Akamai Security

EINFÜHRUNG

Rupesh Chokshi

Senior Vice President und General Manager, Application Security

Bei Kundenmeetings und Branchenveranstaltungen – und fast jeden Tag, wenn ich die Nachrichten lese – ist mir eines klar geworden: Wenn wir das Versprechen der neuen KI-Ära erfüllen wollen, müssen wir uns auch der damit verbundenen Sicherheitsherausforderungen bewusst sein.

Wir haben bereits einige hochkarätige Beispiele dafür gesehen, was passiert, wenn KI nicht richtig gesichert wird. Bei einem der bekanntesten Fälle bösartiger KI-Manipulation überzeugte ein Mann in Watsonville, Kalifornien, den Chatbot eines Chevrolet-Händlerbetriebs davon, ihm einen neuen Chevy Tahoe für einen US-Dollar zu verkaufen. Monate später, im Februar 2024, befand ein kanadisches Gericht Air Canada für die Fehlinformationen haftbar, die sein KI-gestützter Chatbot einem Verbraucher gegeben hatte.

Dies sind natürlich nur einige frühe Beispiele. Derzeit führen Unternehmen auf der ganzen Welt möglicherweise unwissentlich neue KI-Schwachstellen in ihre Umgebungen ein. Die Kosten können erheblich sein – für Ihren Ruf, Ihren Gewinn, in Form von Strafen wegen Nichteinhaltung von Vorschriften und für die sehr hohen Investitionen, die so viele in die Implementierung von KI getätigt haben.

Kürzlich fragte mich mein Arzt bei einer Untersuchung, ob er einen KI-Agenten zum Notieren verwenden dürfe. Das Gespräch ging über meine Gesundheit hinaus – es ging um Wochenendpläne, die College-Wahl meiner Tochter und vieles mehr. Ich habe mich gefragt, wohin diese Informationen fließen. Ob der Arzt es überhaupt wusste? Handelte es sich hier potenziell um einen HIPAA-Verstoß?

Das sind die Fragen, die in Konferenzräumen und Vorstandssitzungen weltweit gestellt werden: Setzen wir KI sicher ein? Entwickeln wir sie sicher? Und wenn diese Fragen nicht gestellt werden, dann müssen sie es. KI hat für eine Welle von Optimismus und Innovation gesorgt. Sie bringt jedoch eine ganz neue Dimension an Cybersicherheitslücken mit sich, die sich mit den bestehenden Sicherheitslösungen nicht bewältigen lassen. Bereits jetzt haben wir eine natürliche Spannung zwischen zwei Parteien beobachtet:

- Chief AI Officer und ihre Entwicklungsteams versuchen händeringend, neue KI-Anwendungen und Geschäftsmodelle bereitzustellen.
- CISOs fragen sich, wie sie sich vor Bedrohungen schützen können, die sie vielleicht noch nicht kennen.