ITDSC UG
Data-Security-Consulting
www.itdsc.de

Informationen zum Thema Datenschutz

Liebe Leserin, lieber Leser,

Ein weiteres Thema in dieser Ausgabe sind die Schwachstellen in der IT, die Cyberangriffe ermöglichen

und so zu immer mehr Datenschutzverletzungen beitragen.

Sie erfahren dabei, dass es nicht nur neue IT-Sicherheitslücken sind, die zu einer großen Gefahr werden können.

Nicht zuletzt beleuchtet diese Ausgabe die Datenschutzprobleme, die bei der Nutzung von KI-Diensten wie ChatGPT auftreten könnten.

Machen Sie am besten gleich den Wissenstest dazu auf der letzten Seite.

Ich wünsche Ihnen viel Spass beim Lesen.

Detlef Riese
Datenschutzbeauftragter

Keine Updates in der IT, kein Datenschutz

Denken Sie auch, dass die vielen Aktualisierungen in der IT lästig sind? Doch ein Verzicht auf regelmäßige Updates würde den Datenschutz und die Datensicherheit aushöhlen: Viele Datenpannen geschehen, weil es offene Sicherheitslücken in der IT gibt.

Nervige Updates?

Kaum ein Tag vergeht, an dem nicht eine Aktualisierung für IT-Geräte heruntergeladen und eingespielt werden muss. Ob im Beruf oder im Privatleben: Die Apps auf Smartphones und Tablets, die Betriebssysteme und Anwendungen auf den PCs und Notebooks, ja sogar die Fernbedienung und das Smart-TV benötigen immer wieder eine Aktualisierung der Software.

Dabei sind neue Funktionen und Erweiterungen eher die Ausnahme. Schaut man sich an, warum eine Aktualisierung ansteht, wird das Update meist mit notwendigen Fehlerbehebungen begründet. Die meisten Fehler aber sind Probleme für den Betrieb des Geräts und für die Sicherheit der Daten.

IT-Fehler sind oftmals Schwachstellen

Die Fehler in der Software passieren meist ungewollt während der Entwicklung. Die Programmiererinnen und Programmierer entdecken ihre Fehler erst spät oder sogar zu spät. Internetkriminelle suchen aktiv nach Fehlern in der IT, um sie auszunutzen und zum Beispiel Berechtigungen und Zugriffsmöglichkeiten zu erlangen, die sie nicht haben sollten.

Die Fehler in der IT sind deshalb auch Schwachstellen oder Sicherheitslücken. Sie machen die gefürchteten und immer stärker zunehmenden Cyberangriffe erst möglich. Eine IT ohne Schwachstellen ließe sich nicht missbrauchen, doch leider gibt es keine fehlerfreie IT.

Wenn Updates zu spät kommen

Kommt es zu einem Angriff, bevor die Schwachstelle durch Updates, auch Patches genannt, behoben ist, haben die Internetkriminellen und Datendiebe meist leichtes Spiel. Viele Datenschutzverletzungen entstehen durch solche Cyberattacken, die IT-Schwachstellen ausnutzen. Tatsächlich sind IT-Sicherheitslücken und entsprechende Angriffe inzwischen eine der Hauptursachen für Datenpannen, wie die Datenschutzaufsichtsbehörden regelmäßig melden.

Nun könnte man denken, die Schwachstellen werden nicht rechtzeitig behoben, weil es keinen Patch dafür gibt. Das kommt zwar vor. Doch sehr häufig würde es durchaus schon ein Sicherheitsupdate geben, aber das jeweilige Unternehmen oder der betroffene Nutzende haben das verfügbare Update nicht installiert. Teils liegt dies an der Unkenntnis, dass es bereits ein Update gibt. Teils wird aber auch der Aufwand für die vielen Aktualisierungen gescheut.

So sagte zum Beispiel Marit Hansen, die Landesbeauftragte für Datenschutz Schleswig-Holstein: „Mit Sorge blicke ich auf das Thema Informationssicherheit“. So hätten immer noch viele Organisationen ihre Hausaufgaben nicht gemacht, um bekannte Schwachstellen in IT-Systemen zu beseitigen. „Die Datenpannen-Meldungen zeigen uns, wie solche Sicherheitslücken immer wieder ausgenutzt werden und oft auch Daten abfließen können“, so Marit Hansen weiter.

