MONTHLY SECURITY SUMMARY

)SCIP(

AUSGABE NOVEMBER 2023
VON EXPERIMENTIERFREUNDIGER KUNST & CVSS

IST DAS KUNST? EIN KI-EXPERIMENT

Generative KI-Programme sind richtig beliebt geworden. Doch wird sich KI in der Szene etablieren? Marisa Tschopp hat sich an ein Experiment gewagt.

SCHAFFT CVSS 4.0 MEHR AUFWAND ALS NUTZEN?

Am 1. November wurde die neue CVSS Version 4.0 veröffentlicht. Bringen die Neuerungen einen Mehraufwand bezüglich genauen Scores mit sich? Wir ordnen ein.

November 2023: Die schrillen Neunziger

Auf den Sozialen Medien kursiert seit geraumer Zeit die sogenannte *AI Yearbook Challenge*. Eine Challenge, bei welcher man sich zurück in seine Schulzeit zurückversetzen lassen kann. Man ladet ein Foto auf einer App namens Epik hoch, und mithilfe eines KI-Filters wird einem der ultimative Retro-Look verpasst. Mit wilden Mustern und fragwürdigen Frisuren wohlgemerkt.

Generative KI-Systeme werden immer beliebter und sind mittlerweile auch in unserem Alltag angekommen, die uns primär entlasten, aber auch zu unserer Unterhaltung dienen. Jüngste Entwicklungen zeigen, dass sich künstliche Intelligenz zum Beispiel auch in der Kunstszene durchsetzt . In dieser Ausgabe unseres Security Summarys zeigen wir zum Beispiel, wie sich Marisa Tschopp an ein Experiment gewagt, und selbst Hand als KI-Künstlerin angelegt hat.

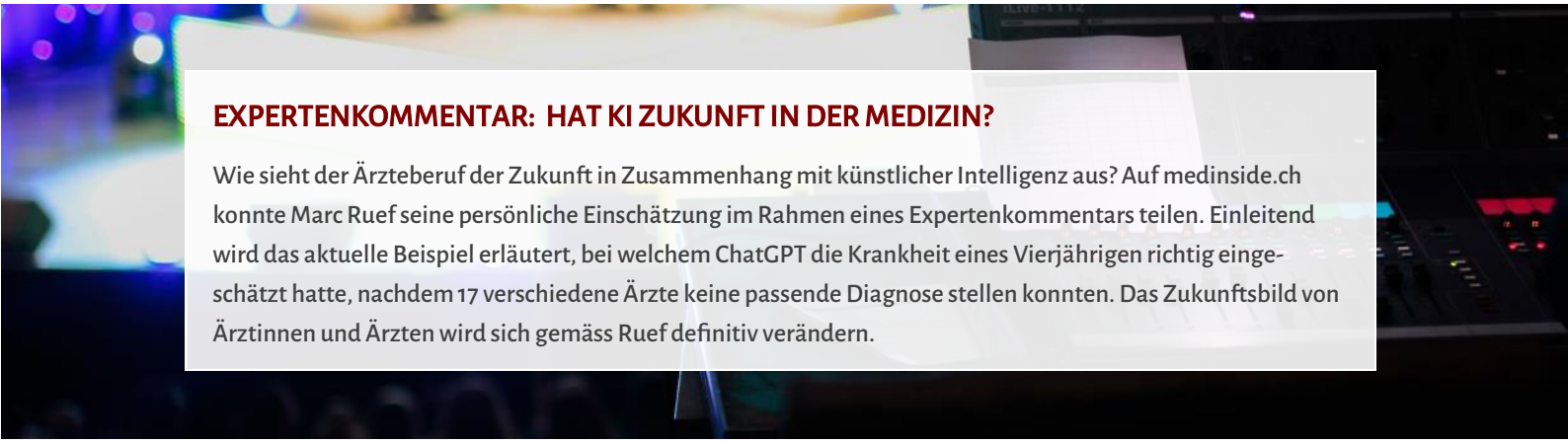
So kreativ die Ergebnisse von Epik und Co. auch sind: Wir müssen uns doch bewusster werden, welchen Preis wir für diese Bespassung zu zahlen bereit sind. Denn was die ganzen KI-Unternehmen gemeinsam haben, ist das Verfügen über unsere Daten. Beinahe kostenlos stellen wir unsere sensibelsten Informationen an Unternehmen zur Verfügung, trainieren ihre Algorithmen mit unseren Gesichtern, Stimmen und Informationen, die wir bereitwillig zur Verfügung stellen. Die Frage ist vielmehr: wollen wir das?

