windows .developer
Veröffentlicht auf *webmagazin* (http://webmagazin.de)

PRISM & Co. - Selbstverteidigung für Nerds [Teil 3]

Autor:

Pascal Turbing

Johannes Mäulen [1]

PRISM & Co. - Selbstverteidigung für Nerds [Teil 3]
[2]

Angesichts der jüngsten Skandale rund um internationale Überwachungsprogramme zur Sammlung und Auswertung von elektronisch gespeicherten Daten steht die Frage im Raum, wie man sich heutzutage überhaupt noch schützen kann. Wie kann man seine Daten vor PRISM, Tempora und Co. verstecken und sich möglichst anonym im Internet bewegen? Dieser Frage gehen Hendrik Schmidt, Niklaus Schiess, Pascal Turbing und Johannes Mäulen vom IT-Security Dienstleister ERNW [3] in unserer dreiteiligen Artikelserie "PRISM und Co. – Selbstverteidigung für Nerds [4]" nach.

Im ersten Teil "Verschlüsselung [5]" erklärte Hendrik Schmidt alles Wissenswerte zum Thema Verschlüsselung und beantwortet Fragen wie: Welche Regeln sollte man beachten, wo und was sollte man überhaupt verschlüsseln und welche Methoden können dabei zum Einsatz kommen?

In Teil 2 widmete sich Niklaus Schiess dem Thema "Anonymität im Netz [6]" und geht dabei auf Proxy- und VPN-Dienste ein.

In Teil 3 setzen sich Pascal Turbing und Johannes Mäulen heute mit der Frage nach Privatsphäre und Datenschutz in Sozialen Netzwerken auseinander.

Soziale Netzwerken

Soziale Netzwerke haben in den letzten Jahren mehr und mehr an Beliebtheit gewonnen. Menschen posten ihre Gedanken, Urlaubsbilder, Einladungen auf Plattformen wie Twitter, Facebook und Google+. Das Leben junger Menschen wird nahezu durch die sozialen Netze bestimmt: Wo man hinsieht werden Fotos und Statusupdates mit dem Smartphone in die Weiten des Internets geladen. Das Thema Privatsphäre gerät

dabei immer mehr in den Hintergrund, man denkt kaum mehr darüber nach wer diese Inhalte alles sehen kann.

Seit der Offenlegung der Vorgänge um Programme und Werkzeuge wie PRISM, Tempora oder xKeyscore wird dieses Verhalten noch kritischer betrachtet: Ein Großteil der enormen Menge persönlicher Daten in allen Arten von Webdiensten war verschiedenen Geheimdiensten großflächig zugänglich.

Der gläserne Nutzer

Doch auch ohne den Datenhunger von Geheimdiensten können die online verfügbar gemachten Daten zu einer Bedrohung für die Privatsphäre werden. Facebook beispielsweise ändert regelmäßig die Einstellungen für den Zugriffsschutz [7] für das eigene Profil; dies kann dazu führen dass fremde Nutzer Daten einsehen können die eigentlich nur für Freunde bestimmt waren. In Kombination mit den umfangreichen Suchmechanismen der Platform wird man so schnell zum gläsernen Nutzer. Prinzipien, die eigentlich offensichtlich erscheinen, werden durch die permanente Nutzung und Allgegenwärtigkeit der sozialen Medien oft vernachlässigt, was zur Preisgabe von Gedanken oder Informationen führt, bei deren öffentlicher Bekanntmachung man zunächst zögern würde. So veranschaulicht die Süddeutsche in einem Onlineartikel [8] zum sorglosen Umgang mit bzw. Kommunikation über Facebook, wie sicher sich Menschen, fühlen wenn sie denken in der Masse unterzugehen. Doch spätestens mit Personensuchmaschinen wie yasni [9] oder People Search [10] sowie Werkzeugen wie DEVONagent Pro [11] gibt es kaum mehr eine Hürde, nahezu alle Informationen über den Online-Abdruck einer Person zu ermitteln.

Sorgloser Umgang

Am sorglosen Umgang und der Leichtsinnigkeit von Social Media-Nutzern möchten sich aber auch Geschäftsleute mit eher fragwürdigen Geschäftsmodellen bereichern. So berichtete beispielsweise Tom Eston schon 2009 in seinem Vortrag „Rise of the Autobots: Into the Underground of Social Network Bots [12]“, dass es bereits gängige Praxis ist, mit sogenannten Fakeprofilen möglichst viele Freunde auf Facebook zu gewinnen. Dadurch werden die meist von vorneherein schon sehr offenen Privatsphäreneinstellungen ausgehebelt und eine Analyse der jeweiligen Nutzer möglich. Daraus gewonnene Informationen können beispielsweise an den Meistbietenden verkauft werden. Denkbar sind auch Angriffe per Phishingnachrichten [13] auf leichtgläubige Nutzer oder klassische Spam-Nachrichten.

Datensammlung

Allerdings geht die Privatsphäre weit über vermeintlich ungünstige Bilder hinaus. Eingebettete Buttons zum direkten „Teilen“ von Informationen und einbettbare Kommentarfunktionen ermöglichen den sozialen Netzen ein Usertracking über die Grenzen der eigentlichen Portale hinaus. Gewonnene Daten werden unter anderem dazu genutzt, um gezielter Werbung zu schalten zu können. Zusätzlich speichern viele Communities auch Zeit und Ort (wie etwa Facebooks „Active Sessions“) der letzten Aktivität – sind diese Informationen doch teils sogar essentieller Bestandteil der geteilten Inhalte. Diese eingebetteten Inhalte, sollte man sich daran stören, lassen sich jedoch gezielt durch zahlreichen Browseraddons [14] blockieren, was zumindest diese Art des Datensammelns unterbindet.

