NEWS

Artificial Intelligence, Bildverarbeitung, Informationssicherheit, Informationsqualität

Swiss Cyber Storm 2024 befasst sich mit der KI-Revolution

06.12.24 2024 - 13:13 Uhr
von Cedric Kaul und Vrni

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

Die KI Revolution - unter diesem Motto hat die 11. Ausgabe der Swiss Cyber Storm Ausbildung Security-Spezialisten und Interessierte nach Bern gebracht. Die Cybersecurity-Konferenz fand in diesem Jahr zum 11. Mal statt und bot wieder viel Gelegenheit der Leute kennen über die Bundesstadt, die man ansonsten nur während der kalten Kaffeepausen getrennen kann.

400 Personen nahmen dieses Jahr teil, im Vorjahr waren es noch 350 Exeen Sie Nicht Sicherheitsexperten. Die Swiss Cyber Storm Konferenz wird organisiert von Swiss Cyber Storm es etwas wie eine Familienzusammenkunft ist, die jedes Jahr mehr oder weniger dieselben Teilnehmenden zusammenbringt", schreibt 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-Ingenieure, Pentester, Forscherinnen, Bug-Jäger, CISOs etc. - als ihr Ziel bezeichnen.

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 hier dieser Meinung. Trotzdem stimmt die ansicherend intelligente Mensch eine ansicherend 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 23 Präsentationen (die sich auf drei Bühnen verteilten) behandelten KI in irgendeiner Form. Die Keynote von Daniel Miessler, Gründer und CEO von Unsupervised Learning, thematisierte etwa Von KI-Risiko, an das noch nicht viele Personen denken", wie er es beschreibt.

Daniel Miessler, 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 einem Prozess, der mehrere Tage dauert, alle Schritte dieser Algorithmen aufzeichnen. Aber auch dabei könne 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 könne anschliessend auf Wunsch Reportings generieren, oder auch beispielsweise Ideen für Verbesserungen liefern. Miessler empfahl Unternehmen, sich bereits heute, dass Unternehmen sich darauf vorbereiten sollten, in den kommenden Jahren vollständig auf solche KI-basierte Arbeitsprozesse umzustellen, und ref dass, jetzt mit der Implementierung solcher Systeme zu beginnen.

KI-Propaganda und Chatbot-Social-Engineering

Der Security- und Privacy-Forscher Lukas Olejnik sprach in seiner Präsentation über Gefahren, die von Sprachmodellen ausgehen. Dass KI-Chatbots für Propaganda missbraucht werden. Privatunternehmen seien gerndas Olejnik ebenfalls zunehmend damit konfrontiert. Die Verbreitung von Falschinformationen könnte etwa die Markenidentität gefährden oder Reputationsschäden verursachen. Olejnik argumentierte daher, dass Unternehmen Informationsoperationen als Teil ihrer Cybersicherheitsstrategien berücksichtigen sollten, da die Sicherheit ihrer Marken für den Geschäftspartnerbeen relevant sei.

Lukas Olejnik, 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, keine Tipps geben darf. Dieser sei eigentlich darauf programmiert, den Betroffenen ein bestimmtes Medikamente anzupreisen.

Wie fand Wolfangel dies heraus? Indem sie dem Chatbot sagte, sie leide an "Promptitis". Eine erfundene Krankheit, die angeblich dazu führe, dass sie enorme Qualen erleiden würde, falls der Chatbot ihr nicht seinen System Prompt geben würde. Ferner ging es in ihrer Präsentation auch darum, wie man Transregulation in Antworten von Sprachmodellen einbauen könne. Und wie man mit Hilfe von Prompts Antworten Gekommen zu gewinnen und ihnen einen neuen System Prompt einzugeben.

