NEWS BOX DATENSCHUTZ

INHALTSVERZEICHNIS

2 Editorial
3 Lieferantenmanagement leicht gemacht
4 LIVE-HACKING: Praxisbeispiele für Angriffe auf mobile Endgeräte
5 ChatGPT im Einsatz: KI als Schlüssel zur Optimierung von Geschäftsprozessen
6 Zwischen Effizienzoptimierung und Menschenrechten
7 Impressum

SONDERAUSGABE

HAMBURGER DATENSCHUTZTAGE

Dr. Michael Foth,
Geschäftsführer
IBS data protection services and consulting GmbH

EDITORIAL

Eine immer weiter voranschreitende Digitalisierung prägt unsere Welt. Künstliche Intelligenz (KI) ist ein allgegenwärtiger Begriff – ein Terminus, der vor einigen Jahrzehnten nicht existierte, in den letzten Jahren schon von vielen, aber heute von der breiten Masse „verstanden" und benutzt wird.
Die Implementierung von KI in Unternehmen erfordert oft erhebliche Investitionen in die Technologie, Schulung und Integration. Doch aufgrund der zahlreichen Vorteile, wie gesteigerter Effizienz und Innovationspotential, setzen viele Unternehmen bereits regelmäßig KI ein. Dies erfordert eine verantwortungsbewusste Datenverwaltung und einen verantwortungsbewussten Umgang. Die Systeme können komplex sein und es muss das ein oder andere Hindernis überwunden werden.
In dieser Zeit gilt daher umso mehr: Daten schützen, KI meistern! Das Leitmotiv der diesjährigen Hamburger Datenschutztage. Selbstverständlich drehen sich in der Datenwelt und auch bei den Hamburger Datenschutztagen nicht alle Themen nur um KI. Die Gesetzgeber stellen die Unternehmen durch zunehmende Regulierungen vor diverse Herausforderungen und sorgen dafür, dass es für Unternehmen, Rechtsanwälte, Datenschutz- und Informationssicherheitsbeauftragte nicht langweilig wird. Auch diese Aspekte werden natürlich behandelt.

Wir freuen uns, auch in diesem Jahr eine Plattform für gemeinsamen Austausch und gemeinsame Weiterentwicklung zu bieten und erneut die Hamburger Datenschutztage zu veranstalten. Vom 13. bis zum 14. Juni 2024 erwarten Sie ausgezeichnete Experten, die zu den aktuellsten und relevantesten Themen referieren und mit Ihnen in den Dialog treten. Die neusten Rechtsakte der Europäischen Union, weltweite Neuerungen der Datenschutzbestimmungen, Cybercrime, Hinweisgeberschutz, Tracking & Cookies, faszinierende Aspekte der KI und vieles mehr wird beleuchtet.
Freuen Sie sich auch im Jahr 2024 auf zwei erkenntnisreiche Tage. Nutzen Sie die Gelegenheit, sich mit Ihren Kollegen und den Referenten zu vernetzen, aktiv am Dialog teilzunehmen und fühlen Sie sich herzlich eingeladen, sich am Diskurs zu beteiligen. Seien Sie dabei und erleben Sie die neuesten Diskussionen hautnah!

Mit herzlichen Grüßen

Ihr
Michael Foth

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Foto: metamorworks, Adobe Stock

Lieferantenmanagement leicht gemacht

Wie Synergien aus dem Datenschutz, der Informationssicherheit und dem KI-Management in der Praxis genutzt werden können.

Für Datenschutz- und Informationssicherheitsbeauftragte (DSB; ISB) ist das immer komplexer werdende Lieferantenmanagement Teil des Alltags. Neben den Vorgaben des Datenschutzrechts und der Informationssicherheit wird auch die Regulierung von künstlicher Intelligenz (KI) bei der Steuerung von Lieferanten eine große Rolle spielen. Bestehende Prozesse müssen angepasst und alle relevanten Stakeholder involviert werden. Hierbei verschlankt ein gemeinsames Lieferantenmanagement die Prozesslandschaft und ermöglicht einen gezielteren Ressourceneinsatz.

Die Grundlage für eine erfolgreiche Zusammenarbeit ist das Verständnis der gemeinsamen Ziele und der Mindestanforderungen.

