Cybersecurity

Schatten-KI als offene Flanke

[11.11.2025] Eine aktuelle Umfrage zum Thema Cybersicherheit, die im Auftrag von Microsoft in Ämtern und Behörden durchgeführt wurde, zeigt, dass die Nutzung nicht autorisierter KI-Tools weit verbreitet ist. So greift fast jeder zweite Mitarbeitende in Bundesbehörden zu solchen Tools. Auf Landesebene sieht es besser aus, denn hier gibt es bereits zahlreiche offizielle KI-Assistenzsysteme.

Künstliche Intelligenz kann Arbeitsprozesse in der öffentlichen Verwaltung vereinfachen. Gleichzeitig machen KI-Tools Cyberangriffe jedoch auch gefährlicher. In deutschen Behörden öffnet der alltägliche Einsatz nicht freigegebener KI-Dienste gefährliche Flanken. Darauf wies Ralf Wiegand, National Security Officer bei Microsoft Deutschland, bei einem Pressegespräch am Montag (10. November 2025) hin.

Unauthorisierte KI-Tools

Wiegand verwies auf die Ergebnisse einer repräsentativen Civey-Umfrage im Auftrag von Microsoft sowie auf Befunde aus dem im Oktober veröffentlichten Microsoft Digital Defense Report 2025. Demnach ist „Schatten-KI“ auf Bundesebene längst Routine: Fast jeder zweite Mitarbeitende (45 Prozent) greift zu Tools, die weder geprüft noch freigegeben sind. Auf kommunaler Ebene sind es mehr als ein Drittel (36 Prozent) und in den Ländern knapp ein Fünftel (19 Prozent). Dieser Befund wiegt umso schwerer, da die Bedrohungslage von Führungskräften in Staat und Verwaltung weiterhin als hoch eingestuft wird.

Die Civey-Befragung zeigt allerdings eine erstaunliche Differenz in der Wahrnehmung zwischen den Verwaltungsebenen. So sehen 80 Prozent der Befragten auf Bundesebene eine hohe Gefahr, auf Länderebene sind es 78 Prozent, in den Kommunen jedoch nur 58 Prozent. Auffällig ist, dass 34 Prozent der kommunalen Entscheidungsträger:innen keine oder nur eine geringe Gefahr sehen. Dies ist laut Wiegand eine Fehleinschätzung, denn gerade Städte und Gemeinden seien in den vergangenen Monaten immer wieder Ziel von Angriffen gewesen, wodurch es teilweise zu wochenlangen Ausfällen zentraler Verwaltungsprozesse kam.

Behörden sind ins Fadenkreuz gerückt

Die Zahlen aus dem Microsoft Digital Defense Report 2025 unterstreichen die Wucht der Angriffe: Täglich werden Abermilliarden Sicherheitssignale korreliert, Millionen neue Malware-Artefakte blockiert und Dutzende Millionen Identitätsrisiken erkannt. Im Fadenkreuz stehen neben IT-Unternehmen vor allem Behörden. Deutlich stärker ins Visier gerückt sind auch Forschungseinrichtungen und Hochschulen. Laut Wiegand ist Deutschland das am häufigsten attackierte EU-Land und rangiert weltweit in der Spitzengruppe. Die Lage werde von staatlich unterstützten Gruppen geprägt, die zunehmend Tools und Dienstleistungen krimineller Akteure zukaufen. Das erschwere die Erkennung und Attribution.

Hohes Gefahrenbewusstsein, geringe Vorsorge

Wiegand erklärte zum Thema Schatten-KI: „Wo Behörden keine geprüften, datenschutzkonformen KI-Angebote bereitstellen, weichen Mitarbeitende auf frei zugängliche Web-Dienste aus – oft ohne den Anbieter, das Herkunftsland oder die Datenschutzregeln zu prüfen.“ Genau hier zeige die Civey-Befragung eine Diskrepanz: Ein hohes Gefahrenbewusstsein treffe auf geringe Eigenvorsorge. So ergreifen sechs von zehn Nutzerinnen und Nutzern keinerlei Schutzmaßnahmen beim Einsatz neuer KI-Tools, während sich gleichzeitig 73 Prozent unzureichend über die Funktionsweise und die Einsatzbereiche von KI informiert fühlen. Besonders groß ist die Wissenslücke bei den älteren Generationen: Bei den Über-65-Jährigen geben mehr als acht von zehn an, sich mit KI nicht gut auszukennen.

Zahlreiche KI-Assistenzsysteme auf Landesebene

Wenig hilfreich sei es, die unkontrollierte Nutzung externer KI-Dienste in den Ämtern und Behörden lediglich zu verbieten, sagte Wiegand. Wirksam sei vor allem, attraktive, behördlich freigegebene Alternativen bereitzustellen – also KI-Funktionen, die in die eigene Compliance- und Governance-Umgebung eingebettet sind, deren Modelle nicht mit vertraulichen Inhalten nachtrainiert werden und die von IT-Sicherheitsmaßnahmen flankiert sind. Wo diese Angebote vorhanden sind, gehe der Griff zu Schatten-KI messbar zurück.

Dies zeigt laut Wiegand vor allem auf Landesebene, wo es bereits zahlreiche KI-Assistenzsysteme für die Beschäftigten in den Behörden und Ministerien gibt, etwa die KI-Assistenz F13 der Landesverwaltung Baden-Württemberg oder den von der Freien und Hansestadt Hamburg und Dataport entwickelten KI-Assistenten LLMoin, der in mehreren Bundesländern im Einsatz ist.. Wiegands Fazit: „Wer Identitäten schützt, Multi-Faktor Authentifizierung erzwingt, Schatten-KI sichtbar macht und KI-gestützte Abwehr aktiviert, reduziert das Risiko signifikant.“ Allerdings passiere das noch zu selten.

(al)

Microsoft Digital Defense Report 2025

Stichwörter: IT-Sicherheit, Microsoft, Cybersicherheit, künstliche Intelligenz