Was wir anstelle von digitalen Throwbacks anstreben sollten, ist eine nachhaltige digitale Zukunft. Da gehört auch ein schärferes Bewusstsein dazu, wie und mit wem wir unsere Daten im Netz teilen. Schliesslich haben wir damals auf dem Pausenhof auch nicht unsere besten Sammelkarten einfach so verschenkt.

Serena Bolt
Business Analystin

NEWS

WAS IST BEI UNS PASSIERT?



EXPERTENKOMMENTAR: HAT KI ZUKUNFT IN DER MEDIZIN?

Wie sieht der Ärzteberuf der Zukunft in Zusammenhang mit künstlicher Intelligenz aus? Auf medinside.ch konnte Marc Ruef seine persönliche Einschätzung im Rahmen eines Expertenkommentars teilen. Einleitend wird das aktuelle Beispiel erläutert, bei welchem ChatGPT die Krankheit eines Vierjährigen richtig eingeschätzt hatte, nachdem 17 verschiedene Ärzte keine passende Diagnose stellen konnten. Das Zukunftsbild von Ärztinnen und Ärzten wird sich gemäss Ruef definitiv verändern.

DIGITALTAG ZENTRALSCHWEIZ 2023 MIT MARISA TSCHOPP

Am diesjährigen Format des zentralschweizerischen Digitaltags am 7. November 2023 konnte Marisa Tschopp eine Keynote zum Thema Trust halten. Interessierende konnten sich auf verschiedene Breakout Sessions freuen, bei welchen Datenunsicherheit und das Thema Vertrauensökosystem näher erläutert wurden. Tschopp, welche aktuell CRO bei Women in AI ist und generell im Thema der Künstlichen Intelligenz forscht, konnte ihre Präsentation vormittags im Luzerner Verkehrshaus halten.

INTERVIEW ZUM THEMA CYBERATTACKEN IM GESUNDHEITSWESEN

Cyberattacken sind auch im Gesundheitswesen präsenter denn je. Marc Ruef konnte sich mit Anna Birkenmeier im Medinside zur aktuellen Lage im Rahmen eines Interviews austauschen und erklärte, wieso Spitäler und das Gesundheitswesen generell nach wie vor schlecht vor Angriffen geschützt sind. Dabei sei das Ziel der Angreifer klar: So einfach wie möglich viel Geld zu verdienen, denn Cybercrime hat sich zu einem lukrativen Geschäftsmodell entwickelt.

Weitere News zu unserem Unternehmen finden Sie auf unserer Webseite.

SCIP BUCHREIHE

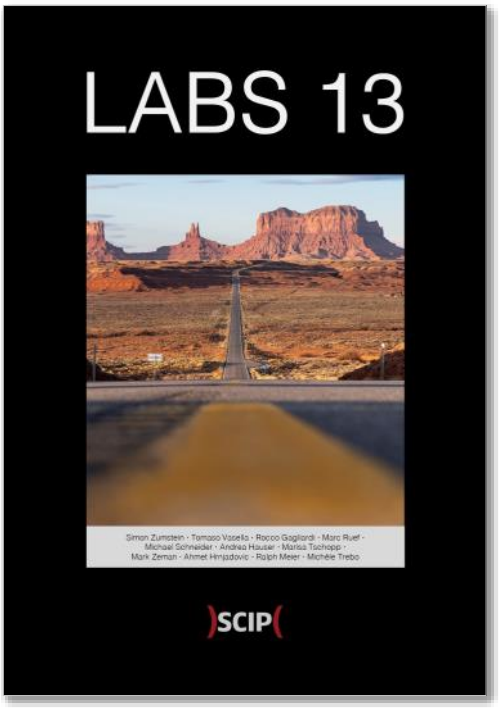
UNSER AKTUELLES JAHRBUCH

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.



