Cybersicherheit 2026: Der Mensch muss neben KI eine maßgebliche Rolle spielen

Die Cybersicherheit wird im Jahr 2026 von noch mehr Extremen geprägt sein. Wie gelingt die Verteidigung gegen rasend schnelle Angriffe in neuer Dimension, und welche Rolle spielt das menschliche Urteilsvermögen angesichts zunehmender KI und Automatisierung? Die Experten von Sophos sehen den Menschen in entscheidender Rolle.

KI ist die Technologie, die Cyberabwehrmaßnahmen schneller, intelligenter und effektiver gestaltet. Sie ist aber auch die treibende Kraft, die Cyberangriffe beschleunigt und intensiviert. Gleichzeitig werden Unternehmen mit einer weniger auffälligen, aber ebenso bedeutenden Bedrohung konfrontiert sein: dem operativen Burnout. Dieser ist ein Ergebnis aus übermäßiger Automatisierung, welche die menschlichen Kapazitäten übersteigt.

Autor:
Michael Veit
Cybersecurity-Experte
Sophos
www.sophos.com

Im Jahr 2026 ist die Cyberverteidigung in Unternehmen so wichtig wie nie zuvor, wobei neben KI die vom Menschen gesteuerte Sicherheit und der effiziente Einsatz von MDR-Services (MDR = Managed detection and response) darüber entscheiden werden, welche Unternehmen angesichts des Wandels in der Cyberbedrohung widerstandsfähig bleiben.

Reichweite und Raffinesse von KI-gestützten Attacken werden exponentiell steigen

In den kommenden Monaten ist davon auszugehen, dass Angreifer KI weiterhin intensiv als Katalysator einsetzen, um bekannte Schwachstellen zu instrumentalisieren, Angriffskampagnen zu orchestrieren, die Hürden für grundlegende Hacking-Angriffe zu senken sowie eine breite, schnelle Ausnutzung im gesamten Internet zu ermöglichen.

Payloads werden schneller als je zuvor angepasst, und Social Engineering wird zunehmend maßgeschneidert sein, einschließlich Phishing.

Deepfake-Audiodateien- und -videos machen BEC-Kampagnen überzeugender und weitaus glaubwürdiger, sodass Mitarbeiter ihnen noch leichter erliegen. KI verschiebt aktuell das Kräfteverhältnis, indem sie selbst wenig erfahrenen Cyberkriminellen hilft, mit einer Geschwindigkeit und Präzision zu operieren, die bisher erfahrenen Angreifern vorbehalten war.

Versteckte Kosten der Geschwindigkeit

Im Jahr 2026 könnten Unternehmen in nahezu allen Branchen Auswirkungen spüren, wenn sie KI für kurzfristige Ziele einsetzen, ohne entsprechende Investitionen in menschliche Aufsicht und Systemverständnis zu tätigen. Da die tägliche Arbeit zunehmend auf Automation stützt, kann die Fehlerquote steigen – nicht weil die Menschen weniger sorgfältig arbeiten, sondern weil die ständige Delegation von Aufgaben das menschliche Urteilsvermögen und die Mustererkennung langsam abstumpft.

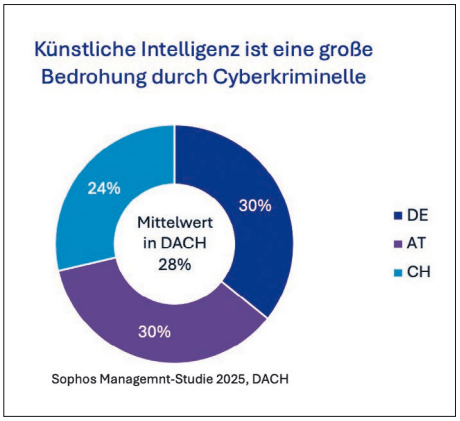
In diesem Zusammenhang wird sich voraussichtlich auch die kognitive Überlastung zu einem realen Betriebsrisiko entwickeln. Denn maschinell erzeugte Ergebnisse und Informationen werden immer schneller und in größerer Anzahl erzeugt, als menschliche Entscheidungen getroffen werden können. Die Folge: ein Rückstau an ungelösten Aufgaben. Zudem kann durch den hohen Grad der Automatisierung eine trügerische Selbstzufriedenheit entstehen, insbesondere wenn Teams Systemen vertrauen, die sie nicht mehr vollständig verstehen. Das Resultat ist eine noch größere Kluft zwischen wahrgenommenem und tatsächlichem Risiko.

