Kommentar

WAS WIR IN DER CYBERSICHERHEIT ANGEHEN MÜSSEN

Die größte europäische IT-Sicherheitsmesse it-sa verzeichnete in diesem Jahr einen Rekord: Erstmals präsentierten sich rund 800 Aussteller. Im Fokus der meisten Besucher stand die Frage, was angesichts der sich eher verschlechternden IT-Sicherheitslage getan werden kann, um eine adäquate IT-Sicherheitsstrategie zu entwickeln und dementsprechend die richtigen Maßnahmen in Sachen Cybersicherheit zu ergreifen. Unser Autor nennt zwei relevante Aspekte, die heute und in Zukunft eine wichtige Rolle spielen.

Wie lässt sich ein angemessenes IT-Sicherheitslevel umsetzen, um gegen intelligente Angriffe geschützt zu sein?

Die Umsetzung des „Stand der Technik", also der am Markt verfügbaren fortschrittlichen und damit bestmöglichen IT-Sicherheitsmaßnahme, schafft ein notwendiges IT-Sicherheitslevel, mit dem Unternehmen und Organisationen einen wirksamen Schutz gegen die derzeit existierenden intelligenten Angriffe etablieren können.

Dies lässt sich dadurch erklären, dass der „Stand der Technik" zwischen dem innovativeren Technologiestand „Stand der Wissenschaft und Forschung" und dem sogenannten altbewährten Technologiestand „allgemein anerkannte Regeln der Technik" angesiedelt ist. Ersterer ist in der Regel wirksamer, aber noch nicht am Markt verfügbar, während IT-Sicherheitsmaßnahmen im Stadium „allgemein anerkannte Regeln der Technik" schon länger erhältlich sind und daher allzu oft keinen ausreichenden Schutz mehr gegen innovative Angreifer bieten. Das lässt sich anhand zahlreicher Beispiele belegen: die Verwendung von Passwörtern für die Authentifikation oder die Nutzung von nicht sicheren Signatur- und Verschlüsselungsalgorithmen. Aber auch Anti-Malware-Lösungen, die überwiegend auf Signaturerkennung basieren, gehören – im Rahmen der fortschreitenden Digitalisierung – dieser nicht mehr angemessenen Kategorie an.

Konsequenterweise fordern beispielsweise die beiden Rechtsquellen „IT-Sicherheitsgesetz" und „EU-Datenschutzgrundverordnung" die Orientierung der IT-Sicherheit am „Stand der Technik", lassen aber offen, was darunter im Einzelnen zu verstehen ist.

Der Bundesverband IT-Sicherheit – TeleTrusT hat daher seit 2015 einen aktiven Arbeitskreis mit über 40 IT-Sicherheitsexperten etabliert, der eine Handreichung zum Stand der Technik mit

konkreten Hinweisen und Handlungsempfehlungen herausgibt. Dieser Leitfaden wird kontinuierlich aktualisiert und erweitert – und steht zum kostenlosen Download zur Verfügung. Der Kompetenzverbund TeleTrusT wird in Zukunft deutlich mehr Unterstützung für Unternehmen anbieten, die zur kritischen Infrastruktur (KRITIS) gehören, damit gerade in diesem Bereich die Gesellschaft auf Basis des „Standes der Technik" angemessen geschützt wird.

KÜNSTLICHE INTELLIGENZ UND IT-SICHERHEIT

Das zweite Thema, das in der Cybersicherheit eine immer wichtigere Rolle spielen wird, ist die künstliche Intelligenz (KI). Die KI hat in den letzten Jahren sehr viele Innovationsschritte durchlaufen – mit deutlich verbesserten Algorithmen und Modellen, aber auch mit einer enormen Leistungssteigerung durch entsprechende Hardware. Hinzu kommt, dass durch die Digitalisierung immer mehr relevante Daten anfallen. Dies ist für die Entwicklung von Vorteil, da die KI sie als Input braucht, um aus ihnen Wissen abzuleiten. Dazu ist es wichtig, dass die Daten auch relevante Informationen enthalten, aus denen Wissen extrahiert werden kann. Daraus erklärt sich insgesamt die Bedeutung von KI als zunehmend bedeutender Baustein für viele Bereiche – auch für die IT-Sicherheit.

ANGREIFER NUTZEN KI SEHR ERFOLGREICH

Doch wo Licht ist, ist auch Schatten, denn Cyber-Kriminelle nutzen KI schon intensiv, um einfacher und erfolgreicher angreifen zu können.