IST DAS KUNST? EIN KI-EXPERIMENT

Bildquelle: https://unsplash.com/photos/lowangle-photography-of-gray-mountains-at-nighttime-KET9k6gNlEg

MARISA TSCHOPP

IST DAS KUNST? PERSÖNLICHE REFLEXIONEN ÜBER KREATIVER AUSDRUCK MIT KI

Vor nicht allzu langer Zeit nahm ich an einem Interview mit SRF teil, bei dem wir uns in den Hype um die Lensa-App vertieften – ein Werkzeug, mit dem Benutzer Avatare nach ihrem Ebenbild erstellen können. Der anschliessende Medienrummel war besonders ausgeprägt, da Frauen Avatar-Veränderungen ausgesetzt waren, wie übertriebene Brustproportionen und Veränderungen von dunklen Hauttönen zu helleren. Verständlicherweise erntete die App eine beträchtliche Menge an Kritik.

Persönlich habe ich mich davor zurückgehalten, mich damit zu beschäftigen; eine bewusste Entscheidung, die aus meinem Bewusstsein für die ethischen Unklarheiten in Bezug auf die Behandlung von Künstlern und ihren Werken resultierte. Die beunruhigende Praxis von Unternehmen, Kunstwerke ohne angemessene Zustimmung zur Schulung ihrer Modelle zu verwenden, war ein Anliegen. Darüber hinaus fand ich den Trend zu sexualisierten und vereinheitlichten Darstellungen ziemlich verstörend.

DANN GING ES BERGAB – MIT BARBIE

Und dann kam der Barbie-Film im Jahr 2023, gefolgt von der Internet-Sensation bAIrbie.me. Nun, es hat das Internet nicht gerade zum Stillstand gebracht, aber es hat meine Prinzipien herausgefordert. Ich zögerte, mich auf dieses eigenartige Unterfangen einzulassen, bei dem zufällige Unternehmen mein Bild für ihnen allein bekannte Zwecke verwenden dürften.

In einem Moment der Schwäche erlag ich der Neugier. Ich kann es nicht ganz erklären, aber hier stehe ich heute, verwandelt in eine virtuelle Barbie-

Version von mir selbst. Ich habe jedoch davon abgesehen, es in sozialen Medien zu teilen, aus Furcht vor möglicher Kritik, weil ich von meinen festen Werten abwich oder weil ich nicht praktizierte, was ich predigte.

ERSTE BEGEGNUNGEN MIT KI-KÜNSTLERN

Einige Monate später fand ich mich in den ehrwürdigen Hallen des Schweizerischen Naturwissenschaftlichen Museums Technorama wieder und stand kurz davor, einen Vortrag zu halten. Dort hatte ich das Vergnügen, auf die bemerkenswerte Grit Wolany zu treffen. Ihre Keynote zur KI-generierten Kunst war nichts weniger als beeindruckend. Sie enthüllte eine Welt lebendiger Schönheit, eine Explosion von Farben und einen einzigartigen Stil, alles unterstrichen von ihrer Echtheit und ansteckenden Begeisterung. Grit teilte auch mit, wie sie diese Technologie in ihren Kursen an der Zürcher Hochschule der Künste (ZhDK) einsetzt, und liess mich völlig fasziniert zurück. Ehrlich gesagt war es eine Offenbarung. Endlich konnte ich aus vertrauenswürdigen Quellen beobachten, wie sie dieses Werkzeug nutzen, um ihre Kreativität zu steigern und ihre künstlerischen Ausdrücke zu bereichern. Es war ein Moment, der Bewunderung nahtlos mit einer gesunden Dosis Neid für ihre kreative Begabung verband!

ERSTE EXPERIMENTE MIT KI-KUNST MIT MIDJOURNEY

Ein paar Wochen später kreuzten sich unsere Wege erneut, diesmal in den ehrwürdigen Hallen der Zürcher Hochschule der Künste (ZHdK). Mir wurde grosszügigerweise die Möglichkeit gegeben, einen Vortrag zu ihrem faszinierenden Kurs AI Encounter beizutragen. Dieses Programm war massgeschneidert für Personen, die begierig waren, in die Welt der KI-Kunst einzutauchen, und bot ihnen die Möglichkeit, verschiedene Software unter Anleitung von Mentoren und vielfältigen Pädagogen zu erkunden. Zusätzlich werden in dem Kurs auch wichtige gesellschaftliche Diskussionen geführt. Mein Vortrag konzentrierte sich auf die psychologischen und ethischen Dimensionen der künstlichen Intelligenz, wobei ich mich insbesondere auf unsere Forschung zu Mensch-KI Beziehungen konzentrierte.

