CYBERSECURITY & KI:

Drei **Sicherheits-trends** für 2025

Die gute Nachricht: Dank KI werden Unternehmen 2025 noch mehr Möglichkeiten und fortschrittlichere Tools zur Verfügung stehen, mit denen sie ihre IT-Systeme und Mitarbeiter effektiv vor Cyber-Angriffen schützen können. Die schlechte Nachricht: KI ist keine Technologie, die ausschließlich für gute Zwecke genutzt wird. Auch in diesem Jahr werden sie sich Cyber-Kriminelle zunutze machen, um Unternehmen gleich mehrere Schritte vorauszusein ... | VON DIETER KEHL

Diese drei Trends sollen einen kurzen Überblick darüber geben, in welche Richtungen sich die Arbeit mit KI im Bereich der Cyber-Sicherheit bewegen wird und welche Herausforderungen sich dadurch ergeben:

1. KI begünstigt neue Angriffsvektoren

Nicht nur Unternehmen, sondern auch Cyber-Angreifer profitieren mit Generative AI von wesentlich mehr Effizienz. Zum einen lassen sich Phishing-Inhalte noch zielgerichteter und glaubwürdiger erstellen – sowohl im Text-, als auch im Audio- und Videoformat. Zum anderen können Akteure diese Spear-Phishing-Kampagnen dank Automatisierung ins Unermeßliche skalieren. Sprich: Es wird für sie ein Leichtes sein, tausend hoch personalisierte E-Mails an tausend unterschiedliche Empfänger gleichzeitig zu senden. Dadurch steigt potentiell die Anzahl erfolgreicher Angriffe. Auf diese Entwicklung müssen sich Unternehmen vorbereiten – unter anderem, indem sie ihre Mitarbeiter für diese Gefahr sensibilisieren.

2. KI und Anwendungssicherheit

In Sachen Anwendungsentwicklung und -sicherheit tun sich für 2025 vor allem folgende Herausforderungen auf: Generative AI wird die Software-Produktion nicht nur enorm beschleunigen, sondern auch zugänglicher machen. Dadurch steigt das Risiko von Schwachstellen und neuen Angriffsvektoren. Softwareunternehmen kommen deshalb nicht umhin, sowohl eine effektive DevSecOps-Umgebung zu schaffen, als auch Application-Security-Testing-Lösungen zu nutzen, um diese Gefahren frühzeitig abzuwenden. Kleinere Teams, denen es an der entsprechenden Expertise mangelt, können mit neuen Lösungen rechnen, die Langzeitherausforderungen wie Reviewing sowie das Identifizieren und Beheben von Code-Schwachstellen adressieren.

3. KI in kleinen und mittelständischen Unternehmen (KMU)

Es ist kein Geheimnis: In vielen KMU mangelt es sowohl an finanziellen Mitteln, als auch an (Fach-)Personal und folglich auch an Expertenwissen und Zeit für produktiveres Arbeiten. Besonders die Wissenslücke im Bereich der Cyber-Sicherheit klafft häufig am weitesten. Dies wird auch weiterhin eine der größten Herausforderungen bleiben. Um dieses Defizit auszugleichen, können betroffene Unternehmen unter anderem mit Managed Security Service Providern und Cloud-basierten Security-Lösungen arbeiten. Zusätzlich lohnt sich auch der Blick in Richtung KI. Mit ihr lassen sich Sicherheitsmechanismen wie Threat Detection and Response automatisieren, sodaß potentielle Angriffe schneller, akkurater und kosteneffizient identifiziert werden. <<

Noch Fragen? ***www.opentext.de***