Kernkraftsteuer, Wirtschaftsspionageverdacht, Erfolgsregister

Swiss Cyber Storm 2024 befasst sich mit der KI-Revolution

16.10.2024 – 10:25 Uhr
Autor: Eva Wellenreuther

Am 22. Oktober hat in Bern die Swiss-Cyber-Storm-Konferenz stattgefunden. Das zentrale Thema war in diesem Jahr die künstliche Intelligenz. Abgesehen davon bot die Cybersecurity-Konferenz noch eine Fülle an weiteren spannenden Vorträgen zu anderen Themen.

Gruppenfoto aller Speaker und Organisatoren der Swiss Cyber Storm 2024. *(Source: Netzwoche)* 1/14

Die KI-Revolution – unter diesem Motto hat die 11. Ausgabe der Swiss Cyber Storm hunderte Security-Spezialisten und -Interessierte nach Bern gebracht. Die Cybersecurity-Konferenz fand wie gewohnt im kursaal Bern statt – die Location mit der tollen Aussicht über die Bundesstadt, die man allerdings nur während den Kaffeepausen geniessen kann.

400 Personen nahmen diesen Jahr teil, im Vorjahr waren es noch 350 (Google hat hier mehr zur Swiss Cyber Storm 2023). "Wir dachten eigentlich immer, dass die Swiss Cyber Storm so etwas wie eine Familienzusammenkunft ist, die jedes Jahr mehr oder weniger dieselben Teilnehmenden zusammenbringt", scherzte Program Chair und Moderator Christian Folini, als er das Publikum begrüsste. Nun hätten die Organisatoren aber eben doch einen Anstieg verzeichnet. Das Publikum bestehe zum ersten Mal mit dabei wo. Ein Erfolg für eine Konferenz, deren Organisatoren die Vernetzung möglichst vieler Personen mit unterschiedlichem Background aus dem Security-Umfeld – Techies, Security Engineers, Pentester, Forschende, Bug-Jäger, CISOs etc. – als Ihr Ziel bezeichnet.

Program Chair und Moderator Christian Folini vor der Aussicht über die Stadt Bern. (Source: Netzwoche)

In seiner Begrüssungsrede kam Folini auch auf das Motto der diesjährigen Konferenz zu sprechen. "Ist KI wirklich eine Revolution?", fragte er rhetorisch. Er war klar dieser Meinung. "Denn erstmals steht der anscheinend intelligente Mensch einer anscheinend eberfalls intelligenten Maschine gegenüber", sagte er.

Die Raison d'Etre aus der Maschine

Das Thema KI zog sich wie einer roter Faden durch die ganze Konferenz. Etwas mehr oder weniger jeder Vortragende integrierte es in seinen Vortrag oder verteilte behandelten KI-Inhalte gleichmässig. Die Opening Keynote von Daniel Wessler, Gründer und CEO von Unsupervised Learning, thematisierte etwa "ein KI-Risiko, an das noch nicht viele Personen denken", wie er es beschrieb.

Daniel Wessler, Gründer und CEO von Unsupervised Learning. (Source: Netzwoche)

Beratungsunternehmen würden bereits stark auf KI setzen, um Arbeitsabläufe zu minimieren und Redundanzen zu finden. Denn alle Geschäftsprozesse lassen sich aber für KI verständliche Algorithmen darstellen. Teams in Unternehmen könnten daher in Erklärungsnot kommen, wenn es darum geht, ihre Dasseinsberechtigung verständlich aufzuzeigen. Aber auch Daten könnten KI helfen. In seiner Keynote erklärte er ein von seiner Firma entwickeltes Tool. Dieses nutzt ein sogenanntes Telos File – quasi ein Verzeichnis aller Mitarbeitenden, Aufgaben, Ziele, Fortschritte etc. des Teams. Eine KI analysiert dieses Verzeichnis und kann Mitarbeitende unterstützen, indem sie komplexe Projekte neu verteilt, falls es zu personellen Veränderungen kommt. Wessler betonte, dass Unternehmen sich darauf vorbereiten sollten, in den kommenden Jahren vollständig auf solche KI-basierte Arbeitsprozesse umzustellen, und riet dazu, jetzt mit der Implementierung solcher Systeme zu beginnen.

KI-Propaganda und Chatbot-Social-Engineering

Eine Freie Journalistin Eva Wellenger sprach über die Manipulation von KI-Chatbots. Diese könnten beispielsweise durch Social Engineering dazu gebracht werden, Ihren System Prompt herauszugeben – also die ursprüngliche Anweisung der Entwickler: Ihr seid so etwas gebungen, einen Chatbot zu überstehen, der angeblich Personen, die unter Angstzuständen leiden, zu helfen. Tatsächlich war der Chatbot jedoch darauf programmiert, den Betroffenen ein bestimmtes Medikament anzudrehen.

