Newsletter März 2016

- Privacy Shield statt Safe Harbour ✔
- Verschlüsselung vs. Verbrechensbekämpfung ✔
- Welle von Verschlüsselungstrojanern ✔
- Neues von den Domains: .sex ✔

Privacy Shield statt Safe Harbour

Das 'Facebook-Urteil', das das Safe Harbour-Abkommen zu Fall brachte, wurde von Datenschützern einhellig begrüßt. Es hat aber vor allem für transatlantisch tätige Unternehmen viel Unsicherheit verursacht. Die Politik stand unter Zugzwang, möglichst schnell einen Nachfolger zu präsentieren.
U.S.-Außenminister John Kerry und die EU-Kommissare Věra Jourová und Andrus Ansip zauberten nach Verhandlungen unter Hochdruck dann die Lösung aus dem Hut: Der Privacy Shield soll es richten. Auf den ersten Blick sieht die Vereinbarung vielversprechend aus. Das amerikanische Handelsministerium will in Zusammenarbeit mit der EU Firmen, die europäische Daten verwenden, überwachen und ihnen bei Datenschutzverstößen die Genehmigung zur Verarbeitung entziehen. Europäische Bürger können sich in Streitfällen an einen unabhängigen U.S.-Ombudsmann wenden.
Die Kritik ließ aber nicht lange auf sich warten. Die Zugeständnisse der Amerikaner sind lediglich Versprechungen Einzelner, aber weder von irgendeiner U.S.-Behörde unterschrieben, noch ein Vertrag oder gar Gesetz. Lediglich die Leitung der U.S.-Geheimdienste wollte schriftlich zusichern, dass Daten nicht massenhaft überwacht werden. Dumm nur, dass deren Chef James Clapper mehrfach durch Lügen aufgefallen ist, wenn er die Tätigkeiten der NSA skizziert, und das sogar gegenüber dem U.S.-Congress. Bei der Umsetzung von Schutzmaßnahmen darf man daher keine allzu hohen Erwartungen an deren Schlagkraft haben.
Das Prozedere ist noch im Gange und viele Fragen sind noch ungeklärt. Die Zeichen für eine nachhaltige Lösung des Konflikts stehen zurzeit eher schlecht. Die Unsicherheiten dürften noch einige Zeit bestehen bleiben.
In Hamburg macht der Datenschutzbeauftragte Johannes Caspar derweil Ernst. Er habe gegen mehrere namhafte deutsche Töchter von U.S.-Unternehmen Verfahren wegen Verletzung des Datenschutzes eingeleitet.

Verschlüsselung vs. Verbrechensbekämpfung

Die Verfechter der Sicherheit persönlicher Daten und die Strafverfolgungsbehörden streiten sich schon lange darum, wo die Grenze zwischen Schutzinteressen des Einzelnen und der der Gesellschaft zu ziehen ist. Ausgerechnet ein amerikanisches Unternehmen hat bei dieser Debatte dem Datenschutz die höchste Priorität gegeben und damit reichlich Öl ins Feuer gegossen.
Apple wurde vor Gericht aufgefordert, ein verschlüsseltes iPhone der San Bernadino-Attentäter zugänglich zu machen. Der Konzern betont, dass es selbst ihm nicht möglich sei, die Verschlüsselung zu brechen. Mit hohem Aufwand wäre es aber möglich, die Bildschirmsperre zu umgehen. Jedoch ist nur Apple in der Lage, eine entsprechende Software zu entwickeln, da sie für den Zugriff auf das Telefon mit Apple-Zertifikaten signiert und die exakte Version des Betriebssystems IOS angepasst sein muss.
Apple-Chef Tim Cook drückt gegenüber den Opfern des Attentats sein Bedauern aus, bleibt in der Sache aber hart. Seiner Ansicht nach ist die Anordnung des Gerichts verfassungswidrig und allein die U.S.-Bürger könnten gesamtheitlich zu einer anderen Rechtsauffassung gelangen. Die Angelegenheit dürfte noch das Verfassungsgericht beschäftigen.

Welle von Verschlüsselungstrojanern

Die Masche ist nicht neu, hat aber Hochkonjuktur: Trojaner kapern Computer und verschlüsseln anschließend alles, was irgendwie nach Daten aussieht. Der betroffene Anwender sieht nur noch plakative Warnmeldungen, die ihn zur Zahlung eines Lösegelds auffordern, und zwar meistens mittels Bitcoins, die an anonyme Empfänger überwiesen werden müssen. Ob die Entschlüsselung tatsächlich erfolgt, hängt vom Entgegenkommen des Erpressers ab. Einige Opfer haben nach Zahlung von mehreren hundert Euro tatsächlich Zugang erhalten, andere haben ihren Verlust nur vergrößert.
Ein neue Variante zielt nicht auf Rechner, sondern auf Webseiten, bei denen Sicherheitslücken ausgenutzt werden. Fein raus ist, wer seine Daten gesichert hat und das Problem durch eine Wiederherstellung und anschließendes Stopfen des Sicherheitslecks lösen kann. Noch besser ist es natürlich, Sicherheitsprobleme im Vorfeld zu beseitigen.
Global Village Kunden waren bisher nicht betroffen. Und selbst wenn es dazu käme – durch unsere Sicherungsstrategie können Websitekunden schlimmstenfalls die Daten der letzten 24 Stunden verloren gehen.

Neues von den Domains

.sex sells
ICM, die Registry für .adult, .porn, .sex und .xxx hat eine Promotion für alle ihre TLDs gestartet. Sämtliche Registrierungen von Standard-Domains, die zwischen dem 1. März und 31. Mai 2016 eingehen, kosten im ersten Jahr nur 10€ zzgl. Mehrwertsteuer, danach verlängern sie sich zum normalen Preis. Der Schutz Ihrer Marken ist in diesem Zeitraum deutlich preiswerter als üblich. Von dem Angebot können Sie unter https://dom-reg.global-village.de/1/domains/registrieren profitieren.

Mit freundlichem Gruß,
Ihr Global Village Team