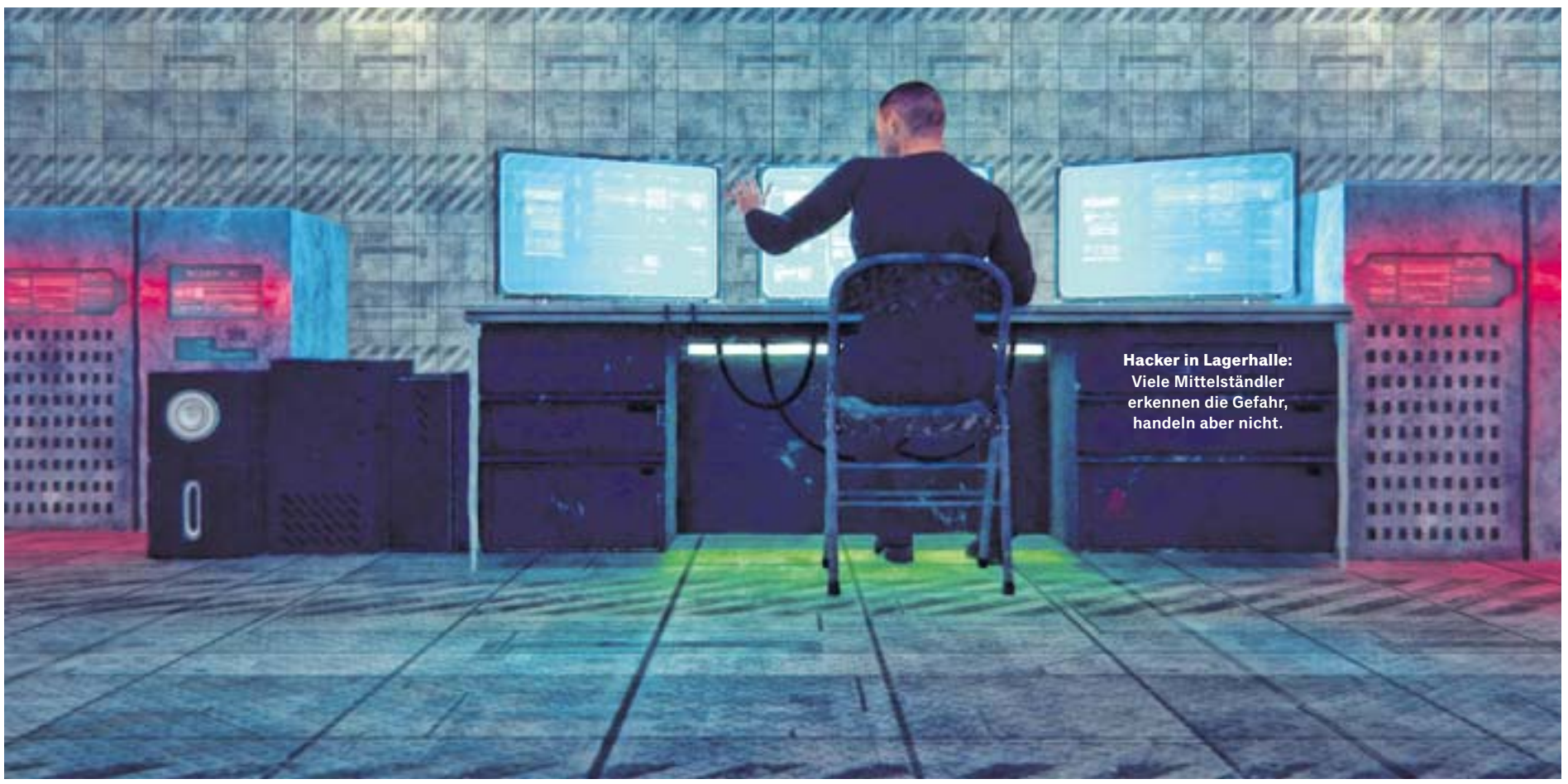
Handelsblatt
DONNERSTAG, 9. NOVEMBER 2023, NR. 217



Hacker in Lagerhalle: Viele Mittelständler erkennen die Gefahr, handeln aber nicht.

