagieren.
- Das BIOS ist nicht nur der Anfangspunkt eines Computerstarts, sondern gleichzeitig ein einfaches Einfalltor für Angreifer mit physischem Zugriff auf das Zielgerät. Deshalb ist es wichtig, das eingesetzte BIOS auf dem aktuellen Stand zu halten und genügend Härtungseinstellungen vorzunehmen.
- Sich alleine auf Voice Authentisierung zu verlassen, ist weder sinnvoll noch zeitgemäss. Diese in Umgebungen mit einem hohen Mass an Sicherheit einzusetzen, ist entsprechend nicht zu empfehlen.
- Um von den Neuerung des Basis-Scores von CVSS v4.0 profitieren zu können, muss ein entsprechender Aufwand betrieben werden und eine Neubewertung durch Fachexperten erfolgen, welche die Zielumgebung kennen und mit der Komplexität der Einstufung vertraut sind. Andernfalls wird mit ungenauen Informationen gearbeitet, was keine Verbesserung gegenüber dem Status quo von CVSS v3.1 darstellt.

- Arbeiten Sie mit Open Source Intelligence Investigation(OSINT)? Unser Leitfaden hilft, mit der Sammlung, Analyse und Interpretation öffentlich zugänglicher Informationen zu arbeiten.

SCIP IN ZAHLEN UND FAKTEN

- Anzahl abgeschlossene Projekte: 101
- Anzahl Unternehmen, die wir unterstützt haben: 43
- Anzahl durchgeführte Web-App Pentests: 53
- In den Medien: 31 Interviews, 19 Vorträge, 4 Podiumsdiskussionen & 4 Podcasts

WAS UNS DIESES JAHR STOLZ GEMACHT HAT

- TEDx Boston über die Zukunft von KI: Vortrag von Marisa Tschopp
- Buchpublikation „Servant by Default“ mit Co-Autorin Marisa Tschopp
- SRF Podcast mit Andrea: Pen-Testing Undercover

DIE WICHTIGSTEN NEWS, BEI WELCHEN WIR INTERVIEWT WURDEN

- Hacker-Attacken auf die Universität Zürich
- Ransomware-Angriff auf Tamedia
- DDos-Attacke gegen Schweizer Bundesverwaltung
- Cyberangriff auf Basellandschaftliche Psychiatrie

EINE AUSWAHL UNSERER LABS WÄHREND 2023

- Deep Dive IT Forensik: Analyse von Bildern und Videos
- Hardware Keylogger: Unsichtbare Bedrohungen
- Software Defined Networking: Zusammenarbeit mit der HSLU

DAS WIRD 2024

Bildquelle: https://unsplash.com/photos/a-group-of-people-in-a-forest-pIfgaWV53z4

MARC RUEF

SCIP CYBERSECURITY FORECAST VORAUSSAGEN FÜR 2024

Wie jedes Jahr möchten wir auch zum Ende des Jahres 2023 einen Forecast für das kommende Jahr 2024 machen. Nachfolgend eben jene Themen, die sich unseres Erachtens manifestieren oder gar noch weiterentwickeln werden. Unabhängig dessen: Bleiben Sie gesund!

RANSOMWARE GEHT NICHT MEHR WEG

Das Geschäftsmodell von Ransomware-Attacken hat sich in den bei den letzten Jahren konsequent etabliert. Dabei sind keine Anzeichen zu sehen, dass dieses Risiko in irgendeiner Weise abnehmen wird. Ganz im Gegenteil ist der Höhepunkt wohl auch für die nächsten Jahre noch nicht erreicht. Zu viele Organisationen haben das Thema Cybersecurity in den letzten Jahren sträflich vernachlässigt. Die Ransomware-Gangs sind auf dieser Suche nach diesen, um schnell und unkompliziert Geld verdienen zu können. Es ist also höchste Zeit, die Gefahr ernst zu nehmen und sich auf den neuesten Stand zu bringen. Neue Schwachstellen, gerade auf exponierten Systemen, müssen ständig im Auge behalten werden, um auch zukünftig Kompromittierungen entgegenwirken zu können.

TRIPLE-EXTORTION GEGEN MITARBEITER UND KUNDEN

Die Erpressung von kompromittierten Organisationen lohnt sich in vielen Fällen. Doch manchmal sind die Opfer nicht gewillt zu zahlen. In diesem Fall kommt eine Double-Extortion zum Tragen, bei der

mit der Veröffentlichung der Daten gedroht wird. Über kurz oder lang werden aber auch Triple-Extortion interessant. Dabei werden die betroffenen Personen, meistens Personal oder Kunden, mit den gestohlenen Daten erpresst. Dieses Vorgehen ist besonders perfide, da diese nicht für die mangelhafte Sicherheit der Organisation verantwortlich sind. Gerade Lohndaten und Patientendaten bieten sich für solche Erpressungsversuche an.

