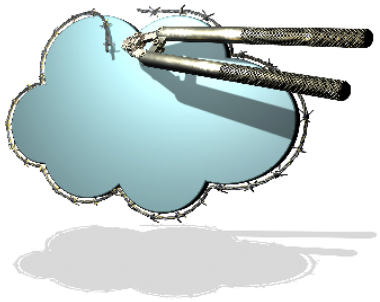

Einfaches Einverständnis reicht nicht

(Datenschutz: Die Daten-GAUs in Office 365; *iX* 5/2019, S. 74)

Ich habe eine kleine Anmerkung zum Punkt der Einverständniserklärung (letzte Spalte auf Seite 74): Das Einverständnis der Nutzer ist nur eine der möglichen Rechtsgrundlagen, auf die sich Microsoft stützen kann, vgl. Artikel 6 Absatz 1 DSGVO. Vertragliche Grundlage (Buchstabe b) ist in dem Fall sicherlich nicht gegeben (da diese Daten zur Vertragserfüllung nicht nötig sind), aber es könnte noch das berechtigte Interesse (Buchstabe f) greifen; auch das kommt in dem Fall aber nicht zum Tragen, da die Grundrechte und Grundfreiheiten der betroffenen Personen immer überwiegen dürften.

Ich wollte aber auf was anderes hinaus. Nach Artikel 7 gibt es eine ganze Reihe an Bedingungen für die Einwilligung. Wichtig ist, dass die Einwilligung aktiv vom Nutzer erteilt wird, informiert erfolgt, freiwillig ist, jederzeit und einfach widerrufbar ist und natürlich vor der Verarbeitung (Übertragung) erfolgt. Den Betroffenen muss also ganz klar sein, was mit den Daten geschieht, zu welchen Zwecken sie verarbeitet werden und natürlich auch welche Daten überhaupt verarbeitet werden. Die Einwilligung ist freiwillig und darf üblicherweise nicht Voraussetzung sein, damit man eine Software nutzen kann. Mehr Infos dazu gibt es auch in einer FAQ der Baden-Württemberger Datenschützer zum Thema Tracking auf Websites (Google Analytics, Facebook-Plug-ins usw.), dies lässt sich aber auch hierauf übertragen.

Das bedeutet unter dem Strich: Eine irgendwie geartete Infobox ist nicht ausreichend. Es muss klar dargelegt werden, was passiert, und eine irreführende Überschrift ist auch nicht zulässig. Es muss genauso einfach sein „nein“ zu sagen wie „ja“ und die Einwilligung muss der Nutzer auch jederzeit ebenso einfach widerrufen können. Mehr Infos zur Einwilligung gibt es auch in einem Kurzpapier der DSK.

ALVAR FREUDE, STUTTGART

Die vom Leser erwähnten Onlinequellen sind auf ix.de/ix1906004 zu finden (d. Red.).

Geschwätzige Xbox

(Datenschutz: Die Daten-GAUs in Office 365; *iX* 5/2019, S. 74)

Ich bin auch schon seit Monaten mit Microsoft im Gespräch per E-Mail, weil es mich stört, dass Aktivitäten gespeichert werden, welche Apps man von Microsoft verwendet hat. Und dass sowohl von Xbox als auch Windows 10, obwohl alles abgelehnt, was geht, Telemetrie, Diagnose usw.

Lapidar hieß es nur, man halte sich an Datenschutz, und wenn es einen stört, soll man sich mit dem Konto auf dem Gerät abmelden. Ist bei Xbox aber nicht möglich, besonders wenn man online spielen möchte. Bei Windows 10 geht es bei O365 auch schlecht, da man das Gerät ja online aktivieren muss und hin und wieder die Lizenz geprüft wird. Aber im Microsoft-Dashboard sieht man dann ständig, dass man Excel und so verwendet hat.

DANIEL, VIA E-MAIL

Klartextpasswörter sind okay

(Datenschutz: Die Daten-GAUs in Office 365; *iX* 5/2019, S. 74)

Der Artikel über Office365 ist leider nicht so gut geworden. Niemand überträgt Passwörter als Salted Hash. Die Idee ergibt schon keinen Sinn. Wenn man das täte, wäre der Salted Hash passwortäquivalent. Jemand mit MITM-Proxy könnte ihn sehen und selber verwenden, um sich als mich anzumelden. Wir hätten nichts gewonnen.

Der direkte Draht zu

Direktwahl zur Redaktion: 0511 5352-387

Redaktion iX | Postfach 61˚04˚07
30604 Hannover | Fax: 0511 5352-361
E-Mail: post@ix.de | Web: www.ix.de

www.facebook.com/ix.magazin
twitter.com/ixmagazin (News)
twitter.com/ix (Sonstiges)

Für E-Mail-Anfragen zu Artikeln, technischen Problemen, Produkten et cetera steht die Redaktion gern zur Verfügung.