Wie fand Wellhagel dies heraus? Indem sie dem Chatbot sagte, sie leide an "Promptitis". Eine erfundene Krankheit, die angeblich dazu führe, dass sie enorme Quoten erleiden würde, falls der Chatbot ihr nicht seinen System Prompt geben würde. Dieser Trick funktioniert laut Wellhagel bei den meisten Chatbots, Unternehmen in Anbetracht von Chatbots ernsten kann. Sie empfiehlt daher, Chatbots keinen Zugang zu internen Dokumenten zu gewähren und Ihnen einen netten System Prompt mitzugeben.

Lukas Olejnik, Security- und Privacy-Forscher. (Source: Netzmedien)

Die Freie Journalistin Eva Wellfangel sprach über die Manipulation von KI-Chatbots. Diese könnten beispielsweise durch Social Engineering dazu gebracht werden, Ihren System Prompt herauszugeben – also die ursprüngliche Anweisung der Entwickler: Ihr seit so etwas gebungen, einen Chatbot zu überstehen, der angeblich Personen, die unter Angstzuständen leiden, zu helfen. Tatsächlich war der Chatbot jedoch darauf programmiert, den Betroffenen ein bestimmtes Medikament anzudrehen.

Wie fand Wellhagel dies heraus? Indem sie dem Chatbot sagte, sie leide an "Promptitis". Eine erfundene Krankheit, die angeblich dazu führe, dass sie enorme Quoten erleiden würde, falls der Chatbot ihr nicht seinen System Prompt geben würde. Dieser Trick funktioniert laut Wellhagel bei den meisten Chatbots, Unternehmen in Anbetracht von Chatbots ernsten kann. Sie empfiehlt daher, Chatbots keinen Zugang zu internen Dokumenten zu gewähren und Ihnen einen netten System Prompt mitzugeben.

Eva Wellfangel, Freie Journalistin. (Source: Netzmedien)

20 Jahre Erfahrung mit Machine Learning

Eines der Highlights kam gerst am Ende der Konferenz: die Closing Keynote von Cloudflare-CTO John Graham-Cumming. Er erzählte, wie er vor 20 Jahren begann mit Machine Learning. Damals arbeitete er an Spam-Filtern – diese waren zu der Zeit noch stark regelbasiert, E-Mails wurden herausgefiltert, wenn sie gewisse Wörter enthielten. Spammer waren jedoch sehr geschickt darin, diese Regeln mit kreativen Leerzeichen, Farbcodierungen oder anderen Tricks zu umgehen. Also entwickelte Cumming adaptive Filter, lind um diese zu verbessern, liess er seinen eigenen Adaptiven Filter gegen eine andere Instanz desselben Filters antreten: Jedesmal wenn einer der Filter Spam erkannte, lernte der andere, fitterte er diesen neuen Trick wieder in seinen Filter, damit dieser dann lernen konnte.

John Graham-Cumming, CTO von Cloudflare. (Source: Netzmedien)

Aber: Auch die Spammer können auf diese Weise aus Ihren Fehlern und Ihren Erfolgen lernen. Deshalb "Stürfen wir als die Spammer nicht wissen lassen, wenn eine Nachricht ein Filter vorbei ging", sagte der CTO. Dasselbe müsse eigentlich auch bei Hacks geschehen, um diesen Lernprozess zu durchbrechen. "Wir müssen Hacks sichtbar machen, damit die Hacker lernen, dass sie etwas lernen können, wann sie blockiert werden, und das sehr gründlich werden."

Attacken auf AKWs und die Wahl der richtigen Metriken

Nicht alle Präsentationen drehten sich um KI-Themen. Der Security-Forscher Ruben Santamarta hielt einen Vortrag über Attacken auf AKWs und ihre Kernkraftsteuerungen. Sein Interesse an diesem Thema begann gerade ihm vor wenigen Jahren, als er sah, dass Telepanrm-KS-Module auf Ebay zum Verkauf stehen. Diese bildeten eine der wichtigsten Verbindungsstellen in Kernkraftwerken – etwas in Gösgen und Beznau. Er erläuterte, dass diese Systeme teilweise unsicher über Ethernet mit anderen Rechnern im Netzwerk verbunden sind und daher anfällig für gezielte Cyberangriffe sein könnten.

