Richtig und falsch reinhacken

Richtig bei Heise Security: „Bei dem Diebstahl von rund 200.000 Kundendaten der Citibank mussten die Kriminellen nicht tief in die Trickkiste greifen, wie ein Sicherheitsexperte gegenüber der New York Times bekannt gegeben hat. Demnach gelang der unberechtigte Zugriff, den die US-Bank bei einer Routinekontrolle Anfang März entdeckt hat, durch das simple Manipulieren eines URL-Parameters.“

The method is seemingly simple, but the fact that the thieves knew to focus on this particular vulnerability marks the Citigroup attack as especially ingenious, security experts said.

Falsch bei Spiegel ~~online~~: „Den beiden Angeklagten wird vorgeworfen, zwischen März 2009 und März 2011 Computer von Musikfirmen manipuliert zu haben. Mit Spionageprogrammen, sogenannten Trojanern, stahlen sie laut Anklage bis dahin unbekannte Songs…“

Wer schützt unsere Kinder eigentlich vor den Verschwörungstheorien der Holzmedien, zu denen auch gedrucktes linkfreies Papier à la Spiegel ~~online~~ gehört? Lugt da wieder die real gar nicht existierende „Online-Durchsuchung“ hervor? Guckst du hier:

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“.