SANOVIS CONSULTING WITH CARE.

CURACON SICHERHEIT GEBEN. LÖSUNGEN BIETEN.

NEWSLETTER DATENSCHUTZ

Liebe Leserin, lieber Leser,

auch wenn das informationelle Selbstbestimmungsrecht schon seit Jahrzehnten besteht, entwickelt sich der Datenschutz dynamisch weiter, da er auf technische und rechtliche Entwicklungen reagieren muss.
In Ihrer neuen Ausgabe finden Sie ganz aktuell Hinweise, wie Sie es vermeiden können, durch Nutzung einer Künstlichen Intelligenz (KI) ungewollt zum Geheimnisverräter zu werden. Nicht minder aktuell sind die Entwicklungen bei den Transfers personenbezogener Daten in die USA und beim neuen Data Privacy Framework (DPF).
Gerade im Bereich der mobilen Endgeräte wie Smartphones und der zugehörigen Apps tut sich sehr viel. Erfahren Sie deshalb, was Sie tun sollten, wenn ein mobiles Gerät verloren geht, und ob Sie den Apps aus den offiziellen App-Stores wie Google Playstore unbesehen vertrauen können. Stammen Spionage-Apps wirklich nur aus den inoffiziellen App-Stores, vor denen seit Jahren schon gewarnt wird?

Wir wünschen Ihnen interessante Erkenntnisse beim Lesen!

Dr. Uwe Günther
Beratungsfeldleiter Datenschutz, Curacon GmbH
Geschäftsführer, Sanovis GmbH

Stefan Strüwe
Beratungsfeldleiter Datenschutz, Curacon GmbH

Oktober_2023

1 GEHEIMNISVERRAT AN DIE KI?

Einen langen Text kürzen, Ergebnisse einer Besprechung zusammenfassen oder Programmcode schreiben – die Möglichkeiten eines KI-Dienstes wie ChatGPT scheinen fast grenzenlos. Doch leider sind auch die möglichen Risiken durch Künstliche Intelligenz (KI) weitreichend. Das darf niemand bei dem Hype um KI vergessen.

Der Hoffnungsträger KI

Künstliche Intelligenz gilt als eine Schlüsseltechnologie, die praktisch überall zum Einsatz kommen soll, ob in der Automobilbranche, im Maschinenbau oder im Dienstleistungsbereich, so der Digitalverband Bitkom.

Unternehmen erhoffen sich schnellere und präzisere Problemanalysen, beschleunigte Prozesse und einen geringeren Ressourcenverbrauch. Aber auch im Personalbereich werden Vorteile gesehen, etwa die Vermeidung menschlicher Fehler und die Möglichkeit, durch KI Expertenwissen ins Unternehmen zu holen. Durch KI können sich Beschäftigte auf andere Aufgaben konzentrieren, hoffen die Unternehmen.

Tatsächlich aber sollte man sich zuerst einmal auf die KI und ihre möglichen Risiken konzentrieren, bevor man durch Dienste wie ChatGPT Aufwände einsparen will.

Das übersehene Risiko KI

Wie bei vielen neuen Technologien erzeugt KI auch Angst und Bedenken. Trotzdem werden ChatGPT & Co. munter genutzt, die Neugierde siegt, mögliche Bedenken werden beiseitegeschoben. Das kann aber mehr als riskant sein, für die eigene Privatsphäre, für den Datenschutz im Unternehmen sowie für die Betriebs- und Geschäftsgeheimnisse.

So hilfreich es erscheint, wenn ein Online-Dienst etwa einen langen Text zusammenfasst oder aus ein paar Notizen ein Besprechungsprotokoll erstellt: Die Inhalte der Notizen und Texte können personenbezogene und andere zu schützende Informationen enthalten. Wenn man zum Beispiel über die neue Produktplanung spricht und sich automatisiert das Protokoll der Planungssitzung erzeugen lässt, besteht die Gefahr, dass die Informationen abfließen, also das Unternehmen verlassen und Dritten bekannt werden könnten.

Letztlich könnte so die Nutzung der KI ungewollt Geheimnisse verraten, denn eine KI lernt von den Eingaben und Reaktionen der Nutzenden auf die Antworten. Lernen bedeutet aber auch, Informationen in den Datenbestand der KI aufzunehmen.

KI braucht Regeln

In den meisten Unternehmen fehlen noch interne Richtlinien für den Umgang mit einer KI. Doch KI-Tools sollten nicht ohne jede Regelung zum Einsatz kommen, so wie beispielsweise die Nutzung einer Cloud nach internen Richtlinien erfolgen sollte.

