Port7

hüneborn | it

Ich weiß, was Du gestern getan hast!

Künstliche Intelligenz in der Suche auf Ihrem PC

Artikel von Jürgen Hüneborn, | Fachanwalt für IT-Recht in Münster
07.06.2024

Microsoft Recall wird den PC, also den „Personal Computer“, etwas weniger persönlich machen, als vielen Recht sein dürfte.
Wir erklären Ihnen, warum.

Microsoft hat die Funktion „MS Recall“ relativ überraschend und kurzfristig als zusätzlichen Assistenten für den MS-Copilot angekündigt.

Die Funktion soll als erweiterte und intelligente Suchfunktion für den Desktop dienen, da sie nicht nach Dateien oder deren Inhalt sucht, sondern Bildschirminhalte der Vergangenheit KI-gestützt interpretiert! Dazu macht das Betriebssystem tatsächlich alle paar Sekunden einen Screenshot des Bildschirms und legt ihn als Grafikdatei mit Zeitstempel in einem Ordner ab. Diese Screenshots werden dann von einer KI analysiert und einerseits nach abgebildetem Text, andererseits aber auch nach abgebildeten Objekten ausgewertet. Erscheint auf dem Screenshot also gerade Ihre Online-PIN für irgend ein Account, merkt sich Recall das. Erscheint dort ein Foto Ihres neuen Mountainbikes, merkt sich Recall "Fahrrad, geländegängig". Beides können Sie also theoretisch über eine Textsuche wiederfinden.
WAS? wird jetzt der ein oder andere aufgeschreckt denken - wird da also jetzt jeder Screenshot in die Cloud übertragen, um die Bildauswertung über OpenAI in der Cloud zu bewerkstelligen? Nein, tatsächlich soll dies lokal auf der Maschine erfolgen! Daher soll MS-Recall zunächst nur auf ARM-PCs mit NPU (Neural Processing Unit) installierbar sein, also vermutlich Surface-Geräten mit ARM-Prozessoren und eben NPU Coprozessor. Redakteure von heise.de haben aber bereits mittels verschiedener Anleitungen im Web es auch geschafft, die Vorschauversion auf einem älteren ARM-PC zu installieren und laufen zu lassen. Sie lief dort allerdings verhältnismäßig zäh, was an der fehlenden NPU liegen mag.
Interessanter waren allerdings die technischen Findings: Die konkrete Ausführung der Funktion wirkt auf den ersten Blick etwas … frickelig. Als hätte jemand mal eben schnell noch den Code fertig gestellt. Die gewonnen Daten für die Suche werden nämlich einfach im Klartext im Benutzerordner abgelegt! Unter c:\Users\ps\AppData\Local\ wird ein neuer Ordner \CoreAIPlatform.00 erzeugt, in dem sich dann sowohl eine SQLite-Datenbank, also auch ein "ImageStore"-Unterordner befindet, in dem die Screenshots einfach als JPEGs liegen. Ein Rechner, der sehr lange in Gebrauch war und eine hohe Bildschirmauflösung hat, dürfte dort also nach einiger Zeit gigabyteweise Bildmaterial horten.

Grundsätzlich ist bei dieser Konstruktion der Ordner für jeden Nutzer einsehbar, der einen Account auf dem Rechner hat. Das können also auch mal Arbeitgeber, SysAdmin, Ehefrau, Kinder oder Kollegen sein.
Das ist an sich schon sehr zweifelhaft und "unpersonal" für einen "PC".
Schwierig ist allerdings: Wenn denn mal jemand die Sicherheit des PCs kompromittiert hat und - auf welchem Wege auch immer - Zugriff erlangt hat, kann er nicht nur die Daten eines Nutzers, sondern dank der KI-Funktion auch das Verhalten (!) des Nutzers in der Vergangenheit durchsuchen. Er kann sich also anschauen, wo der Nutzer gesurft ist, welche Programme er geladen und

wie benutzt hat, in welcher Zeit er inaktiv war, in welcher Zeit er vielleicht unter einem anderen Account aktiv war etc. Er kann sogar das Webcam-Bild von Leuten sehen, mit denen der Nutzer gechattet hat, Kontostände, die der Nutzer kurz aufgerufen hat etc.

Juristisch weiß ich jetzt gar nicht, an welche Stelle ich mit meinen Bedenken anfangen soll. Arbeitsrechtlich ist das ganze für Unternehmenscomputer höchst fragwürdig. Ein Arbeitgeber darf und will ja vermutlich gar nicht alles sehen, was ein Arbeitnehmer im Laufe eines Arbeitstages so auf seinem Bildschirm aufruft. Ob sich das effektiv verhindern läßt, ist mir momentan unklar.
Datenschutzrechtlich haben wir insbesondere das Problem, das - bisher flüchtig - gerade bei Videokonferenzen die personenbezogenen Daten Dritter auf dem Bildschirm auftauchen. Diese werden jetzt verarbeitet und perpetuiert, so daß grundsätzlich Einwilligungen einzuholen wären. Auch kann das optische "Mitschneiden" ohne Erlaubnis einen Eingriff in Persönlichkeitsrechte darstellen, daneben auch den Straftatbestand "Verletzung der Vertraulichkeit des Wortes" bzw. "Verletzung des höchstpersönlichen Lebensbereiches durch Bildaufnahmen", §§ 201, 201a StGB erfüllen. Je nach Konstellation (Anwaltsrechner in einer Firma, Krankenhäuser…) kann dies sogar eine "Verletzung von Privatgheimnissen", § 203 StGB darstellen.
Die Strafbarkeit hängt natürlich immer vom Vorsatz ab, wobei allerdings bei diesen Delikten in der Regel "Eventualvorsatz" ausreicht.

Erstaunlich ist auch, daß Microsoft die Funktion offenbar bereits ab Mitte Juni 2024 offiziell ausrollen möchte! Das ist deutlich früher, als die meisten Experten es vom Entwicklungsstand her erwartet hatten.

Fazit: Gerade bei beruflich genutzten Rechnern kann ich momentan nicht zu einem bedenkenlosen Aktivieren dieser Funktion raten! Prüfen Sie vorher sorgfältig, wie die Einsatzbereiche des Rechners sind, wer diesen administriert, ob Konten geteilt werden oder Nutzerverzeichnisse in einer Cloud oder einem Backup liegen. Überlegen Sie genau, ob datenschutzrechtliche Einwilligungen erforderlich werden!

In allen IT-rechtlichen Fragestellungen berät Sie gern:

hüneborn | it

Port7 Rechtsanwälte
Jürgen Hüneborn, Rechtsanwalt, Fachanwalt für IT-Recht
hueneborn@port7.de
0251-203 188 00 | 0163 – 6839657
Am Mittelhafen 16, 48155 Münster
www.port7.de

Nachtrag: Microsoft hat aktuell (Juni 2024) bekannt gegeben, daß die Funktion „Recall“ vorerst - aufgrund diverser geäußerter Bedenken - doch nur innerhalb des sog. „Insider-Programms“ verteilt wird. Es wird sich also vorerst (!) noch nicht um eine regulär ausgespielte Funktion handeln. Da allerdings die Funktion früher oder später mit Sicherheit für alle Windows-PCs kommen wird, lohnt es sich bereits jetzt, datenschutzrechtliche und arbeitsrechtliche Überlegungen anzustellen, wie mit dieser Funktion umzugehen ist.