idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Press release

CISPA Helmholtz Center for Information Security
Felix Koltermann

07/13/2023
http://idw-online.de/en/news817843

Research results, Scientific Publications
Information technology
transregional, national

Betreiber:innen von Websites nehmen Sicherheit wichtiger als Datenschutz

Im Jahr 2022 wurden weltweit mehr als 1,14 Milliarden Websites gezählt. Viele davon sind in der Europäischen Union (EU) gehostet oder werden von Menschen aus der EU genutzt. In diesen Fällen findet seit dem Jahr 2018 die europäische Datenschutz-Grundverordnung (DSGVO) Anwendung. Sie verpflichtet Unternehmen und Webseitenbetreiber:innen sicherzustellen, dass die personenbezogenen Daten ihrer Kund:innen und Nutzer:innen geschützt bleiben. Die CISPA-Forscherin Christine Utz und ihre Kolleg:innen haben nun untersucht, wie die Betreiber:innen von Websites auf die mangelnde Umsetzung der DSGVO sowie der ePrivacy-Richtlinie hingewiesen werden können.

Wenn Nutzer:innen im Internet über einen Webbrowser eine Website aufsuchen, ist damit in der Regel auch ein Datenaustausch verbunden. So verfolgen die Seitenbetreiber:innen zum Beispiel häufig, von welcher IP-Adresse die Webseite aufgerufen wird. Außerdem geben Kund:innen oft selbst viele persönliche Daten an, etwa wenn sie Produkte im Internet erwerben und sie sich diese nach Hause liefern lassen. Mit der seit 2018 gültigen Datenschutz-Grundverordnung (DSGVO) wurde erstmals eine europaweit einheitliche Richtlinie zur Verarbeitung personenbezogener Daten eingeführt. Ziel ist der Schutz der Nutzer:innen vor übermäßiger Datenspeicherung. Bereits die Speicherung einer IP-Adresse gilt als Speicherung persönlicher Daten. Die DSGVO findet für alle diejenigen Websites Anwendung, die in der EU gehostet sind oder in Europa aufgerufen werden können. Verantwortlich für die Umsetzung der Richtlinie sind die Betreiber:innen der Websites, während die Kontrolle den nationalen Datenschutzbehörden obliegt.

CISPA-Forscherin Utz untersuchte im Jahr 2019 mit ihrem Kollegen Martin Degeling von der Ruhr-Universität Bochum, wie sich Websites nach der Einführung der DSGVO verändert haben. „Unsere Haupterkenntnis war, dass sich zwar an der tatsächlichen Praxis des Trackings kaum etwas geändert hatte, aber die Transparenzbemühungen der Websites etwa über das Zurverfügungstellen von Datenschutzerklärungen sowie die Einführung von Cookie-Bannern gestiegen waren“, erzählt Utz. Dies war einer der Ausgangspunkte für ihre aktuelle Studie. Darüber hinaus hatte CISPA-Faculty Dr. Ben Stock, in dessen Gruppe Utz heute forscht, in einer früheren Studie untersucht, wie die Betreiber:innen von Websites mit Hilfe von E-Mail-Kampagnen über Sicherheitslücken informiert werden können. „Daraus entstand dann die Idee, zu untersuchen, ob die Betreiber:innen von Websites mithilfe einer solchen Kampagne auch auf mangelnden Datenschutz hingewiesen werden können“, so Utz weiter.

Studiendesign und Vorgehen bei der Untersuchung

Nach umfangreichen Vorrecherchen erfolgte die konkrete Umsetzung der Studie mit einem Set von ca. 160000 Websites. Kriterien für die Aufnahme einer Website in die Stichprobe war das Vorhandensein eines Datenschutzproblems wie etwa dem Fehlen einer Datenschutzerklärung, dem Nicht-Vorhandensein oder zu spätem Anzeigen von Cookie-Bannern sowie Inputfeldern für persönliche Daten ohne Absicherung mit HTTPS. Als Vergleichskriterium wurde darüber hinaus noch ein Sicherheitsproblem in die Studie aufgenommen. Dies war ein ungesicherter Zugang zu einem sogenannten Git Repository, also einer auf einem externen Server gespeicherten Arbeitskopie der Website-Entwickler:innen. Anfang November 2021 wurden die Betreiber:innen automatisiert per Mail angeschrieben und auf die Probleme hingewiesen.

Über zwei Monate hat Utz dann bei den Angeschriebenen sowie in einer Kontrollgruppe beobachtet, ob die Probleme auf den Seiten behoben wurden oder nicht. Um tiefergehende Erkenntnisse über die Umsetzung bzw. Nicht-Umsetzung sowie deren Gründe zu erlangen, verschickten die Forschenden mit den E-Mails auch einen Fragebogen und untersuchten die E-Mail-Kommunikation mit den Website-Betreiber:innen.