Wer also einen KI-Dienst betrieblich nutzen will, sollte zuerst klären, ob das im Unternehmen erlaubt und gewünscht ist. Dann gilt es zu klären, zu welchem Zweck und mit welchen Daten der erlaubte KI-Dienst eingesetzt werden darf. Maßstab sollte dabei immer sein, die KI wie einen Dritten, der nicht zum Unternehmen gehört, anzusehen. Soll eine Information das Unternehmen nicht verlassen, gehört sie auch nicht in das Eingabefeld einer KI.

Tipp: Auch bei KI gibt es Datenschutzeinstellungen

KI-Dienste wie ChatGPT bessern gegenwärtig bei ihren Datenschutzoptionen nach. Es ist wichtig, sich auch hier mit den Einstellungen zu befassen und zum Beispiel die Übernahme der Eingaben in den Datenbestand der KI zu verbieten. Gleichzeitig sollte man der KI trotzdem

keine vertraulichen und sensiblen Daten anvertrauen, um jeden Geheimnisverrat zu vermeiden.

2 DAS EU-U.S. DATA PRIVACY FRAMEWORK

Was lange währt, wird endlich gut. Dieses Motto gilt hoffentlich für das EU-U.S. Data Privacy Framework. Sie kennen dieses Stichwort noch gar nicht? Es geht um eine neue Rechtsgrundlage für Datenübermittlungen in die USA. Dabei gilt es einige Fallstricke zu beachten.

Der 16. Juli 2020 weckt böse Erinnerungen

Der 16. Juli 2020 war für alle Unternehmen, die auf Datenübermittlungen in die USA angewiesen sind, ein schwarzer Tag. Denn damals erklärte der Europäische Gerichtshof (EuGH) den Angemessenheitsbeschluss der EU-Kommission zum „Privacy Shield“ für nichtig. Von diesem Tag an konnten Unternehmen Datenübermittlungen in die USA nicht mehr auf den Angemessenheitsbeschluss als Rechtsgrundlage stützen.

Das war schmerzlich, denn Datenübermittlungen auf seiner Basis verursachten nur einen geringen rechtlichen Aufwand. Alle denkbaren Alternativen, auf die sie von da an zurückgreifen mussten, waren für die Unternehmen dagegen zum Teil mit wahren Papierbergen verbunden.

Der rechtliche Schwebezustand hat jetzt ein Ende

Seit dem 10. Juli 2023 gibt es wieder einen Angemessenheitsbeschluss der EU-Kommission, den Unternehmen für Datenübermittlungen in die USA nutzen können. Darin ist festgehalten, dass unter bestimmten Bedingungen in den US-Unternehmen ein angemessenes Datenschutzniveau herrscht.

Wohlgemerkt: unter bestimmten Bedingungen. Aber wenn sie erfüllt sind, funktioniert wieder alles so, wie man es vor dem 16. Juli 2020 mit dem „Privacy Shield“ gewohnt war. Unternehmen in der EU können also wieder personenbezogene Daten an ihre US-Geschäftspartner übermitteln, ohne dafür umfangreiche zusätzliche Datenschutzregelungen vereinbaren zu müssen.

Der Jubel ist trotzdem eher verhalten

Die neuen Regelungen wurden in der Wirtschaft dankbar registriert. Immerhin bringen sie erhebliche Erleichterungen für den „Datenschutzalltag“. Echte Begeisterung spürt man allerdings nur selten. Eher herrscht eine gewisse Skepsis, was die Zukunft der neuen Regelungen angeht. Über kurz oder lang wird es auf irgendeinem Weg dazu kommen, dass der EuGH auch sie rechtlich überprüft. Werden sie dann Bestand haben?

Die neuen Regelungen werden bis auf Weiteres tragfähig sein

So verständlich solche Befürchtungen sind – im Augenblick helfen die neuen Regelungen wirklich weiter.

Das Grundschema, nach dem sie funktionieren, ist relativ einfach: US-Unternehmen können sich in den USA in eine Art Datenschutzregister eintragen lassen. Es trägt die Bezeichnung „Data Privacy Framework List“. Dazu müssen sie ziemlich viele Voraussetzungen erfüllen. So müssen etwa ausreichende Datensicherungsmaßnahmen vorhanden sein.

Wenn ein US-Unternehmen diesen Zertifizierungsprozess erfolgreich abgeschlossen hat, können sich seine Geschäftspartner in der EU darauf verlassen, dass in diesem US-Unternehmen ein angemessenes Datenschutzniveau herrscht. Das bildet die rechtliche Basis dafür, dass die Übermittlung personenbezogener Daten dorthin zulässig ist.

