Newsletter Datenschutz

konzept 17

Ihr Datenschutz-Info Blatt für mehr Sicherheit in Ihrem Unternehmen

Liebe Leserin, lieber Leser,

kaum ein technologisches Thema wird gegenwärtig so stark diskutiert wie Künstliche Intelligenz (KI). Die meisten Beschäftigten sagen, sie hätten bereits mit KI erste Versuche angestellt. Sie vielleicht auch. Doch wissen Sie, wie Sie mit KI-Werkzeugen richtig umgehen? Fehler im Umgang mit KI können Daten in Gefahr bringen und so den Datenschutz verletzen. Lesen Sie deshalb im ersten Beitrag, welche Datenschutz-Tipps es für den Einsatz von KI gibt.

Auch in vielen anderen Bereichen kommt es auf das richtige Verhalten und auf den korrekten Umgang mit Daten an. Das gilt für Krankmeldungen von Kolleginnen und Kollegen genauso wie für E-Mails und andere Nachrichten, die verdächtig erscheinen und die zu einer Phishing-Attacke gehören könnten.

Ihre neue Ausgabe liefert Ihnen wertvolle Tipps zur Vermeidung entsprechender Datenpannen und zeigt anhand aktueller, lebensnaher Fälle auf, wie sich Daten besser schützen lassen. Auch im Datenschutz gilt es, aus Fehlern zu lernen, um selbst Fehler und damit Datenpannen zu vermeiden.

Ihr Frank Berns, Datenschutzbeauftragter

Impressum
Redaktion: Frank Berns,
Datenschutzbeauftragter, Geschäftsführer

Anschrift:
Konzept 17 GmbH
Westring 3
24850 Schuby
Amtsgericht Flensburg: HRB 12329
Telefon: 0049 4621 5 30 40 50
E-Mail: mail@konzept17.de

KI ja – aber bitte datenschutzkonform!

KI ist etwas Wunderbares. Einige einfache Spielregeln stellen sicher, dass ihr Einsatz datenschutzkonform abläuft.

Vorgaben des Unternehmens sind bindend

Die wichtigste Spielregel wirkt fast schon banal: Das Unternehmen kann festlegen, ob KI eingesetzt werden darf, und falls ja, welche KI das ist. Dies muss bei aller Begeisterung für die Möglichkeiten der KI immer bewusst sein. Auch der Einsatz von KI-Anwendungen, die im Internet für alle frei zugänglich sind, ist in einem Unternehmen nicht automatisch erlaubt.

Unternehmensinterne KI-Anwendungen sind die bessere Wahl

Wer eigene KI-Anwendungen seines Unternehmens nutzt und dabei die Vorgaben des Unternehmens beachtet, ist auf der sicheren Seite. Auch wenn die unternehmenseigene KI-Anwendung scheinbar oder tatsächlich weniger komfortabel ist – das rechtfertigt es nicht, eigenmächtig auf eine allgemein zugängliche KI-Anwendung im Internet auszuweichen.

Frei zugängliche KI-Anwendungen haben besondere Tücken

Wer eine KI-Anwendung nutzt, die im Internet frei zugänglich ist, muss sich immer über eines im Klaren sein: solche KI-Anwendungen sind generell verwendbar, also nicht auf einen bestimmten Einsatzzweck zugeschnitten. Lösungen für individuelle Anforderungen an die Vertraulichkeit von Daten können sie nicht bieten.

Eine Registrierung sollte man möglichst vermeiden

Manche KI-Anwendungen im Internet verlangen vom Nutzer eine Registrierung, andere dagegen nicht. Wenn eine Wahl besteht, sollte man die Anwendung bevorzugen, die man ohne Registrierung benutzen kann.

Mit Mailadressen muss man vorsichtig umgehen

Bei frei zugänglichen KI-Systemen im Internet ist oft eine Registrierung mit einer Mailadresse erforderlich. Mailadressen, die den eigenen Namen enthalten, sind für eine solche Registrierung nicht geeignet. Mailadressen für Funktionspostfächer, die keinen Namen einer Person enthalten, eignen sich dafür viel besser.

Vertraulichkeitsvorgaben gelten auch bei KI-Anwendungen

Interne Daten müssen intern bleiben. Was sonst nicht nach außen weitergegeben.

werden dürfte, darf man auch nicht in eine frei zugängliche KI-Anwendung eingeben. Dies gilt für personenbezogene Daten genauso wie für Geschäftsgeheimnisse mit oder auch ohne Personenbezug. Denn es lässt sich nie vorhersagen, was eine KI-Anwendung mit eingegebenen Daten macht.

