idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Press release

Martin-Luther-Universität Halle-Wittenberg
Tom Leonhardt

11/07/2023
http://idw-online.de/en/news823484

Research projects, Transfer of Science or Research
Information technology
regional

IT-Sicherheit: KI hilft dabei, Kommunen vor Cyberangriffen zu schützen

Informatiker der Martin-Luther-Universität Halle-Wittenberg (MLU) helfen Kommunen und öffentlichen Einrichtungen dabei, sich besser auf Cyberattacken vorzubereiten und diese abzuwehren. In einem Forschungsprojekt entwickelten sie einen neuen Ansatz zur Überwachung von Netzwerken mit Hilfe Künstlicher Intelligenz (KI). Diese soll dabei helfen, Cyberangriffe frühzeitig zu erkennen und größere Schäden zu verhindern. Die Experten für Cybersicherheit haben an der MLU auch ein IT-Sicherheitslabor aufgebaut, in dem internetfähige Geräte auf Schadsoftware getestet werden können. In einigen Kommunen Sachsen-Anhalts wird das hallesche Sicherheitskonzept bereits eingesetzt.

Bei Cyberangriffen gilt: Je eher das Problem erkannt und behandelt wird, desto besser. Gerade für kleinere Unternehmen und viele öffentliche Einrichtungen ist das aber nicht ohne Weiteres möglich. "Geschultes IT-Personal, speziell zur IT-Sicherheit, ist ein rares Gut. Oft sind die Mitarbeiterinnen und Mitarbeiter für mehrere Bereiche zuständig und chronisch überlastet", sagt Dr. Sandro Wefel vom Institut für Informatik der MLU. Bestehende Angebote zur Überwachung von Computernetzwerken seien oft zu teuer und unflexibel. Deshalb würden viele Unternehmen und öffentliche Einrichtungen eher auf händische Überwachung setzen. "Um einen Cyberangriff zu erkennen, müsste man aber genau zum richtigen Zeitpunkt auf das richtige System schauen und dann das Problem direkt identifizieren. Das ist sehr aufwändig und unwahrscheinlich", sagt Wefel.

Die halleschen Informatiker erarbeiteten in Kooperation mit mehreren Kommunen und öffentlichen Einrichtungen eine neue, praktikable Lösung. Dabei setzen die Forschenden auf frei verfügbare Software und auch auf Künstliche Intelligenz. "In einem ersten Schritt lernt unser System den normalen Datenverkehr der jeweiligen Einrichtung über mehrere Tage kennen", erklärt Wefel. Dafür muss die KI keine E-Mails mitlesen oder Dateien anschauen. Stattdessen werden sogenannte Metadaten analysiert: etwa die Uhrzeit, Dauer und der Umfang bestimmter Aktionen. "Beobachtet werden lediglich Kommunikationsmuster. Der Schutz sensibler Daten ist mit unserem Angebot gewährleistet", sagt Wefel.

Nach dem Training wacht die KI konstant über das Netzwerk. Erkennt sie Auffälligkeiten, erhalten die IT-Beauftragten sofort einen Hinweis und können im Ernstfall reagieren. Die KI kann sogar automatisiert Gegenmaßnahmen ergreifen und Angriffe abwehren. Die Lösung der MLU lernt dabei beständig dazu, so dass seltene Aktionen, die zum Beispiel nur einmal im Jahr durchgeführt werden, in Zukunft direkt als unschädlich erkannt werden. Analysiert wird auch der Datenverkehr von internetfähigen Geräten, zum Beispiel Smartphones, Internetradios oder Webcams im Büro. "Die Bedienung dieser Geräte ist oft sehr bequem. Leider sind sie auch ein beliebtes Einfallstor für Hacker, da sie nicht regelmäßig gewartet werden", sagt Wefel.

Das MLU-Team hat auch ein IT-Sicherheits-Labor für Tests und Demonstrationszwecke eingerichtet: Hier können zum Beispiel einzelne Hardwarekomponenten, Computer und Server sowie weitere internetfähige Geräte auf einen möglichen Befall mit Schadsoftware untersucht werden. Außerdem lässt sich der Datenverkehr der jeweiligen Geräte erfassen und sich somit herausfinden, wie diese über das Internet kommunizieren und an welchen Stellen womöglich Sicherheitsrisiken sind. Das Labor wird auch in der Lehre sowie für Weiterbildungen eingesetzt.

Das Angebot für das neue, KI-basierte Sicherheitskonzept steht öffentlichen Einrichtungen und kleinen sowie mittelständischen Unternehmen der Region offen. "Auf Anwenderseite ist der Aufwand für die Einrichtung und den langfristigen Betrieb vertretbar", so Wefel. In mehreren Kommunen Sachsen-Anhalts ist das hallesche Sicherheitskonzept bereits im Einsatz.

Das Angebot der MLU basiert auf dem gemeinsamen Forschungsprojekt "CyberSecurity Verbund Sachsen-Anhalt" mit der Hochschule Harz und der Otto-von-Guericke-Universität Magdeburg, das in den vergangenen Jahren vom Land Sachsen-Anhalt und aus Mitteln des Europäischen Fonds für regionale Entwicklung (EFRE) gefördert wurde.

Weitere Informationen zum gesamten Projekt unter: https://cslsa.de/