Wenn Sicherheit zum Unsicherheitsfaktor wird

07.08.2026, 10:40 | IT, New Media & Software

Pressemitteilung von: *idw - Informationsdienst Wissenschaft*

URL-Scanner-Dienste wie URLScan, VirusTotal oder Cloudflare Radar analysieren Webseiten automatisch auf verdächtige Inhalte. „Sie prüfen beispielsweise Netzwerkanfragen, die Reputation der Seiten oder eingebettete Skripte und helfen so Unternehmen und Privatpersonen, schädliche Webseiten frühzeitig zu erkennen“, erklärt Ali Mustafa. Viele Unternehmen nutzen laut dem CISPA-Forscher solche Dienste inzwischen als festen Bestandteil ihrer Sicherheitsmaßnahmen. So prüfen sie zum Beispiel automatisch Links in eingehenden E-Mails der Mitarbeitenden. Doch genau hier entsteht ein bislang zu wenig beachtetes Risiko.

Die Kehrseite des Komforts

Internetadressen bestehen heute oft nicht mehr nur aus einem Link zu einer Webseite. Sie enthalten häufig auch sogenannte Tokens. Das sind zufällig erzeugte Zeichenfolgen, die als digitaler Schlüssel dienen. Solche Links werden etwa für Passwort-Zurücksetzungen, Anmeldungen ohne Passwort oder den schnellen Zugriff auf Dokumente und Buchungsunterlagen verwendet. „Das ist für Nutzende überaus bequem. Es kann aber zum Problem werden, wenn URL-Scanner-Dienste, die Links veröffentlichen. Denn Dritte können darüber auf Dokumente oder personenbezogene Informationen zugreifen und unter Umständen sogar Aktionen im Namen der betroffenen Person ausführen“, erklärt Mustafa.

Aber warum machen die Scanning-Dienste die Links überhaupt öffentlich? „Zum einen demonstrieren die öffentlichen Scan-Feeds, wie umfangreich und schnell die Analysen der Services sind. Die Veröffentlichung ist wahrscheinlich Teil des Businessmodells. Zum anderen dienen die öffentlichen Feeds dazu, Erkenntnisse über verdächtige URLs mit anderen zu teilen“, so Mustafa weiter.

Das Problem erstmals im großen Maßstab betrachtet

Einzelne Berichte über veröffentlichte Zugangslinks mit sensiblen Informationen tauchten in der Vergangenheit hin und wieder in Blogbeiträgen oder Fallberichten aus der IT-Sicherheitsbranche auf. Die Forschenden wollten jedoch wissen, wie verbreitet das Problem tatsächlich ist. Dafür entwickelten sie das Analysesystem LEAKYLINKS. Damit konnten sie Internetadressen aus den öffentlichen Feeds von sechs großen URL-Scanner-Diensten sammeln, irrelevante Einträge herausfiltern und mithilfe eines Large Language Models automatisch analysieren, ob die verbleibenden Links sensible personenbezogene Informationen zugänglich machen könnten.

Insgesamt sammelte und analysierte das Team automatisiert mehr als zwei Millionen URLs von sechs verschiedenen URL-Scanner-Diensten und identifizierte mit 97 Prozent Präzision über 4.000 Fälle, in denen öffentlich zugängliche Links den Zugriff auf sensible Informationen ermöglichten. „Darunter befanden sich unter anderem Visa-Unterlagen, Regierungsdokumente und Buchungsinformationen. Wir waren selbst überrascht, was wir da alles gefunden haben“, sagt Mustafa.

Damit die Untersuchung nicht selbst zum Datenschutzrisiko wurde, legten die Forschenden großen Wert auf ethische Standards. Sie verzichteten weitgehend darauf, die gefundenen Inhalte manuell auszuwerten. Stattdessen übernahm das auf geschützten internen Servern betriebene Sprachmodell die automatische Klassifizierung. So mussten die Forschenden nur einen kleinen Teil der Ergebnisse selbst überprüfen, und sensible Daten wurden weder an externe KI-Dienste noch an andere Dritte übermittelt.

Stießen sie auf tatsächliche Datenlecks, informierten die Forschenden die betroffenen Organisationen sowie die Betreiber der untersuchten URL-Scanner-Dienste nach den Grundsätzen der Responsible Disclosure. Welche Unternehmen betroffen waren, nennt das Paper bewusst nicht, um zusätzlichen Schaden zu vermeiden.

Wer beobachtet die veröffentlichten Links?

Die Forschenden wollte außerdem wissen, ob die veröffentlichten Links überhaupt von Dritten beobachtet werden. Dafür richteten sie sogenannte Honeypages ein. Das sind speziell präparierte Köder-Webseiten, mit denen sich Zugriffe nachvollziehen lassen. Sie ließen diese URLS durch die Scanning-Dienste laufen und auf deren Seite veröffentlichen.

Die Ergebnisse zeigen, dass die öffentlichen Feeds keineswegs unbeachtet bleiben. Die Forschenden registrierten automatisierte Besucher:innen, Zugriffe auf eingebettete Inhalte und weitere Aktivitäten, die deutlich über gewöhnliches Surfverhalten hinausgingen. Trotzdem bleiben sie bei der Interpretation vorsichtig. „Wir können keine böswillige Absicht nachweisen", sagt Mustafa. Der beobachtete Datenverkehr zeigte jedoch, dass veröffentlichte Links tatsächlich von Dritten aufgerufen werden.

Wie sich das Risiko verringern lässt

Laut Mustafa gibt es verschiedene Möglichkeiten, das Risiko für Datenlecks deutlich zu verringern. „Website-Betreiber:innen könnten sensible Zugangslinks kürzer gültig machen oder zusätzliche Sicherheitsabfragen verlangen. URL-Scanner-Dienste sollten Links mit potenziell sensiblen Inhalten standardmäßig nicht öffentlich anzeigen.“ Nach Berechnungen der Forschenden blieben selbst dann mehr als 99 Prozent aller gescannten URLs weiterhin öffentlich verfügbar. „Der Nutzen der Dienste würde also kaum eingeschränkt, das Risiko für Betroffene jedoch deutlich sinken“, sagt Mustafa.

Für ihn zeigt die Studie vor allem eines: Sicherheitsrisiken entstehen oft nicht durch einzelne Fehler, sondern durch das Zusammenspiel verschiedener Systeme. Gerade deshalb müsse bei der Entwicklung digitaler Sicherheitsinfrastrukturen stärker berücksichtigt werden, welche unbeabsichtigten Folgen deren Zusammenspiel haben kann.

wissenschaftliche Ansprechpartner:

Originalpublikation:
https://cispa.de/de/research/publications/104817-leakylinks-measuring-the-security-and-privacy-risks-of-url-scanning-services

CISPA Helmholtz Center for Information Security

AnnabelleTheobald (Mitarbeiter in der Presse- und Öffentlichkeitsarbeit)

theobald@cispa.de

News-ID: 1320115 • Views: 80 (Stand: 10.08.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/1320115/Wenn-Sicherheit-zum-Unsicherheitsfaktor-wird-idw.html