Mitten in dieser aufschlussreichen Erfahrung präsentierte sich mir eine faszinierende Möglichkeit: Eine Einladung, Midjourney auszuprobieren, ein Programm, von dem ich nur Flüstern gehört hatte, aber nie gewagt hatte, mich hineinzubegeben, teilweise wegen seiner kostenpflichtigen Natur. Der Reiz war unwiderstehlich. Schliesslich, wie könnte ich das Programm eloquent auseinandernehmen und möglicherweise sogar kritisieren, ohne eigene Erfahrungen? Oder ist das nur eine Ausrede, die sich als rationale Entscheidung tarnt? Es war ein erfreuliches Dilemma, das mich über die schmale Grenze zwischen Neugierde und beruflicher Verantwortung nachdenken liess.

TEAM IMAGINE

Nun, einige könnten argumentieren, dass ich keine Ahnung habe, wenn ich das Programm noch nie benutzt habe, und ich verstehe das – also loggte ich mich in Discord ein und begann das Ritual des promptens, oder wie die Midjourney-Enthusiasten es nennen, "imagine". Ja, zählt mich zum Team Imagine. Also? Wie startet man eine Vorstellung, wenn man keine Ahnung hat, was man sehen möchte? Ich entschied mich für den sicheren Weg und begann mit etwas Vertrautem. Nur wenige Tage zuvor hatte ich ein Bild von meinem Mann und mir stolz vor unserem neuesten Erwerb aufgenommen, einem 1969er Chevrolet El Camino, der zur Restaurierung bestimmt war. Also war meine anfängliche Aufforderung festgelegt: "Ein Paar vor einem 1969 El Camino". Und voilà, das war das Ergebnis!

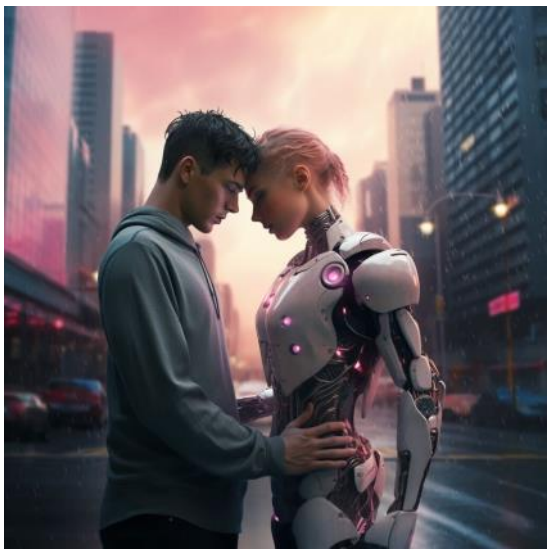
Mein erster Prompt, der in Nacktheit resultierte, markiert sicherlich eine unerwartete Wendung. Doch unter der Anleitung unserer Mentorin, Grit, verfeinerten wir unsere Aufforderungen und korrigierten schnell etwaige technische Fehler, und schmiedeten so einen kollaborativen Prozess, der dem des Miterschaffens ähnelt. Als ich mich darauf vorbereitete, jede Aufforderung einzureichen und die rechnerischen Räder von Midjourney zu beobachten, überkam mich ein Gefühl der gespannten Erwartung. Es war vergleichbar mit dem Flattern von Schmetterlingen im Bauch – diese aufregende Unsicherheit darüber, welche visuellen Wunder es als Nächstes heraufbeschwören würde. Dieses Gefühl war besonders ausgeprägt, als ich versuchte, Bilder von tiefgreifender persönlicher Bedeutung zu schaf-

fen. Mein Ziel war es, eindringliche Bilder für meine Forschung zu Mensch-KI-Beziehungen zu schaffen – Bilder, die die Grenze zwischen Realität und Phantasie überspannten, in denen Menschen und Cyborgs nahtlos in den strahlenden Landschaften einer zukünftigen Ära miteinander existierten.

Aus guten Gründen warnen viele auf Social-Media-Plattformen vor der Verwendung solcher humanisierten, Science-Fiction-Bilder in einem KI-bezogenen Kontext. Auch wenn diese Warnungen zweifellos berechtigt sind, legten sie auch die Verletzlichkeit unserer Wünsche offen. Ich sehnte mich nach diesen Bildern und liebte sie. Ich habe unzählige Stunden damit verbracht, imaginative Bilder für meine Freunde zu gestalten, habe mit unkonventionellen Aufforderungen experimentiert, die die Grenzen der Kreativität ausreizten. Vom Zusammensetzen eines Gesichts aus verschiedenen Puzzlestücken über das Modellieren eines Mannes aus einem Schwarm von Insekten bis hin zur Erschaffung eines Berges, der vollständig aus anmutigen Schmetterlingen bestand, habe ich eine vielfältige Palette künstlerischer Ausdrucksformen erkundet.

