Egger hackt Webseiten der Kapo Zürich und Bern

***Update (5. Januar 2008 – 22:50 Uhr)**: Die Sicherheitslücke bei der Kapo Zürich wurde mittlerweile geschlossen. Die Kapo Bern braucht wohl noch einen Moment. Wahrscheinlich feiern deren Informatiker, wie meine Wiener, Arbeitskollegen morgen die heligen drei Könige und haben darum eine Brücke gemacht *

Auf das neue Jahr hin sind die Eggers unter die Hacker gegangen. Nachdem der „Hack“ auf die Kapo Zürich und Kapo Bern einen solchen medialen Wirbel verursacht hat, haben wir uns gedacht die Methode ebenfalls einzusetzen um Werbung für unsere Seite zu machen.

Hier also Screenshots der von uns gehackten Webseiten der Kantonspolizei Zürich und Bern.

Eggers Beweisbild des Kapo ZH Hacks

Eggers Beweisbild

des Kapo BE
Hacks

Und zum Beweis, dass es sich um keine Fotomontage handelt, finden sich hier direkt die Links zu den gehackten Webseiten:

Link zur gehackten Webseite der Kantonspolizei Zürich
Link zur gehackten Webseite der Kantonspolizei Bern

Ich hoffe die tagelangen Recherchen, stundenlangen Diskussionen mit angetrunkenen Hackern und das bezahlen einiger tausender hat sich gelohnt und unsere Webseite schnellt nun medial in andere Hemisphären.

Wie immer wird auch hier das Gericht nicht so heiss serviert wie es gekocht wurde. Sprich, ich wollte mit dieser Aktion nur darauf hinweisen, wie „blindlings“ sich die Medien auf solche Meldungen stürzen und einfach irgendwas abdrucken.

Meine Kritik richtet sich hier speziell an Manuel Bühlmann von 20min, da verschiedene andere Verlage auf seinen Artikel verweisen. So schreibt er in seinem Artikel auf 20 Minuten:

> *Zurzeit machen die Kapo Bern und Kapo Zürich unfreiwillig Werbung für die IT-Cracks vom Chaos Computer Club. [..] sie sind auch auf die Websites der Kantonspolizei Zürich, bzw. Bern eingedrungen. Beide Seiten haben sie klammheimlich mit ihrem Logo des Chaos Communication Congress (25C3) markiert.*

Lieber Herr Bühlmann. Von einem „eindringen“ kann doch gar keine Rede sein. Die Hacker haben weder irgend einen der beiden Polizei-Server gehackt noch wurde auch nur ein Bit irgend einer Datei – welche für die Darstellung der Webseite zuständig ist – auf irgend eine Art und Weise manipuliert.

Vielmehr ist es so, dass die beiden Webseiten schlicht und ergreifend nicht genügend gegen Cross Site Scripting (XSS) geschützt wurden. Dies bedeutet, dass das Logo nur derjenige

sieht, welcher auch genau den Link mit dem untergejubelten Bild verwendet. Genau so verhält es sich auch mit meinem untergejubelten Bild. Besucht man die Webseite „regulär“ wird man von dem Logo nichts sehen.

Genau so reisserisch, lieber Gerr Bühlmann, ist dann auch Ihre Aussage, dass die Kapo Zürich nichts von der Attacke gemerkt hat.

> *Bei der Kapo Zürich hatte man die Attacke erst gar nicht bemerkt, wie die Anfrage von 20 Minuten Online ergab. Die Manipulation bleibt zwar in diesem Fall ohne grosse Auswirkungen, zeigt jedoch, dass selbst die Polizei nicht vor ungebetenen Gästen gefeit ist.*

Wie ich bereits erwähnt habe, hat die Kapo Zürich deswegen nichts bemerkt, weil es schlicht und ergreifend nichts zu bemerken gab. Das Logo bekommt nur derjenige zu Gesicht, der auch genau den einen Link aufruft. Wer die Suchfunktion der Webseite ganz normal verwendet, der wird das Logo nie sehen.

Und dass „selbst die Polizei nicht vor ungebetenen Gästen gefeit ist“ liegt doch wohl auf der Hand. Schliesslich wird die Webseite nicht von „Polizisten“ gehostet sondern von irgendwelchen IT Admins in irgend einem Datencenter. Ob da nun die Webseite der Polizei darauf zu finden ist oder die Webseite von Fritzli Müller ist absolut irrelevant. Mit einer derartigen Aussage versuchen Sie jedoch dem Leser ein Bild zu suggerieren, dass die Polizei als leicht trottelige Dorfpolizisten darstellt und die Hacker als spitzbübische, dreiste Technikfreaks.

Aber wie Marcel Strebel, Chef Informationsabteilung der Kantonspolizei Zürich richtig sagt:

> *Es handelt sich im vorliegenden Fall nach ersten Einschätzungen um eine harmlose Manipulation.*

Natürlich will ich die Lücke nicht verharmlosen. Denn durch eine XSS Lücke ist es nicht nur möglich ein Bild einzufügen, sondern man kann auch – mit einiger Geduld und dem nötigen HTML, JavaScript wissen vorausgesetzt – HTML und JavaScript Inhalte in die Webseite einpflanzen, welche dann den Anschein erwecken, es handle sich um regulären Inhalt der Kapo Webseite.

Doch auch hier ist die Gefahr gering, dass damit „grober Unfug“ angestellt werden kann. Schliesslich wird wohl niemand auf der Webseite der Polizei irgend eines seiner Passwörter eintippen (wozu auch?) noch die Webseite als Startpunkt für seine Internet-Reisen verwenden. Denn nur das anbringen von manipulierten Links (die z.B. auf Webseiten von echten gehackten Webservern verweisen) wäre noch das das einzige interessante Feature, welches XSS bietet.