Newsletter 10/2024

FOX Group

Künstliche Intelligenz-Richtlinie – was ist das?

Die Künstliche Intelligenz (KI) wird in der Wirtschaft als Innovation und Wirtschaftsmotor gesehen. Kaum ein Unternehmen, das sich nicht mit der Thematik auseinandergesetzt hat. Ob im Marketing oder in der Produktentwicklung, die Künstliche Intelligenz soll im Berufsalltag als Arbeitserleichterung eingesetzt werden.

Eine KI-Richtlinie setzt hierbei klar die Regeln, nach denen die KI einzusetzen ist, welche Ziele sie mit dem Einsatz von KI erreichen wollen, wo eine KI nicht eingesetzt werden soll und welche Standards dabei gelten. Eine KI-Richtlinie ist deshalb essenziell, um Rechtsverstöße im Unternehmen zu verhindern. Mitarbeitenden ist oft nicht bewusst, wo die rechtlichen Risiken beim Einsatz von den mittlerweile frei verfügbaren KI-Anwendungen liegen.

Zu berücksichtigen ist, dass Rahmenbedingungen in Form einer Richtlinie gesetzt werden, damit sensible und geschützte Informationswerte aus den Bereichen des Geschäftsgeheimnisses, des Datenschutzes, des Urheberrechts und der Vertraulichkeit das Unternehmen nicht versehentlich verlassen.

Gefahr durch Makros in vorhandenen Word-Dokumente

Der Erfolg des Emotet-Virus ist darauf zurückzuführen, dass veraltete Dokumente im Unternehmen weiterhin Verwendung finden. Es gibt kaum ein Unternehmen, das seine Dokumentenablage nicht über Microsoft M365 tätigt. Die größte Gefahr liegt bei den unzähligen veralteten Windows Dokumentenformaten (**DOC, DOT, DOCM, DOTM, XLA, XLS, XLT, XLSB, XLSM, XLTM, XLAM, PPT, PPTM, POTM, PPSM, PPAM, PPA)** selbst, die seit über zehn Jahren als veraltet gelten und damit keine Berechtigung im modernen Dokumentenaustausch mehr haben.

Wir erhalten vereinzelt Dokumente per E-Mail mit diesen Endungen, die von unserem Viren-Scanner geblockt werden. So schützen wir uns vor möglichen Attacken per E-Mail-Anhang. Auch veraltete pdf Dokumente können eine Gefahr bedeuten.

Trotz aller technischer und organisatorischer Maßnahmen (Firewall, Spam-Abwehr, Virenscanner, Sichere Einstellungen, Warnmeldungen) sind immer noch die Beschäftigten der entscheidende Faktor. Sie sollten besonders kritisch darauf achten, diese Datei-Endungen nicht zu öffnen, geschweige denn – ggf. erneut - in Umlauf zu bringen.

Erst kürzlich wurde der renommierte Heise-Verlag, der unter anderem mit c't und heise online selbst IT-Fachmedien-Spezialist ist, Opfer von Emotet. Ein Mitarbeiter öffnete arglos ein Word-Dokument mit der Endung „doc" und damit eine (gefälschte) Fehlermeldung, die den Mitarbeiter aufforderte, ein hinterlegtes Makro zu aktivieren. Dieser Aufforderung kam der Mitarbeiter nach. Emotet legt u.a. IT-Systeme lahm oder dringt ein, um an sensible Daten zu gelangen.

Die Aufräumarbeiten nach einem Cyberangriff gehen meist so weit, dass Unternehmen ihre komplette Infrastruktur erneuern müssen. Nur so lässt sich sicherstellen, dass bei der Bereinigung der befallenen Server nicht doch ein Virus übersehen wurde und die Infektion weiterhin vorhanden ist.

Es empfiehlt sich, im E-Mail-Server den Empfang und das Versenden dieser Dokumentenformate zu blockieren. Datenordner mit Word-, Excel- und PowerPoint-Vorlagen sind zu erneuern bzw. zu löschen und gezielte Säuberung der Firmenlaufwerke sind durchzuführen, damit Hacker keine Chance haben.

Versehentlich E-Mails an falsche Adressaten

Statistisch gesehen sind 13,5 % aller Datenschutzverletzungen darauf zurückzuführen, dass Mitarbeitende versehentlich sensible Informationen an den falschen Adressaten schicken. Die Dunkelziffer ist mit großer Wahrscheinlichkeit höher. Die Funktion „E-Mail zurückrufen“ ist hierfür wenig zielführend.

Aus Sicht des Datenschutzes ist ein solcher Fehlversand ein Datenschutzvorfall, sobald sensible Informationen, die für autorisierte Mitarbeitende oder Dienstleister bestimmt waren, an einen unbefugten Empfänger weitergeleitet wurden. Solch ein Fehlversand passiert schnell, insbesondere dann, wenn Menschen mobil arbeiten bzw. unter Zeitdruck stehen. E-Mail-Zwischenspeicher (Cache) und die Auto-Fill Funktion erhöhen die Wahrscheinlichkeit eines Fehlversands.

Eine Richtlinie zum sicheren Umgang mit Dokumenten oder der zusätzliche Einsatz von Software minimiert das Risiko. Auch eine Informationsveranstaltung zum Umgang mit Informationen im Unternehmen kann das Bewusstsein erhöhen.

Eine weitere technische Variante besteht darin, dass die E-Mail z.B. zuerst eine voreingestellte Zeit im Postausgang aufbewahrt wird, wo der Versand gestoppt werden kann, bevor sie schlussendlich zeitverzögert im Ordner „gesendete Elemente“ auftaucht. Dies lässt sich als Regel einrichten und eingrenzen. Es gilt zu klären, ob auch die internen E-Mails zeitverzögert verschickt werden sollen bzw. ein gewisser Personenkreis von Empfängern von dieser Regel auszunehmen ist, um Verzögerungen in der Zusammenarbeit zu vermeiden.

Diese Variante funktioniert im regulären E-Mail-Empfang (An:) als auch in der Kombination mit dem „Carboin Copy“ (cc:) sowie zusammen mit dem Blind Carbon Copy (Bcc:). Wissenswert ist: Stehen alle Empfangsadressen im Bcc greift der verzögerte Versand nicht.

Impressum

complimant AG, Edt 4, 84558 Kirchweidach

Vorstand: Franz Obermayer, Ann-Karina Wrede

Vorsitzender des Aufsichtsrates: Christian Volkmer

Telefon: +49 8683 99390-40

E-Mail: info@complimant.de / datenschutz@complimant.de

www.complimant.de

Eintragung im Handelsregister: Amtsgericht: Traunstein

Registernummer: HRB 20500 Steuernummer: 141/120/07009

Umsatzsteuer-Identifikationsnummer gemäß §27a

Umsatzsteuergesetz: DE274380239

Verantwortlich für den Inhalt nach § 55 Abs. 2 RStV Franz Obermayer