KI-Anwendungen nutzen eingegebene Daten weiter

Die Optimierung von KI-Anwendungen lebt davon, dass alle eingegebenen Daten auch diesem Zweck der Optimierung dienen. Nach Erledigung der Aufgabe, die ein Nutzer einer KI-Anwendung stellt, sind die eingegebenen Daten nicht „verschwunden". Sie stecken vielmehr – bildlich gesprochen – weiter in der Anwendung und dienen ihrer Optimierung.

Die Eingabeprotokollierung bitte abschalten

KI-Anwendungen sind so voreingestellt, dass sie die eingegebenen Fragestellungen und Aufgaben protokollieren. Viele Anwendungen bieten jedoch die Möglichkeit, diese Protokollierung auszuschalten. Davon sollte man unbedingt Gebrauch machen.

Korrekter Umgang mit Krankmeldungen

Im Umgang mit Krankmeldungen gilt es Vorsicht walten zu lassen. Was manche bisweilen vergessen:

Es gibt datenschutzrelevante Aspekte zu berücksichtigen,

die nicht nur die verschiedenen „Chefebenen", sondern auch den Kreis der Kolleginnen und Kollegen – besonders bei der Zusammenarbeit in einem Team – betreffen. Deshalb geht das Thema alle im Unternehmen an.

Krankmeldungen bestehen aus Gesundheitsdaten.

Eine Krankmeldung ist

eine Ansammlung von Gesundheitsdaten. Denn sie zeigt, wer sich krankgemeldet hat und wann das erfolgt ist. Manchmal enthält sie sogar weitergehende Informationen. So schreiben Betroffene manchmal – ohne dies zu müssen – hinein, dass sie sich in einem Krankenhaus befinden. In jedem Fall gilt für Krankmeldungen der besondere Schutz, den die DSGVO für Gesundheitsdaten vorsieht.

Krankmeldungen sind rechtlich bedeutsam

Eine Krankmeldung hat in vielfacher Hinsicht rechtliche Bedeutung, etwa für den Anspruch auf Lohnfortzahlung. Sollte die Krankheit auf einem Arbeitsunfall beruhen, bestehen Meldepflichten des Arbeitgebers gegenüber der Berufsgenossenschaft. Es liegt auf der Hand, dass der Arbeitgeber die Daten aus der Krankmeldung für solche Zwecke verarbeiten darf. Denn anders könnte er seine Pflichten aus dem Arbeitsvertrag und den einschlägigen Gesetzen nicht erfüllen.

Die Mitwirkung externer Dienstleister geht in Ordnung

Kaum ein Arbeitgeber kann noch alles selbst erledigen. Meist ist er auf die Unterstützung durch externe Lohnabrechnungsbüros oder Steuerberater angewiesen. Die Übermittlung der notwendigen Daten an solche Stellen ist rechtlich problemlos. Sie muss sich aber auf das beschränken, was wirklich erforderlich ist. Außerdem müssen die Daten bei der Übermittlung ausreichend gegen den Zugriff durch Unbefugte geschützt sein.

Die Erforderlichkeit ist das wesentliche Kriterium

In größeren Unternehmen darf eine Krankmeldung an alle Organisationseinheiten gehen, die die Informationen aus der Meldung brauchen, um ihren Job machen zu können. Dazu gehört in jedem Fall die Personalabteilung. Aber auch die Buchhaltung braucht die Angaben, um die Lohnfortzahlung korrekt vornehmen zu können. Geht es um einen Arbeitsunfall, muss auch der Sicherheitsbeauftragte informiert werden. All dies liegt auf der Hand und ist durch die DSGVO erlaubt.

Die gegenseitige Vertretung muss gesichert sein

Weitere Personen dürfen informiert werden, wenn ihre Arbeitsabläufe oder ihre Arbeitsaufgaben durch die Abwesenheit des erkrankten Beschäftigten berührt werden. Dies hört sich zunächst etwas abstrakt an. In der Praxis ist jedoch meist schnell klar, um wen es dabei geht. Falls Beschäftigte einander vertreten müssen, muss der Vertreter von der Abwesenheit seines „Vertretungspartners" erfahren. Dasselbe gilt, wenn ein Team gebildet ist. Dann müssen die anderen Teammitglieder wissen, wer da ist und wer nicht.

