KI-gestützte Anomalieerkennung – Angriffe früh erkennen

Immer häufiger wird über Cyberangriffe auf große Unternehmen, aber auch kleine und mittelständische Betriebe berichtet.

*Das Wissensnugget **„KI-gestützte Anomalieerkennung – Angriffe früh erkennen“** unterstützt dabei, solche Angriffe frühzeitig zu erkennen.*

Einleitung

Viele Cyberangriffe bleiben lange unentdeckt. Daten werden still entwendet, Systeme manipuliert oder Logins ausprobiert – oft über Wochen.
Hier hilft die **Anomalieerkennung**, also die automatische Erkennung ungewöhnlicher Aktivitäten mithilfe von KI.

Wie funktioniert das?

KI-Systeme analysieren das normale Verhalten von Nutzer:innen und Systemen – z. B.:

- Wann sich jemand einloggt,
- wie viele Daten übertragen werden,
- welche Dateien häufig genutzt werden.

Wenn etwas davon stark abweicht, schlägt das System Alarm.

Beispiele für Anomalien

- Unerwartete Logins außerhalb der Arbeitszeiten
- Große Datenmengen, die plötzlich verschickt werden
- Programme, die ungewöhnliche Zugriffe starten

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

Mittelstand-Digital

aufgrund eines Beschlusses des Deutschen Bundestages

Praxistipps – Früherkennung stärken

1. **Monitoring aktivieren:** Überwache Systeme kontinuierlich.
2. **KI-basierte Sicherheitssoftware einsetzen.**
3. **Regelmäßige Updates durchführen:** Sicherheitslücken schließen.
4. **Mitarbeitende sensibilisieren:** Auffälliges Verhalten melden.
5. **Alarmmeldungen ernst nehmen:** Sofort nachforschen, bevor Schaden entsteht.

Fazit

Anomalieerkennung ist ein Frühwarnsystem für die IT-Sicherheit.

Merke: Je früher ein Angriff erkannt wird, desto geringer der Schaden. KI hilft, Warnzeichen sofort zu registrieren.

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

Mittelstand-Digital

aufgrund eines Beschlusses des Deutschen Bundestages