»KI ist zugleich Bedrohung und Lösung«

Vom »Human Factor« über KI bis zu Zero-Day-Attacken: Die Welt der IT-Security dreht sich schnell. IT WELT.at sprach mit Matthias Hausegger, Vorstand bei ONTEC AG, und Franz Großmann, Geschäftsführer bei schoeller GmbH.

Welche Rolle spielen heute Zero-Day-Attacken?
Franz Großmann Bei Zero-Day-Attacken werden unbekannte, theoretische oder erst kurz bekannte Sicherheitslücken miteinander kombiniert, um in Fremdsysteme einzusteigen. Das Zeitfenster zwischen Bekanntwerden einer Sicherheitslücke und deren Ausnutzung wird immer kleiner, sodass die Reaktionszeit für Hersteller und Administratoren immer kürzer ausfällt.
Matthias Hausegger Meist bemerkt man eine Attacke erst, wenn ein tatsächlicher Schaden eingetreten ist. Daher hat diese Art des Angriffs oft schwerwiegende Folgen für die Betroffenen. Für das Erkennen von Zero-Day-Attacken spielt die Erfassung und richtige Interpretation von Logs und anderer Betriebsparameter eine zentrale Rolle.

Franz Großmann Im Prinzip ist es ein Rüstungswettbewerb zwischen Hackern und Herstellern. Setzen Hacker auf KI-unterstützte Tools, so ist es sinnvoll diesen mit den besten Verteidigungsmechanismen zu begegnen. Setzt man hier KI ein, trainiert jeder neue Angriff auch die KI der Verteidiger.

Viele aktuelle Security-Tools können geloggte Ereignisse nicht immer Kategorien zuordnen. Wie kann dieses Problem angegangen werden?
Franz Großmann Aktuelle Log-Analyse-Tools verwenden hauptsächlich manuell definierte Regeln in Parsern, um Einträge zu analysieren. Hier können nur solche Einträge erkannt werden, für die in den Parsern auch Regeln stehen. Ein alternativer Ansatz ist die Verwendung von NLP (Natural Language Processing). In diesem Teilbereich der KI geht es um das Verständnis geschriebener Sprache. Eine solche NLP-KI kann Log-Files auch ohne zuvor manuell definierte Regeln verstehen und interpretieren. Schoeller bietet hier mit der KI L.A.R.A. eine einzigartige Lösung dafür an..

Welche Rolle spielt aus Ihrer Sicht der Human Factor im IT-Security-Bereich und wie bekommt man ihn am besten in den Griff?
Matthias Hausegger Das kann man auf zwei Ebenen betrachten. Einerseits ist der Faktor Mensch eine der größten Schwachstellen der IT-Security, andererseits ist der Einsatz von gut ausgebildeten Fachkräften für sichere IT-Systeme unumgänglich. Es gibt aber Aufgaben, wie die Analyse und Interpretation von tausenden Log-Daten, die durch Menschen nicht sinnvoll erfüllt werden können. Diese sind prädestiniert für den Einsatz von KI.
Franz Großmann KI kann auch dabei helfen, Bedrohungen durch den Faktor Mensch selbst zu minimieren. Bringe ich als potenzieller Angreifer jemanden dazu, mich ins System zu lassen, brauche ich es nicht mehr zu hacken. Durch Deep Fakes lassen sich Menschen besonders leicht täuschen. KI ermöglicht diese Art der Täuschung immer einfacher. Das ist wieder ein Beispiel, wo KI die Bedrohung, aber auch die Lösung ist. Bringe ich in diesem Szenario einer KI bei, Deep Fakes schon vorab zu erkennen, lässt sich das Risiko einer Täuschung vermindern.