KÜNSTLICHE INTELLIGENZ VERÄNDERT BERUFE

Wohl keine Entwicklung der Künstlichen Intelligenz ist dermassen breitflächig in der Gesellschaft wahrgenommen worden, wie ChatGPT. Das Sprachverständnis ist faszinierend. Es vermag bei der Generierung und Überarbeitung von Texten zu helfen oder diese gar gänzlich zu automatisieren. Die hohe Qualität wird unmittelbaren Einfluss auf bestimmte Berufe haben. Viele Textschreiber bei Medienhäusern werden sich durch solche Lösungen wegautomatisieren lassen. Gerade kürzere Texte, die in erster Linie auf Meldungen von Nachrichtendiensten basieren, bieten sich für diese Transformation an. Was mit den obsolet gewordenen Journalisten passiert, ob diese zum Beispiel mehr Zeit für aufwändige Recherchen investieren dürfen, ist unklar.

KÜNSTLICHE INTELLIGENZ WIRD DÜMMER

Höher, schneller, weiter. Das ist auch das Motto der Künstlichen Intelligenz. Durch ein Mehr an Training können entsprechende Lösungen aber auch kaputttrainiert werden. Die Verarbeitungs- und Datenqua-

lität nimmt sodann ab. Dies ist vor allem auch dem Umstand geschuldet, dass KI mit zunehmender Zeit auf der Basis von Daten trainiert wird, die ebenfalls von einer KI generiert wurden. Dieser Feedback-Loop wird zur Verstärkung von negativen Effekten führen, die wohl in einer ersten Phase nur durch menschliche Intervention unterbunden werden kann.

KÜNSTLICHE INTELLIGENZ WIRD REGULIERT

In den USA geben vor allem Copyright-Verstösse bei durch öffentlich zugänglichen Daten trainierten Künstlichen Intelligenzen zu reden. Die Rechteinhaber wollen den Zugriff verhindern oder am Profit beteiligt werden. Im europäischen Raum stehen Bedenken bezüglich der Privatsphäre im Mittelpunkt. Das Sammeln, Auswerten und Nutzen von persönlichen Daten soll eingeschränkt werden. Diese Diskussionen sind wichtig und richtig. Gleichzeitig verhelfen Sie den chinesischen Bestrebungen zu einem Vorsprung, der da ungehindert ausgebaut werden kann.

SOZIALE MEDIEN VERARMEN

Die Menschen sind der klassischen Sozialen Medien überdrüssig. Facebook kämpft verzweifelt gegen einen Nutzerschwund. Und mit der Übernahme von Twitter durch Elon Musk haben sich die Zukunftsprognosen von X auch nicht unbedingt massgeblich verbessert. Die dreisten Algorithmen und die nervtötenden Werbungen machen die Plattformen zunehmend unattraktiv. Das Ausbleiben des Publikums führt zwangsweise zu Einbussen bei Werbeeinnah-

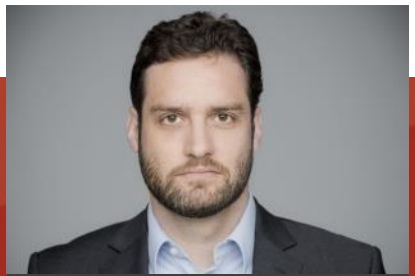
men. Das überhebliche und herablassende Verhalten der superreichen Besitzer dieser Plattformen ist in dieser Hinsicht auch nicht unbedingt förderlich.

MILITÄRISCHE NOTWENDIGKEIT VON CYBER

Mit der anhaltend angespannten politischen Lage in Osteuropa und der Eskalation im Nahen Osten wird das Thema Cyber im militärischen Umfeld in der breiten Gesellschaft als wichtig wahrgenommen. Politisch und militärisch motivierte Angriffe können eine Gesellschaft, auch schon unter der Kriegsschwelle, empfindlich schädigen. Wirtschaft und kritische Infrastruktur müssen sich darum bemühen, den drohenden Gefahren eine nachhaltige Robustheit entgegenbringen zu können.

CYBER THREAT INTELLIGENCE ALS NEUES WERKZEUG

Cyber Threat Intelligence wird zunehmend als hilfreiches Mittel verstanden, um drohende Gefahren frühzeitig erkennen und auf diese reagieren zu können. Die klassische Analyse von Malware und IP-Zugriffen wird durch verhaltensbasierte Ansätze erweitert. In den folgenden Jahren wird sich bei vielen Organisationen, die ein hohes Niveau im Cybersecurity-Bereich erreicht haben, CTI als zusätzliches zentrales Werkzeug etablieren. Gerade im Zeitalter von systematischen Ransomware-Angriffen, die empfindliche Schäden anrichten können, wird dadurch die Verteidigung massgeblich gestärkt.



Marc Ruef

BESINNLICHE & SICHERE FESTTAGE
WÜNSCHT IHNEN DIE SCIP AG.

Bildquelle: https://unsplash.com/de/fotos/haus-zwischen-baumen-und-dock-unter-grauem-himmel-cQxwarmp4ag

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

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.

scip AG
Badenerstrasse 623
8048 Zürich
Schweiz

+41 44 404 13 13
www.scip.ch