Follow-up: Datenschutz-GAU Office 365

Ruhet sanft

Lukas Grunwald, Jürgen Seeger

Mittlerweile hat Microsoft USA auf unsere Enthüllungen im letzten Heft reagiert, mag aber das Problem nicht verstehen. Wir haben derweil auch einen Blick auf Google geworfen und einen Datenschutzexperten um seine Einschätzung gebeten.

Ein Artikel in *iX* 5/2019 [1] hatte erhebliche Sicherheits- und Datenschutzprobleme bei Office 365 dargelegt. Kurz zusammengefasst: Wir konnten den TLS-verschlüsselten Datenverkehr durch eine Man-in-the-Middle-Attacke aufbrechen und so sowohl die Credential-Daten im Klartext auslesen als auch nachweisen, dass schon vor jeder Benutzereinwilligung Telemetriedaten in Richtung USA fließen.

Wir hatten schon für diesen Artikel um eine Stellungnahme von Microsoft gebeten, die aber bis zum Redaktionsschluss der *iX* 5/2019 nicht vorlag. Vier Wochen später traf nun ein Statement vom Microsoft Security Response Center ein: „What's described does not represent a real-world scenario. Under normal usage scenarios data transmitted is protected through TLS encryption. Microsoft is committed to protecting our customers' privacy and providing the tools and resources that help put them in control of their data. It is a priority for Microsoft to ensure that all our products and services comply with applicable law, including the GDPR …"

In einer Erläuterung wird noch einmal ausgeführt, dass – sinngemäß – Hackerangriffe nicht zum normalen Benutzungsszenario der Office-Software gehören. Das ist, vorsichtig ausgedrückt, für Sicherheitsspezialisten eines Softwarekonzerns eine recht exotische Einstellung.

An dieser Stelle sei noch einmal darauf hingewiesen, dass es durch eine flapsige Formulierung im *iX*-Artikel zu Missverständnissen kommen konnte. Aus der Kritik an der Klartextübermittlung des Passworts sollte nicht der Schluss gezogen werden, dass man das Passwort schon im Client hashen (und „salzen") sollte, sondern dass dieses im Webumfeld (auch bei

Datenschutz bei Telemetriedaten

Die Frage nach der Datenschutzkonformität von Office 365 beschäftigt die Gemüter. Im November 2018 ergab eine Untersuchung im Auftrag des holländischen Justizministeriums zur „allgemeinen Datenschutz-Folgenabschätzung bei der Nutzung der Microsoft Office Software" datenschutzrechtliche Bedenken. Regierungsorganisationen sollen „den Wechsel auf die reine Webversion von Office 365 so lange verzögern, bis Microsoft ausreichende Garantien in Bezug auf die Art der personenbezogenen Daten und den Zweck der Verarbeitung gegeben hat", heißt es darin. Hintergrund war dabei insbesondere, dass Microsoft bei Installation und Nutzung des Office-365-Pakets „Telemetriedaten" überträgt.

Telemetriedaten sind nicht per se personenbezogene Daten. Nach dem Datenschutzrecht – in der EU insbesondere nach der Datenschutz-Grundverordnung – kommt es entscheidend darauf an, ob solche Daten einen Personenbezug aufweisen.

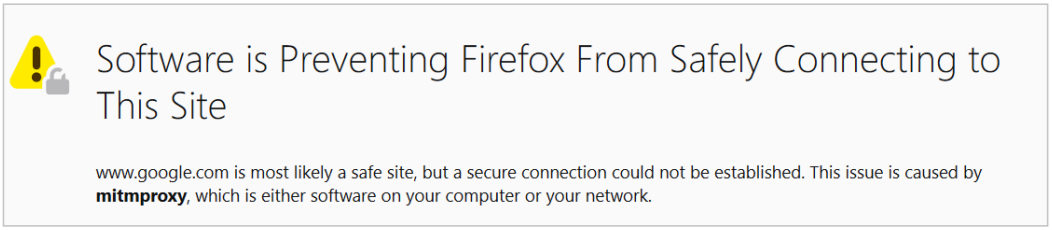
Definition nach Artikel 4 Nr. 1 DSGVO: Personenbezogene Daten sind „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person … beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind".