Viele Schwachstellen bleiben offen, obwohl ein Update verfügbar wäre

Ein Beispiel zeigt, wie gefährlich es sein kann, ein verfügbares Update nicht zu installieren. So berichtete das Bundesamt für Sicherheit in der Informationstechnik (BSI) davon, dass bei einem weltweit breit gestreuten Angriff Tausende Server mit Ransomware infiziert und kriminell verschlüsselt wurden, um Lösegeld zu erpressen. Dabei nutzten die Angreifer eine Schwachstelle in einer bestimmten IT-Lösung aus, die bereits lange bekannt war und für die es schon länger eine Fehlerbehebung gab.

Es ist zwar auch richtig und wichtig, eine bereits ausgenutzte Schwachstelle zu schließen, also „die Tür zu schließen“, durch die die Angreifenden gekommen waren. Doch weitaus besser wäre es, nicht erst nach dem erfolgreichen Angriff die Empfehlungen zur Behebung der Schwachstellen zu lesen und umzusetzen. Mit dem erfolgreichen Angriff ist es sehr oft bereits zu einer Datenpanne gekommen.

Tipp: Priorisieren, Automatisieren und die Bedeutung der Updates bedenken

Statt die Vielzahl der Updates zu beklagen oder sogar verfügbare Updates nicht zu installieren, sollten Unternehmen wie auch Privatpersonen überlegen, wie sie den zweifellos bestehenden Aufwand verringern, aber auch rechtfertigen können.

Zum einen sind nicht alle Updates gleichermaßen kritisch. Denn die möglichen Folgen einer offenen Schwachstelle unterscheiden sich. In Schwachstellen-Datenbanken gibt es deshalb zu Schwachstellen und Updates in aller Regel eine Bewertung, wie hoch das Risiko durch die jeweilige Schwachstelle ist.

Sind der mögliche Schaden und die Wahrscheinlichkeit eines Angriffs hoch, muss die betreffende Schwachstelle eine hohe Priorität zur Behebung erhalten. Dabei sollten möglichst Lösungen genutzt werden, die Updates automatisch herunterladen und installieren oder aber zumindest auf die verfügbaren Updates hinweisen.

Nicht zuletzt sollte man bedenken: Ohne Updates ist heute kein Datenschutz mehr möglich. Es würden Löcher bleiben, durch die Daten abfließen können, Datenpannen wären oft die Folge. Updates gehören deshalb zum Datenschutz dazu.

Wenn die KI zum Datenleck wird

Datenschützer warnen schon länger davor, dass die unbedachte Nutzung von Künstlicher Intelligenz (KI) zum Risiko für die Privatsphäre werden kann. Dienste wie ChatGPT sorgen nun für eine einfache Verbreitung von KI in Unternehmen und Haushalten. Höchste Zeit, den Umgang mit KI zu hinterfragen.

KI: Mehr als ein nützlicher Assistent

Der Chatbot antwortet druckreif auf jede Frage, oder die App malt ein Bild nach Anweisung und im gewünschten Stil – eine breite Öffentlichkeit hat in den vergangenen Wochen und Monaten ausprobiert, was Künstliche Intelligenz inzwischen leisten kann, berichtete der Digitalverband Bitkom. Rund drei Viertel der Bundesbürgerinnen und Bundesbürger (73 Prozent) sind nun der Meinung, dass KI eine Chance ist.

Auch Unternehmen sind offen für KI-Dienste wie ChatGPT & Co: Bereits jedes sechste Unternehmen plant laut Bitkom den KI-Einsatz zur Textgenerierung. „Die aktuellen Entwicklungen in der Künstlichen Intelligenz ermöglichen es uns, erstmals direkt mit der KI zu interagieren, und schaffen völlig neue Einsatzbereiche quer durch alle

Branchen“, sagte Bitkom-Präsident Achim Berg. „KI wird künftig zum Büroalltag genauso dazugehören wie heute der PC. KI hat das Potenzial, die massiven Auswirkungen der demografischen Entwicklung und des sich verschärfenden Fachkräftemangels abzufedern.“

Datenschützer sind alarmiert

Datenschutzaufsichtsbehörden weisen auch auf mögliche Risiken hin. KI-Systeme wie ChatGPT, die plötzlich zur Internet-Suche oder zum Schreiben von Texten zu allen möglichen Zwecken Verwendung finden: eine gute Sprachqualität, doch „ausgedachte“ Behauptungen werden wie echte Fakten präsentiert, Betroffenenrechte laufen leer, überzeugende Antworten auf die Fragen des Datenschutzes fehlen, so zum Beispiel das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein.