Für Personaldaten gelten Besonderheiten

Die Frage, ob auf dieser Basis auch eine Übermittlung von Personaldaten zulässig ist, lautet: „Ja, aber …“. Die Übermittlung solcher Daten an ein US-Unternehmen setzt voraus, dass dieses Unternehmen zusätzliche Verpflichtungen eingeht. Dazu gehört insbesondere die Verpflichtung, mit den Datenschutz-Aufsichtsbehörden in der EU zusammenzuarbeiten.

Die Zertifizierung ist jedes Jahr zu erneuern

US-Unternehmen, die auf der „Data Privacy Framework List“ stehen, müssen ihre Zertifizierung jedes Jahr erneuern lassen. Sonst werden sie von der Liste gestrichen. Deshalb müssen sich ihre Geschäftspartner in der EU jedes Jahr vergewissern, dass die Zertifizierung erneuert wurde. Im Augenblick richten alle betroffenen Unternehmen in der EU die dafür nötigen Abläufe ein, wenn sie nicht ohnehin schon vorhanden sind.

Microsoft 365 bleibt eine Herausforderung

Viele Unternehmen hatten gehofft, dass der neue Angemessenheitsbeschluss alle vorhandenen Probleme bei Datenübermittlungen in die USA löst. Dies galt besonders für den Einsatz von Microsoft 365. Hier gießen jedoch die ersten Aufsichtsbehörden für den Datenschutz schon wieder Wasser in den Wein. Sie verweisen darauf, dass bei Microsoft 365 weiterhin unklar sei, welche Daten Microsoft in den USA verarbeitet und was dabei geschieht.

Ob diese Behauptung zutrifft, sei dahingestellt. Dass der neue Angemessenheitsbeschluss nicht von der Pflicht befreit, die Datenverarbeitung transparent zu gestalten, steht auf alle Fälle fest. Sofern es Unklarheiten gibt, bietet der Angemessenheitsbeschluss keine Hilfe. Hier gilt es also weiterhin, Lösungen zu finden.

3 PFLICHTEN BEIM VERLUST MOBILER ENDGERÄTE

Mobile Endgeräte sind bei Dieben beliebt. Außerdem bleiben sie gern einmal auf der Parkbank liegen oder im ICE. Der Klassiker ist dabei der liegen gelassene Laptop. Worauf ist dann zu achten? Eines steht von vornherein fest: Wer einen solchen Verlust gegenüber seinem Unternehmen verschweigt, macht alles nur noch schlimmer!

So sieht eine peinliche Situation aus

Sie waren auf Geschäftsreise. Ihr Laptop hat Sie begleitet. Abends, zurück in Ihrer Wohnung, stellen Sie fest, dass der Laptop weg ist. Sie rekonstruieren, wo er geblieben sein könnte. Ein Anruf im Hotel, in dem Sie übernachtet haben, bleibt erfolglos. Also kann es nur im ICE oder im Taxi passiert sein. Am nächsten Morgen beginnen Sie mit entsprechenden Nachforschungen. Das dauert natürlich. Sollen Sie im Unternehmen jetzt schon etwas erzählen oder lieber einmal abwarten, ob sich das Problem noch von allein löst?

Der Kontrollverlust ist das Problem

Sicher kostet ein guter Laptop einiges. Falls er nicht wiedergefunden wird, hat das Unternehmen deshalb einen entsprechenden Schaden. Aus der Sicht des Datenschutzes liegt das eigentliche Problem aber woanders. Dieses Problem lautet: Kontrollverlust über das Endgerät! Das bedeutet gleichzeitig den Verlust der Kontrolle über die dort gespeicherten Daten. Die Vertraulichkeit dieser Daten ist möglicherweise nicht mehr gewährleistet. Das gilt jedenfalls dann, wenn sie nicht gut verschlüsselt waren. Außerdem sind die Daten nicht mehr verfügbar. Anders ist das höchstens dann, wenn sie beispielsweise über eine Cloud-Lösung auch noch an anderer Stelle gespeichert sind.

Das führt zu einem meldepflichtigen Datenschutzvorfall

Mit „meldepflichtiger Datenschutzvorfall“ ist gemeint, dass die zuständige Aufsichtsbehörde für den Datenschutz unterrichtet werden muss. Hinzu kommt die Information der Menschen, deren Daten betroffen sind. Natürlich kommt es bei alledem immer auf den Einzelfall an. Die gesetzlichen Vorschriften lassen manche Spielräume. Es gibt Ausnahmefälle, in denen eine Meldung an die Aufsichtsbehörde für den Datenschutz nicht erforderlich ist. Das sind aber Themen für Fachleute. Daher sollten Sie das auch den Fachleuten überlassen. Melden Sie deshalb den Verlust des Endgeräts gleich am nächsten Morgen im Unternehmen!