In einer besonders abenteuerlichen Sitzung wagte ich mich in unbekanntes Terrain und experimentier-

te mit Ketchup als Medium. Letztendlich entschied ich jedoch, diese Kreationen zu entfernen, da sie in das, was die Community als Gore bezeichnet, vordrangen und somit gegen etablierte Richtlinien verstossen. Es war eine unheimliche Offenbarung, die Licht auf die Längen wirft, die Personen gehen, um Bilder zu generieren, die kreativ stimulierend sind, aber möglicherweise unbeabsichtigt die Grenzen der Akzeptanz überschreiten. In dieser dynamischen, scheinbar makabren Welt werden Szenen von Blutvergiessen und Gewalt geschickt durch Tomatensauce ersetzt, und Kampfsituationen werden in choreografierte Martial-Arts-Darbietungen umgewandelt. Diese faszinierende Dichotomie betont den komplexen Tanz zwischen künstlerischem Ausdruck und Gemeinschaftsstandards.



Stunden um Stunden wurden in die akribische Erstellung von Bildern für meine liebevoll benannte Dune-inspirierte Sammlung investiert. Dies entsprang einer echten Begeisterung für ein filmisches Meisterwerk, das ich allen wärmstens empfohlen habe, wobei ich insbesondere die jüngste Adaption betonte, ohne die Vorzüge des Originals zu verkennen. Die Herausforderungen waren erheblich. Das Modellieren einer dunkelhäutigen arabischen Frau erforderte eine feinfühlige Balance zwischen Kunstfertigkeit und Präzision. Ebenso verlangte die Integration eines Raumschiffs inmitten einer Kulisse aus lodernden Flammen und wirbelndem Staub einen akribischen Ansatz bei der Neugestaltung, beim Remixen, Hochskalieren, Hinein- und Hinauszoomen. Es war ein Prozess geprägt von Hingabe, bei dem jede Aufforderung (und zugegebenermassen Grits meisterhafte Hilfe) zur Verwirklichung einer lebendigen Vision beitrug.

WELCHER WEG WEITER

Wenn Sie auch nur ein wenig künstlerische Neigung haben, werden Sie vielleicht meine Begeisterung nachvollziehen können. In meiner Teenagerzeit träumte ich davon, Manga-Künstlerin zu werden, und tauchte vollständig in die Welt des Zeichnens japanischer Comics ein. Es war ein Prozess, der Stunden der Konzentration und Hingabe verlangte. Ich ging darin auf, oft zufrieden mit dem Ergebnis. Ich konnte Charaktere und Geschichten zum Leben erwecken, wissend, dass jedes Detail, von den Augen bis zu den winzigsten Haarsträhnen, von meiner eigenen Hand geschaffen wurde. Das Gefühl, das ich jetzt beim Arbeiten mit KI-generierter Kunst habe,

FAZIT

Eine der dringendsten rechtlichen und ethischen Probleme liegen im Bereich des geistigen Eigentums, bei der Bestimmung des rechtmässigen Eigentums und der Urheberschaft von von KI-Systemen produzierter Kunst. Darüber hinaus rücken Fragen der Zustimmung und Handlungsfähigkeit in den Vordergrund, da KI-Systeme nicht in der Lage sind, informierte Zustimmung zu geben oder die Auswirkungen ihrer Kreationen zu verstehen.

Der Artikel von Jiang et al., präsentiert auf der AIES-Konferenz 2023, bietet eine fesselnde Lektüre. Doch ein Wort der Warnung: Er könnte Ihre Perspektive darüber verändern, wie Sie KI-generierte Kunst betrachten und nutzen.

Meine eigenen Erfahrungen sind für mich eine eindringliche Erinnerung an die ethischen Dilemmas, die im Schatten technologischer Innovationen lauern. Es ist ein Zeugnis dafür, wie schnell wir von kreativem Ausdruck zu fragwürdiger Ausbeutung abrutschen können. Der Zusammenprall von Künstlertum, Zustimmung und Unternehmensgier steht im Mittelpunkt und lässt uns darüber nachdenken, wie weit wir gehen wollen, um den perfekten Avatar zu erreichen.