Überträgt eine Office-Anwendung, etwa durch Audit-Logs, Namen, E-Mail-Adressen, IP-Adressen oder Nutzer-IDs, handelt es sich dabei um personenbezogene Daten nach der DSGVO. Wenn ein Dateiname den Namen oder einen Hinweis auf eine bestimmte oder bestimmbare Person enthält, gilt das Gleiche. Aber auch dann, wenn nur „rein technische Daten", etwa die genaue Version des Betriebssystems in Kombination mit anderen Daten des Endgeräts, verwendet werden, ist ein Personenbezug oftmals gegeben. Datenschutzrechtlich genügt es nämlich, wenn eine Person darüber „identifiziert" werden kann. Die Ermittlung der auf einem Rechner installierten Programme ist eine Art Fingerabdruck, der – mit weiteren Informationen – oftmals eine Zuordnung eines Geräts zu einer jedenfalls bestimmbaren Person ermöglicht. Hierfür gilt das Datenschutzrecht. Dabei geht es nicht darum, ob demjenigen, der diese Daten erhebt, ein Personenbezug möglich ist oder er diesen beabsichtigt. Es geht rein darum, ob objektiv ein Personenbezug vorhanden ist.

Aus diesem Grund hat auch der Europäische Gerichtshof noch vor Wirksamwerden der DSGVO geurteilt, dass auch dynamische IP-Adressen personenbezogene Daten sind. Dass ein Webseitenbetreiber diese Daten nicht ohne Hilfe etwa eines Internetzugangsanbieters mit einer Person verknüpfen kann, hilft dabei nicht. Dies gilt dann aber konsequenterweise auch, wenn etwa Microsoft erfasst, welche Anwendungen wann und wie lange genutzt werden. Die Relevanz solcher Daten wird deutlich, wenn man sich überlegt, dass Arbeitgeber daraus ableiten könnten, ob sich ihre Mitarbeiter an die Arbeitszeiten halten. Dass Microsoft diese möglichen Erkenntnisse eher nicht nutzt, ist datenschutzrechtlich belanglos, ebenso wie eventuelle technische Vorteile durch die Übermittlung der Telemetriedaten.

Fazit

Die Übermittlung von Daten im Rahmen der Installation oder Nutzung von Software, wie etwa Office-Produkten, hat in den meisten Fällen Personenbezug und ruft den Datenschutz auf den Plan. Dabei entstehen nur selten Daten, die einen rein technischen Bezug haben und nicht auf eine bestimmte oder bestimmbare Person schließen lassen – auch wenn dies nur dadurch gelingt, dass weitere Informationen hinzugenommen werden. Die Verarbeitung sogenannter Telemetriedaten ist daher in der Regel nur zulässig, wenn es die DSGVO oder eine den Anforderungen entsprechende Einwilligung des Betroffenen gestattet. Werden solche Daten im Rahmen des Installationsprozesses übermittelt, bevor eine Einwilligung eingeholt wurde, ist diese Praxis datenschutzrechtlich zumindest bedenklich. *Tobias Haar, LL.M. Rechtsinformatik*



Aufgepasst: Firefox verwehrt den Zugang wegen des MITM-Proxy (Abb. 1).

heise online) übliche Verfahren zum einen für eine operativ eingesetzte Bürokommunikationssoftware nicht ausreicht, zum anderen, und wichtiger noch, schlecht implementiert ist. Da nämlich Microsoft dabei auf die Verifizierung des Servers verzichtet, konnten wir durch die Man-in-the-Middle-Attacke ein Fake-Zertifikat unterschieben. Diese Art des Aufbrechens der TLS-Kommunikation ist übrigens weit verbreitet, unter anderem arbeiten, wie bereits im letzten Artikel erwähnt, Next-Generation-Firewalls damit.

Google kanns

Dass es auch anders geht, zeigt Google. Auf dem durch den „Man in the Middle" überwachten Enterprise-Windows-10-System, auf dem die Office-365-Tests stattfanden, haben wir ebenfalls versucht, das kostenlose Office-Pendant Google G Suite einzurichten. Via Firefox klappte das nicht, der Browser gab sofort eine Warnung bezüglich des Proxy aus. Doch Microsoft Edge störte sich, man ist geneigt zu sagen „natürlich", daran nicht. Edge übertrug auch das Passwort als Web-Request im Klartext.

