

Ablaufplan

Nachrichtenübertragung: Kindernetz: Die Kinder werden in einem gleichmäßigen Raster aufgestellt und jedem eine „IP“ gegeben. Sie bekommen Zettel und sollen Nachrichten mit (Absender, Empfänger, Inhalt) hin- und herschicken. Dann schicken wir noch eine Nachricht mit sensiblem Inhalt (Geheimnisse, Passwörter) durchs „Netz“ und diskutieren, was jeder Router damit machen kann (lesen, verändern, einstecken, etc.)

Pause

Verschlüsselung: Teil 1: Cäsarchiffre erklären und auf einfache Worte/Sätze anwenden. Teil 2: Unterschied zwischen Weg- und Ende-zu-Ende-Verschlüsselung wird anhand von Email und einer Art Mini-Kindernetz (2 Clients jeweils mit einem Internetanbieter) erklärt. Verschlüsselung wird mit „Truhen“ (am besten wären unterschiedliche, eine haben wir bereits, hat jemand noch weitere?) symbolisiert, die bei der Wegverschlüsselung vom Anbieter und bei der Ende-zu-Ende-Verschlüsselung erst vom Empfänger geöffnet wird. Dann wird am Bildschirm in einem Browser der Unterschied zwischen einer Verschlüsselten und einer Plaintextseite gezeigt und HTTPS Everywhere vorgestellt (zum Thema Wegverschlüsselung) und PGP und Signal zum Thema Ende-zu-Ende-Verschlüsselung genannt.

Pause

Metadaten: Ein paar Slides dazu, was man alles mit Metadaten herausfinden kann (aus den letzten Vorträgen). Dann wird per Lightbeam gezeigt, wie viele Tracker es im Web bei großen Websites gibt (wird dann wiederholt nachdem man Privacy Badger, Disconnect oder Ghostery installiert hat).

Ggf. nochmal Pause (je nachdem wies so läuft)

Verhalten: Slides zu Datenvermeidung und sicheren Passwörtern (hier noch ein paar Standardpasswörter bei howsecureismypassword.net eingeben und zeigen, wie schnell sich sowas brute forcen lässt).

Soziale Netzwerke: Es wird gefragt, wer welche sozialen Netzwerke nutzt. Dann Geschäftsmodelleraten (womit machen Karstadt, Amazon,..., Facebook ihr Geld?). Dann Slides zu Verhalten in sozialen Netzwerken und Diskussion über einzelne „Beispielposts“.