Marisa Tschopp

Sie brauchen Unterstützung?

Die Welt dreht sich ungebremst und die Entwicklung schreitet rasant voran. Die Sicherheit Ihrer Daten ist dabei als selbstverständlich vorausgesetzt. Aber wie?

Unser Blue Team beschäftigt sich täglich mit genau diesen Themengebieten sowie Spannungsfeldern und unterstützt unsere Kunden tatkräftig und nachhaltig bei deren Bewältigung, Umwälzung und Verhinderung.

SCIP

https://www.scip.ch

MICHAEL SCHNEIDER

EINFÜHRUNG VON CVSS V4.0: MEHR AUFWAND ALS NUTZEN?

Am 1. November 2023 wurde das Common Vulnerability Scoring System Version 4.0 (CVSS v4.0) veröffentlicht. Die Vorgängerversion CVSS v3.0 wurde im März 2016 vorgestellt und galt seither als Standard zur Bewertung des Schweregrads von Schwachstellen. Im Artikel CVSSV3 als Risikometrik haben wir die Version 3 analysiert. Die CVSS v4.0 Spezifikation und das Tool zur Berechnung des CVSS v4.0 Scores wurden auf der Webseite des Forum of Incident Response and Security Teams (FIRST) veröffentlicht. Dieser Artikel zeigt die Änderungen zur Version 3.1, diskutiert die Veränderungen zur Einstufung der Basismetrik und die Herausforderung zur Erstellung eines genauen Scores für eine Schwachstelle.

ÄNDERUNGEN ZU CVSS V3.1

Um den Basis-Score einer Schwachstelle präziser einstufen zu können, wurde die Metrik Attack Requirements (AT) eingeführt und die Metrik User Interaction (UI) in die Werte *Passive* (P) und *Active* (A) aufgeteilt. Die Metrik Scope (S) wurde durch die Auftrennung der Impact-Metrik in Vulnerable System (VC, VI, VA) und Subsequent System (SC, SI, SA) ersetzt. Die Auswirkungen auf den Basis-Score wird im nachfolgenden Kapitel beschrieben.

Die Metrikgruppe Temporal wurde in Threat umbenannt und vereinfacht. Sie enthält nur noch die Exploit Maturity (E), welche die Wahrscheinlichkeit beschreibt, dass die Schwachstelle ausgenutzt wird. Dazu können die Werte *Attacked* (A), *Proof-of-Concept* (P) oder *Unreported* (U) verwendet werden. Diese Information wird von FIRST als Threat Intelligence bezeichnet und die Metrik sollte laufend aktualisiert werden.

Durch den Wegfall der Metrik Remediation Level (RL) geht die Information verloren, ob ein Patch oder Workaround verfügbar ist. Dies ist eine wesentliche Information für das Vulnerability Management, die nicht adäquat ersetzt wird.

Das Ziel der neuen Metrikgruppe Supplemental ist, dass Unternehmen zusätzliche Informationen zu einer Schwachstelle definieren können, die hilfreich zur Risikoanalyse sind. Die Metrikgruppe ist optional und hat keinen Einfluss auf den CVSS-Score. Mit den

Metriken können Unternehmen folgende Fragen zur Schwachstelle beantworten:

- **Safety**: Hat diese Schwachstelle einen Einfluss auf die Sicherheit der Organisation?
- **Automatable**: Kann die Schwachstelle automatisiert ausgenutzt werden?
- **Recovery**: Können die Ressourcen nach einen Angriff wiederhergestellt werden?
- **Value Density**: Welche Ressourcen wird ein Angreifer kontrollieren nach einer Ausnutzung der Schwachstelle?
- **Vulnerability Response Effort**: Welcher Aufwand ist für die erste Reaktion notwendig?
- **Provider Urgency:** Wie lautet der Schweregrad der Schwachstelle durch den Hersteller?