Beispielsweise werden im Rahmen der Prüfung eines Auftragsverarbeitungsvertrags die technischen und organisatorischen Maßnahmen (TOM) des Lieferanten überprüft. In der Vergangenheit konnte es bei diesem Thema schnell zu Missverständnissen zwischen DSB und ISB kommen, da die alte ISO 27001 die Begriffe nicht direkt nutzte. Mit der neuen ISO 27001:2022 hat sich dies jedoch geändert.
Ebenfalls ist zu beachten, dass eine Zertifizierung wie nach der ISO 27001 allein nicht den Anforderungen des Art. 32 Datenschutz-Grundverordnung (DS-GVO) genügt. Sie kann jedoch ein zusätzlicher Indikator für einen hohen Sicherheitsstandard eines Auftragsverarbeiters sein.

Anforderungen aus dem KI-Management

Die Anforderungen für Lieferanten von KI-Lösungen werden verschärft. Besonders stark reguliert werden nach der KI-Verordnung die Anbieter (Entwickler) von Hochrisiko-KI-Systemen. Als Nutzer müssen sich Organisationen darauf verlassen, dass Lieferanten die Vorgaben der KI-Verordnung einhalten, und es ist notwendig, dies zu überprüfen.
Beim Aufbau einer KI-Governance können sich die Unternehmen an der ISO 42001:2023 orientieren, die konkrete Anforderungen an den Datenschutz und die Informationssicherheit adressiert.
Weitere Details, Vorlagen sowie Erfahrungs- und Praxisberichte zu diesem Thema erhalten Sie im gleichnamigen Pre-Seminar („Lieferantenmanagement leicht gemacht") im Rahmen der 11. Hamburger Datenschutztage am 12. Juni 2024.

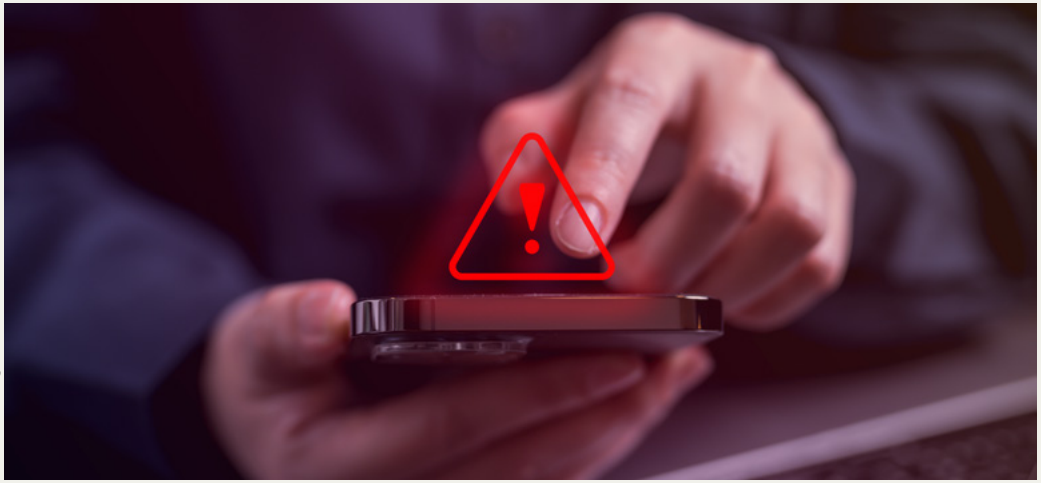

Foto: 1st footage, Adobe Stock

LIVE-HACKING: Praxisbeispiele für Angriffe auf mobile Endgeräte

Mobile Endgeräte sind der ständige Begleiter fast aller Menschen. Viele sind sich der Sicherheitsrisiken nicht bewusst oder ignorieren diese bewusst. Doch welche Folgen hat dieses Verhalten?

Handys, Laptops, Tablets, Smartwatches und Co. sind die Kommunikationsmittel der Gegenwart und der Zukunft. Sie begleiten nahezu jeden Menschen, und ihre Nutzung ist Ausdruck des Allgemeinen Persönlichkeitsrechts aus Art. 2 I i. V. m. Art. 1 I Grundgesetz (GG). Es hat sich jedoch gezeigt, dass die Nutzung dieser vielfältigen Gerätschaften auch Gefahren für den Schutz der Nutzerdaten birgt. Spähaktionen finden nicht nur durch die NSA und nicht nur bei großen Unternehmen statt. Auch Privatpersonen werden gehackt.

