Analytik NEWS
Das Online-Labormagazin

www.analytik-news.de Publikationsdatum: 07.03.2019

Datenschutz und Datensicherheit im Internet

Dr. Torsten Beyer

Analytik NEWS

Datenschutz und Datensicherheit sind schon seit den Anfängen des World Wide Web vor mehr als 25 Jahren ein Problem. Etliche Skandale in der jüngeren Vergangenheit, bei denen Abermillionen Passwörter und sensible Daten zum Schaden von Unternehmen und Personen missbraucht wurden, sind eine eindringliche Warnung an jeden Nutzer von Internetdiensten und jedes Unternehmen, das eine eigene Webseite betreibt, sich intensiver mit dem Thema zu beschäftigen.

Dazu gehört zu wissen, wie man beeinflussen kann, welche Daten wo und wie lange gespeichert werden, und was jeder zusätzlich für die Sicherheit seiner eigenen Daten tun kann. In diesem Zusammenhang spricht man heute oft von „Digitaler Kompetenz“, die leider an vielen Stellen nicht in ausreichender Form vorhanden ist. Denn meistens sind es vermeidbare menschliche Fehler, die es Hackern und Datendieben allzu leicht machen.

> *„Datenkraken lieben das Biotop Internet.“*
>
> Helmut Glaßl (*1950)

Was in Logfiles und im Cache gespeichert wird, warum Cookies problematisch sein können, wieso die Verschlüsselung von Webseiten essentiell ist, was bei Passwörtern und Accounts zu beachten ist und welche Gefahren in E-Mails und Newslettern lauern können, sind in diesem Zusammenhang die wichtigsten Themen. Nur fundierte Kenntnisse ermöglichen eine Beurteilung der möglichen Risiken und eine selbstbestimmte Entscheidung über die Verwendung der eigenen Daten.

Server-Logfiles

Wer eine Webseite besucht hinterlässt dort automatisch eine Reihe von Daten in einem Protokollfile, dem sogenannten Server-Logfile. Dazu zählen unter anderem die exakte Uhrzeit des Besuchs, die aufgerufenen Seiten, die verwendete Software und die eigene IP-Adresse. Diese wird in dem Zusammenhang als persönliche Information angesehen, da darüber eine Identifizierung und die Verfolgung aller Aktivitäten möglich ist, insbesondere in Kombination mit anderen Trackingverfahren, von denen noch die Rede sein wird. Daher dürfen IP-Adressen nur zeitlich begrenzt in Logfiles gespeichert werden.

Eine Verschleierung der eigenen IP-Adresse ist technisch aufwändig und im beruflichen Umfeld kaum umsetzbar. Man muss darauf vertrauen, dass die besuchten Seiten seriös damit umgehen und bestehende Gesetze einhalten.

Browser-Cache

Der verwendete Browser speichert alle besuchten Seiten in einer Chronik auf dem lokalen Zugangsgerät. Dieser sogenannte „Browser-Cache“ kann und sollte individuell konfiguriert werden, da in den Standardeinstellungen maximal viele Daten gespeichert werden. Dies ist in der Regel überflüssig und wird schlimmstenfalls zum Problem, beispielsweise wenn mehrere Personen das gleiche Gerät nutzen oder es gestohlen wird. Passwörter, über die Unbefugte Zugang zu sensiblen Daten erhalten könnten, sollten nie im Browser gespeichert werden, auch wenn es vielleicht bequem ist. Denn die Daten sind in der Regel nicht verschlüsselt.

Wer über ein Firmennetzwerk auf das Internet zugreift sollte wissen, dass der Arbeitgeber bzw. der Systemadministrator theoretisch auf den Cache oder Logfiles jedes Mitarbeiters zugreifen kann. Was erlaubt ist, muss in einer zusätzlichen Betriebsvereinbarung geregelt werden. Bei internationalen Konzernen sollte man sich sehr genau über Art und Umfang der Speicherung informieren, da das Rechtsverständnis und die gesetzlichen Grundlagen weltweit sehr stark variieren.

