

22. Nov. 1984

Hacker vom Chaos Computer Club demonstrieren Sicherheitsmängel

HANDELSBLATT, Mittwoch, 21.11.1984
 beu/HB HAMBURG/DÜSSELDORF. Was noch wenige Tage zuvor von Angehörigen der Post heftig bestritten worden war, zuletzt auf einer Datenschutz-Podiumsdiskussion am 15. November in Köln, konnten Angehörige des Hamburger „Hacker“ Clubs „Chaos Computer Club“ (CCC) Postminister Schwarz-Schillings Männern nun beweisen: Die posteigene Bildschirmtext-Software hat Schwachstellen und ist nicht ausreichend sicher.

Die Hamburger Computer-Freaks, selbst Anbieter in Btx, haben in den letzten Wochen systematisch Btx auf Schwachstellen abgeklopft. Unter den Augen der hamburgischen Datenschutz-Aufsichtsbehörde wollten sie anhand einer ganz bestimmten Schwachstelle beweisen, daß sie mit ihrer Kritik recht haben.

Sie erstellten nach vorheriger Rücksprache mit dem Landesdatenschutzbeauftragten diverse Seiten in Btx mit der Besonderheit, den gesamten verfügbaren Platz in der Seite zu belegen. Dies ist einfach zu bewerkstelligen, weil Btx beim Editieren einer Seite anzeigt, wieviele Zeichen noch frei sind. Wird eine solche Seite abgesendet, so entsteht Datensalat. Aus fremden Seiten erscheinen Daten im eigenen Text. Mit etwas Glück erwischt man auch die Kennungen anderer Benutzer. Und damit ist der Einstieg „unter fremder Flagge“ ein Kinderspiel. Bei dem am 19. November vom CCC durchgeführten Versuch fanden die Hacker auch die Kennung der Hamburger Sparkasse (Haspa).

Die Chaos-Hacker meldeten sich unter dem Namen der Haspa beim Btx-System an und liessen die Informationen — zu Lasten des Haspa-Btx-Kontos — abrufen, die der Club selbst anbietet. Sinnigerweise eine Sequenz, die der Club in seinen Informationen als „Spendenseite“ Be-

nutzern empfiehlt: die sich bei der Post und bei öffentlichen Vorführungen Btx zeigen lassen und dabei nebenbei dem Club bescheidene Mittel zu Lasten des Vorführers zukommen lassen. Kostenpunkt: 9,97 DM pro Sendung.

Um nicht die ganze Nacht arbeiten zu müssen, wurde ein Computer abgeschlossen, der auf Kosten der Hamburgischen Sparkasse im 20-Sekunden-Takt diese Spendenseite abrief. Lohn der Nacht: 135 000 DM hätte die Sparkasse an die Post zugunsten des Chaos Computer Clubs überweisen müssen, wenn dieser nicht darauf verzichtet hätte.

Gegen diese Rechnung hätte das Institut keine Möglichkeiten gehabt. Der Beweis, man habe die Informationen des Clubs nicht selbst abgerufen, wäre praktisch nicht zu erbringen. Allerdings wären in diesem Fall wohl alle rechtlichen Schritte ausgenutzt worden, um der Post ihre Fahrlässigkeit zu beweisen; ein Weg, den betroffene private Btx-Teilnehmer gegen die Post schwer durchstehen würden.

Die Findigkeit der Hamburger Chaos-Hacker hat der Hamburger Sparkasse Respekt abgenötigt; bei ihr und anderen dem Btx-System angeschlossenen Banken aber auch deutliche Irritationen ausgelöst. Der sofortige Austausch der Codewörter war eine Sache. Die noch nicht abgeschlossenen Überlegungen, welche weitergehenden Konsequenzen aus der Datenpanne gezogen werden müssen, sind eine andere.

Ogleich die Hacker weder im Rechner der Haspa selbst, geschweige denn auf einem Kundenkonto Unfug anrichteten, wird der Vorfall ernst genommen. Denn der CCC wollte nichts anderes, als diese eine Schwachstelle — eine unter vielen nach ihrer Aussage — möglichst schlagkräftig und rechtlich abgesichert nachweisen. Sie hatten — unlautere Absichten unterstellt — wesentlich schlimmere Schäden erreichen können, beispielsweise durch den Aufruf völlig fremder Sei-

ten zu Lasten diverser Benutzer, und das ohne jede Ankündigung oder sonstige Publicity.

„Wir werden“, so heißt es von seiten der Haspa, „besonders argwöhnisch beobachten, was sich beim Btx tut, und haben es zur Zeit nicht besonders eilig, uns dem Rechnerverbund der Banken anzuschließen.“

Der Vorgang überrascht nicht. Bereits im August 1984 hatte „Der Datenschutz-Berater“, ein Informationsdienst im Handelsblatt-Verlag, über die Aktivitäten des CCC berichtet. Auch auf der Datenschutzfachtagung der Gesellschaft für Datenschutz und Datensicherung (GDD) (Handelsblatt vom 20.11.) kam eine Reihe weiterer Schwächen offener Netze (Btx und Datex-P) zutage. So soll eine Mailbox beispielsweise dadurch zerstört werden können, indem mehrere Seiten für einen Empfänger angelegt werden. Die letzte Seite erhält dann eine Zeichenfolge (die Hacker haben diese Kombination allerdings nicht verraten), mit der die Mailbox wieder die erste Seite aufruft. Einmal in ein solches Perpetuum mobile gebracht, kann die Mailbox nur noch durch die Bundespost gelöscht werden.

Der Bundespostminister nahm am 20. November zu den Vorgängen in Hamburg Stellung. Danach wurden die „von einem jetzt erkannten Programmfehler betroffenen Eingabefunktionen sofort gesperrt“. Die Post hofft den Fehler in Kürze beheben zu können. Das Ministerium tröstet Btx-Benutzer mit dem Hinweis: „Soweit bei der Benutzung des Btx-Dienstes vergütungspflichtige Seiten abgerufen werden, wird auch nachträglich eine eindeutige Zuordnung der entstandenen Kosten ermöglicht, so daß eine unmittelbare Schädigung eines Btx-Teilnehmers ausgeschlossen ist“.

Außerdem unterstreicht die Post ihre Bemühungen um Datenschutz und Datensicherheit. Man arbeite derzeit mit Fachleuten an einem Untersuchungskonzept, um die Systemsicherheit „noch weiter zu erhöhen“.

HAMBURGER BTX-PANNE / 135 000 DM bei Hamburger Sparkasse abgebuht-Bundespost will Sicherheit der Software erhöhen

SCHLECHTE VORLAGE