Eine Verschlüsselung ist in jedem Fall Gold wert

Normalerweise ist die Festplatte auf Ihrem Laptop verschlüsselt. Normalerweise bedeutet: wenn Sie nichts daran verändert haben. Sie sind sich unsicher? Fragen Sie im Unternehmen nach! Im günstigsten Fall ist alles in Ordnung und Sie können sehr beruhigt sein. Das hat einen einfachen Grund. Wenn eine Festplatte nach dem aktuellen Stand der Technik verschlüsselt ist, können Unbefugte normalerweise nicht auf die Daten zugreifen. Das beugt einer schlaflosen Nacht vor, wenn ein Laptop verloren geht. Es bringt aber auch viele rechtliche Vorteile für das Unternehmen.

Dank Verschlüsselung entfällt die Meldepflicht gegenüber der Aufsicht

Wenn die Kontrolle über personenbezogene Daten verloren geht, muss dies normalerweise der zuständigen Aufsichtsbehörde für den Datenschutz gemeldet werden. Wie erwähnt gibt es davon aber Ausnahmen. Die DSGVO formuliert das in schönem Juristendeutsch so: Wenn „die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt“, entfällt die Pflicht zur Meldung an die Aufsichtsbehörde (Art. 33 Abs. 1 Satz 1 DSGVO). Davon ist bei guter Verschlüsselung auszugehen.

Ihre Meldepflicht gegenüber dem Unternehmen bleibt aber bestehen

Wohlgemerkt: Es entfällt die Meldepflicht des Unternehmens gegenüber der Aufsichtsbehörde für den Datenschutz. Und auch das nur, wenn die Voraussetzungen dafür eindeutig erfüllt sind. Mit Ihrer eigenen Meldepflicht gegenüber dem Unternehmen hat das nichts zu tun. Sie ergibt sich aus dem Arbeitsvertrag. Denn das Unternehmen muss die Chance haben, den Vorfall zu untersuchen. Ansonsten steht rasch eine Abmahnung im Raum, wenn nicht mehr.

Eine gewisse Vorsicht wäre gut

Am besten wäre es natürlich, wenn Sie sich von vornherein so verhalten, dass nichts gestohlen wird und nichts verloren geht. Das ist leicht gesagt, aber oft schwer getan. Prüfen Sie vor allem, ob Sie das Gerät wirklich ständig bei sich haben müssen. Wenn nach der schwierigen Konferenz ein gemütliches Abendessen angesagt ist, könnten Sie den Laptop dorthin mitnehmen. Aber vielleicht hat das Hotelzimmer ja einen passenden Safe, in dem er viel besser untergebracht ist.

4 VORSICHT, SPIONAGE-APPS!

Sicherheitsforschende warnen vor einer Zunahme mobiler Apps, die die Nutzenden von Smartphones und Tablets ausspionieren. Chats, Anruflisten, E-Mails, Kontakte – nichts ist dann noch sicher, alles wird ausgespäht. Dabei stammen die Spyware-Apps nicht etwa nur aus zwielichtigen App-Stores, sondern auch aus offiziellen Quellen.

Wenn Sicherheitshinweise zu kurz greifen

Kein Wunder, wenn das mobile Endgerät verseucht ist, könnte man denken. Sicherlich hat die Nutzerin oder der Nutzer eine scheinbar nützliche App aus einem App-Store heruntergeladen, der nur so von Schadsoftware überquillt. Dabei lautet die Empfehlung der IT-Sicherheit doch schon seit Jahren, mobile Anwendungen niemals aus einem inoffiziellen App-Store zu beziehen.

In solchen App-Stores gibt es keine Kontrolle, dort kann jeder eine App zum Herunterladen anbieten. Das nutzen natürlich die Internetkriminellen aus und platzieren dort ihre Spionage-Software. Statt eine angeblich neuartige App mit tollen KI-Funktionen zu installieren, hat sich das Opfer eine Spyware eingefangen, die nun alle E-Mails, Chatnachrichten und Kontakte ausliest und an den Auftraggeber, also den Datendieb, überträgt.

Auch wenn genau das häufig genug passiert: Es kann auch alles ganz anders gewesen sein.

Jeder App-Store kann schädliche Apps enthalten

Leider zeigt sich, dass selbst die Nutzenden, die Apps nur aus dem offiziellen App-Store von Google oder Apple beziehen, in Gefahr sind, heimtückische Spyware-Apps zu installieren. Doch wie kann das sein? Prüfen diese App-Store-Betreiber etwa nicht, ob sich Schadsoftware unter den angebotenen Apps befindet?

