

Was ist und zu welchem Ende betreiben wir Social Engineering?

[Spiegel Online](#) (ein [Link zur Quelle](#), o Wunder!) fantasiert wieder wahllos herum: „Denn Bronk hackte sich in deren E-Mail-Konten...“ Das hätte die Taz auch nicht schlechter formulieren können. Wie zum Teufel, „hackt“ man sich in E-Mail-Konten? Etwa mit einer real gar nicht existierenden „Online-Durchsuchung“?

Nein, der Kerl war kein echter „Hacker“, sonder jemand, der sich des guten alten [Social Engineering](#) bediente: „Ausgestattet mit dem derart zusammengetragenen Hintergrundwissen ging er daran, die E-Mail-Passwörter seiner Opfer zu ändern. Dazu machte er sich nicht etwa die Mühe, zuerst deren Passwort herauszufinden. Stattdessen gab er sich deren E-Mail-Providern gegenüber als Inhaber des jeweiligen Accounts aus und beantragte, mit der Begründung, er habe sein Passwort vergessen, online ein neues. Weil viele Provider immer noch Standardabfragen, beispielsweise nach dem Mädchennamen der Mutter, verwenden, um in solchen Fällen die Identität des Antragstellers zu überprüfen, fiel es Bronk nicht schwer, die E-Mail-Konten zu übernehmen.“

„Social Engineering nennt man zwischenmenschliche Beeinflussungen mit dem Ziel, unberechtigt an Daten oder Dinge zu gelangen. Social Engineers spionieren das persönliche Umfeld ihres Opfers aus, täuschen falsche Identitäten vor oder nutzen Verhaltensweisen wie Autoritätshörigkeit aus, um Dinge wie geheime Informationen oder unbezahlte Dienstleistungen zu erlangen. Meist dient Social Engineering dem Eindringen in ein fremdes Computersystem, um vertrauliche Daten einzusehen; man spricht dann auch von Social Hacking.“

Also bitte keine Computermythologie, Technik-Schamanismus oder anderen Regenzauber: Man kann sich nicht einfach so irgendwo „reinhacken“.