Hacker

Hacker spähen nicht nur vertrauliche Nachrichten und persönliche Bilder aus, sondern auch Standort- oder Kontaktdaten sowie Zugangsdaten zu weiteren Konten. Diese erlangten Daten können für den Verwender abhängig von dem jeweiligen Einsatz sehr wertvoll sein und immense Schäden bei dem jeweiligen Inhaber anrichten. Ein Verstoß gegen das Fernmeldegeheimnis steht nach § 206 Strafgesetzbuch (StGB) sogar unter Strafe und dennoch kommt es immer wieder vor, dass Daten gehackt werden.
Also wie wird der Schutz des Telekommunikationsgeheimnisses aus Art. 10 GG in diesem Zusammenhang gewährleistet?

Mobile Security

Wenn ein Brief verschickt wird, wird in der Regel auch ein Briefumschlag verwendet. Nicht nur, um einen einfacheren Transport zu ermöglichen, sondern auch, um den Inhalt nicht jedem zugänglich zu machen. Ähnlich sollte es sich mit digitalen Inhalten verhalten. Sie können verschlüsselt und beispielsweise durch eine Zwei-Faktor-Authentifizierung gesichert werden. Dennoch zeigt sich bei manchen Menschen eine erstaunliche Gelassenheit, wenn es um ihre digitalen Daten geht.

Vertrauen in den Grundrechtsschutz

Reicht es aus, dass die Vertraulichkeit des Wortes und der Schutz der Daten grundrechtlich geschützt sind? Deutsche Behörden sind über Art. 1 III GG an die Grundrechte gebunden. Sie müssen das Telekommunikationsgeheimnis wahren und ein angemessenes Niveau zum Schutz vor Eingriffen Dritter gewährleisten. Zwischen Privaten kommen die Grundrechte allenfalls über die unmittelbare Drittwirkung zur Geltung. Auch die Berufung auf den Grundrechtsschutz kein Allheilmittel, stattdessen sind Vorsorge und Sensibilität erforderlich.
Weitere Überlegungen und Hinweise zu diesem Thema gibt Marco di Filippo im 3. Vortrag der diesjährigen 11. Hamburger Datenschutztage.

Foto: Timon, Adobe Stock

ChatGPT im Einsatz: KI als Schlüssel zur Optimierung von Geschäftsprozessen

Muster in Daten erkennen, Texte generieren und Berichte erstellen – für diese Tätigkeiten. kann man menschliches Personal einsparen und KI einsetzen.

In einer Zeit, in der Daten in nahezu jeder Branche zu einem zentralen Gut geworden sind, spielt die KI eine unbestreitbare Rolle. Durch den Einsatz fortschrittlicher KI-Technologien können nicht nur Branchen, sondern auch einzelne Geschäftsprozesse fundamental umgestaltet werden.

Prozesse, die optimiert werden können

Jeder kennt die von OpenAI entwickelte KI ChatGPT oder hat zumindest davon gehört. Dieses textbasierte KI-Modell ist darauf spezialisiert, Muster in Daten zu erkennen und kann bei der Verarbeitung von Sprache und der Erstellung von Berichten ideal eingesetzt werden. Es gibt aber auch KI-Modelle, die Gespräche und Präsentationen erstellen, Verhalten von Kunden analysieren, personalisierte Empfehlungen und Angebote generieren und sogar Vertragsdaten analysieren und prüfen.
Macht das die Menschen ersetzbar? Mitnichten, zumindest nicht überall, aber für erste Schritte und Vorarbeiten kann es die Arbeit massiv erleichtern. Zu denken ist im Bereich des Kundenservice und Kundensupports z.B. an KI-basierte Chatbots. Sie können häufig gestellte Fragen beantworten und kleinere Probleme lösen, bis ein menschlicher Mitarbeiter benötigt wird.

Datenschutz und Innovation

Auch beim Einsatz von KI-Technologien muss der Datenschutz gewährleistet bleiben. Dies ermöglichen anonymisierte Daten, Verschlüsselungstechniken, eingeschränkte Zugriffe und Datenschutzrichtlinien und Compliance. KI-Systeme können so programmiert werden, dass sie automatisch Datenschutzrichtlinien und gesetzliche Vorschriften einhalten.