> *„Datenschutz sollte beidseitig sein: Unsere Daten zu schützen und uns vor ihnen.“*
>
> Erhard Blanck (*1942)

Cookies

Cookies sind kleine Textdateien, die beim Besuch einer Homepage von dieser auf dem Zugangsgerät gespeichert werden können (sogenannte „First Party Cookies“). Sie speichern beispielsweise Sitzungen bei einem Login, die Fehlerbehandlung in Formularen, die Ablage von Artikeln in Warenkörben oder dienen statistische Auswertung von Besuchersitzungen. Das ist in der Regel unkritisch, da es nur den aktuellen Besuch betrifft und die Speicherdauer in der Regel sehr begrenzt ist.

Problematischer sind Cookies, die von Seiten gesetzt werden, die man gar nicht aktiv besucht hat (sogenannte „Third Party Cookies“). Die besuchte Seite gestattet anderen Seiten das Setzen solcher Cookies. Hier handelt es sich entweder um Werbenetzwerke, die Seitenbesucher markieren und ihre Interessen speichern; besucht man später andere Seiten des Netzwerks, die solche Cookies

auslesen und ändern können, wird dazu passende Werbung angezeigt. Oder es handelt sich um eine Webanalyse-Software wie Google Analytics, mit der Seitenbetreiber weitaus mehr Aufschlüsse über die Besucher erhalten können als über die oben erwähnten Server-Logfiles. Hierfür muss aber die IP-Adresse anonymisiert werden, damit kein Bezug mehr zu einer bestimmten Person hergestellt werden kann.

„Wir wissen, wo du bist. Wir wissen, wo du warst. Wir wissen mehr oder weniger, worüber du nachdenkst."

Eric Schmidt (*1955)

Was solche Werbenetzwerke alles wie lange speichern und wie die Daten aggregiert und vielleicht mit persönlichen Daten wie E-Mail- oder Postadressen zusammengeführt werden, bleibt leider weitgehend im Verborgenen. Über allem steht die Angst, dass Nutzer so „gläsern" und schlimmstenfalls manipulierbar werden könnten. Vor diesem Hintergrund sollte man bei mobilen Geräten überlegen, ob Ortungsdienste immer aktiviert sein sollten und welchen Apps man Zugriff auf den aktuellen Standort gibt.

Browser-Einstellungen

Im Browser sollte man auf jeden Fall Änderungen an der Standardkonfiguration vornehmen, da standardmäßig Cookies unbegrenzt gespeichert werden. Man findet die einzelnen Optionen in der Regel unter „Datenschutz und Sicherheit", braucht aber leider fast eine Schulung, um die ganzen Optionen zu verstehen. Die generelle Löschung aller Cookies ist nicht empfehlenswert, da manche Seiten dann nicht mehr korrekt funktionieren. Third Party Cookies hingegen kann man bedenkenlos sperren oder zumindest ihre Speicherdauer auf die aktuelle Browsersitzung begrenzen.

In diesem Zusammenhang muss auch darauf verwiesen werden, dass es Tracking-Techniken jenseits von Cookies gibt, die man kaum unterbinden kann. Es besteht Anlass zur Befürchtung, dass die geplante stärkere gesetzliche Reglementierung von Cookies durch die EU daher langfristig ins Leere laufen könnte.

Seit Inkrafttreten der Datenschutzgrundverordnung (DSGVO) muss offengelegt werden, welche Cookies warum gespeichert werden und wie man deren Speicherung unterbinden kann. Wer sich die Zeit nimmt, die Datenschutzbestimmungen von Webseiten zu lesen, die er regelmäßig besucht, wird wahrscheinlich erschrecken, was da alles so im Hintergrund an Datenströmen fließt. Daten sind oft der Preis, den man für kostenfreie Dienstleistungen, Accounts oder Informationen zahlt.