KI beschleunigt Arbeitstempo

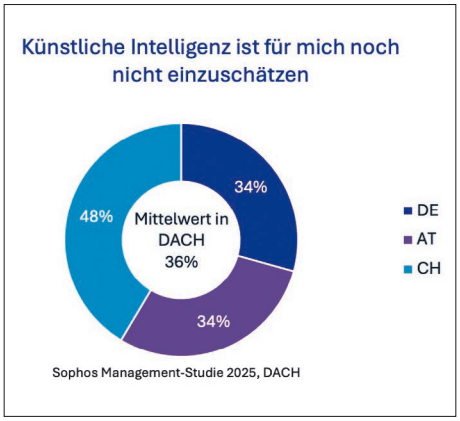
Auch der Burnout kann noch weiter zunehmen, wenn KI das Arbeitstempo weiter über das hinaus beschleunigt, woran sich Einzelpersonen und Organisationen nachhaltig anpassen können. Eine Folge kann das Verschwimmen klarer Zuordnungen von Verantwortlichkeit zwischen Mensch und Maschine in der Prävention oder bei einer Attacke sein. In diesem Umfeld erscheint Geschwindigkeit nur so lange als Fortschritt, bis sich ihre versteckten Kosten in Form von verminderter Stabilität, schwächerer Widerstandsfähigkeit und schwindender menschlicher Leistungsfähigkeit zeigen.

MDR 2026: Menschliche Urteilskraft, ROI und Versicherungsliebling

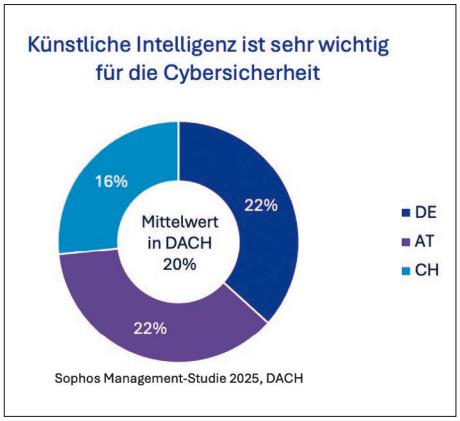
MDR-Dienste werden beweisen müssen, dass Menschen weiterhin in die Security-Prozesse eingebunden sind. Bei KI-gesteuerter Cybererkennung und -abwehr als Standard wächst beim Kunden der Wunsch nach Transparenz darüber, wer ihre Umgebung überwacht, wer Entscheidungen trifft und wo menschliches Urteilsvermögen zum Einsatz kommt. Die stärksten Anbieter werden diejenigen sein, die KI einsetzen, um menschliche Analysten zu unterstützen, um Untersuchungen, Priorisierungen



KI als Bedrohung



KI lässt sich schwer einschätzen



KI ist für Cybersicherheit wichtig

und Reaktionen zu beschleunigen, anstatt sie zu ersetzen.

Weiterhin spielt MDR zunehmend eine wichtige Rolle als strategischer Hebel für Versicherbarkeit, Geschäftskontinuität und einen klaren ROI. Versicherer erkennen zunehmend, dass Unternehmen mit einer 24/7-Erkennung, Bedrohungssuche und schnellen Reaktionszeit weniger schwere Verluste erleiden, und sie belohnen diese Reife mit besseren Prämien und einem umfassenderen Versicherungsschutz.