E+/Getty Images

Cyberkriminalität

Der Feind in meinem Netz

Hilft Künstliche Intelligenz im Kampf gegen Hacker? Wie Mittelständler ihre IT-Systeme sinnvoll schützen.

Eli Hamacher Berlin

Die Zahl schreckt auf: Laut einer aktuellen Umfrage des Digitalverbands Bitkom erwarten 82 Prozent der deutschen Firmen in den kommenden zwölf Monaten eine Zunahme von Cyberangriffen auf das eigene Unternehmen. Zu Recht, sagt Manuel Bach: „Nie war die Gefahr, durch einen Cyberangriff aus dem Markt gedrängt oder empfindlich geschädigt zu werden, größer als heute“, so der Leiter des Referats Cybersicherheit für kleine und mittlere Unternehmen im Bundesamt für Sicherheit in der Informationstechnik (BSI).

Umso erstaunlicher ist, wie unzureichend viele Mittelständler auf derartige Attacken vorbereitet sind. „Der größte Irrtum ist, dass viele immer noch glauben, sie seien zu klein, um ein lohnendes Ziel für einen Angriff darzustellen“, sagt Bach. „Sie tun daher oft zu wenig in puncto Prävention und sind deshalb nicht adäquat geschützt.“

Was viele nicht wissen: Kriminelle wählen kleine und mittlere Unternehmen (KMU) in der Regel nicht gezielt aus, meist werden sie von großflächig und automatisiert durchgeführten Angriffen getroffen. Oft mit gravierenden Folgen: Auf 206 Milliarden Euro beziffert Bitkom den jährlichen Gesamtschaden durch Datendiebstahl, Spionage und Sabotage. Jeder zweite Betrieb fühlt sich durch Cyberangriffe sogar in seiner Existenz bedroht.

Doch wie können sich KMUs, die über eine geringe oder gar keine eigene IT-Kompetenz verfügen, wirksam gegen kriminelle Hacker schützen? Und welche neuen Möglichkeiten bietet etwa Künstliche Intelligenz (KI)?

Das BSI rät gerade den kleinsten Unternehmen, sich zunächst um die Prävention im eigenen Haus zu kümmern. So nehmen laut der jüngsten DIHK-Digitalisierungsumfrage nur knapp zwei Drittel der Betriebe mit weniger als zehn Mitarbeitenden regelmäßig Sicherheitsupdates vor. Lediglich 46 Prozent gaben an, ihre Beschäftigten regelmäßig zu Fragen der IT-Sicherheit zu schulen.

Die Bundesbehörde hat daher eine eigene Website speziell für KMUs eingerichtet, auf der Informationen und Hilfe zum Thema Cybersicherheit aufbereitet sind (www.bsi.bund.de/kmu), darunter auch ein Cyberrisiko-Check für Unternehmen mit weniger als 50 Mitarbeitenden.

Bei IT-Dienstleistern können Mittelständler eine standardisierte Beratung erhalten, um den Status quo ihres Systems und so mögliche Schwachstellen zu ermitteln. Eine solche Bestandsaufnahme dauert nicht länger als zwei Stunden. Inklusive Vor- und Nachbesprechung sowie der Erstellung eines Berichts kommt etwa ein Arbeitstag eines IT-Experten zusammen – ein überschaubarer Aufwand.

> Der größte Irrtum ist, dass viele Mittelständler glauben, sie seien zu klein, um ein lohnendes Ziel für einen Angriff darzustellen.
>
> **Manuel Bach**
> BSI

Der Bericht beinhaltet konkrete Empfehlungen, auf deren Basis sich die Unternehmen Angebote von IT-Dienstleistern einholen können. Bei der Suche nach einem passenden und vertrauenswürdigen Partner hilft beispielsweise die DIHK. Sowohl für den Risiko-Check als auch für den Service eines IT-Anbieters gibt es staatliche Fördermittel, die entsprechenden Programme stehen im Bericht.

