Von hoffnungsvoll bis feindselig:
Cyberkriminelle sind gegenüber KI noch unentschieden

Es ist natürlich nur eine Frage der Zeit, aber bis dato haben Cyberkriminelle die Vorteile von Künstlicher Intelligenz (KI) noch nicht sehr wirkungsvoll für ihre Angriffe einsetzen können. Und das, obwohl sie in Rekordzeit Millionen von Daten scannen kann. Diesen Faktor macht sich die Cyberabwehr jedoch sehr wohl zu Nutze – auch wenn es noch ein paar Hürden bei der Mensch-Maschine-Zusammenarbeit gibt.

Von Chester Wisniewski, Field CTO bei Sophos.

KI ist und bleibt ein faszinierendes Thema. In unterschiedlichsten Szenarien planen und setzen wir bereits die Leistungskraft von Maschinen ein, auch in der Cyberabwehr. Aber kommen sie auch auf der Seite der Angreifenden zum Einsatz? Die Haltung der Cyberkriminellen zu KI ist bislang uneins und reicht von hoffnungsvoll bis regelrecht feindselig. Die KI-Early Birds unter den Cyberkriminellem teilen ihre Tools, auch wenn die Ergebnisse noch nicht sehr eindrucksvoll sind. Einige haben aber für sich entschieden, dass LLMs (Large Language Models) noch zu sehr in den Kinderschuhen stecken, als dass sie für erfolgreiche Angriffe taugen. Eine breit angelegte Untersuchung cyberkrimineller Kommunikation zeigt ihr indifferentes Meinungsbild,
https://news.sophos.com/en-us/2023/11/28/cybercriminals-cant-agree-on-gpts/.

Bei der proaktiven Aufdeckung von Cybergefahren konzentriert sich KI auf die Klassifizierung von Telemetrie. Die Menge an Daten, selbst bei einem kleinen Kundenstamm, ist gewaltig. Daher ist das Finden von Mustern und die Alarmierung der menschlichen Analyst:innen ein unverzichtbarer Bestandteil moderner Sicherheitslösungen.

Günstig, schnell und mit Freude an der Arbeit: KI ist Fleiß-Vorbild im Team
KI verbessert die Fähigkeit, verdächtige Muster und Verhaltensweisen zu erkennen, indem sie ein Maß an Robustheit einführt, die bei manuellen, regelbasierten Systemen nicht möglich ist. Wenn das Maß an Cybersecurity-Daten wächst, wird das Beibehalten von manuellen Systemen sehr teuer und zeitraubend – im Vergleich dazu blüht KI angesichts von immer mehr Informationen regelrecht auf. Ihrer statistischen Natur gemäß entwickelt sie komplexe Entscheidungen über verdächtiges Verhalten, die mit menschlichem Bemühen nicht reproduzierbar sind.

Um die Einbindung von KI strategisch anzugehen, sollten Organisationen zunächst behutsam die Pflege der Daten planen. Das bedeutet, zum Beispiel nicht in die Falle der willkürlichen Datensammlung zu geraten, denn gute Daten sind die Lebensader von KI. Schlechte Planung bei der Datensicherung kann zu Verzögerungen und hohen Kosten für zu generierende Gütesiegel führen.

Bedrohungen schneller entdecken mit KI
Der Einsatz von KI in der Cyberabwehr bietet eindeutig Vorteile. Durch das Trainieren von Angriffsmustern kann KI etwa lernen, verdächtige Aktivitäten in Echtzeit zu bemerken – selbst bei immensen Datenmengen. KI lässt sich so als Hilfe bei automatisierten Prozeduren einsetzen. Ein Beispiel: KI-generierte Einschätzungen des Schweregrades einer Abweichung könnten als Grundlage für eine Regel verwendet werden, die ein System automatisch in Quarantäne setzt. Bei der Wiederherstellung kann KI bei der Triage, also der Entscheidung

der Handlungsreihenfolge, nützen. Ebenso bei dem Verständnis der Folgen einer schadhaften Aktivität.

Die greifbaren Vorteile sind daher zahlreich: von einer genaueren Aufdeckung von Gefahren, über geringere Response-Zeiten und effizienteren Einsatz Analysten-Zeiten bis hin zur Fähigkeit zur Generalisierung für zukünftige Vorfälle. Zudem halten KI-generierte Lösungen die Kosten und Wartungen manueller Ansätze kleiner.

Integration der KI ins menschliche Team
Bei der Implementierung von Cybersicherheitslösungen steht man vor einigen Herausforderungen. Die Beschaffung von Qualitätsdaten ist ein dauerhaftes Problem, weil es so unverzichtbar ist für das Training performanter KI-Modelle. Schlampiger Umgang mit Daten mündet unmittelbar in teuren Konsequenzen und fehlerhaften Modellen. Ein eher praktisches Problem bei der KI-Integration ist die Vertrauensbildung mit den menschlichen Analyst:innen. Viele KI-Modelle liefern wenig zufriedenstellende Erklärungen für ihre Vorhersagen, und benötigen daher sehr sorgfältige Auswertungen und umfassendes Testen.

Hinsichtlich der Zusammenarbeit muss man bedenken: KI dient als eine Art Powermultiplikator, der die Produktivität verbessert und neue Möglichkeiten schafft. Aber es ist wichtig zu verstehen, dass KI – auch mit der Ausbreitung von LLMs – kein Allheilmittel ist, weil sie unrichtige Informationen als Fakt herausgeben kann. KI bleibt eine sehr effektive Lösung für zahlreiche Probleme, kann aber den Bedarf an menschlicher Intervention und Qualitätskontrolle nicht ersetzen. In der näheren Zukunft könnten wir einen Paradigmenwechsel sehen, wo menschliche Expert:innen zu KI-Editoren werden. Menschen könnten KI die Initialisierung von bestimmten Prozessen erlauben und die Ergebnisse mithilfe ihrer menschlichen Expertise feinjustieren.

In einer modernen Cyberabwehr ist Cybersecurity-as-a-Service ein essentieller Bestandteil. Angriffe werden immer komplizierter und Unternehmen werden sich immer mehr an ausgebildete SOCs wenden, auch angesichts limitierter eigener Sicherheitskapazitäten. KI ist eine Pflicht-Komponente für den Erfolg groß angelegter SOCs, damit eine begrenzte Zahl an menschlicher Expertise mit globalem Umfang arbeiten kann.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de