Vorgesetzte brauchen die erforderlichen Infos

Selbstverständlich müssen auch unmittelbare Vorgesetzte darüber informiert sein, wenn jemand nicht zur Verfügung steht. Denn schließlich müssen sie die Arbeit dann so organisieren, dass trotzdem möglichst alles erledigt wird. Sofern eine Telefonzentrale vorhanden ist, muss auch sie Bescheid wissen. Nur so ist es ihr möglich, Anrufe zum Beispiel an einen Vertreter weiterzuleiten.

Es kommt auf die Details an

Genau zu unterscheiden ist jeweils, ob jemand im Unternehmen lediglich über die Abwesenheit Bescheid wissen muss oder auch darüber, dass sie gerade auf Krankheit beruht. So muss die Telefonzentrale lediglich wissen, dass jemand nicht da ist. Die Personalabteilung braucht dagegen auch die Angabe, dass es sich um eine Abwesenheit wegen Krankheit handelt. Vorgesetzte benötigen diese Information ebenfalls. Das gilt schon wegen ihrer Pflichten aus dem betrieblichen Gesundheitswesen. Der Krankenstand ist dabei eine wichtige Kennziffer.

Große Mailverteiler sind gefährlich

Recht erheblich ist bisweilen der Wissensdrang von Kolleginnen und Kollegen. Er ist jedoch kein ausreichender Grund dafür, um beispielsweise die gesamte Abteilung über Krankmeldungen zu informieren. Dennoch geschah genau dies in einem Hamburger Unternehmen. Dort ordnete ein Abteilungsleiter an, alle eingehenden Krankmeldungen über einen besonderen Mailverteiler allen 25 Mitarbeiterinnen und Mitarbeitern dieser Abteilung zuzuleiten. Natürlich beanstandete die Datenschutzaufsicht diese Vorgehensweise.

Es gibt eine gute Faustregel

Insgesamt lautet eine gute Faustregel: Wenn gefragt wird, warum jemand Kenntnis von einer Krankmeldung erhält, muss man dafür einen guten Grund nennen können. Ansonsten ist die Zuleitung der Krankmeldung an diesen Empfänger so gut wie sicher rechtswidrig.

Aus Datenpannen lernen, nicht nur aus den eigenen

Kommt es zu einer Datenschutzverletzung, gilt es die Ursache zu finden und eine Wiederholung zu vermeiden. Es muss aber nicht erst eine Datenpanne im eigenen Unternehmen auftreten, um das zu tun. Die Aufsichtsbehörden nennen viele Beispiele für Vorfälle, aus denen man lernen kann und sollte.

Datenpannen sind kein abstraktes Risiko

Wenn in den Nachrichten über eine Datenschutzverletzung berichtet wird, geht es meist um einen weltweit operierenden Konzern, von dem Kundendaten millionenfach ungeschützt im Internet aufgetaucht sind. Kleine und mittlere Unternehmen scheinen da nicht betroffen zu sein. Doch weit gefehlt:

Datenpannen passieren leider überall, in Unternehmen jeder Größe, in Behörden und auch bei einzelnen Bürgerinnen und Bürgern. Die bekannten Großkonzerne haben nur einen „höheren“ Nachrichtenwert und werden deshalb häufiger im Fernsehen, im Radio und in den Zeitungen genannt.
Doch auch andere Datenschutzverletzungen können relevant sein für das eigene Unternehmen und die eigene Person, denn man kann aus ihnen lernen, wie genau gegen den Datenschutz verstoßen wurde, wie dies passieren konnte und was geschehen muss, um dies in Zukunft oder an anderer Stelle zu vermeiden. Aus Fehlern kann und sollte man lernen, das gilt auch im Datenschutz!

Berichte der Datenschutzaufsichtsbehörden bieten viele Beispiele

Nicht unbedingt in den Abendnachrichten lernt man die Datenschutzvorfälle kennen, aus denen man für sich selbst etwas lernen kann, sondern in den Berichten der Aufsichtsbehörden für den Datenschutz. Ein gutes Beispiel ist der Bericht „Best of Datenschutz“, denn er enthält lebensnahe Datenschutzfälle. Veröffentlicht wird dieser Bericht vom Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz. Doch auch alle anderen Datenschutzaufsichtsbehörden berichten von Vorfällen im Datenschutz, insbesondere in ihren Tätigkeitsberichten, die auf den Webseiten der Aufsichtsbehörden zu finden sind.

Sicheres Löschen vor Rückgabe oder Weitergabe von Geräten

Besonders wertvoll sind dabei Beispielvorfälle, die aus dem Alltag stammen, aber nicht nur privat relevant sind, sondern auch aufzeigen, wie man am Arbeitsplatz Datenpannen besser verhindern kann. Hierzu ein Beispiel aus Rheinland-Pfalz: Eine Frau hatte in einem Elektronikmarkt eine Virtual-Reality-Brille als Weihnachtsgeschenk für ihren Sohn erworben.