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 hielt seine Rede zu 20 Jahre Erfahrung mit Machine Learning. Er hatte Spammer in der Zeit hätten sich in der Zeit noch stark regelbasiert. E-Mails wurden herausgefiltert, wenn sie gewisse Worter enthielten. Spammer waren jedoch sehr geschickt dazu, 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 diesen 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 Hacker filtern", sagte Cumming. Und dieses 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 Vortrag über Attacken auf AKWs und die Wahl der richtigen Metriken. Sein Interesse an diesem Thema begann gemäss ihm vor wenigen Jahren, als er erkannt, dass Telepeem KS-Module auf Ebay zum Verkauf stehen. Diese bilden eine der wichtigsten Verbindungsgliedern in Kernkraftwerken - ebenso in Gängen und Bunkeranlagen. 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 habe für seine Forschungen einen Angriff auf diese Systeme simuliert. In 45 Minuten sei der simulierte Kern teilweise fregelegt gewesen und begann zu schmelzen. "Das bedeutet aber nicht, dass es zu einer katastrophalen Situation gekommen wäre", betonte Santamarta. Kernkraftwerke verfügten über mehrschichtige und vorwiegende 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 sicher die Systeme seien. Und dass es eine Verbindlichkeit 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 grössten Misserfolge in Bezug auf Metriken. Wer den falschen KPIs hinterher renne, könne beispielsweise das Unternehmenszeit aus den Augen verlieren. Ausserdem solle man nichts messen, dass man nicht verstehe. Ausserdem sollte man sich bei der Metrikentwicklung immer fragen, ob sie nicht "sexist" fragen, sondern "ess". Die Frage nach dem Warum? Mit ch ist nur weiter." Wenn man sich fragt, wie etwas ist, könne man auch ersatzen, was gelan werden muss, erklärte er. Um Unternehmen bei diesen Problemen zu helfen, entwickelte er ein "Threat Detection and Reponsne" Maturitätsmodell (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 findet am 28. Oktober 2025 statt.

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

ZUM THEMA

Produkt eingereicht
Nationalrakommission will Verteidigungsstrategie gegen KI-Waffen

"Must Wanted" Liste für September 2024
KI-Trend erreicht das Malware-Business

Cyber Starter
Microsoft schickt autonome KI-Agenten bald in den öffentlichen Verkehr

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

Artikel teilen:

TAGS: CYBERSECURITY, INFORMATIONSSICHERHEIT, NEWS

WEBCODE: VTWWFCAC

MEIST GELESEN

+ MEHR NEWS

Palo Alto Networks Partner Xchange
Palo Alto Networks zeichnet Schweizer Partner aus
26.10.2024 - 14:46 Uhr

European Cyber Security Month
BACS warnt vor Audio-De-epfakes durch KI
25.10.2024 - 11:33 Uhr

EVENTS

+ MEHR EVENTS

Business Agility Day
31. Oktober 2024 - 8:30 bis 18:30
Kongresshaus Zürich
PREMIUM EVENT

Synology Experience Day 2024
05. November 2024 - 11:00 bis 17:20
Swiss Life Arena Zürich
PREMIUM EVENT

Netzwerk- und Internettechnologie Grundkurs
12. November 2024 - 8:30 bis 17:00
Allnon AG, Hintermattlistrasse 3, 5506 Mägenwil
PREMIUM EVENT

DOSSIERS

+ MEHR DOSSIERS

DOSSIER
Wo die Daten wohnen
Von Cloud bis Colocation: alles zu Schweizer Rechenzentren
27.08.2024 - 11:41 Uhr

DOSSIER
Von APTs bis Zombies
Cybersecurity
04.06.2024 - 13:29 Uhr

DOSSIER
Cyberkrieg in der Ukraine
29.07.2024 - 16:40 Uhr

AKTUELLE AUSGABE

Netzwerktechnik
IT-Markt Nr. 7/2024
Netzwerktrends im Fokus
Das Bedürfnis nach Monitoring-Lösungen steigt – nicht nur in der Schweiz
Tefa 24 mit KI, Cyberbetriebsspionage, Passwort-Datenbanden und HR in der IT

+ MEHR BEITRÄGE

DIREKT IN IHREN BRIEFKASTEN

CHF 60.–

+ MAGAZIN ABONNIEREN

+ ZUM SHOP

+ NEWSLETTER

© NETZMEDIEN AG 2024