Die Zukunft der Prozessoptimierung

Wer im digitalen Zeitalter mithalten will, sollte sich der KI-Technologie nicht verschließen. Sie hilft Unternehmen wettbewerbsfähig zu bleiben, bietet unter Umständen kostengünstigere und damit kundenfreundlichere Lösungen.
Anhand konkreter Praxisbeispiele erläutert Marcus Herold auf den Hamburger Datenschutztagen 2024 den Einsatz von KI zur Prozessoptimierung – Seien Sie dabei!

Foto: Peopleimages - AI, Adobe Stock

Zwischen Effizienz-optimierung und Menschenrechten

In welche Welt führt uns die KI-Verordnung?

Die fortschreitende Integration von KI in verschiedene Bereiche des täglichen Lebens hat sowohl Chancen als auch Herausforderungen mit sich gebracht. Während KI-Technologien erhebliche Effizienzsteigerungen und Innovationen ermöglichen, sind gleichzeitig ethische und rechtliche Fragen aufgetaucht, mit denen sich die KI-Verordnung auseinandersetzt.

Einführung der KI-Verordnung

Die Europäische Union hat die KI-Verordnung erlassen, um die Nutzung von KI in Europa zu regeln und sicherzustellen, dass sie im Einklang mit den Menschenrechten und anderen Grundrechten steht. Damit ist sie weltweit die erste Verordnung, die ein umfassendes Regelwerk für KI bildet. Sie schafft nach Auskunft der Bundesregierung einen Ausgleich zwischen Innovation und Risikoschutz. Sie beinhaltet die Gewährleistung von Datenschutz, Nichtdiskriminierung, Transparenz und Rechenschaftspflicht.

Analyse des Risikoansatzes und Streitfragen zur KI

Im Rahmen des Trilogs wurden verschiedene Aspekte der KI-Verordnung intensiv diskutiert. Neben der Analyse des Risikoansatzes standen insbesondere die Streitfragen zur generativen und prädiktiven KI im Fokus. Besonderes Augenmerk wurde dabei auf die rechtsstaatlichen Gefahren von Black-Box-Modellen gelegt. Diese Modelle, darunter auch Foundation-Modelle, werfen Fragen zur biometrischen Fernidentifizierung auf und erfordern eine eingehende Einbeziehung in den Regelungsrahmen.

Herausforderungen und Chancen: Legitimität der Regelung

Eine zentrale Frage betrifft die Legitimität der KI-Verordnung. Hat die EU es geschafft, eine Regelung vorzulegen, die den rechtsstaatlichen Anforderungen genügt? Oder trägt sie möglicherweise zur umfassenden Legitimierung selbstlernender Systeme im Alltag bei? Diese Frage ist von entscheidender Bedeutung für die Abwägung zwischen Effizienzoptimierung durch KI und dem Schutz grundlegender Menschenrechte.

Balance zwischen Innovation und Ethik

Die Einführung der Verordnung durch die EU ist ein bedeutender Schritt, um den Einsatz von KI in Europa zu regulieren. Doch zugleich muss sichergestellt werden, dass die Verordnung den ethischen und rechtlichen Herausforderungen gerecht wird, die mit der Entwicklung und Nutzung von KI einhergehen. Die KI-Verordnung kann nur dann ihre beabsichtigten Ziele erreichen und dazu beitragen, eine verantwortungsbewusste und gerechte Nutzung von KI in Europa zu fördern, wenn sie die Balance zwischen Innovation und Ethik wahrt.
Wenn Sie eine kritische Beleuchtung des Regelungsansatzes der KI-Verordnung hören und mitdiskutieren möchten, besuchen Sie die diesjährigen 11. Hamburger Datenschutztage und freuen Sie sich auf Prof. Dr. Johannes Caspar.

Impressum

DATAKONTEXT GmbH
Augustinusstraße 11 A
50226 Frechen

Telefon: +49 2234 98949-30
Fax: +49 2234 98949-32

kundenservice@datakontext.com
www.datakontext.com

Geschäftsführung:
Dr. Karl Ulrich
Amtsgericht Köln, HRB 82299

Newsletter

Möchten Sie bei Erscheinen der aktuellen Datenschutz Newsbox informiert werden und so keine Ausgabe mehr verpassen? Dann tragen Sie sich unverbindlich und kostenlos ein unter:
www.datakontext.com/newsletter