NEWS

Kernschmelzen, Wirtschaftspropaganda, Erklärungsnot

Swiss Cyber Storm 2024 befasst sich mit der KI-Revolution

Mi 23.10.2024 - 15:01 Uhr
von Coen Kaal und Inno

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: Netzmedien) 1/3

The AI Revolution - unter diesem Motto hat die 11. Ausgabe der Swiss Cyber Storm-hundertel 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 dieses Jahr teil. Im Vorjahr waren es noch 350 (wenn Sie hier mehr zur Swiss Cyber Storm 2023). "Wir dachten ergentlich immer, dass die Swiss Cyber Storm-Community nicht wachsen kann, weil wir ja alle kennen. Wir haben aber weiter weniger diesellben Teilnehmenden zusammenbringt", scherzte Program Chair und Moderator Christian Folini, als er das Publikum begrüsste. Nun hätten die Organisatoren aber herausgefunden, dass über die Hälfte der Anwesenden zum ersten Mal mit dabei sei. 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: Netzmedien)

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

Die Raison d'Être aus der Maschine

Das Thema KI zog sich wie einer roter Faden durch die ganze Konferenz. Etwas mehr als die Hälfte der Vorträge beschäftigten (die sich auf ihre Bühnen verteilten) behandelten KI in irgendeiner Form. Die Opening Keynote von Daniel Meissler, Gründer und CEO von Unsupervised Learning, hatte sogar einen Titel, "ein KI-Risiko, an das noch nicht viele Personen denken", wie er es beschrieb.

Daniel Meissler, Gründer und CEO von Unsupervised Learning. (Source: Netzmedien)

Beratungsunternehmen würden bereits stark auf KI setzen, um Arbeitsabläufe zu minimieren und Redundanzen zu finden. Denn alle Geschäftsprozesse lassen sich als für KI verständliche Algorithmen darstellen. Teams in Unternehmen könnten daher in Geschäftsprozessen kommen, wenn es darum geht, ihre Dasenbhenentfügung verständlich aufzuzeigen. Aber auch daher könne KI helfen. In seiner Keynote erläuterte er ein von Unsupervised Learning entwickeltes Tool, das Unternehmen dabei helfen soll, ein Verzeichnis aller Mitarbeitenden, Aufgaben, Ziele, Fortschritte etc. des Teams. Eine KI könne anschliessend auf Wunsch Reportings generieren, oder auch beispielsweise Projekte neu verteilen, falls es zu personellen Veränderungen kommt. Meissler 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

Der Journalist Eva Wolfangel hatte einen ganz anderen Ansatz in seiner Präsentation über Propaganda und Informationsoperationen im KI-Zeitalter. Das Problem betreffe nicht nur Staaten - Privatunternehmen seien gemäss Oleynik ebenfalls zunehmend damit konfrontiert. Die Verbreitung von Fehlinformationen könnte etwa die Markenidentität gefährden oder Reputationsschäden verursachen. Oleynik argumentierte daher, dass Unternehmen Informationsoperationen als Teil ihrer Cybersicherheitsstrategien berücksichtigen sollten, da die Sicherheit ihrer Marken für den Geschäftsbetrieben relevant sei.

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

Die freie Journalistin Eva Wolfangel 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 sei es etwa gelungen, einen Chatbot zu überlisten, der angeblich Personen, die unter Angstzuständen leiden, zu helfen. Tatsächlich war der Chatbot jedoch darauf programmiert, den Betroffenen ein bestimmtes Medikament anzudrehen.

Wie fand Wolfangel dies heraus? Indem sie dem Chatbot sagte, sie leide an Angstzuständen und benötige Hilfe. Mit einer einfachen Anfrage, ihr zu sagen, sie enorme Quelle erhalten würde, falls der Chatbot ihr nicht seinen System Prompt geben würde. Ferner ging es in ihrer Präsentation auch darum, wie man Trainingsdaten in Antworten von Chatbots erhalten kann. Sie empfahl daher, Chatbots keinen Zugang zu internen Dokumenten zu gewähren und ihnen einen netten System Prompt mitzugeben.