Firmen, die Opfer einer Cyberattacke geworden sind, können den Vorfall dem BSI über ein Formular auf der Website melden. Das Lagezentrum schickt dann umgehend Tipps für Sofortmaßnahmen. Die Behörde geht nach Recherchen im Darknet aber auch aktiv auf angegriffene Unternehmen zu – oft bevor diese den Angriff überhaupt bemerkt haben.

Bis Künstliche Intelligenz (KI) bei Mittelständlern digitale Angriffe vorhersagen oder gar abwehren kann, ist es noch ein weiter Weg. „Dafür bräuchte ein Unternehmen einen sehr genauen Überblick über seine Systemarchitektur und verteilte Sensoren, damit die KI Anomalien erkennen kann“, sagt Axel Deininger, Vorstandschef des IT-Dienstleisters Secunet Security Networks. „Bei KMUs ist das aber oft nicht der Fall.“ Zudem sei der finanzielle Aufwand sehr groß und der Einsatz der smarten Tools kompliziert.

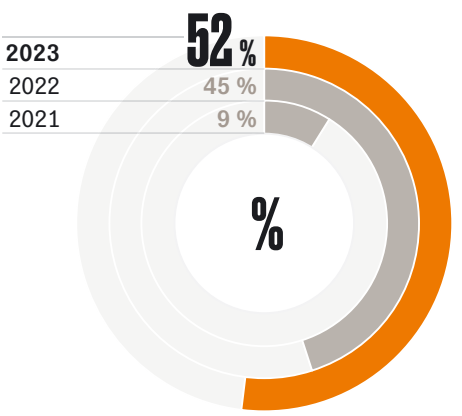
Das BSI warnt vielmehr vor möglichen Risiken und Herausforderungen bei der Nutzung von KI-Tools wie ChatGPT. Dazu gehören Datenschutzprobleme, Manipulationsmöglichkeiten und die Notwendigkeit, robuste Sicherheitsmaßnahmen gegen Missbrauch zu implementieren.

Sinnvoller als hochkomplexe KI-Tools seien für die meisten Unternehmen bewährte technische Maßnahmen wie etwa Penetrationstests, so Deininger. Dabei schlüpft ein Experte in die Rolle des Hackers und versucht, Schwachstellen im IT-System zu finden und auszunutzen – häufig mit Erfolg. „Viele Unternehmen nutzen Standardsoftware mit den Default-Einstellungen, die die Angreifer natürlich auch kennen.“ Ist eine Lücke einmal entdeckt, kann sie geschlossen werden. Für das Management hat das künftig auch persönliche Vorteile: Im Oktober 2024 tritt eine EU-Richtlinie in Kraft, die unter anderem vorsieht, dass Führungskräfte für Schäden haftbar sind, die durch fahrlässig verursachte IT-Sicherheitslücken entstehen.

Laut Bitkom sind die häufigsten Einfallstore für Cyberkriminelle immer noch Phishing und Angriffe auf Passwörter. Gegen den Faktor Mensch ist jede noch so raffinierte KI machtlos.

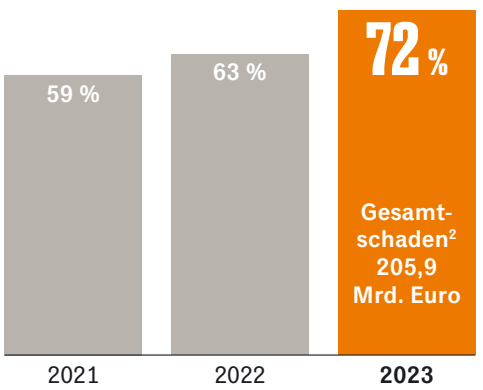
Die Angst wächst …

Bedrohen Cyberattacken die geschäftliche Existenz? Angaben der Befragten in Prozent[1]



… der Schaden auch

Anteil von Cyberangriffen an Gesamtschäden, Angaben der Befragten in Prozent



HANDELSBLATT

1) Umfrage unter 1.002 Unternehmen 2023; 2) Diebstahl, Industriespionäge und Sabotage • **Quelle:** Bitkom