Die Anwendungsbereiche für KI sind dabei vielfältig, beispielsweise wird sie benutzt, um Schwachstellen zu entdecken und IT-Sicherheitsmaßnahmen zu überwinden. Besonders ChatGPT bietet Kriminellen nochmals neue Angriffsunterstützung – nachfolgend nur einige Beispiele:

- Social Engineering: ChatGPT schreibt und antwortet wie ein Mensch, wodurch Angreifer deutlich effizienter Phishing- und Fake-News-Attacken durchführen können, auch in Sprachen, die sie eigentlich nicht beherrschen.
- Programmierunterstützung: ChatGPT hilft Angreifern dabei, zum Beispiel sogenannte polymorphe Malware zu produzieren, wodurch die Erkennungsraten von Anti-Malwarelösungen stark reduziert und somit Malware-Angriffe erfolgreicher werden.

KI FÜR IT-SICHERHEIT

Auf der anderen Seite schafft der Einsatz von KI in der IT-Sicherheit einen deutlichen Mehrwert für den Schutz von Unternehmen und Organisationen. Ein erstes wichtiges Themenfeld ist die Erhöhung der Erkennungsrate von Angriffen.

Dabei geht es konkret um die Erkennung von Angriffen über das Netzwerk und in den Endgeräten, Servern, Internet-of-Things-(IoT)-Geräten und Cloudanwendungen. Hierfür benötigt man adaptive KI-Modelle, um auch neue Angriffsvektoren und Bedrohungen frühzeitig detektieren zu können.

Wichtig ist hier aber, dass die notwendigen sicherheitsrelevanten Daten aus den Netzwerken und IT-Systemen allgemein zur Verfügung gestellt werden, damit die KI daraus nützliche Ergebnisse zur Verbesserung des Schutzniveaus erzielen kann. Andere Bereiche aus der Erkennung sind zum Beispiel das Erkennen von Malware, Spam, Fake News und Deepfakes.

Ein weiterer relevanter Vorteil der KI im Rahmen der IT-Sicherheit ist, dass sie IT-Sicherheitsexperten unterstützen und damit entlasten kann – denn derzeit sind über 100.000 Stellen im Bereich IT-Sicherheit unbesetzt.

So kann die KI zum Beispiel dabei helfen, wichtige sicherheitsrelevante Ereignisse zu analysieren und mit einer Priorisierung zu versehen, um dem IT-Sicherheitsexperten zeitaufwendige Analysearbeit abzunehmen. Dabei untersucht ein KI-System die zu hunderten oder tausenden eingehenden sicherheitsrelevanten Ereignisse von den IT-Systemen und zeigt dann auf, nach welchen Prioritäten diese vom IT-Sicherheitsexperten abgearbeitet werden müssen, um den höchsten Schutz in der aktuellen Situation für das Unternehmen zu erzielen.

Ein anderes Beispiel lässt sich im Bereich der (Teil-)Autonomie bei Reaktionen finden: Wenn ein Angriff oder eine besondere Bedrohung erkannt wird, können mithilfe der KI sofort Firewall- und E-Mail-Regeln automatisch so reduziert werden, dass die wichtigen Prozesse für ein Unternehmen aufrechterhalten bleiben, aber die Angriffsfläche für die Angreifer deutlich geringer wird, damit Schäden verhindert oder zumindest gemindert werden.

Es gibt noch viele weitere Bereiche der IT-Sicherheit, in denen KI – auch mit ChatGPT oder ChatGPT-ähnlichen Lösungen – IT-Sicherheitsexperten unterstützen kann, wie zum Beispiel sichere Softwareentwicklung, IT-Forensik und Threat Intelligence.

FAZIT

Die Umsetzung des Standes der Technik und die künstliche Intelligenz sind beides Themen, die IT-Sicherheitsverantwortliche, Wissenschaftler und Entwickler noch lange beschäftigen werden. Besonders die KI ist eine Medaille mit zwei Seiten: Als Werkzeug hilft sie sowohl CISOs als auch den Kriminellen. Wie das genau ausgeht, lässt sich heute noch nicht sagen – auf jeden Fall wird 2024 aber spannend. ■

*Die **„HANDREICHUNG ZUM STAND DER TECHNIK"** gibt konkrete Hinweise und Handlungsempfehlungen. Das Paper ist kostenfrei als PDF verfügbar: www.teletrust.de/publikationen/broschueren/stand-der-technik/*

NORBERT POHLMANN
ist Professor für Cybersicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.