Recht auf Information über eigene Daten

Möchte man sich einen Überblick verschaffen was beispielsweise Facebook über die eigene Person weiß, gibt es die Möglichkeit, ein Archiv mit gespeicherten Daten des eigenen Profils herunterzuladen. In den Kontoeinstellungen befindet sich ein unscheinbarer Link mit dem Titel „Download a copy of your Facebook data“. Dort finden sich bereits gelöschte Bilder, Nachrichtenverläufe und jede IP-Adresse von der sich bisher in den Account eingeloggt wurde. Diese IP-Adressen lassen sich meist leicht auf Örtlichkeiten abbilden, und gepaart mit möglicherweise vorhandenen GPS-Daten aus hochgeladenen Bildern lassen sich komplette Bewegungsprofile über Monate oder Jahre hinweg erstellen. Entsprechende Anfragen kann man, basierend auf dem deutschen Bundesdatenschutzgesetz und dem Recht auf Information über die eigenen Daten, jederzeit an alle Plattformen stellen. Selbst vermeintlich anonymisierte Daten, wie etwa über Nutzungsstatistiken, lassen sich dazu verwenden, sensible Informationen über einzelne Personen abzuleiten: Bereits 2006 wurde diese Möglichkeit basierend auf einem offengelegten Datensatz von Yahoo demonstriert [15]. Wer soziale Netze nutzen möchte, aber seine private Kommunikation vertraulich halten möchte, kann dies über die Nutzung bestimmter Chat-Clients und Verschlüsselungstechnologien [16] sicherstellen.

Bewusst handeln

Während Maßnahmen zur Sicherung der Privatsphäre ein wirksames und empfehlenswertes Werkzeug zum Schutz der eigenen Daten sind, helfen sie leider dennoch wenig gegen das großflächige Abgreifen von Daten durch Geheimdienste. Hier hilft lediglich das Bewusstsein über die eigene aktuelle Umgebung, sei sie virtuell oder physisch. Es liegt auf der Hand, dass man sich in den eigenen vier Wänden vergleichsweise sicher fühlt. Für ins Internet eingegebene Daten spielt es allerdings keine Rolle, ob man sich mit Smartphone im Wohnzimmer oder mit Hunderten fremden Menschen auf Gleis 7 des örtlichen Hauptbahnhofes befindet.

Es gibt Organisationen, die sich unter anderem auch den Bildungsauftrag im Bereich Medienkompetenz auf die Fahne geschrieben haben. So begleitet beispielsweise ein Fernsehteam [17] der Sendung nano des Senders 3sat den Chaos Computer Club Mannheim bei seinem Projekt „Chaos macht Schule [18]“ und klärt Schüler anhand der eigenen Profile darüber auf, was mit frei zugänglichen Daten angestellt werden kann und wie man sich dagegen schützt. Die Vermeidung von Inhalten, die man in der „realen Welt“ auch nicht preisgeben würde, ist somit das höchste Paradigma, das bei der Nutzung von sozialen Netzen befolgt werden sollte.

Aufmacherbild: *Security concept: Social Security on Building Foto [19] via Shutterstock / Urheberrecht: Maksim Kabakou*

Tagline:
Soziale Netzwerke

Links:
[1] http://webmagazin.de/Johannes-Maeulen
[2] http://webmagazin.de/sites/default/files/preview_images/prism_teil3_t.jpg
[3] https://www.ernw.de/
[4] http://webmagazin.de/web/security/PRISM-Co-Selbstverteidigung-fuer-Nerds-168394
[5] http://webmagazin.de/web/security/PRISM-Co-Selbstverteidigung-fuer-Nerds-168223
[6] http://webmagazin.de/web/security/PRISM-Co-Selbstverteidigung-fuer-Nerds-Teil-2-168546
[7] http://www.rp-online.de/digitales/internet/facebook-macht-alle-profile-oeffentlich-1.3738972
[8] http://www.sueddeutsche.de/digital/kommentarkultur-auf-facebook-keineswegs-unsichtbar-1.1791428
[9] http://www.yasni.de
[10] http://search.yahoo.com/web?fr=people
[11] http://www.devontechnologies.com/de/produkte/devonagent/devonagent-pro.html
[12] http://www.slideshare.net/agent0x0/rise-of-the-autobots-into-the-underground-of-social-network-bots
[13] http://www.honeynet.org/papers/phishing
[14] https://addons.mozilla.org/de/firefox/addon/ghostery/
[15] http://en.wikipedia.org/wiki/AOL_search_data_leak
[16] https://www.encrypteverything.ca/index.php?title=Setting_up_OTR_and_Pidgin_for_encrypted_chat_on_Facebook,_Google_Talk,_and_IRC(among_others)
[17] http://www.3sat.de/page/?source=/nano/technik/158180/index.html
[18] https://www.ccc-mannheim.de/wiki/Chaos_macht_Schule
[19] http://www.shutterstock.com/de/pic-159959108/stock-photo-security-concept-social-security-on-building-background-d-render.html?src=gOGC5qrMVhfv_S9FXN0VLA-1-87