Verschlüsselung

Die DSGVO schreibt in Artikel 32 vor, dass jeder Betreiber einer Webseite die Sicherheit der Verarbeitung personenbezogener Daten gewährleisten muss und nennt dabei explizit die Verschlüsselung als geeignetes Mittel. Es gibt verschiedene Arten von Zertifikaten je nach gewünschter Sicherheitsstufe. Für die meisten Webseiten reichen sogenannte domainvalidierte SSL-Zertifikate, bei denen lediglich geprüft wird, ob die Domain korrekt ist. Neben diesen in der Regel kostenlosen Zertifikaten gibt es kostenpflichtige Varianten für höhere Sicherheitsanforderungen. Das liegt im Ermessen des Seitenbetreibers.

Man erkennt verschlüsselte Verbindungen an einem Schloss neben der Webadresse oder an entsprechenden Warnhinweisen. Leider ist das nicht einheitlich gelöst. Ein zweifelsfreies Indiz ist das „s" (secure) in der Adresse. Beginnt diese mit „https://", handelt es sich um eine verschlüsselte Seite, beginnt sie mit „http://", so ist die Seite unsicher und man sollte dort weder Kontaktformulare ausfüllen noch einen Account anlegen. Es ist erstaunlich, dass immer noch etliche Unternehmen, auch in der Laborbranche, und sogar Online-Medien keinerlei Verschlüsselung einsetzen. Sie gefährden dadurch ihre Nutzer und Kunden und setzen sich der Gefahr hoher Strafen durch die DSGVO aus.

Accounts

Das Anlegen eines persönlichen Accounts auf einer Webseite, in einer Cloud, einem sozialen Netzwerk oder einem Online-Shop ist das größte Vertrauen, dass man einem Webseitenbetreiber entgegen bringen kann. Werden dort persönliche Daten, Kreditkarteninformationen oder vertrauliche Dokumente abgelegt, sollte man vorab prüfen, ob der Anbieter vertrauenswürdig ist, wo er seinen Firmensitz hat und welche Sicherheitsmaßnahmen zum Datenschutz bestehen. Dazu hilft ein Blick in die Datenschutzbestimmungen. Noch wichtiger ist es aber, sich die Frage zu stellen, welche Folgen ein unbefugter Zugriff, ein Kapern des Accounts oder eine Veröffentlichung der Daten haben könnte.

Beim Anlegen eines Accounts räumt man dem Seitenbetreiber oft viele Rechte ein, was die Speicherung und Weitergabe von Daten an Dritte und personalisierte Werbung angeht. Gerade soziale Netzwerke kennen ihre Nutzer oft besser als der eigene Partner und mehrere Wahlen der jüngeren Vergangenheit stehen im Verdacht der Beeinflussung durch gezielte Ansprache Unentschlossener auf diesem Wege.

Persönliche Daten sind oft der Preis für einen kostenlosen Service. Auf Basis der DSGVO kann jeder eine Datenauskunft verlangen und die Daten im Zweifel löschen lassen. Oder solche Accounts schließen.

„Es ist heute leichter zu sterben, als sich im Internet irgendwo abzumelden."

Justus Vogt (*1958)

Passwörter

Die Sicherheit von Passwörtern liegt in der Verantwortung jedes Einzelnen. In der Liste der beliebtesten Passwörter tauchen „123456", „qwertz" oder „passwort" an vorderer Stelle auf. Daher ist es wenig verwunderlich, dass Zugänge relativ leicht geknackt werden können, insbesondere wenn der zugehörige Login-Name eine öffentlich zugängliche E-Mailadresse oder der Nachname ist.

Die Verwendung der immer gleichen Zugangsdaten auf unterschiedlichen Seiten ist noch fahrlässiger, denn wird eine Seite gehackt, hat jemand Zugriff auf alle Zugänge. Die Kombination von beidem ist „digitaler Selbstmord“. Auch wenn es unbequem ist, sollte man sich bessere und unterschiedliche Passwörter ausdenken. So wird im Zweifel nur ein Account wegen einer Sicherheitslücke beim Betreiber geknackt und Betrüger kommen mit den Zugangsdaten nicht in Accounts auf anderen Seiten.