Mit der Metrikgruppe Environmental können Unternehmen die Basismetrik einer Schwachstelle an die spezifischen Eigenschaften der eigenen Umgebung anpassen. Bereits implementierte Massnahmen, die einen Einfluss auf die Ausnutzung einer Schwachstelle haben, können so berücksichtigt werden. Wird der Dienst beispielsweise in einem isolierten Netzwerk betrieben wird, kann der Attack Vector von *Network* auf *Adjacent* reduziert werden. In dieser Metrikgruppe wurde mit der Schaffung des Wertes *Safety* für Integrity (MSI) und Availability (MSA) ein stärkerer Fokus auf Operational Technology (OT), Industrial Control Systems (ICS) und die Sicherheit (Safety) im Allgemeinen gelegt.

BASISMETRIK

Bei der Einstufung der Basismetrik wird davon ausgegangen, dass der Angreifer detaillierte Kenntnisse über die Schwachstelle des Zielsystems hat. Dazu gehören die Basiskonfiguration und Standardabwehrmechanismen wie eine Host-Firewall oder die Beschränkung von Abfragen (Rate Limits). Falls spezifische Abwehrmassnahmen, wie unter anderem eine Zugriffsliste für bestimmte Netzwerkbereiche, implementiert wurden, sollen diese in der Metrikgruppe Environmental berücksichtigt werden und keinen Einfluss auf die Basismetrik haben.

VERFEINERTE EINSTUFUNG DER EXPLOITABILITY-METRIK

Die bisherige Definition der Attack Complexity (AC) wurde durch die Schaffung der Attack Requirements (AT) angepasst. AC misst nun die Hürden, die ein Angreifer zur Ausnutzung der Schwachstelle überwinden muss. Dazu gehören beispielsweise die Techniken Address Space Layout Randomization (ASLR) und Data Execution Prevention (DEP). Beide Techniken erschweren die Entwicklung von Exploits. Ein weiteres Beispiel für AC ist ein Geheimnis (Secret), das ein Angreifer kennen muss, wie ein geheimer Schlüssel zum Brechen eines Kryptokanals.

Die Attack Requirements (AT) beschreiben die notwendigen Vorbedingungen, die einen Angriff auf ein verwundbares System ermöglichen. Der Unterschied zu AC ist, dass diese Bedingungen nicht explizit existieren, um einen solchen Angriff zu verhindern, sondern eine natürliche Folge des Betriebs des Systems sind. Beispiele hierfür sind die Notwendigkeit einer Machine-in-the-Middle-Attacke (MitM) oder die Abhängigkeit der erfolgreiche Ausnutzung eines Exploits vom Gewinn einer Race Condition.

Der Penetration Tester Konstantin beschreibt jedoch in seinem Artikel zum CVSS v4.0 Public Preview, dass die Trennung zwischen AC und AT nicht immer so klar ist. Sein Beispiel zeigt eine verwundbare Applikation, die in einem Container betrieben wird. Grundsätzlich können Container als Gegenmassnahme gegen einen Angriff betrachtet werden, da der den Container das Hostsystem vom Dienst trennt. Container sind auch ein nützliches Feature für die Skalierbarkeit von Applikationen und somit ist die Verwendung eines Containers eine natürlich Konsequenz. Hier ergibt sich ein Interpretationsspielraum, der im konkreten Fall nur durch den Entwickler der Applikation beantwortet werden kann.

Bei der Metrik User Interaction (UI) erleichtert die Einführung der Werte Passive (P) und Active (A) die Unterscheidung. Wenn eine Webapplikation eine Stored-XSS-Schwachstelle aufweist, reicht es aus, wenn der Benutzer die Applikation normal verwendet, damit der JavaScript-Code in seinem Browser ausgeführt wird. Handelt es sich jedoch um eine Reflected-XSS-Schwachstelle, muss der Benutzer aktiv auf einen präparierten Link klicken, damit der Schadcode ausgeführt wird.

Die Unterscheidung zwischen *Active* und *Passive* einer XSS-Schwachstelle beträgt 0.2 Punkte, der CVSS-Vektor-String für eine Stored-XSS-Schwachstelle (Score 5.1) ist CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N und für die Reflected-XSS-Schwachstelle (Score 5.3) CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N.

ERWEITERTE DEFINITION DES WIRKUNGSBEREICHS

Die Metrik Scope wurde durch die Unterteilung des Wirkungsbereichs in Vulnerable System (VC, VI, VA) und Subsequent System (SC, SI, SA) ersetzt. Neu wird auch die Auswirkung der Schwachstelle auf umliegende Systeme auch in Confidentiality, Integrity und Availability unterteilt, was zu einer Verlängerung des Basisvektorstrings führt. Ein verwundbares System wird in der Spezifikation folgendermassen definiert:

> Formally, a system of interest for scoring a vulnerability is defined as the set of computing logic that executes in an environment with a coherent function and set of security policies. The vulnerability exists in one or more components of such a system. A technology product or a solution that serves a purpose or function from a consumer's perspective is considered a system (e.g., a server, workstation, containerized service, etc.).