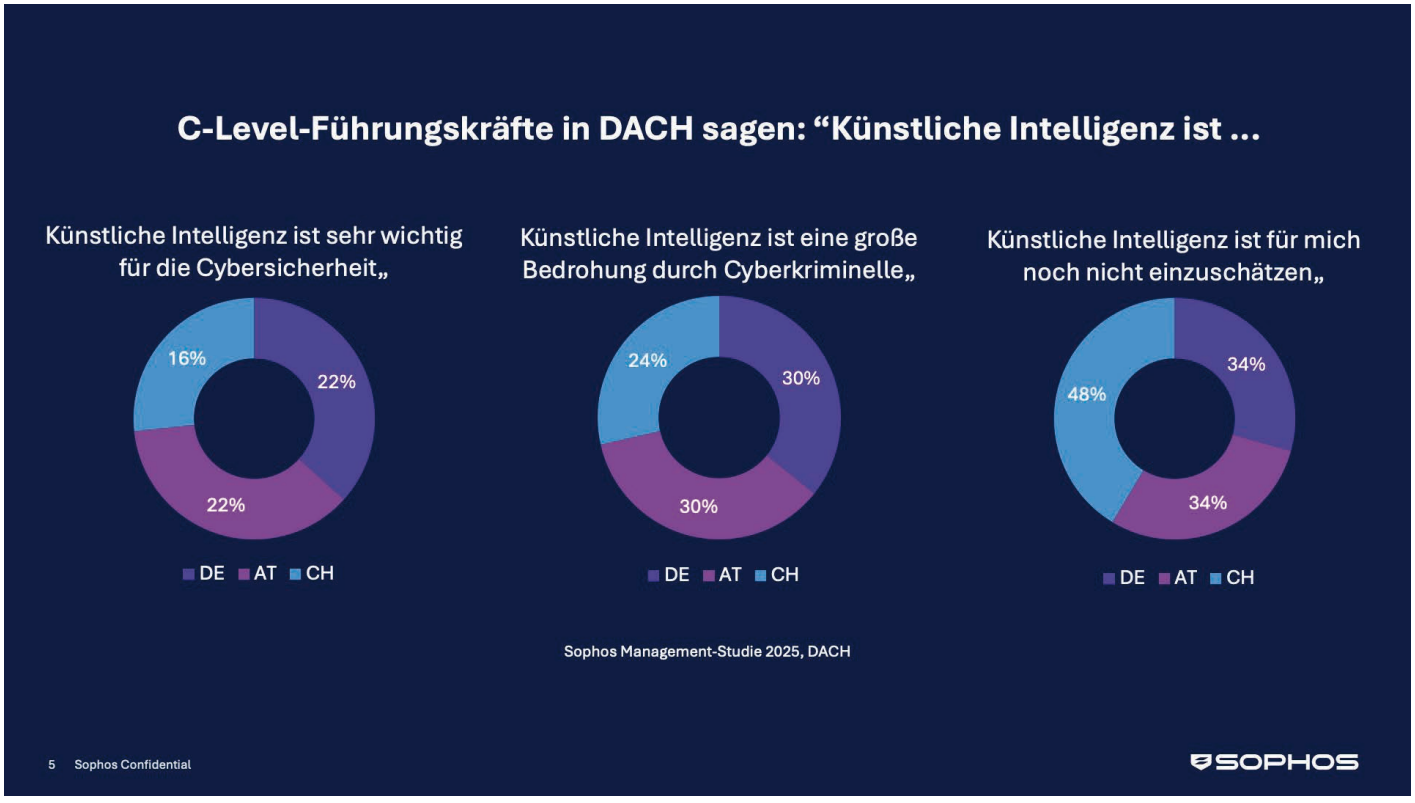
KI-gesteuerte MDR-Funktionen können zudem die Ergebnisberichterstattung verbessern, indem sie Automatisierung mit menschlicher Expertise kombinieren und so Evidenzboards liefern, die Versicherer verstehen und denen sie vertrauen.

Die Sicherung von Microsoft-Umgebungen wird zunehmend geschäftskritisch

Da fast vier Millionen Unternehmen Microsoft 365 nutzen, zählt die Sicherung von Microsoft-Umgebungen zum entscheidenden Faktor. Da Angreifer verstärkt Entra ID, Microsoft 365, Endpunkte und Cloud-Workloads als eine einzige, miteinander verbundene Angriffsfläche ins Visier nehmen, reichen punktuelle Abwehrmaßnahmen nicht mehr aus. Sicherheitsteams müssen über isolierte Schutz-Tools hinauszugehen und eine einheitliche Transparenz über Identitäten, Endpunkte, E-Mails und Cloud-Aktivitäten hinweg schaffen.

Die Botschaft für 2026

„Effektive Resilienz verschaffen sich Unternehmen, die starke Cybersecurity-Grundlagen verantwortungsbewusst und menschenzentrierten mit neuen Sicherheitstechnologien verbinden“, so Michael Veit, Cybersecurity-Experte bei Sophos. „Diejenigen, die KI wohlüberlegt einsetzen, in von Experten geleitete MDR investieren und ihre Kernplattformen ganzheitlich sichern, sind am besten gegenüber kommenden disruptiven Ereignissen aufgestellt.“ ◄



Antworten der Umfrage