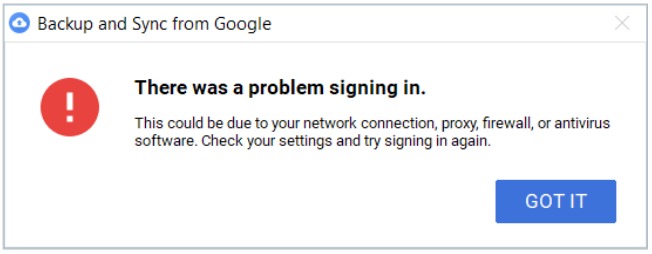
Aber: In beiden Fällen verwehrte die Installationsroutine der G Suite nach dem Download die Installation mit einer Fehlermeldung, mit Verweis auf einen Proxy, eine Firewall oder Antivirussoftware. Der Grund dürfte sein, dass Google im Gegensatz zu Microsoft das Serverzertifikat fest in das Installationsprogramm gebrannt hat und es beim Log-in überprüft.

In Sachen Sicherheit hat Google also die Nase vorn. Doch genau wegen der besseren Transportsicherheit lassen sich keine Aussagen über eventuelle Datenabflüsse treffen.

Auch Microsoft war früher besser, das Challenge-Response-Verfahren NTLM wurde in Redmond entwickelt und wird heute auch von Open-Source-Software breit eingesetzt, vom Apache Webserver über Curl bis Samba. Warum der Click-to-Run-Installer für Office 365 dahinter zurückfällt, ist schwer nachvollziehbar.

DSGVO hin, GDPR her

Zudem weist Microsoft USA in seiner Antwort auf das Office-ProPlus-Update hin, das es erlauben soll, Art und Umfang der gesendeten Daten einzuschränken (siehe ix.de/ix1906030 sowie Seite 25 in diesem Heft). Dieses Update kam Ende April, für diesen Zeitpunkt hatte der Konzern unter anderem den niederländischen Datenschützern Besserung in Sachen Datenschutz versprochen. Die waren nämlich dabei, ihre Beschwerden wegen der DSGVO-Verstöße in Richtung EU zu eskalieren. Ob das erwähnte Update die Niederländer zufriedenstellt, prüfen diese derzeit noch.



Auch nachdem Edge kein Fehler auffiel, verweigert der Google-Updater letztendlich den Zugriff (Abb. 2).

Und auch für die deutschen Datenschutzbehörden ist noch nicht geklärt, ob Office 365 und Windows 10 DSGVO-konform sind. „Aktuell sind die entsprechenden Untersuchungen aber sowohl im technischen als auch im rechtlichen Bereich noch nicht abgeschlossen, sodass eine konkrete Bewertung zum gegenwärtigen Zeitpunkt noch nicht möglich ist. Grundsätzlich hält der BfDI die Übertragung von Telemetriedaten aber für durchaus kritisch", teilte uns dazu auf Anfrage die Pressestelle des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit mit.

Im Detail ist die juristische Einschätzung der DSGVO-Konformität nicht ganz trivial, wie im Kasten „Datenschutz bei Telemetriedaten" nachzulesen ist. Man sollte dabei im Kopf haben, dass jeder Telemetriedatensatz die Lokation, die User-ID, die Installations- und Hardware-ID enthält sowie die IP-Adresse und den WLAN-SSID.

Was zumindest auf keinen Fall geht: Daten über den Teich schicken, ehe der Benutzer überhaupt irgendeine Chance hat, sich darüber zu informieren und zuzustimmen oder abzulehnen. Allen, die sich nicht sicher sind, was ihre MS-Software mit Redmond an Daten austauscht, sei der Nachbau der in *iX* 5/2019 beschriebenen MITM-Installation empfohlen [2]. (js@ix.de)

Quellen

[1] Datenschutz: Die Datenschutz-GAUs in Office 365; *iX* 5/2019; S. 74
[2] Datenschutz: Windows 10 in der Linux-Sandbox; *iX* 5/2019; S. 112
[3] Online-Informationen: ix.de/ix1906030