„Im Internet gibt es mehr Kriminelle als in den Gefängnissen."

Fred Ammon (*1930)

Im Hintergrund laufen auf allen Webseiten mit Login-Masken täglich milliardenfach automatisierte Scans mit Standardpasswörtern oder bei Hacks erbeuteten Zugangsdaten. Und bei gängigen Content-Managementsystemen suchen die Kriminellen zusätzlich nach veralteten, unsicheren Installationen, die dann leicht geknackt werden können. Nicht wenige Webseiten konnten so schon gekapert werden.

E-Mails

Auch die E-Mail ist von jeher ein beliebtes Ziel für Hacker, um Viren einzuschleusen oder Computer oder ganze Firmennetzwerke zu kapern und Lösegeld zu verlangen. Neben veralteter Software und unzureichenden E-Mail-passwörtern gibt es noch weitere Probleme: Manipulierte Links zu gefälschten Webseiten, virenverseuchte Anhänge oder Nachrichten, die mit der Veröffentlichung brisanter Daten drohen oder mit einer Erbschaft locken. Leider sind viele dieser E-Mails täuschend echt und man sollte daher sehr vorsichtig und misstrauisch sein, da jeder Absender und jedes Layout gefälscht sein kann. Kein seriöser Anbieter bittet um die Übermittlung von Zugangsdaten! Und bei Links sollte man immer durch Überstreichen mit der Maus prüfen, ob sie nicht zu einer anderen, möglicherweise gefälschten Webseite führen als der Linktext vorgibt.

Unternehmen sind im Bereich der E-Mail-Kommunikation in der Pflicht, Verschlüsselungstechniken einzusetzen und vertrauliche Inhalte nur durch Nutzung der digitalen Signatur zu versenden. Leider hat sich das noch nicht durchgesetzt und ist somit ein großes Risiko, da eine unverschlüsselte E-Mail ungefähr so geschützt ist wie eine Postkarte.

Ein spezielles Problem kann zusätzlich bei E-Mail-Newslettern entstehen. Es gibt Versender, die alle Klicks durch spezielle Tracking-Techniken personalisieren und so unerlaubt detaillierte Nutzerprofile anlegen, solche Informationen an Dritte weitergeben oder für eigene Werbezwecke missbrauchen. Das ist nicht erst seit der DSGVO illegal! Hier sollte man bereits beim Abonnieren eines Newsletters – wenn möglich – dem Tracking widersprechen oder es nachträglich sperren lassen.

Fazit

Jeder Einzelne kann viel dazu beitragen, dass weniger Daten gespeichert und die vorhandenen sicherer werden. Eine restriktive Browserkonfiguration für Cache und Cookies, bessere und überall unterschiedliche Passwörter, das Meiden unverschlüsselter Webseiten, die Verschlüsselung sensibler E-Mails und das zeitnahe Einspielen von Sicherheitsupdates bei allen verwendeten Zugangsgeräten zum Internet reduzieren die Risiken enorm.

Die DSGVO bietet darüber hinaus umfangreiche Auskunfts- und Löschmöglichkeiten, und die wahrscheinlich bald in Kraft tretende E-Privacy-Verordnung der EU wird vieles bei den Themen Cookies und Tracking deutlich strenger regeln.

Auch Unternehmen sind in der Pflicht, sichere Software für Firmennetzwerke und Webseiten zu nutzen, die DSGVO endlich vollständig umzusetzen und die Nutzer nicht unwissentlich zu überwachen oder Daten aus kommerziellen Gründen ohne ihr Wissen und damit gegen ihren Willen zu sammeln und weiterzugeben.

Nur so kommen wir zukünftig zu mehr Datenschutz und Datensicherheit und hoffentlich weniger Skandalen, die enorme Schäden verursachen können.

„Wenn es irgendetwas gibt, was man nicht über Sie wissen sollte, dann sollten Sie es vielleicht gar nicht erst tun."

Eric Schmidt (*1955)