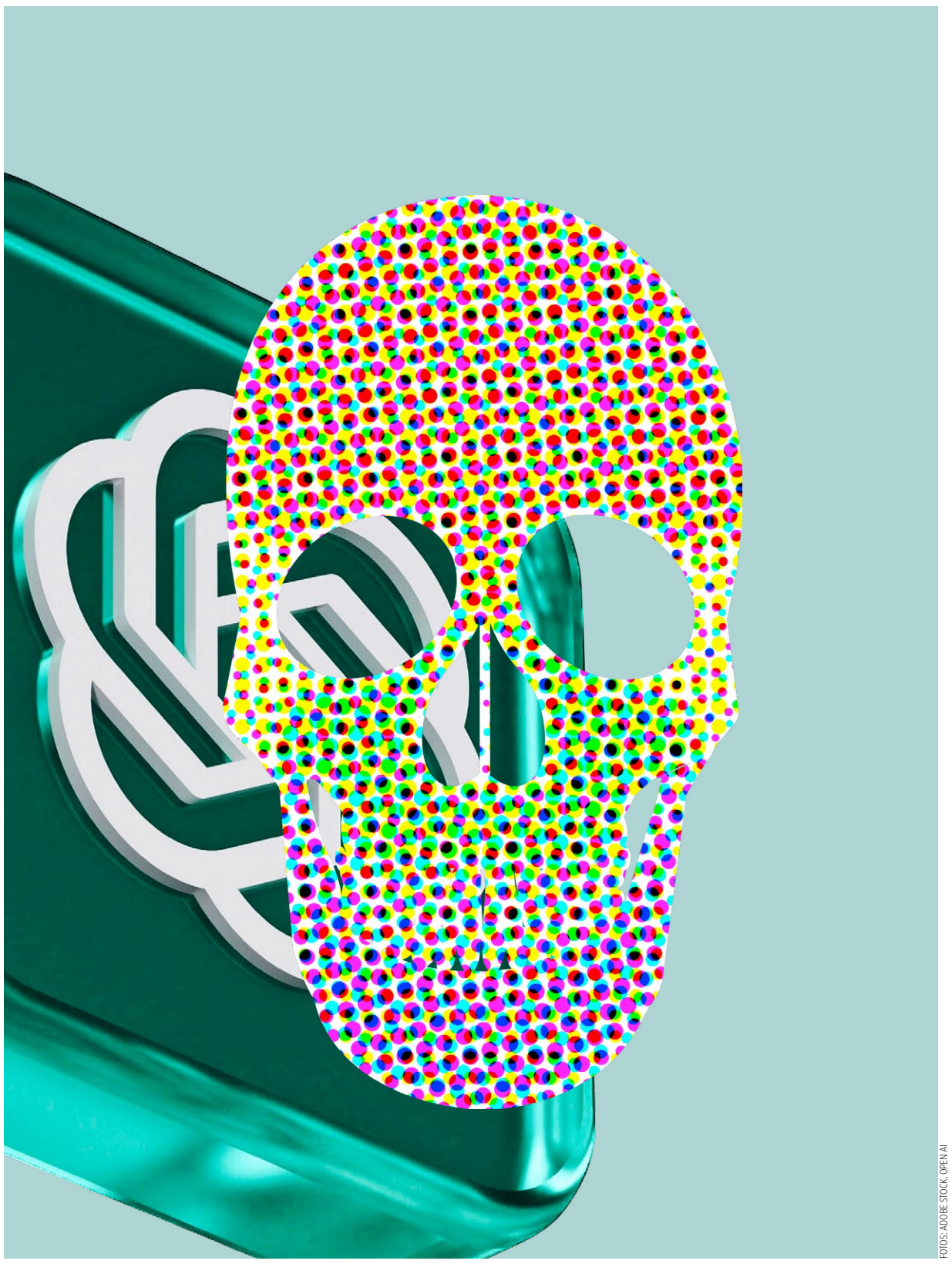
Die Schatten-IT auf dem Privatcomputer

Mitarbeitende nutzen **KI-Tools** ohne das Wissen ihrer Vorgesetzten und bauen so eine parallele Tech-Welt auf. Das birgt enorme Risiken für Firmen.

Viele Angestellte nutzen den öffentlich zugänglichen Dienst Chat GPT, auch wenn ihre Firma die Nutzung verboten hat. Sie verwenden KI-Tools auf ihrem privaten Gerät, um effizienter zu arbeiten. So entsteht eine **IT-Piraterie,** die für Firmen grosse Gefahren birgt.



FOTOS: ADOBE STOCK, OPEN AI

TEXT: TINA FISCHER
ILLUSTRATION: BERNA

Mit nur einem Prompt schreibt Chat GPT eine Mailvorlage, analysiert ganze PDF- oder Excel-Dateien und erstellt Texte für Präsentationsfolien. Nur: Wer promptet, macht das nicht immer ganz legal. Viele Firmen wie Roche, Helvetia oder die Zürcher Kantonalbank haben ihre IT-Policen überarbeitet und den Gebrauch öffentlich zugänglicher künstlicher Intelligenzen geregelt. Die Begründung liegt auf der Hand: Die Applikation ist zwar gratis, doch sie sammelt die eingegebenen Daten für das Training sowie die Weiterentwicklung der KI. Entsprechend überlegt sollte die Dateneingabe erfolgen.

Doch wenn keine adäquate Alternative im Raum steht, dann nutzen Mitarbeitende KI-Tools wie Chat GPT, Git Hub, Quill Bot, Otter oder Riverside trotzdem. Sie tun dies im Verborgenen – ohne das Wissen ihrer Vorgesetzten. Die Eingabe von Firmendaten erfolgt im Homeoffice und über den privaten Computer. So entsteht abseits der offiziellen Firmen-IT-Welt eine zweite Welt: eine Schatten-IT.

Die Risiken der Schatten-IT

Diese Schatten-IT ist seit dem Eintritt der generativen KI nahezu explodiert. Bereits im vergangenen Jahr gaben bei einer Studie von Gartner über 40 Prozent der Befragten an, Technologien ausserhalb des Firmen-IT-Universums erworben oder genutzt zu haben. Kurz darauf doppelte der Research-Service Core nach, Schatten-IT habe um 59 Prozent zugenommen, die Studie verortet den Auslöser bei der Remote-Arbeit.

Dass sich eine Schatten-IT überhaupt aufbauen kann, ist ein Indikator für einen ungenügenden Zustand der IT in der Firma. Innovationsrückstände, langsame Reaktionen oder unpassende Applikationen – so lässt sich zusammenfassen, warum Mitarbeitende lieber auf eigene Faust KI-Tools nutzen, statt auf die Firma zu warten.

«Können interne Programme nicht mit den Erwartungen oder Markttrends mithalten, dann nehmen Mitarbeitende ihr Glück selbst in die Hand, um diese Lücke zu schliessen und die eigene Effizienz zu gewährleisten», sagt Tim Cadenbach. Er ist Entwickler beim KI-Unternehmen Deepl. «Die Existenz von Schatten-IT ist eine Art Wink mit dem Zaunpfahl seitens der Belegschaft.»

Löbliche Absichten mit unlöblichem Ergebnis

Denn: Die Absichten der Mitarbeitenden sind eigentlich löblich, da sie sich durch die Nutzung eine Effizienzsteigerung erhoffen. Die Erfahrung lehrte sie, dass sie mit dem Tool schneller ans Ziel gelangen, als wenn sie den komplizierten Firmenweg nehmen. Doch sie vergessen dabei, dass bei der Nutzung von Gratis-KI grosse Risiken bestehen. Die Belegschaft füttert die KI mitunter mit ganz sensiblen internen Dateien. Die KI wiederum nutzt die Unterlagen zum Lernen – und spuckt deren Inhalt im Extremfall als Antwort auf eine Frage der Konkurrenz aus. Im Fachjargon nennt sich diese Situation «gelernter Output».

Noch riskanter ist, wenn Hacker ins Innere der KI gelangen. Sie erhalten Zugang zu allem, was jemals hochgeladen wurde, und können diese Informationen gegen die Firmen verwenden. Oder aber eine Firma wie Open AI nutzt die Trainingsdaten für sich, und die KI verkauft die Informationen als ihre Eigenkreationen – was die Urheberrechte verfälschen kann. Damit keines dieser Schreckensszenarien in Kraft tritt, müssen Firmen aktiv werden. Laut der jüngsten Datenerhebung von Deloitte nutzen schweizweit bereits mehr als 60 Prozent der Computernutzer und -nutzerinnen täglich ein generatives KI-Tool – «bisweilen auch ohne das Wissen ihrer Vorgesetzten».

