heise webcasts

SOPHOS

Inhalt des Live-Webcasts

# KI-gestützte Cyberangriffe: So rüsten Sie Ihre Abwehr richtig auf

**Datum und Uhrzeit:** **22. Oktober 2026, 11:00 Uhr**
**Dauer:** **ca. 60 Minuten**

**Cyberkriminelle nutzen KI, um Angriffe schneller und gezielter durchzuführen. Wie Sie Ihre Sicherheitsarchitektur darauf ausrichten, erfahren Sie im Live-Webcast am 22.10. um 11 Uhr.**

Künstliche Intelligenz ist längst kein Werkzeug mehr, das nur auf der Seite der Verteidiger eingesetzt wird. Cyberkriminelle nutzen KI-Technologien gezielt, um Schwachstellen in IT-Systemen automatisiert und in einem Tempo aufzuspüren, das manuellen Methoden weit überlegen ist. Angriffe werden dadurch präziser, schneller und schwerer vorherzusagen – eine Entwicklung, die Unternehmen jeder Größe unter Druck setzt.

Wer glaubt, mit einer Handvoll separater Sicherheitslösungen ausreichend geschützt zu sein, unterschätzt die aktuelle Bedrohungslage erheblich. Einzelne, voneinander getrennt operierende Werkzeuge – etwa für Firewalls, Endpoint-Schutz oder Netzwerküberwachung – tauschen keine Informationen miteinander aus und reagieren zu langsam auf komplexe, mehrstufige Angriffe. Das Ergebnis: Sicherheitslücken entstehen genau dort, wo die einzelnen Lösungen aneinanderstoßen.

Gefragt sind stattdessen integrierte Sicherheitssysteme, bei denen die einzelnen Komponenten alle Schutzmechanismen eines Unternehmens miteinander verknüpfen. Dabei werden Bedrohungsdaten in Echtzeit ausgetauscht und automatisiert auf Vorfälle reagiert. Detection & Response – also das frühzeitige Erkennen und gezielte Reagieren auf Angriffe – wird dabei zu einem zentralen Baustein moderner Cyberabwehr. Doch Technologie allein reicht nicht: Die enge Zusammenarbeit zwischen menschlichem Fachwissen und KI-gestützten Systemen entscheidet künftig darüber, ob Angriffe rechtzeitig abgewehrt werden können. Konkret sieht das so aus, dass die KI bei eindeutigen Angriffen selbsttätig in Maschinengeschwindigkeit reagiert, der Mensch aber verantwortlich ist und gegebenenfalls der KI die Grenzen setzt.

Im Live-Webcast am 22.10. um 11 Uhr gibt Michael Veit, Technology Evangelist bei Sophos, einen fundierten Einblick in die veränderte Bedrohungslandschaft und zeigt auf, welche Strategien und Architekturen Unternehmen heute brauchen, um handlungsfähig zu bleiben. Im Mittelpunkt stehen dabei folgende Fragen:

- Wie setzen Angreifer KI ein, um Schwachstellen schneller zu identifizieren?
- Welche Sicherheitsstrategien helfen, KI-gestützte Bedrohungen frühzeitig zu erkennen?
- Wie unterscheidet sich ein Verteidigungssystem von klassischen Verwaltungsplattformen?

Michael Veit beantwortet während der Live-Sendung auch Fragen der Teilnehmer. Moderator ist Martin Seiler von Heise Business Services. Jetzt anmelden!

**Sprecher:**

**Michael Veit, Manager Sales Engineering, Sophos GmbH**

Michael Veit (Jahrgang 1968) ist der SOPHOS Technology Evangelist.

Nach seinem Studium der Wirtschaftsinformatik an der TU Darmstadt ist er seit über 25 Jahren in der IT Security tätig. In dieser Zeit hat er viel praktische Erfahrung im Design, der Implementierung und der Überprüfung von IT-Sicherheitsinfrastrukturen gesammelt. Nach der Leitung des Bereiches IT-Security in einem Systemhaus ist Michael Veit seit 2008 bei Sophos beschäftigt. Neben seiner Funktion als Manager Sales Engineering ist Michael Veit heute das „Sophos-Gesicht nach außen“ in Presse und Fernsehen sowie Referent und Keynote-Speaker auf Sicherheitskonferenzen und Messen.

**Martin Seiler, Heise Business Services**

Martin Seiler, Heise Business Services Martin Seiler befasste sich als IT-Redakteur bei der Computerwoche viele Jahre lang mit Themen wie Netzwerke, Telekommunikation oder Security. 2006 wechselte er in den Eventbereich von IDG, für den er Fachveranstaltungen unterschiedlichster Art wie Seminare, Konferenzen, Roadshows und Webcasts entwickelte, organisierte und moderierte. Seit 2010 arbeitet Martin Seiler für Heise Business Services.