Listing-Service:
Sämtliche in iX seit 1990 veröffentlichten Listings sind über den iX-FTP-Server erhältlich: ftp.heise.de/pub/ix/

Einer der Gründe, wieso man Passwörter im Klartext überträgt, ist, weil nur so der Server die Passwörter nicht im Klartext speichern muss. Man kann ein Klartextpasswort mit einem Salted Hash verifizieren. Eine der Seiten muss das Passwort im Klartext haben, und für die Verifikation braucht man beides. Wenn also der User über die Leitung einen Salted Hash schickt, was wie oben gesehen nichts bringt, dann müsste das Klartextpasswort vom Server kommen. Jetzt kann man natürlich argumentieren, dass beim User leichter Daten wegkommen, weil der weniger Security haben wird. Das Risiko sollte man aber als Schaden × Eintrittswahrscheinlichkeit betrachten. Auf dem Server liegen gleich ne Million Passwörter, daher wäre der Schaden höher und damit das Risiko. Das ist schon gut so.

Der Punkt mit der Telemetrie ist natürlich immer noch skandalös, da habt ihr völlig Recht, aber den Kampf haben wir, fürchte ich, verloren. Würde mich aber freuen, wenn ihr den Trend noch umgedreht kriegt. Ich fürchte nur, dass ihr dem Ziel mit dem Artikel eher geschadet habt, wegen dem Hash-Fauxpas.

Das Certificate-Pinning-Argument ärgert mich auch ziemlich, ehrlich gesagt. Aber aus anderen Gründen. Das ist eine Krücke, um zu übertünchen, dass das Zertifikatskonzept von TLS schlicht unzureichend ist. Und anstatt mal darüber zu reden, fordern wir jetzt Pinning. Pinning hat auch Nachteile. Nehmen wir mal an, ich pinne mein Zertifikat, und dann geht der Anbieter pleite oder der Anbieter wird als unvertrauenswürdig markiert. Dann hab ich doch erst mal ein massives Problem, das nur aufzubrechen ist, wenn wir von einer App oder einem Out-of-Band-Pinning-Mechanismus reden, der über eine 3rd Party wie den Google Play Store geht. Das ist ja wohl nicht die Zukunft, die wir haben wollten, oder? War nicht mal der Plan, dass jeder ohne externe Plattformen gleichberechtigter Teilnehmer sein kann?

FELIX VON LEITNER (FEFE) VIA E-MAIL

Wo Root-Zertifikat installieren?

(Datenschutz: Die Daten-GAUs in Office 365; *iX* 5/2019, S. 74)

Ein interessanter Artikel über Microsoft 365 ist Ihnen gelungen, mit Wonne gelesen ...

Nicht ohne Grund haben einige wenige Staaten (zu wenige) Microsoft in ihren Behörden verboten, wie die italienische Polizei, die arbeiten nun mit Open-Source-Komponenten. Aber leider existieren Rahmenverträge mit Microsoft.

Ich habe eine Frage: Wurde für den MITM-Proxy ein Root-Zertifikat auf dem Client installiert?

N.SJÖGREEN, VIA E-MAIL

Das Root-Zertifikat wurde auf dem Client installiert, ähnlich machen es auch NG Firewalls, Endpoint-Protection-Tools und AV-Software. Hier die technische Beschreibung: https://mitmproxy.org/ (d. Red.).

Klartext-Credentials bei Heise

(Datenschutz: Die Daten-GAUs in Office 365; *iX* 5/2019, S. 74)

Für das Nutzen von heise+ muss man sich bei heise mit seinem Account einloggen. Hier wartete die erste Überraschung auf uns: Das Login-Passwort wird im Klartext übermittelt, man konnte es via MITM-Proxy auslesen. Dass schon im letzten Jahrhundert Passwörter nur noch als Salted Hash übertragen werden sollen, damit sie nicht mitgelesen werden können, hat Heise ignoriert. Eine TLS-Verschlüsselung kann kein Grund für einen Verzicht auf ein Hashing des übertragenen Passworts sein. Denn zum einen gibt es ja offensichtlich MITM-Angriffe, zum anderen wird Heise die Passwörter nicht ernsthaft im Klartext speichern wollen – es gibt keinen Grund, warum ein Dienstleister ein Kundenpasswort im Klartext erhalten sollte. Obendrein kommt, kaum noch überraschend, auch beim Login-Server das fehlende Zertifikat-Pinning dazu. Ob ich da wirklich Zahlungsdaten eingeben sollte ... ich weiß ja nicht.

SEBASTIAN HERTZ-EICHENRODE, HAMBURG

Der Leser hat im zitierten Text aus dem Artikel „Microsoft“ durch „Heise“ ersetzt, denn auch beim Einloggen für heise+ werden die Credentials im Klartext übertragen. Ein paar Erläuterungen dazu sowie zu den in anderen Leserkommentaren aufgeworfenen Fragen sind im Artikel „Ruhet sanft“ auf Seite 30 zu finden. (d. Red.). Onlinequellen: ix.de/ix1906004

Die *iX*-Redaktion behält sich Kürzungen und auszugsweise Wiedergabe der Leserbriefe vor. Die abgedruckten Zuschriften geben ausschließlich die Meinung des Einsenders wieder, nicht die der Redaktion.