Auf die Bescherung folgte eine böse Überraschung, so die Datenschutzaufsicht: Mit dem Gerät waren bereits Facebook- und Instagram-Konten verknüpft – mit personenbezogenen Daten und vermutlich wenig kindgerechten Inhalten. Ein anderer Kunde hatte die Virtual-Reality-Brille zuvor gekauft, ausprobiert und innerhalb der Widerrufsfrist zurückgegeben. Im Vorweihnachtsstress hatte ein Mitarbeiter des Elektronikgeschäfts vergessen, die auf dem Gerät gespeicherten Daten des ersten Kunden vor dem Wiederverkauf zu löschen.

Dabei muss es keine VR-Brille und kein Weihnachtsgeschäft sein, Datenpannen dieser Art passieren auch häufig in Unternehmen. Zum Beispiel werden Festplatten oder ganze Computer ausgemustert und dann verschenkt oder für den Weiterverkauf vorgesehen. Wird vergessen, die darauf befindlichen Daten sicher zu löschen, dann werden mit den Geräten auch vertrauliche Daten an Dritte ungewollt weitergegeben oder verkauft. Eine sichere Datenlöschung vor dem Recycling, der Weitergabe oder dem Verkauf von Altgeräten ist Pflicht!

Vertrauliches ist nicht für fremde Ohren

Die Datenschutzaufsicht berichtet von weiteren Vorfällen, die auch im eigenen beruflichen Alltag passieren können: Weil eine Bankberaterin ein Beratungstelefonat nicht in einem separaten Büro, sondern im öffentlichen Schalterraum geführt hatte, waren sensible Informationen zu den Vermögenswerten und den Lebensplänen einer Kundin in unbefugte Ohren gelangt. Vertrauliche Gespräche im öffentlichen Bereich finden aber nicht nur in diesem genannten Schalterraum einer Bank statt.

In Arztpraxen, bei Behörden, in der Kantine eines Unternehmens, aber auch im Frühstücksraum des Hotels bei der Dienstreise, im Zug oder im Wartebereich am Flughafen: Es gibt viele Situationen, in denen private und vertrauliche Gespräche und Informationen in fremde Ohren gelangen können. Es reicht also nicht, zum Beispiel den Bildschirm des Notebooks im Zug vor ungewollten Einblicken Dritter zu schützen. Auch bei Telefonaten und anderen Gesprächen muss die Vertraulichkeit gewahrt werden. Hier hilft auch keine Blickschutzfolie, wie dies für Notebooks angeboten wird. Hier sind wir Menschen selbst gefragt. Was nicht für Dritte bestimmt ist, sollte in deren Anwesenheit auch nicht erzählt werden.

Fragen Sie Ihren Datenschutzbeauftragten nach weiteren Beispielen und nach dem Tätigkeitsbericht der zuständigen Aufsichtsbehörde. Man kann sehr viel daraus lernen!

Phishing-Attacken beschreiten neue Wege

Bei Passwortdiebstahl über Phishing-Attacken denken viele an E-Mails, die auf gefälschte Anmeldeseiten locken sollen. Doch Phishing-Mails sind nicht das einzige Risiko. Datendiebe gehen jetzt neue und unerwartete Wege, um an Ihre Daten zu kommen.

Angriffe kommen (nicht nur) über E-Mail

Cyberangriffe mithilfe von E-Mails sind weiterhin eine große Bedrohung für Unternehmen, Organisationen und Bürgerinnen und Bürger, so das Bundesamt für Sicherheit in der Informationstechnik (BSI). Insbesondere Phishing-Mails, mit denen Zugangsdaten oder ganze Identitäten gestohlen werden sollen, sind ein weithin genutztes Angriffsmittel.

Diese Warnung der IT-Sicherheitsbehörde des Bundes darf aber nicht missverstanden werden. Viele Cyberattacken beginnen mit einer bösartigen E-Mail, die einen schadhaften Anhang oder einen Link auf eine gefälschte Login-Seite enthält. Das bedeutet aber nicht, dass Datendiebe nur auf E-Mails setzen, um ihre Opfer zu erreichen.

