Techniken der Datensammler: Was dagegen tun?

Jondonym stellt die Techniken der Datensammler vor, fasst die Risiken zusammen und gibt gleichzeitig Argumentationshilfen, warum man sicher und anonym surfen sollte:

– Tracking mit Cookies: Cookies sollte man ganz ausstellen!

– Flash-Cookies und EverCookies: Dagegen hilft z.B. das Firefox-Add-on Better Privacy.

– Fingerabdruck des Browsers: „Das Demonstrations-Projekt Panopticlick der EFF zeigt, dass mehr als 80% der Surfer anhand des Fingerabdrucks des Browsers eindeutig erkennbar sind. (…) Es werden die verwendete Software (Browser, Betriebssystem), installierte Schriftarten, Bildschirmgröße und Browser-Plugins ausgewertet. Zusätzliche Informationen werden mit einem Flash-Applet gesammelt. Bluecava erreicht damit bis zu 30% bessere Erkennungsraten, als Cookie-basierte Lösungen."

– Cache des Browsers: Cache beim Herunterfahren des Browsers löschen – das kann man so einstellen.

– Referer: Abhilfe z.B.: RefControl.

– Risiko JavaScript (ausschalten! Empfehlenswert: Noscript: „Das FBI nutzte im August 2013 bösartige Javascripte, die auf Tor Hidden Services platziert wurden, um durch Ausnutzung eines Bug im Firefox einen Trojaner zu installieren und Nutzer des Anonymisierungsdienstes zu deanonymiseren." (Sorry, aber wer Tor nutzt und gleichzeitig Javascript erlaubt, sollte geteert und gefedert werden – mein Mitleid hält sich da in Grenzen.)

– Risiko Plug-ins: „Der (Staats-) Trojaner der Firma

HackingTeam wird beispielsweise mit einer signierten JAR-Datei auf dem Zielsystem installiert. Der Trojaner belauscht Skype, fängt Tastatureingaben ab, kann die Webcam zur Raumüberwachung aktivieren und den Standort des Nutzers ermitteln. Nur das Deaktivieren aller Plug-ins im Browser bringt Sicherheit.“ Java deaktivieren! Statt Adobe kann man auch den Foxit-Reader neben. Ich habe Adobe-Produkte übrigens komplett von meinen Rechnern entfernt.

– History-Sniffing: Abhilfe: keine History bzw. Browserverlauf anlegen.

– Webbugs, Werbebanner und Like-Buttons: „Eine andere unangenehme Eigenschaft von Webbugs ist, dass sie beim Abruf neben Cookies auch Ihre IP-Adresse automatisch an den Statistikdienst übermitteln. Selbst mit einer sehr guten Browserkonfiguration, dem Abschalten von Cookies und automatischen Webbug-Filtern können Sie dies niemals zuverlässig verhindern. Dagegen hilft nur die Verwendung eines Anonymisierungsdienstes.“

– TCP-Zeitstempel: Der Zeitstempel kann vom Client- und/oder Server-Gerät eingesetzt werden, um die Performance zu optimieren. „Jedoch kann ein Internetserver Ihren Computer anhand der Zeitstempel wiedererkennen und verfolgen: Indem er die Abweichungen in der Uhrzeit misst, kann er ein individuelles Zeit-Versatz-Profil für Ihren Computer berechnen. Außerdem kann er die Zeit schätzen, zu der Ihr Rechner zuletzt neu gestartet wurde.“ Abhilfe nur per Anonymisierungsdienst.

– IP-Adresse: Die IP-Adresse offenbart zum Beispiel den aktuellen Aufenthaltsort, den Zugangsprovider, die Anbindung und Zugangstechnologie, das Unternehmen / die Behörde. Abhilfe nur per Anonymisierungsdienst.

– MAC-Adresse (kann man selbst ändern!).