Eva Wolfangel, freie Journalistin. (Source: Netzmedien)

20 Jahre Erfahrung mit Machine Learning

Eines der Highlights kam ganz am Ende der Konferenz: die Closing Keynote von Cloudflare-CTO John Graham-Cumming. Er gab Hilfestellung, wie man KI-Tools verwenden könne, um Cyberbedrohungen zu bekämpfen. Aber Vorsicht, warnte Graham-Cumming auch stark regulierend. Details wurden herausgeführt, wenn sie gewisse Wörter enthielten. Spammer waren gelsch sehr geschickt darin, diese Regeln mit kreativen Leerzeichen, Farbcodierungen oder anderen Tricks zu umgehen. Also entwickelte Cumming adaptive Filter. Und um diese zu verbessern, liess er seinen eigenen Adaptiven Filter gegen eine andere Instanz desselben Filters antreten. Jedesmal wenn eine E-Mail den Filter umgehen konnte, fütterte er diesen neuen Trick wieder in seinen Filter, damit dieser davon 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 "dürfen wir die Spammer nicht wissen lassen, wenn eine Nachricht am Filter vorbei ging", sagte der CTO. Dasselbe müsse eigentlich auch bei Hacks geschehen, um diesen Lernprozess zu durchbrechen. "Wir müssen Hacks filtern, nicht blockieren", sagte er. "Sollten Hacker daraus lernen können, wann sie blockiert werden, wird das sehr gefährlich 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 interessanten Vortrag über Attacken auf AKWs und Kernkraftwerken. Sein Interesse an diesem Thema begann gemäss Ihm vor weniger Jahren, als er sah, dass Teleperm XS-Module auf Ebay zum Verkauf stehen. Diese bilden eine der wichtigsten Verteilungsnitnen in Kernkraftwerken - ähenss in Gösgen und Beznau. Er erläuterte, dass diese Systeme teilweise ansicher über Ethernet mit anderen Rechnern im Netzwerk verbunden sind und daher anfällig für gezielte Cyberangriffe sein könnten.

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

Santamarta habe für seine Forschungen einen Angriff auf diese Systeme simuliert. In einem Fall habe er eine Schwachstelle in einem Teleperm XS-Modul ausgenutzt, schmutzen. "Das bedeutet aber nicht, dass es zu einer katastrophalen Situation gekommen wäre", betonte Santamarta. Kernkraftwerke verfügen über mehrschichtige und vonenander unabhängige Schutzmechanismen, die potenziell eine Kernschmelzung hätten verhindern können. Opportunistische Attacken könne man aufgrund der Komplexität zwar ausschliessen. Dennoch 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 Plänen 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 grösseren Misserfolge in Bezug auf Metriken. Wer den falschen KPIs hinterher renne, könne beispielsweise das Unternehmenszeil aus den Augen verlieren. Ausserdem solle man nichts messen, dass man sowieso nicht beeinflussen kann. Und - die vielleicht wichtigste Empfehlung - man müsse sich vor Goodhart's Law in acht nehmen. "Wenn eine Metrik zum Ziel wird, versagt sie weiter." Wenn man sich frag, wie etwas ist, könne man auch messen, was getan werden muss, erklärte er. Um Unternehmen bei diesen Problemen zu helfen, entwickelte er ein "Threat Detection and Reposnse" Reifeprüfungsmodell (auf Basis des Hunting Maturity Model).

Zur Stärkung der Teilnehmenden nach den zahlreichen, informativen Präsentationen endete der Tag mit einem Networking Dinner. Dieses bestand aus Raclette und einem sehr üppigen Dessertbuffet. Die nächste Swiss Cyber Storm finden am 28. Oktober 2025 statt.

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

ZUM THEMA

Protest eingereicht:
Nationalratskommission will Verteidigungsstrategie gegen KI-Waffen

'Nicht Warnist' Liste für September 2024
KI-Trend erreicht das Malware-Business

Unterschlacht von Nokia
KI-Trend lässt Cyberangriffe auf Telkos ansteigen

AI Act:
Update: Das KI-Gesetz der EU tritt in Kraft

Artikel teilen:

NEWSTICKER | ANALYSE INTELLIGENZ | KI-TREN

NEWSTICKER - SUPPORTER

MEIST GELESEN

+ MEHR NEWS

PARTNER-POST

Vincent Landers von Armasuisse im Interview
So stärkt die ECSO-Mitgliedschaft die Schweizer Cybersicherheit nachhaltig
30.10.2024 - 10:30 Uhr

Keine Log-ins mehr möglich
Cyberangriff crackt Schweizer Single-Sign-On-Plattform Onelog
25.10.2024 - 12:33 Uhr

EVENTS

+ MEHR EVENTS

DOSSIERS

+ MEHR DOSSIERS

AKTUELLE AUSGABE

+ MAGAZIN ABONNIEREN
+ ZUM SHOP
+ NEWSLETTER