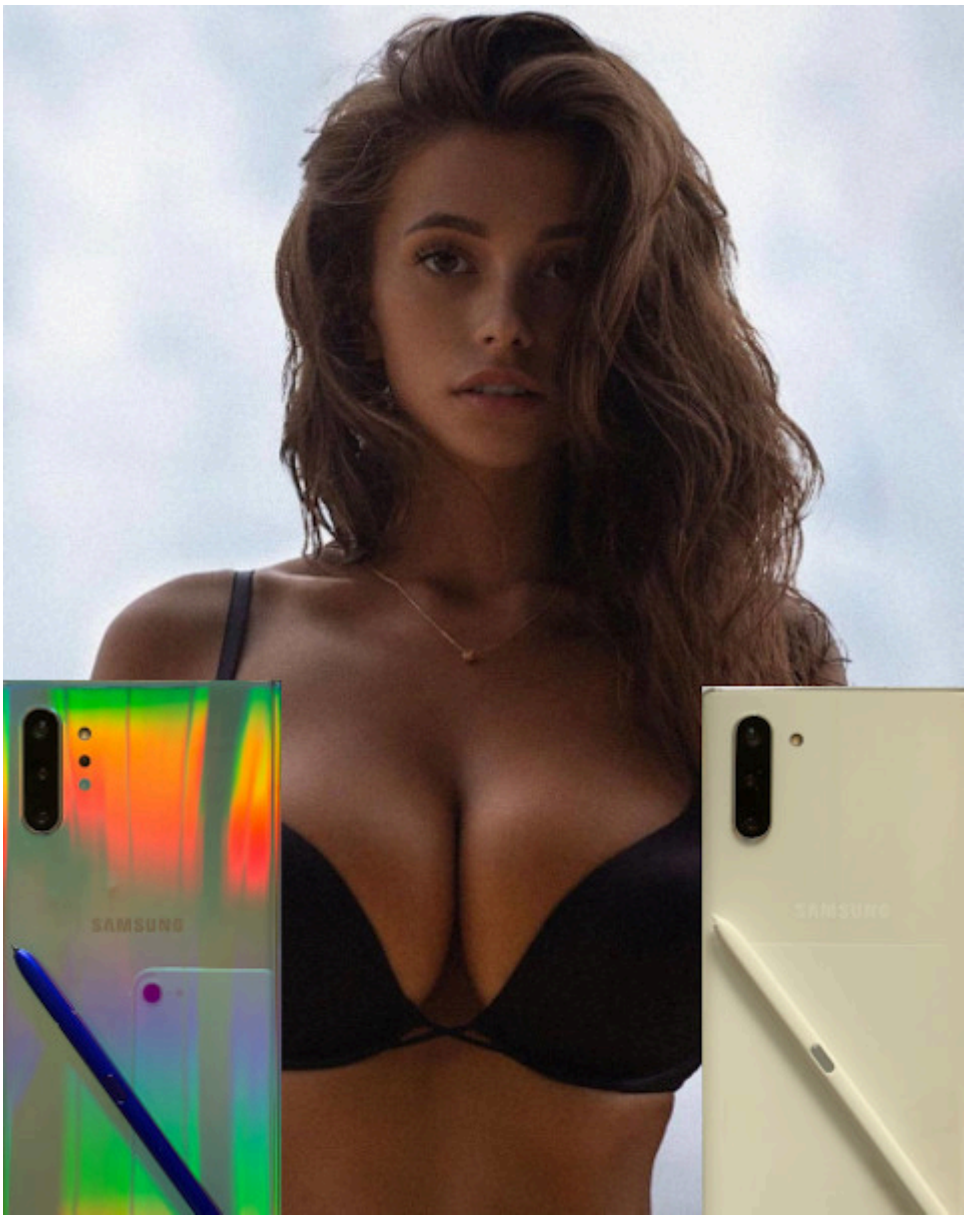
Unter clientsidigen verdecktmaßnahmigen Cybersicheren an ihren Endgeräten



Eine Userin und ihre Endgeräte (Symbolbild)

Netzpolitik.org hat die feuchten Träume ~~des Ministeriums für Wahrheit~~ der üblichen Verdächtigen veröffentlicht.

Ein hohes Datenschutzniveau, ein hohes Maß an Cybersicherheit,

einschließlich einer durchgängigen und sicheren Ende-zu-Ende-Verschlüsselung in der elektronischen Kommunikation sind für die Bundesregierung unerlässlich.

Dieses Neusprech bedeutet:*…will das Innenministerium am umstrittenen „Client-Side-Scanning“ festhalten. Der Einsatz dieser Technologie würde dazu führen, dass E-Mails, Messenger-Dienste und weitere Kommunikationsplattformen anlasslos und massenhaft überwacht werden. Beim Client-Side-Scanning werden Inhalte auf den Geräten der Nutzer vor dem Versand von Nachrichten durchsucht und somit eine spätere Ende-zu-Ende-Verschlüsselung unterlaufen.*

Denglisch, Neusprech und irgendetwas mit cyber? Wait a minute. Da kann nur Bullshit-Bingo herauskommen, auch bei den Berichterstattern. Es geht um eine *…Verfahrensweise, bei der versendete oder empfangene Dateien lokal auf dem Endgerät einer Person (…) durchsucht werden, bevor diese weiter verschickt beziehungsweise verarbeitet werden.* Höre ich da die Online-Durchsuchung trapsen?

Ich kenne meine „Endgeräte“ (Anfangsgeräte besitze ich hingegen nicht.) Ich sitze zum Beispiel gerade vor einem. Das möchten „die“ *durchsuchen*, bevor ich darauf/davon/damit eine verschlüsselte E-Mail absende? Darf ich vorsichtig nach der Methode fragen, wie das gehen soll? Nein? Quod erat demonstrandum. Auch netzpolitik.org fragt nicht nach, wie schon bei der ominösen „Online-Durchsuchung„, wie „Client-Side-Scanning implementiert wird“.

Die streiten sich alle wieder um die Kleider eines nackten Kaisers. Wir lassen stattdessen Jörg Ziecke zu Wort kommen, den ehemaligen Chef des BKA. Der erklärte 2007, wie das geht mit dem Onlinedurchsuchen:

Die Online-Durchsuchung ist einerseits der heimliche Zugriff auf die Festplatte, auf der anderen Seite ist es der heimliche Zugriff durch Quellen-TKÜ. Dieses Programm, was wir da

entwickeln, muss ein Unikat sein, darf keine Schadsoftware sein, darf sich nicht selbst verbreiten können und muss unter der Kontrolle dessen stehen, der es tatsächlich einbringt, wobei die Frage des Einbringens die spannendste Frage für alle überhaupt ist. Ich kann Ihnen hier öffentlich nicht beantworten, wie wir da konkret vorgehen würden. Sie können sich die abstrakten Möglichkeiten vorstellen, mit dem man über einen Trojaner, über eine Mail oder über eine Internetseite jemanden aufsucht. Wenn man ihnen erzählt hat, was für eine tolle Website das ist oder eine Seite mit ihren Familienangehörigen, die bei einem Unfall verletzt worden sind, sodass sie dann tatsächlich die Seite anklicken. Die Geschichten sind so vielfältig, dass es kaum jemanden gibt, der nicht auf irgendeine Form dieser Geschichte hereinfällt. Oder aber wir gehen den Weg über verdeckte Maßnahmen.

Wisst ihr Bescheid.

Ich habe kein Personal wie netzpolitik.org und würde mich daher mit einem Zehntel zufriedengeben.