Die Antwort lautet: Doch, das tun sie, aber es reicht nicht.

Zum einen erscheint jeden Tag eine unglaubliche Fülle an neuen Apps, ganz abgesehen von den zahllosen Updates, die zu bereits verfügbaren mobilen Applikationen veröffentlicht werden. Aus diesem Grund überprüfen die App-Stores die Apps in aller Regel automatisiert. Doch wie bei allen IT-Sicherheitslösungen existiert auch hier eine Fehlerrate. Es gibt also bösartige Apps, die bei einer Überprüfung nicht auffallen.

Zum anderen müssen die Apps bei der Erstinstallation gar nicht schädlich sein, aber die Applikation sieht vor, später weitere Inhalte, Funktionen oder auch Werbung zur Finanzierung der meist kostenlosen Apps nachzuladen. Wenn darunter Schadsoftware ist, kann das ein App-Store nicht vorab erkennen. Deshalb lautet die traurige Wahrheit, dass jeder App-Store bösartige Apps enthalten kann.

App-Sicherheit darf mit dem Download nicht enden

Die vorgelagerten Sicherheitsmaßnahmen der App-Store-Betreiber allein reichen also nicht aus. Es muss auch nach der Installation geprüft werden, ob sich die App gut oder böse verhält. Deshalb prüfen die offiziellen App-Stores auch nach der Installation noch die Sicherheit der bereits auf dem Gerät befindlichen Apps, so wie sie prüfen, ob ein Update erforderlich ist oder nicht.

Aber diese Prüfung kann nur punktuell erfolgen. Entscheidend ist, dass ein Endgerät immer eine aktive, professionelle Mobile-Security-Lösung hat, die dauerhaft auf verdächtige Aktivitäten

der Apps achtet. Das ist auch dann notwendig, wenn man sich zuverlässig daran hält, immer nur offizielle App-Stores zu nutzen. Andernfalls kann die neue App zu einem heimlichen Spion und Datenrisiko werden. Genau das passiert gegenwärtig sehr häufig, da Smartphones, Tablets und Apps immer beliebter und so zu einem attraktiven Angriffsziel und -werkzeug geworden sind.

Wissen Sie, wie Sie sichere Apps installieren?

Machen Sie den App-Test!

Offizielle App-Stores bürgen für sichere Apps. Stimmt das?

1. Nein, leider können auch dort schädliche Apps versteckt sein, trotz der Kontrollen der App-Store-Betreiber.
2. Ja, schädliche Apps gibt es nur in den inoffiziellen App-Stores, die man meiden muss.

Lösung:

Die Antwort 1. ist richtig. Zweifellos ist das Risiko, eine Spionage-App zu installieren, bei unkontrollierten, inoffiziellen App-Stores höher. Doch auch im Google Playstore und im App-Store von Apple finden sich immer wieder gefährliche Apps, die bei der Überprüfung nicht gleich erkannt wurden. Auch bei der Verwendung der offiziellen App-Stores sind zusätzliche Sicherheitslösungen auf Smartphone und Tablet erforderlich.

Die Sicherheit bei der Installation der Apps ist entscheidend. Ist das so?

1. Ja, hat man eine sichere App installiert, ist das Risiko von mobiler Spyware gebannt.
2. Nein, anfangs harmlose Apps können später bösartig werden, die Apps müssen dauerhaft überprüft werden.

Lösung:

Die Antwort 2. ist richtig. Mobile Apps erhalten in kurzer Folge immer wieder Aktualisierungen, um Fehler zu beheben und Funktionen zu erweitern. Bei diesen Updates und Upgrades können die Apps auch mit bösartigen Funktionen versehen werden. Zudem laden Apps Inhalte oder Werbeanzeigen nach, zum Beispiel aktuelle Videos oder Nachrichten, aber auch Werbung (In-App-Advertising), die oftmals der Finanzierung der Apps dient. Diese neuen Inhalte können Schadsoftware mit sich führen. Apps müssen deshalb nicht nur im App-Store überprüft werden, sondern fortlaufend, auch nach der Installation.

IMPRESSUM

Redaktion

Dr. Uwe Günther
Sanovis GmbH
Riedenburger Straße 7
81677 München
089 9927579-22
Uwe.Guenther@Sanovis.com

Stefan Strüwe, RA
CURACON GmbH Wirtschaftsprüfungsgesellschaft
Am Mittelhafen 14
48155 Münster
0251 92208-209
Stefan.Struewe@Curacon.de