Als erste Aufsichtsbehörde in Europa hatte die italienische Datenschutzbehörde der Firma OpenAI untersagt, personenbezogene Daten von italienischen Bürgerinnen und Bürgern im Rahmen der Anwendung ChatGPT zu verarbeiten. Zu klären ist insbesondere, wie mit personenbezogenen Daten der Nutzer oder Dritter umgegangen wird. Wer speichert sie, zu welchem Zweck und wie lange?

Neue und verschärfte Sicherheitsrisiken

IT-Sicherheitsforschende warnen davor, dass solche KI-Dienste dafür genutzt werden könnten, bei Cyberangriffen die Opfer leichter zu täuschen, indem zum Beispiel „erfolgreiche“ Phishing-Mails leichter zielgenau erstellt werden können.

Doch auch legitime Nutzerinnen und Nutzer könnten mit solchen KI-Diensten die Datensicherheit aushöhlen, indem sie dem KI-Service vertrauliche Daten übermitteln, die in den Datenbestand des Dienstes aufgenommen, ausgewertet und an Dritte ausgegeben werden könnten. Zum Beispiel könnte womöglich der Versuch, ein Bewerbungsschreiben per KI optimieren zu lassen, zu einer ungewollten Datenweitergabe an Dritte führen.

Verschiedene Unternehmen haben bereits intern Verbote erlassen, vertrauliche Daten in Dienste wie ChatGPT einzutragen. Dieser Gefahr sollten sich aber alle Nutzenden bewusst sein.

Wissen Sie, wie KI-Dienste zum Datenleck werden könnten? Machen Sie den Test!

Frage: Wenn man in einen KI-Dienst seine eigenen Daten eingibt, damit diese zum Beispiel in einen professionellen Lebenslauf verwandelt werden, bleibt dies vertraulich. Stimmt das?

1. Nein, es ist nicht ohne Weiteres auszuschließen, dass die eingegebenen Daten in den gesamten Datenbestand aufgenommen werden.
2. Ja, jede Nutzung eines KI-Dienstes ist so vertraulich wie ein Gespräch unter vier Augen, nur zwischen KI und Nutzer oder Nutzerin.

Lösung: Die Antwort 1. ist richtig. KI-Dienste sind darauf angelegt, zu „lernen“, also auf die Eingaben der Nutzenden zu reagieren, um die Antworten immer weiter zu optimieren. Dabei ist es die Idee von KI, aus möglichst vielen Quellen Daten zu beziehen. Ob die Daten dann später für andere Zwecke genutzt werden als die ursprünglichen, ist eine Frage an den Datenschutz, den die KI gewährleistet. Automatisch kann man nicht von der Einhaltung der Zweckbindung ausgehen.

Frage: Antworten, die eine KI gibt, sind sorgfältig geprüft und vertrauenswürdig. Ist das so?

1. Ja, jede KI basiert auf einer Qualitätssicherung, sodass man den Ergebnissen vertrauen kann.
2. Nein, die Antworten können fehlerhaft sein. Eine weitere Prüfung ist notwendig.

Lösung: Die Antwort 2. ist richtig. KI-Expertinnen und Experten warnen davor, einer KI einfach zu vertrauen. KI-Lösungen sind nicht fehlerfrei. Es kann sogar sein, dass Dritte eine KI so trainiert haben, dass sie gezielt falsche Antworten gibt, um zum Beispiel Nutzende zu manipulieren. Dazu werden die Trainingsdaten „vergiftet“. Man spricht von Data Poisoning. Es ist denkbar, dass über Antworten von KI Nutzende zu Aktivitäten verleitet werden sollen, die Sicherheitslücken und Datenpannen nach sich ziehen, wie zum Beispiel die Preisgabe von Zugangsdaten und Geschäftsgeheimnissen.

Impressum

Detlef Riese (ITDSC UG)
Datenschutzbeauftragter
Anschrift:
ITDSC UG • Bethanienstrasse 8 • 03172 Guben
Telefon: 03561 5595574 • E-Mail: d.riese@itdsc.de