Why today’s security models struggle against AI attacks

Friday, March 27, 2026

Today’s top story, from reporter Patrick Lucas Austin:

AI may be in the process of revolutionizing business operations and cybersecurity preparedness alike, but it can also be dangerous in the hands of bad actors. A series of high-profile cyberattacks over the past year has shown that conventional cybersecurity tactics and tools are no longer enough when you’re dealing with hackers using AI-powered tools. That was the topic of conversation at RSA 2026 this week, where IBM experts discussed how the combination of smart agentic AI adoption and thorough AI governance can put enterprises at the forefront of defending against threats.

A new study from the IBM Institute for Business Value (IBV) and Palo Alto Networks suggests that AI is no longer an optional security layer, but an essential component to protecting both traditional and AI-enhanced business operations. Of 1,000 executives surveyed, 67% said they’ve been targeted by AI attacks within the past year. The majority agreed that today’s cybersecurity threats are evolving at a rate difficult to keep pace with.

Securing themselves against those attacks is proving to be a challenge. 61% of surveyed leaders said that elements of their AI framework have been compromised, making securing AI systems a priority. Difficulties arise when attempting to scale AI agents across the enterprise, which often use outdated permissions structures and have unfettered access to systems not integral to their task.

Other challenges included the use of AI agents lacking data management safeguards and observability roadblocks, increasing enterprises’ overall security debt. AI agents can enhance day-to-day workflows, but ensuring they’re operating within a secure environment presents challenges, with 45% of leaders citing gaps in identity and access controls as core weak points in AI security posture.

According to Mark Hughes, Global Managing Partner of Cybersecurity Services for IBM Consulting and co-author of the report, the findings suggest that when not factored in at the start, security can be

“a real barrier to successfully scaling trusted AI.” He added, “Organizations need stronger guardrails around how AI systems behave, what they can access and how they’re monitored. When organizations build this foundation, AI becomes safer, more predictable and far more capable of delivering business value at scale.”

The cybersecurity landscape is, in short, a struggle between enterprises and malicious attackers, both using AI-powered tools. That dynamic has led nearly one in four organizations the researchers surveyed to push forward when it comes to focusing on exposure management integration and AI operations, with many reporting faster resolution when dealing with cybersecurity threats.