Wo ist IT-Security in österreichischen Unternehmen in der Regel angesiedelt? Bereits im Top-Management?
Matthias Hausegger Das ist sehr unterschiedlich. Häufig gibt es einen CISO, der meist bei der IT angesiedelt ist. Da gibt es keinen wirklichen Standard, aber wir haben beobachtet, dass diese oft unter dem CFO oder COO organisiert ist.
Franz Großmann Natürlich rücken IT-Security-Themen nach Bekanntwerden großer Attacken, oder wenn man selbst Opfer einer Attacke wird, immer besonders in den Vordergrund. Trotzdem würde ich auch das generelle Bewusstsein für IT-Security bei den Unternehmen mittlerweile als sehr hoch einschätzen. wf

Wie können sich Unternehmen vor künftigen, heute noch unbekannten Angriffen schützen?
Matthias Hausegger Oft finden Hersteller die Schwachstellen ihrer Systeme selbst und beheben sie, bevor sie ausgenützt werden können. Sich gegen nicht gefundene Zero-Day-Exploits zu schützen ist schwieriger, da sie per Definition unbekannt sind. Ich kann aber KI-Systeme bauen, die wissen was normal ist und dann in weiterer Folge Abweichungen vom Normalzustand feststellen. Ein Angriff kann so im Idealfall automatisch und in Echtzeit erkannt und abgewendet oder der Schaden zumindest begrenzt werden.
Franz Großmann Grundsätzlich ist es aber empfehlenswert, immer auf dem neuesten Patch-Stand zu sein, um alle bekannten Bedrohungen auszuschließen. Das macht Kapazitäten frei, um sich auf unbekannte Sicherheitslücken zu konzentrieren.

Welchen Nutzen hat KI im IT-Security-Bereich?
Matthias Hausegger Für den Einsatz von KI in der IT-Security gibt es viele Möglichkeiten. Etwa indem man eine KI mit bekannten Angriffsmustern so trainiert, dass sie diese und ähnliche Bedrohungen erkennt und bekämpft. Eine andere Strategie wäre, eine KI den Normalzustand erlernen zu lassen um, dann Abweichungen festzustellen.

»Das Fehlen von 24.000 IT-Experten verursacht einen jährlichen Wertschöpfungsverlust von rund 3,8 Milliarden Euro und schwächt den Wirtschaftsstandort. 40 Prozent der im Rahmen des Infrastrukturreports befragten Manager nennen das Fehlen von IT-Mitarbeiter, weitere 33 Prozent fehlende IT-Qualifikationen als die größten Digitalisierungshürden. Das verlangsamt die digitale Transformation unseres Wirtschaftsstandorts. Dafür brauchen wir Lösungsansätze.«

Alfred Harl, Obmann des Fachverbands UBIT

»Am Anfang des Weges zu einer Data Driven Company muss eine klare Management-Entscheidung stehen. Denn die Umsetzung einer entsprechenden Strategie betrifft alle Bereiche des Unternehmens und benötigt entsprechende Investments sowie Änderungen in Abläufen und Verantwortlichkeiten. Im nächsten Schritt muss die Datenbasis geschaffen werden.«

Christian Lutz, Gründer und Director of the Board bei Crate.io

»Zero Trust ist weniger eine Technologie als vielmehr eine Denkweise – ein Design-Muster. Aus dieser Perspektive könnte man Zero Trust genauso gut als bessere Sicherheit bezeichnen. Niemand kann behaupten, dass dieser Rahmen alle Angriffe verhindern kann, aber wir versuchen nicht, einen Zustand der Perfektion zu erreichen; wir versuchen, die Sicherheit stetig zu verbessern, und die Implementierung von Zero Trust hilft ganz sicher dabei.«

Wendy Nather, Vorsitzende des CISO-Fachbeirats bei Cisco

»Einerseits ist der Faktor Mensch eine der größten Schwachstellen der IT-Security, andererseits ist der Einsatz von gut ausgebildeten Fachkräften für sichere IT-Systeme unumgänglich. Es gibt aber Aufgaben, wie die Analyse und Interpretation von tausenden Log-Daten, die durch Menschen nicht sinnvoll erfüllt werden können. Diese sind prädestiniert für den Einsatz von KI.«

Matthias Hausegger, Vorstand bei ONTEC AG