Wenn ein System seine Funktionalität ausschliesslich einem anderen System zur Verfügung stellt, oder es nur für die Nutzung durch ein anderes System entwickelt wurde, dann werden beide Systeme zusammen in den Scope aufgenommen. Wenn die Auswirkung einer Schwachstelle über das definierte System hinausgeht, dann kann dies neu in den Subsequent System Metriken berücksichtigt werden.

Diese unscharfe Definition des Systems führt zu Interpretationsspielraum. Aus den Beispielen von FIRST lässt sich unter anderem ableiten, dass bei einer Schwachstelle in einer virtuellen Maschine (Guest) wie CVE-2023-21989 der Hypervisor (Host) als Subsequent System gilt, da der Hypervisor auch andere virtuelle Maschinen bereitstellt. In den Beispielen zu OpenSSL Heartbleed oder log4shell wird

das gesamte System/Gerät (Webserver und Betriebssystem) in den Scope des Vulnerable System aufgenommen. Hier wäre es aber auch möglich, die Grenze bei der Webserver-Komponente zu ziehen und das darunter liegende Betriebssystem als Subsequent System zu betrachten. In der Einstufung der Schwachstelle Spring4shell wird darauf hingewiesen, dass je nach Einsatz von Spring auch andere Systeme betroffen sein können, dies aber in den Environmental-Metriken berücksichtigt werden sollte.

IM AUGE DES BETRACHTERS

Die Komplexität der Einstufung einer Schwachstelle wird durch CVSS v4.0 erhöht und der Aufwand für die Definition einer genauen Einstufung steigt. Zudem liegt die Einstufung einer Schwachstelle mehr denn je im Auge des Betrachters. Aus der Sicht eines Sicherheitsforschers und Entdeckers einer Schwachstelle sollte die höchstmögliche Auswirkung angenommen werden, beispielsweise eine Remote-Code-Execution-Schwachstelle (RCE) wird mit den höchsten Rechten ausgeführt und betrifft das gesamte System, was zu einem hohen CVSS-Score führt. Wenn nun diese verwundbare Komponente in einem Penetration Test entdeckt und die Schwachstelle ausgenutzt wird, liegt es im Ermessen des Penetration Testers, ob er die Auswirkung neu einstuft oder nicht. Wird der Code auf dem System beispielsweise von einem nicht-privilegierten Service-Account ausgeführt, ist die Auswirkung geringer und sollte entsprechend dem Scope korrigiert werden. Alternativ wird die Metrik Environmental zusätzlich für den Penetration Test verwendet, um Diskussionen zu vermeiden, warum die Einstufung in einer Schwachstellendatenbank X und im Bericht Y ist.

Der Kunde wiederum betreibt das System in einem abgeschotteten Container, so dass die Auswirkung weiter begrenzt wird. Basierend auf der CVSS-Spezifikation kann und soll der Kunde dies in der Metrik Environmental selbst berücksichtigen. Je nach Ansatz liegen nun zwei korrigierte Metriken vor, beziehungsweise die Metrik Environmental kann vom Kunden weiter ausgeprägt werden.

FAZIT

Der CVSS-Score liefert mit dem Schweregrad einer Schwachstelle einen Beitrag zur Risikobewertung einer Schwachstelle. Wenn der CVSS-Score aus einer Schwachstellendatenbank übernommen wird, gibt es Unbekannte, wie unter anderem was als Scope des verwundbaren Systems verwendet wurde. Um einen exakten Score zu erhalten, sollte der Score durch das Unternehmen entsprechend der Umgebung neu bewertet werden. Die in Version 4 eingeführte Trennung der Auswirkungen wird daher zu Interpretationsspielraum und unterschiedlichen Ergebnissen führen. Ohne eine Neubewertung wird daher mit ungenauen Informationen weitergearbeitet, was das Gegenteil des Ziels eines solchen Scores ist.

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.

Michael Schneider

Bildquelle: https://unsplash.com/photos/scenery-of-forest-field-and-mountain-TCCCKgdFmBo

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.

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