Tilman Herbrich
Schriftleitung
Datenschutz-Berater

Datenschutz in der Bedrohungslage?

Sehr geehrte Leserinnen und Leser,

befindet sich der Datenschutz aktuell in einer Bedrohungslage? Diese Frage drängt sich auf, wenn man die jüngsten Entwicklungen aus Brüssel betrachtet. Anfang September erreichten uns Breaking News: Unter der Überschrift „Reality check on the Cookie Policy Framework under Article 5(3) ePrivacy Directive" hat die Kommission für den 15. September zur Anhörung geladen. Aus Brüsseler Kreisen hört man, dass sogar eine Abschaffung der Cookie-Regelung debattiert wird, nachdem man die ePrivacy-VO im vergangenen Jahr beerdigt hatte (vgl. Herbrich DSB 2023, 317). Man wolle nun die „Cookie-Fatigue" zum Schutz der Wirtschaft endgültig beenden.

Nichts scheint mehr übrig vom einstigen Geiste der Kommission, den unzureichenden Schutz der informationellen Selbstbestimmung aufgrund der Widerspruchslösung in Art. 5 Abs. 3 RL 2002/58/EG mit Konsolidierung durch die RL 2009/136/EG durch ein striktes Einwilligungserfordernis abzulösen, das so letztlich auch Eingang in § 25 TDDDG gefunden hat. Kernanliegen der Reform im Jahr 2009 war laut KOM(2007) 698 endgültig: „Ausweitung des Schutzes der Privatsphäre und der personenbezogenen Daten der Bürger in der elektronischen Kommunikation, insbesondere durch verschärfte Sicherheitsbestimmungen und verbesserte Durchsetzungsmechanismen."

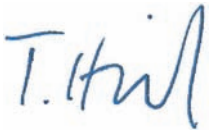
ErwGr. 24 ePrivacy-RL formuliert es unmissverständlich: „Spyware, Web-Bugs, Hidden Identifiers und ähnliche Instrumente können ohne das Wissen des Nutzers in dessen Endgerät eindringen und eine ernsthafte Verletzung der Privatsphäre darstellen." Dazu zählen auch Cookies, ergänzt ErwGr. 25 ePrivacy-RL. Wir wissen seit den Snowden-Enthüllungen, dass die NSA auch über Cookies Nachverfolgungen vorgenommen hat – mit nicht zu unterschätzendem Erfolg. Ein Klick auf eine Werbeanzeige kann Spyware über sogenannte In-Ad-Tags in Werbemitteln installieren. Bei Cookies geht es nicht um kleine Textdateien, sondern um den Schutz der Privatsphäre vor permanenter Identifizierung und Profilierung während wir uns im Internet politisch informieren oder sensibel einkaufen. Was daran ist heute weniger wichtig als vor 15 Jahren?

Der Skandal um Metas Local Host-Tracking verdeutlicht die Brisanz: Forscher der Radboud Universität in den Niederlanden stellten im Mai 2025 fest, dass native Android-Apps – darunter Facebook, Instagram und mehrere Yandex-Apps – heimlich auf festen lokalen Ports des Browsers zu Tracking-Zwecken Netzwerkverkehr mitschneiden und dabei alle Sicherheitsmechanismen des Browsers umgehen. Meta zweckentfremdete Websites, die den Meta Pixel integriert hatten, als Gehilfen, ignorierte Nutzerentscheidungen und umging Sicherheitsmechanismen wie den Private Mode, das Löschen von Cookies und Berechtigungskontrollen von Android, um eine persistente, nicht mehr löschbare ID zu generieren und das Nutzerverhalten außerhalb der App auszuspionieren. Dabei öffnet Meta für andere Apps, die die offenen Netzwerksignale ansteuern, Tür und Angel für den Missbrauch von Nutzerdaten. Zwei-Faktor-Authentifizierung hilft nicht mehr, wenn mein Endgerät gehijackt wurde. Endgeräte als Einstiegspunkt in die unternehmensinterne Infrastruktur? Meta macht's möglich. Es drängt sich die Frage auf: Hat Meta einen Data Breach auf sechs Millionen Websites ausgelöst? Es dürfte schwerfallen, die Erfüllung aller Tatbestandsmerkmale der Legaldefinition in Art. 4 Nr. 12 DSGVO zu negieren.

Würde man Art. 5 Abs. 3 ePrivacy-RL streichen, gäbe es möglicherweise keine Pflicht zur informierten Einwilligung und auch keine Transparenz für Endgerätezugriffe. Es gäbe auch weniger Fachwissen von Datenschutzberater:innen, weniger kritische Nachfragen „beim Marketing" und damit generell weniger Freiheit in unserem Land. Ich wünsche Europa deshalb in diesen Bedrohungszeiten ein starkes Parlament und einen starken Rat, der versteht, warum die Endgeräteintegrität einen besonderen Schutz benötigt, nicht zuletzt, um Manipulation bei demokratischen Willensbildungsprozessen zu verhindern. Das BVerfG hat kürzlich in Trojaner I und II zum Grundrecht auf IT-Sicherheit vorgelegt, Berlin und Brüssel sollten nicht in die Gegenrichtung schlafwandeln.

Wir werden Sie über die weiteren Entwicklungen auf dem Laufenden halten; für den Moment wünsche ich Ihnen im Namen der Redaktion eine wie gewohnt spannende Lektüre.

Ihr



Tilman Herbrich