Öffentlicher Sektor - Zukunft gestalten Blog
By PwC Deutschland | 26. September 2024

KI bringt neue Sicherheitsrisiken – und -chancen

Organisationen müssen ihre IT-Sicherheitsarchitektur nicht neu erfinden, aber anpassen.

Auch für Institutionen und Unternehmen im öffentlichen Sektor führt künftig kein Weg an künstlicher Intelligenz (KI) vorbei. Mit der Technologie lassen sich insbesondere repetitive Aufgaben automatisieren, während sich die menschlichen Mitarbeiter:innen interessanteren und wichtigeren Aufgaben widmen können. Gerade in Zeiten des Fachkräftemangels kann KI so auch dazu beitragen, den öffentlichen Sektor effizienter und attraktiver zu machen.

Phishing-Mails und Deep-Fake-Videos

Allerdings bringt KI, wie jede neue Technologie, auch gewisse Risiken mit sich: Stellen Institutionen beispielsweise Datensets zusammen, um eine KI auf die spezifischen Anforderungen der Organisation zu trainieren, besteht die Gefahr, dass große Mengen sensibler Daten in die Hände Unbefugter gelangen.

Und Angreifer:innen können KI nutzen, um IT-Systeme zu attackieren – etwa mit massenhaft generierten, individualisierten Phishing-Mails oder sogenannten Deep-Fake-Videos – also KI-generierten, täuschend echt wirkenden, aber gefälschten Clips.

Organisationen im öffentlichen Sektor sollten deshalb zunächst überprüfen, wie gut ihre IT-Sicherheitsarchitektur auf die neuen, KI-spezifischen Risiken eingestellt ist. Die gute Nachricht: KI erfordert in der Regel keine komplett neuen Strukturen und Prozesse – meist geht es eher darum, die bestehenden neu auszurichten. Auf die Bestandsaufnahme folgt eine KI-Sicherheitsstrategie: Sie erlaubt es, die Sicherheitsarchitektur mit standardisierten Prozessen effizient auf neue KI-Anwendungen auszuweiten und dabei übergeordnete Sicherheitsanforderungen im Blick zu behalten.

KI kann die Sicherheit auch erhöhen

Elementarer Bestandteil einer solchen Strategie ist es, die Beschäftigten mit Fortbildungen für die Funktionsweise und Risiken von KI zu sensibilisieren. Außerdem braucht es Sicherheitssysteme, die (potenzielle) Sicherheitslücken in den verwendeten KI-Systemen identifizieren und Angriffe abwehren können – gewissermaßen eine KI-Firewall. Nutzen Organisationen eigene Datensets, um KI-Systeme zu trainieren, benötigen sie auch für diese Daten besondere Sicherheitsvorkehrungen.

Für die IT-Sicherheit stellt künstliche Intelligenz allerdings nicht nur ein Risiko, sondern auch eine Chance dar: Denn mit KI-Anwendungen lassen sich Sicherheitslücken und Angriffe schneller erkennen, weil sie große Datenmengen automatisiert und mit großer Zuverlässigkeit analysieren können. Dies erhöht die Sicherheit – und entlastet die IT-Mitarbeiter:innen.

Ansprechpartner:
Manuel Seiferth

Zu weiteren PwC Blogs

Schlagwörter

Artificial Intelligence (AI), Datensicherheit, Digitalisierung, IT-Sicherheit, IT-Systeme

Kontakt

Prof. Dr. Rainer Bernnat

Frankfurt am Main

rainer.bernnat@pwc.com