Auch bei Teams & Co gibt es (gefährliche) Nachrichten

Da Videokonferenzen über Teams und vergleichbare Dienste zunehmend verbreitet sind und häufig genutzt werden, hat auch die Zahl der darüber verschickten Nachrichten zugenommen. Während eines Video-Calls sendet der Gesprächspartner zum Beispiel den Link zum gerade besprochenen Projekt. Leider können auch die Links, die über Teams & Co verschickt werden, gefälscht und manipuliert sein. Microsoft warnt explizit vor möglichen Phishing-Nachrichten über Teams. Security-Unternehmen wie AT&T Cybersecurity berichten von konkreten Vorfällen, bei denen Teams-Nachrichten für Angriffe genutzt wurden.

Cyberkriminelle begnügen sich nicht mit E-Mails, um die Empfänger zu täuschen und auszutricksen. Sie setzen auf jede Form der Kommunikation. Leider beschränken sich aber viele Schutzmaßnahmen auf den E-Mail-Kanal. Typische Phishing-Filter zur Erkennung und Blockade von Phishing kontrollieren nur den E-Mail-Eingang.

Die Kreativität der Datendiebe kennt kaum Grenzen, jede Möglichkeit wird genutzt, um mit den Opfern zu kommunizieren und sie zu täuschen. Phishing kennt viele Wege, überall ist Vorsicht angesagt, nicht nur bei E-Mails.

Auch SMS oder Briefe mit QR-Code können Phishing sein

Der „Global Mobile Threat Report 2024“ von Zimperium berichtet von einem deutlichen Anstieg an „Mishing“-Bedrohungen (Mobile Targeted Phishing). Mittlerweile zielen 82 Prozent der Phishing-Seiten auf mobile Endgeräte, denn dort sind die Displays klein und die Bereitschaft, etwas über den Touchscreen des Smartphones anzuklicken, ist groß. Dabei können die Phishing-Links auch in der guten, alten SMS enthalten sein, denn SMS sind schon lange keine reinen Textnachrichten mehr. Viele Smartphones verarbeiten SMS in Applikationen (Apps), die wie Chat-Programme arbeiten und zum Beispiel aktive Links unterstützen, die sich anklicken lassen und dann gleich den mobilen Browser auf dem Smartphone öffnen.

Polizeibehörden wie das Landeskriminalamt (LKA) NRW und Verbraucherschützer warnen aktuell vor einer weiteren Variante von Phishing: mithilfe von QR-Codes. Datendiebe verbinden ihre digitale Betrugsmasche mit klassischen Informationswegen. Mit QR-Codes, die in Briefen eingedruckt sind, locken sie auf gefälschte Internetseiten. Sie verschicken falsche Bank-Briefe, überkleben Codes auf E-Ladesäulen und verteilen sogar gefälschte Strafzettel mit QR-Codes, die auf Phishing-Seiten führen.

Wissen Sie, wie vielfältig die Phishing-Gefahr ist?

Frage 1: Phishing ist ein digitales Risiko. Stimmt das?

1. Nein, Angreifende versuchen auch per Fax, Brief, Telefon oder persönliche Ansprache vertrauliche Daten zu erlangen.
2. Ja, erst mit der Digitalisierung sind auch die Phishing-Attacken möglich geworden, denn sie locken die Opfer auf manipulierte Links und Webseiten.

Lösung Frage 1: Die Antwort 1. ist richtig. Phishing ist der Versuch, insbesondere an Passwörter der Opfer zu gelangen. Ob dies über eine bösartige E-Mail, eine Fax-Nachricht oder einen täuschenden Anruf erfolgt, spielt für die Gefahr nicht wirklich eine Rolle. Es geht auf allen Wegen darum, die Opfer auszutricksen und zu gefährlichem Verhalten zu verleiten, also zum Beispiel einem Dritten ihre Passwörter anzuvertrauen.

Frage 2: Auch SMS-Nachrichten können Phishing-Links enthalten und einen Angriff darstellen. Stimmt das?

1. Ja, jede Form der Kommunikation kann für Phishing genutzt werden.
2. Nein, bei SMS gibt es doch gar keine Links, auf die man klicken könnte.

Lösung Frage 2: Die Antwort 1. ist auch hier richtig. Auch die SMS-Nachricht kann für Phishing genutzt werden. In der Praxis geschieht dies sogar sehr häufig. Ein typisches Beispiel ist die angebliche SMS des Paketdienstes mit einem Link zur Nachverfolgung der Lieferung. Klickt man den Link in einer SMS an, öffnet sich eine womöglich gefälschte Webseite, wie man es von E-Mails kennt. Da Smartphones keine einfachen Telefone sind, haben sie auch Browser und Internetzugang und können so zum Ziel der Phishing-Angriffe werden.