Mit Künstlicher Intelligenz gegen Cyberangriffe wappnen

Am Donnerstag dieser Woche waren fünf deutsche Regional-Flughäfen nicht zu erreichen. Offenbar russische Hacker hatten die Internetseiten blockiert. An diesem Wochenende tagte die Nato, um sich mit der Cyberabwehr zu befassen. Es kann also Reisende treffen oder unser Militär, Wirtschaftsunternehmen, die gesamte Infrastruktur oder jeden Fahrer eines unserer intensiv vernetzten Autos. Sind wir also schutzlos? Nein, sagen Experten Prof. Marco Barenkamp. Der Vorstandsvorsitzende der Osnabrücker LMIS AG will den Angreifern mit künstlicher Intelligenz (KI) an den Kragen, getreu den Firmennamen. LMIS steht für Let‘s make it smarter.

Barenkamp spricht von KI-Softwarelösungen, die innerhalb angegriffener Netzwerke Anomalien erkennen und automatisch abwehren können. Die Software analysiert die Metadaten eines Netzwerks in Echtzeit. Bei Anomalien, die auf einen unerlaubten Datenzugriff hindeuten, unterbindet sie diesen Zugriff bereits im Ansatz. Eine Voraussetzung für den Erfolg nennt Prof. Barenkamp in seinem Beitrag „KI-basierte Anomalieerkennung als Abwehrmechanismus bei Cyberangriffen“ in der Fachzeitschrift „Wirtschaftsinformatik und Management“: Eine effiziente und effektive Abwehr von Cyberangriffen setze die Schaffung von Transparenz im eigenen Netzwerk voraus, was aufgrund der heutigen Komplexität auch nicht mehr ohne KI zu erreichen sei.

Cyberattacken oder Hackerangriffe sind längst keine Einzelfälle mehr, sondern eine allgegenwärtige Gefahr, nicht nur für Unternehmen und jeden Einzelnen Internetznutzer und Autofahrer, sondern ebenfalls für ganze Länder. Denn kriegerische Auseinandersetzungen finden zunehmend im Internet statt. Nach Angaben des Bundeskriminalamts sollen sich Cybercrimedelikte seit 2015 mehr als verdoppelt haben. Allein im Jahr 2021 registrierte die Behörde insgesamt rund 150.000 Cyberstraftaten, die laut Wirtschaftsschutzbericht einen Schaden von rund 223,5 Milliarden Euro verursachten.

Dementsprechend ist nationale Cybersicherheit zum Thema geworden, sowohl für Staaten und ihre kritische Infrastruktur als auch für Unternehmen und natürlich für jeden Bürger, der heute nicht nur auf der privaten Ebene von Internetbetrügern bedroht wird, sondern aus der Ukraine hört, dass nicht nur Raketen Stromnetze, Wasserversorgung und Heizungen stilllegen können.

Die Fähigkeit, kleinste Anomalien in den Netzwerkaktivitäten zu erkennen, ermöglicht der KI, – so Prof. Barenkamo – unbekannte Bedrohungen und neue Angriffsmuster von Cyberkriminellen bereits in einem frühen Stadium zu identifizieren. Hierin sieht er die besondere Stärke der selbstlernenden KI. Sie sei eben nicht nur in der Lage, einen Angriff in Echtzeit zu erkennen, sondern auch selbstständig und intelligent auf diesen zu reagieren und ihn abzuwehren, bevor ein großer Schaden entstehen kann. (aum)

Bilder zum Artikel

Foto: