03/2024 /// WWW.DIGITALBUSINESS-CLOUD.DE

D, A, CH: 11,50 | weitere EU-Länder: 13,70 | ISSN 2510-344X

DIGITAL BUSINESS CLOUD

EXPERTENMAGAZIN FÜR DIGITALE TRANSFORMATION

Eine Publikation der WIN Verlag GmbH & Co. KG | Ausgabe-Nr.: 191

CYBERSECURITY

DIE GEFAHREN DER SCHATTEN-KI

EKLATANTE RISIKEN BEI COMPLIANCE, DATENSICHERHEIT UND DEM SCHUTZ VON BETRIEBSGEHEIMNISSEN

SMC

Eine Sovereign Managed Cloud ermöglicht individualisierbare Clouds und erfüllt höchste Datensicherheitstandards.

NACHHALTIGKEIT

Experten-Talk: Wie moderne IT dazu beiträgt, die Nachhaltigkeitsziele von Unternehmen zu unterstützen.

MANAGED HOSTING

Eine attraktive Option, vorhandenene Ressourcen gezielt einzusetzen und den Fokus aufs Kerngeschäft zu legen.

Die Gefahren der Schatten-KI

Immer mehr Arbeitnehmer setzen KI-Tools ein, ohne dass der Chef davon weiß. Das verursacht Probleme bei Compliance, Datenschutz, Datensicherheit und dem Schutz von Betriebsgeheimnissen, sagt Experte Dr. Harald Schönfeld im exklusiven Interview.

VON HEINER SIEGER

WÄHREND DIE FÜHRUNGSSPITZE IN VIELEN UNTERNEHMEN EHER NOCH bei der Einführung von künstlicher Intelligenz (KI) zurückhaltend agiert, machen viele Mitarbeiter bereits „Nägel mit Köpfen". Sie nutzen KI längst „still und heimlich" für zahlreiche betriebliche Aufgaben. Das beobachtet der Management-Experte Dr. Harald Schönfeld, Herausgeber des Fachbuchs „Künstliche Intelligenz als Business-Booster im Unternehmen" und Geschäftsführer der Personalberatung Butterflymanager, die Interim Manager als Führungskräfte auf Zeit an Firmen vermittelt.

Wie häufig treffen Sie und Ihre Interim-Management-Kollegen inzwischen auf Schatten-KI?
Dr. Harald Schönfeld: Das kommt in 100 Prozent der Unternehmen vor. Zumindest wird das hinter der vorgehaltenen Hand eingeräumt, wenn man vertrauensvoll nachfragt. KI-Tools wie ChatGPT werden im großen Stil für E-Mails, Kundenbriefe, betriebliche Analysen oder Zusammenfassungen für das Management eingesetzt. Zum Beispiel im Marketing werden solche KI-Anwendungen regelmäßig genutzt, um Präsentationen zu erstellen. Dazu gibt es im Web Dutzende von Angeboten. Diese Präsentationen werden auch innerhalb der Firmen verschickt. Da hat inzwischen fast jeder Mitarbeiter einen individuellen Werkzeugkasten an KI, zum Teil sogar selbst bezahlt. Das ist ein regelrechter Wildwuchs. Viele Mitarbeiter sind ja im Homeoffice, und es mischen sich zunehmend Tools, die von der Firma angeschafft und installiert wurden und den Compliance-Anforderungen entsprechen, mit Versionen von Tools, die sich die Mitarbeiter im Netz zusammensuchen. Diese KI-Revolution von unten ist wirklich gefährlich.

Was sind die größten Gefahren dieser Schatten-KI?
Dr. Harald Schönfeld: Eine solche Schatten-KI bringt für die betroffenen Firmen erhebliche Probleme mit sich, etwa in Bezug auf Compliance, Datenschutz, Datensicherheit und den Schutz von Betriebsgeheimnissen. Das Hochladen von Kundendaten verletzt die Datenschutz-Grundverordnung, die Erstellung neuer Texte anhand vorhandener Dokumente verrät unbeabsichtigt Betriebsgeheimnisse Und die KI-Nutzung als Grundlage für Bewertungen oder Entscheidungen führt zu ethisch bedenklichen Ergebnissen, ohne dass es zunächst auffällt. Schatten-IT gab es schon immer und hat zu einem gewissen Kontrollverlust der IT-Abteilung geführt. Doch die Schatten-KI geht weit darüber hinaus. Sie birgt die Gefahr des Kontrollverlustes auf Geschäftsführungs- oder Vorstandsebene.

Ist den Mitarbeitern bewusst, dass sie damit möglicherweise ihren Arbeitgeber gefährden?
Dr. Harald Schönfeld: Viele probieren zunächst Demoversionen aus und kaufen die Software dann auch, wenn sie ihnen Vorteile bei der Arbeitsbewältigung bringt. Das geschieht ja oft im guten Glauben, seine Arbeit zu verbessern. Aber das ist weder professionell noch Compliance-gerecht. Jeder Security-Verantwortliche im Unternehmen schlägt die Hände über dem Kopf zusammen. Und nein, die Risiken sind den Leuten überhaupt nicht bewusst. Denn da werden ja firmenbezogene Daten in irgendein System hochgeladen, von dem man nicht weiß, wer dann im Hintergrund Zugriff darauf hat. Teilweise sind das zudem sehr vertrauliche Informationen. Was damit möglich ist, das freut jeden Industrie-Spion.

Auf welchen Bereichsebenen spielt sich das ab?
Dr. Harald Schönfeld: Je höher die Position, desto stärker die KI-Nutzung.

Wird denn intern über mögliche Schäden gesprochen?
Dr. Harald Schönfeld: Über Schäden redet man offiziell nicht. Da müssten ja Datenlecks eingeräumt werden. Und Mitarbeiter riskieren in dem Fall auch Abmahnungen. Da hält man lieber die Füße still. Allerdings werden wir Interim Manager hinter vorgehaltener Hand eingeweiht, was alles schon so passiert ist. Ich bin sicher: Die ersten Skandale werden kommen und auch bekannt werden. Etwa, wenn die Daten eines großen internationalen Mittelständlers plötzlich weg sind oder in Asien Baupläne von neuen innovativen Produkten auftauchen. Oder Finanzkennziffern in einer M&A-Situation in die Hände von Wettbewerbern geraten. Da sind Szenarien denkbar, die enorm zukunftsbedrohend für die betroffene Firma und deren Eigentümer sein können.

BERICHTE AUS DER PRAXIS

Wie mannigfach die Potenziale und die Verbreitung von KI in unterschiedlichen Firmenfunktionen wie Personalwesen, Marketing oder Controlling bzw. in verschiedenen Marktsegmenten wie der Bau- oder der Modebranche sind, dokumentiert Dr. Harald Schönfeld in seinem neuen Buch „Künstliche Intelligenz als Business-Booster für Unternehmen". Darin kommen elf Interim Manager zu Wort, die von ihren Erfahrungen beim betrieblichen KI-Einsatz berichten.

Sind sich denn die Unternehmensleitungen des Problems bewusst?

Dr. Harald Schönfeld: Das ist differenziert zu betrachten: Zum einen begreifen möglicherweise viele Firmenleitungen das Thema nicht in seiner Tragweite. Es herrscht also eine gewisse Inkompetenz des Managements vor. Zum anderen tun sich Unternehmen, die es vielleicht verstehen, trotzdem schwer, entsprechende Richtlinien zu entwickeln in Bezug auf die Anschaffung und Nutzung von KI. Die meisten Unternehmen sind im Tagesgeschäft damit überfordert. Die Chefs wissen ja durchaus, dass ihre Mitarbeiter produktiver arbeiten mit solchen Tools. Wichtig ist es aber, die richtigen Policies zu entwerfen und zu implementieren. Der Handlungsbedarf ist groß. Denn das ist eine schnelle Entwicklung. In manchen Bereichen kommen ja wöchentlich neue Tools auf dem Markt, und die Unternehmen kommen irgendwann nicht mehr hinterher, wenn sie das Risiko nicht frühzeitig im Keim ersticken.

Schatten-IT gab es schon immer und hat zu einem gewissen Kontrollverlust der IT-Abteilung geführt. Doch die Schatten-KI geht **weit darüber hinaus**. Sie birgt die Gefahr des Kontrollverlustes auf Geschäftsführungs- oder Vorstandsebene.

Wie ist die Schatten IT im Zusammenhang mit dem EU AI Act zu bewerten?

Dr. Harald Schönfeld: Die aktuelle KI-Regulierung der Europäischen Union durch den EU AI Act läuft bei Schatten-KI weitgehend ins Leere. Wenn die Marketingabteilung Kundendaten in eine KI hochlädt, um darauf basierend gut formulierte Anschreiben an die Kundschaft zu verschicken, mag dies zwar keinen Verstoß gegen den AI Act darstellen, aber sicherlich gegen die Datenschutz-Grundverordnung. Und wenn die HR-Abteilung Bewerberprofile durch die KI prüfen und bewerten lässt, verstößt dies über den AI Act hinaus gegen weitere Rechtsgrundsätze.

Welche Lösungsansätze empfehlen Sie?

Dr. Harald Schönfeld: Unternehmen benötigen eine Wandelkompetenz: Zum ersten grundsätzlich eine Expertise, den digitalen Wandel zu gestalten und zum zweiten im Umgang mit dieser völlig neuen Technologie. Da muss das Management lernen, diesen schnellen Wandel zu gestalten. Das beginnt mit dem Bewusstsein für die Problematik, geht über die Einrichtung von entsprechenden Arbeitsgruppen bis zu Regelungen, die auch gewisse Spielräume erlauben, aber auch klare Grenzen aufzeigen. Es wird keine einheitliche Lösung dafür geben. Wichtig ist es, das Thema auf die Tagesordnung zu setzen. Fast noch wichtiger ist ein weiterer Aspekt: Dieses Thema müssen auch Aufsichtsräte und Beiräte jetzt dringend auf den Tisch legen und die Vorstände damit konfrontieren. Und die Frage stellen: Habt Ihr ein Konzept für Schatten-KI? Nach unserem Einblick haben mindestens 90 Prozent der Unternehmen das noch nicht auf dem Schirm. Auch nicht die Aufsichtsräte. Das müssten sie aber haben, um ihrer Verantwortung gerecht zu werden. Leider haben sie meisten da selbst keine Kompetenz. Und dann muss das Thema alle drei Monate wieder auf den Tisch und angeschaut werden, da die Entwicklung in dem Bereich derart rasant ist. •