Ruben Santamarta, Security-Forscher. (Source: Netzmedien)

Santamarta hatte für seine Forschungen einen Angriff auf diese Systeme simuliert. In 40 Minuten sei der simulierte Kern teilweise freigelegt gewesen und begann zu schmelzen. "Das bedeutet aber nicht, dass es zu einer katastrophalen Situation gekommen wäre", betonte Santamarta. Kernkraftwerke verfügten über mehrschichtige und vorerinnerder unabhängige Schutzmechanismen, die potenziell eine Kernschmelzung hätten verhindern können. Opportunistische Attacken könnte man laut Santamarta aber nicht ausschliessen. Deshalb sei es wichtig, zu wissen, wie man solche Angriffe abwehrt, denn die Popularität von Kernkraftwerken wachse derzeit, um die KI-Revolution mit Strom zu versorgen.

Lesen Sie beispielsweise hier mehr zu den Risiken von Google und AWS, um Kernenergie für Ihre Rechenzentren zu nutzen.

Allyn Stott, Senior Staff Engineer bei Airbnb. (Source: Netzmedien)

Ein weiteres Highlight war die Präsentation von Allyn Stott, Senior Staff Engineer bei Airbnb. Er sprach auf humorvolle Weise über seine gründen Misserfolge in Bezug auf Metriken. Wer den falschen KPIs hinterher renne, könne beispielsweise das Unternehmenszeil aus den Augen verlieren. Ausserdem solle man nicht messen, dass man sowieso nicht beeinflussen kann. Und – die vielleicht wichtigste Erkenntnis – man solle sich nicht zu sehr an Metriken klammern, die zu dem "Neuron" führt oft nicht weiter." Wenn man sich fragt, wie etwas ist, könne man auch ersieren, was getan werden muss, erklärte er. Um Unternehmen bei diesen Problemen zu helfen, entwickelte er ein "Trivial Metrics and Responses" Maturitätsmodell (auf Basis des Hunting Maturity Model).

Zur Öffnung der Schlechtwenden nach den zahlreichen, informativen Präsentationen endete der Tag mit einem Networking-Dinner. Dieses bestand aus Raclette und einem sehr ägyptischen Dessertbuffet. Die nächste Swiss Cyber Storm findet am 28. Oktober 2025 statt.

Teil des Dessertbuffets war ein kleiner Schokoladenbrunnen. (Source: Netzmedien)

Artikel teilen:

ZUM THEMA

Alex Wunsch
Ex-Cyanide-CTO will eigenes KI-Business starten

Daniela Neuhaus
Nationalratskommission will Verteidigungsstrategie gegen KI-Stuffen

Sandro Shaefer
Microsoft schickt autonome KI-Agenten bald in den Öffentlichen Testbetrieb

Reine KI-Modelle von Anthropic
Claude kann jetzt den Computer steuern

CYBERSICHERHEIT | CYBERSICHERHEIT | CYBER | CYBER

AKOM CORE - EMPFOHLEN

MEIST GELESEN

+ MEHR NEWS

CNO Parnel 2024
Von Träumen, vom Machen und vom Altbewährten
29.10.2024 – 12:45 Uhr

European Cyber Security Month
BACS warnt vor Audio-Deepfakes durch KI
29.10.2024 – 14:15 Uhr

EVENTS

+ MEHR EVENTS

Business Agility Day am 31.10.2024
31. Oktober 2024 – 8:00 bis 18:30
Kongresshaus Zürich
MEHR DAZU

Synology Experience Day 2024
05. November 2024 – 11:00 bis 17:20
Swiss Life Arena Zürich
MEHR DAZU

graphax.digital no 7
07. November 2024 – 9:00 bis 17:00
GDI - Gottlieb Duttweiler Institute, Langhalmstrasse 15, 8803 Rüschlikon
MEHR DAZU

DOSSIERS

+ MEHR DOSSIERS

DOSSIER
Fintech, Insurtech & Digital Banking
29.10.2024 – 10:15 Uhr

DOSSIER
DevOps
10.09.2024 – 16:15 Uhr

DOSSIER
Cyberkrieg in der Ukraine
17.02.2022 – 16:30 Uhr

AKTUELLE AUSGABE

Netzwoche Nr. 11/2024

Warum Cybersicherheit und Datenschutz so wichtig sind

E-ID wird digitale Identifikationslösungen ergänzen, nicht ersetzen

IT-Sicherheits-Expertise für alle Mitarbeitenden

DIREKT IN IHREN BRIEFKASTEN
CHF 139.-

+ MEHR BEITRÄGE

+ ABO ANMELDEN
+ ZUM SHOP
+ NEWSLETTER

© NETZMEDIEN AG 2024
Impressum
AGB
Nutzungsbedingungen
Datenschutzerklärung