Herausforderungen bei der Umsetzung

Eine Studie mit einer sechsstelligen Stichprobe bringt eine Reihe von Herausforderungen mit sich, die sich unter anderem aus der Automatisierung vieler Arbeitsschritte ergeben. So liegt ein Risiko in falsch-positiven Ergebnissen, weil zum Beispiel automatische Tools zur Durchsuchung der HTML-Quelltexte tatsächlich vorhandene Datenschutzerklärungen etwa aufgrund uneinheitlicher Benennungen nicht erkennen. Eine weitere Hürde ist die Auswahl der E-Mail-Adressen, da frühere Studien gezeigt haben, dass die Nutzung von generischen Adressen wie info@- oder webmaster@- Nachteile mit sich bringt. Deswegen wurden, sofern möglich, die E-Mails an konkrete, auf der Website erkannte E-Mail-Adressen geschickt. „Die größte Schwierigkeit war jedoch zu verhindern, dass unsere E-Mails von den Empfänger:innen als Spam eingestuft werden“, erklärt Utz. Um dies zu verhindern, ergriffen Utz und ihre Kolleg:innen eine Reihe von Vorkehrungen. So wurde ein externer Server für das Hosting genutzt und die E-Mails signiert. Der externe Server sollte auch verhindern, dass alle vom CISPA stammenden E-Mails als Spam eingestuft und aussortiert werden und damit dem Zentrum Schaden entstehen könnte.

Ergebnisse verweisen auf hohe Hürde der Methode

Das wichtigste Ergebnis der Studie war, dass es grundsätzlich möglich ist, mit einer großangelegten Benachrichtigungskampagne Betreiber:innen von Websites per E-Mail über Datenschutzprobleme zu informieren. Gleichwohl ist der Erfolg hinsichtlich der Problembehebung angesichts der immensen Ressourcen, die für die Durchführung einer solchen Studie nötig sind, recht begrenzt. Dies zeigt sich vor allem daran, dass nur ein sehr kleiner Teil der Informierten überhaupt auf die E-Mails reagierte. Die Anzahl der Websites, auf denen im Beobachtungszeitraum Veränderungen vorgenommen wurden, bewegte sich im niedrigen einstelligen Prozent-Bereich. Darüber zeigte sich im Vergleich, dass Sicherheitslücken eher behoben werden als Datenschutzprobleme. Einen Grund sieht die CISPA-Forscherin darin, dass Sicherheitslücken oft mit weniger Aufwand geschlossen werden können.

Weitere Gründe für den beschränkten Erfolg der Kampagne innerhalb des zweimonatigen Untersuchungszeitraums ergab die qualitative Untersuchung der ausgefüllten Fragebögen sowie der E-Mail-Kommunikation. Utz fand heraus, dass sich Website-Betreiber:innen weniger offen für Benachrichtigungen über Datenschutzprobleme als über Sicherheitslücken zeigen. Darüber hinaus konnten weitere Hürden zur Umsetzung von Änderungen herausgearbeitet werden. Dazu zählten etwa Sprachbarrieren aufgrund mangelnder Englischkenntnisse auf Seiten der Empfänger:innen der E-Mails oder das Einstufen der E-Mails als Spam. Als weitere Hürde erwies sich interessanterweise der DSGVO-Bezug selbst. So wurde von einigen Betreiber:innen bezweifelt, dass die eigene Webseite überhaupt in den Anwendungsbereich der DSGVO fällt, oder der Hinweis auf mangelnden Datenschutz pauschal als nicht zutreffend zurückgewiesen. Gewünscht hätte sich die Teilnehmer:innen mehr und detailliertere Informationen zu den datenschutzrelevanten Fragen.

Kooperation mit Datenschutzbehörden als Ziel

Utz‘ Anliegen ist es, mit ihrer Forschung die Durchsetzungsfähigkeit der DSGVO zu erhöhen. „Datenschutzbehörden haben oft keine Kapazitäten, die mangelnde Umsetzung der DSGVO auf Websites zu erkennen und die Betreiber:innen darauf hinzuweisen“, erzählt sie. „Aber wir als Forschende könnten die Behörden dabei unterstützen.“ Ein wichtiger Faktor ist, dass die Forschenden und die dahinterstehenden Institutionen über die notwendigen technischen und personellen Ressourcen für solche Projekte verfügen. Umgekehrt könnten die Forschenden von der Autorität der Behörden profitieren. „Die Datenschutzbehörden können besser vermitteln, warum die DSGVO wichtig ist“, so Utz. Eine Kooperation wäre also eine Win-Win-Situation für alle Beteiligten. Dabei ist es laut Utz jedoch unerlässlich, dass breit

angelegte Benachrichtigungskampagnen per E-Mail in Zukunft von anderen Maßnahmen, wie etwa Informationskampagnen über den Anwendungsbereich der DSGVO, flankiert werden. Des Weiteren schlägt sie die Implementierung eines neuen Standards vor, wie die Betreiber:innen von Websites einfacher erreicht werden können, damit E-Mail-Benachrichtigungskampagnen zu größerem Erfolg führen. Die könnte etwa durch eine auf allen Websites hinterlegte Datei privacy.txt geschehen, die Informationen darüber erhält, wie die Betreiber:innen bei datenschutzrelevanten Fragen kontaktiert werden können.

Original publication:

Utz, Christine and Michels, Matthias and Degeling, Martin and Marnau, Ninja and Stock, Ben
(2023) Comparing Large-Scale Privacy and Security Notifications.
In: PETS 2023, July 10–15, 2023, Lausanne, Switzerland.
Conference: PETS Privacy Enhancing Technologies Symposium (was International Workshop of Privacy Enhancing Technologies)
(In Press)

Infografik zum Paper „Comparing Large-Scale Privacy and Security Notifications“
CISPA