Auf die Nachfrage, wie Firmen diese Problematik minimieren können, erklärt Marc Beierschoder, Studienautor und Leiter AI & Data bei Deloitte Schweiz, deren Massnahmenkalender: «Aller Anfang macht eine Informationskampagne, die das Bewusstsein fördert und Transparenz schafft.» Dabei müssen aber nicht nur die Mitarbeitenden informiert werden, auch die Firma muss lernen, was sich ihre Belegschaft wünscht.

Darauf aufbauend definiert eine Firma Richtlinien und bietet – wo nötig und möglich – Alternativen an. Sauer aufstossen dürfte einigen in der Firma der nächste Schritt: die Überwachung. Firmen dürfen grundsätzlich jederzeit auf die geschäftlichen Daten der Angestellten zugreifen, wie Rechtsanwältin Nicole Vögeli Galli weiss. Es gibt auch Applikationen, die Alarm schlagen oder eine Seite sperren, wenn Mitarbeitende beispielsweise auf Cloud-Services zugreifen wollen, die nicht erlaubt sind.

Die Mitarbeitenden schulen

Damit keine Misstrauenskultur in Firmen entsteht, müssen Firmen ihre Leute schulen – und erneut kommunizieren. Dazu gehört auch eine Anlaufstelle für KI, an die sich die Mitarbeitenden bei Fragen wenden können. «Das Ziel ist die Errichtung eines kontinuierlichen Prozesses», erklärt Beierschoder.

Denn: «Der Trend um KI wird weitergehen, das bedingt ein positives Umfeld, in dem sich Mitarbeitende auch äussern und ihre Anliegen in Bezug auf KI und Daten einbringen können.»

Nachgefragt

«Arbeitgeberinnen können auf E-Mails zugreifen»

Was die Schatten-IT für Firmen bedeutet, erklärt Arbeitsrechtsexpertin Nicole Vögeli Galli.

Welche Risiken bestehen arbeitsrechtlich, wenn Angestellte eine Schatten-IT nutzen?
Entscheidend ist, wie der Umfang der unerlaubten Nutzung ausfällt und welche Inhalte über externe Kanäle bearbeitet werden. Es ist weit weniger problematisch, wenn ich Chat GPT frage, wie eine schöne Grussformel für das Geschäftsmail auf Französisch lautet, als wenn ich ein ganzes Arbeitszeugnis mit Namen schreiben lasse.

Was, wenn Mitarbeitende KI auf eigene Faust nutzen, weil sie mit dem Angebot ihrer Firma unzufrieden sind?
Die Nutzung externer IT-Infrastruktur stellt eine Fehlerquelle dar, die ein erhebliches Haftungsrisiko für die Arbeitgeberinnen und die Mitarbeitenden birgt. Dies kann nicht nur zu Vermögensschäden, sondern auch zu Personen- sowie Sachschäden führen, womit wiederum die Strafbarkeit ebenfalls Thema ist. Deshalb muss die Nutzung von KI geschult sein und sorgfältig erfolgen.

Wie erfahren Firmen von Schatten-IT?
Selbst wenn ich als Arbeitgeberin den Zugriff auf anderweitige Tools sperre, kann ich nicht verhindern, dass Mitarbeitende auf privaten Geräten KI nutzen und dort unrechtmässig Daten eingeben. Doch eine ständige Überwachung des Verhaltens der Mitarbeitenden mit technologischen Möglichkeiten ist grundsätzlich unzulässig. Deshalb erfolgt die Überwachung in der Regel auf anonymisierter Basis zur Sicherung des Systems und die personenbezogene Auswertung erst bei konkretem Verdacht auf Missbrauch. Dies ist zulässig, wenn in arbeitsvertraglichen Dokumenten vorgesehen, und nur möglich, sofern geschäftliche Geräte oder ein VPN genutzt wird.

Auf welche Daten auf einem Computer eines Mitarbeiters darf die Firma zugreifen?
Jegliche geschäftliche Nutzung und deren Produkte wie Dokumente, E-Mails oder Daten gehören der Arbeitgeberin. Diese darf und muss jederzeit darauf Zugriff haben. Insofern können Arbeitgeberinnen jederzeit auf die geschäftlichen Daten inklusive E-Mails zugreifen. Sie haben jedoch Privates unbeachtet zu lassen.

Interview: Tina Fischer

Nicole Vögeli Galli
Arbeitsrechtsexpertin