Ablaufplan

Nachrichten bertragung: Kindernetz: Die Kinder werden in einem gleichm igen Raster aufgestellt und jedem eine „IP“ gegeben. Sie bekommen Zettel und sollen Nachrichten mit (Absender, Empf nger, Inhalt) hin- und herschicken. Dann schicken wir noch eine Nachricht mit sensiblem Inhalt (Geheimnisse, Passw rter) durchs „Netz“ und diskutieren, was jeder Router damit machen kann (lesen, ver ndern, einstecken, etc.)

Pause

Verschl sselung: Teil 1: C sarchiffre erkl ren und auf einfache Worte/S tze anwenden. Teil 2: Unterschied zwischen Weg- und Ende-zu-Ende-Verschl sselung wird anhand von Email und einer Art Mini-Kindernetz (2 Clients jeweils mit einem Internetanbieter) erkl rt. Verschl sselung wird mit „Truhen“ (am besten w ren unterschiedliche, eine haben wir bereits, hat jemand noch weitere?) symbolisiert, die bei der Wegverschl sselung vom Anbieter und bei der Ende-zu-Ende-Verschl sselung erst vom Empf nger ge ffnet wird. Dann wird am Bildschirm in einem Browser der Unterschied zwischen einer Verschl sselten und einer Plaintextseite gezeigt und HTTPS Everywhere vorgestellt (zum Thema Wegverschl sselung) und PGP und Signal zum Thema Ende-zu-Ende-Verschl sselung genannt.

Pause

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

Ggf. nochmal Pause (je nachdem wies so l uft)

Verhalten: Slides zu Datenvermeidung und sicheren Passw rtern (hier noch ein paar Standardpassw rter bei howsecureismypassword.net eingeben und zeigen, wie schnell sich sowas brute forcen l sst).

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