Thomas Barth

Hackersubkultur zwischen Web 2.0 und Bürgertrojaner. Der 24. Chaos Communication Congress

2008

https://doi.org/10.17192/ep2008.2.763

Veröffentlichungsversion / published version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Barth, Thomas: Hackersubkultur zwischen Web 2.0 und Bürgertrojaner. Der 24. Chaos Communication Congress. In: *MEDIENwissenschaft: Rezensionen | Reviews*, Jg. 25 (2008), Nr. 2, S. 124–126. DOI: https://doi.org/10.17192/ep2008.2.763.

Perspektiven

Thomas Barth

Hackersubkultur zwischen Web 2.0 und Bürgertrojaner

Der 24. Chaos Communication Congress

Als größte und traditionsreichste Veranstaltung nimmt der jährliche Chaos Communication Congress (CCC) der deutschen Hackersubkultur eine Sonderstellung unter den Conventions und LAN-Parties von Computerfans ein. Seit Anfang der 90er-Jahre zieht der Kongress auch Wissenschaftler aus Informatik, Sozial- und Medienwissenschaften an, die dort lernen, lehren oder einfach eine florierende, selbstorganisierte Medienkultur jenseits der üblichen, rein kommerziellen Eventwirtschaft beobachten können. Der CCC erlebte vom 27. bis 30. Dezember im Berliner Congress Center einen erneut angewachsenen Zulauf von Nachwuchshackern. Statt bislang 3500 versammelten sich diesmal 4200 Computerfans beim jährlichen Treffen des Chaos Computer Club (www.ccc.de). Mitte der 90er-Jahre waren es noch wenige Hundert gewesen. Die Avantgarde der Netzkultur profitiert augenscheinlich vom ungebremsten Ansturm der Jugend auf das neue Massenmedium. So entfaltete die virtuelle Medienkultur sich teils als wissenschaftlicher Kongress mit ordentlichem Call for papers, teils als medienpolitische Kundgebung, zumeist aber als netzkultureller Karneval und Happening im Sinne einer digitalen „Spaßguerilla". Das Web 2.0, Netzdemokratie, Datenhygiene, Biometrie und Überwachung waren aktuelle Schwerpunkte der größten europäischen Hacker-Convention des Jahres 2007. Der Althacker und Computerkünstler padeluun warnte vor neuen Gefahren eines stetig weiter aufgerüsteten Orwell-Staates und wünschte der Bevölkerung in diesem Sinne einen „guten Rutsch ins Jahr 1984."

Hacker haben auch in diesem Jahr zahlreiche Schwachstellen bei Servern aufgedeckt. Hunderte Websites wurden auf diesem Wege mit grotesken Botschaften oder dem Logo des Kongresses „geschmückt". Offenbar sittlich weniger an Jugendschutz orientierte Hacker platzierten bei den Kontrolleuren der Länderstelle www.jugendschutz.net eine spärlich bekleidete Schönheit. Einige der Website-Grafitti schienen politisch motiviert zu sein, wenn CDU und SPD-Websites den Rücktritt von Bundesinnenminister Wolfgang Schäuble (CDU) zu fordern vorgaben. Im Jahr 2004 rief ein vom Kongress ausgehender Massenhack zahlreicher kommerzieller Websites noch das LKA Berlin auf den Plan: Die Razzia endete jedoch ohne Erfolg, da eine Identifizierung der IP-Adressen der Täter nicht möglich war und die Beamten nur mit der Zusicherung abzogen, der Schaden würde repariert werden. Mehr Wirkung hatte die Reaktion der Geschädigten selbst, die ihrerseits massenhaft bei der Kongressleitung anriefen und den

entnervten Hackern ihr Leid klagten oder erbittert mit Schadenersatzklagen wegen entgangener Umsätze drohten. Nach dieser Erfahrung wurde angeregt, das Thema Hacker-Ethik wieder etwas öfter zu diskutieren. Ethisch desorientierten Hackern sollte eine „Hacker Ethics Hotline" im kongressinternen Telefonnetz helfen, im Einzelfall die moralischen Implikationen zu reflektieren. Man wollte damit, anders gesagt, dafür sorgen, dass ungebetene Sicherheitstester der Netzkultur nicht über die Stränge schlagen – was sich in diesem Jahr wohl wieder andeutete, ohne dass die Ethic-Hotline viel bewirkt hatte.

Besonders erbost hatte viele Hacker 2007 der sogenannte „Bundestrojaner", auch „Remote Forensic Software" genannt, der den Sicherheitsbehörden mittels online-Hausdurchsuchungen künftig einen gläsernen Bürger sichern soll. In einer spontanen Demonstration marschierten über 1000 Hacker vom Alexanderplatz zur Mitte des östlichen Stadtzentrums, um dort gegen die neuesten Sicherheitsgesetze zu protestieren. Nicht der Islam sei die größte Gefahr für unsere Gesellschaft, wie uns die bürgerlichen Medien rund ums Jahr vorbeten, siehe beispielsweise die vier schwarz grundierten Islam-Gefahr-Titelblätter des *Spiegel* im vergangenen Jahr. Höchst gefährlich sei vielmehr die politische Korruption. „Wir brauchen den Bürgertrojaner für mehr Bürgerbeteiligung", beschwor ein CCC-Aktivist die versammelten Computerfans und rief zu einer stärkeren Überwachung auf - allerdings nicht von Bürgern oder Moslems, sondern von „Problempolitikern". Für den Schutz unserer Gesellschaft sei es notwendig, frühzeitig Maßnahmen zur Abwehr der hohen Korruptionsgefahren zu treffen.

Ein auf dem Kongress heiß umstrittenes Thema war das sogenannte „Web 2.0". Der Terminus bezeichnet beliebte Internetdienste, die auf die Mitarbeit ihrer Nutzer abzielen, wie Flickr.com, YouTube oder Myspace. Dies wurde zwar als demokratische Innovation der passiven Surfer-Netzkonsumkultur gefeiert, als Rückkehr zu den aktiven Wurzeln des frühen Internet. Diese Mitarbeit liefert jedoch heute den kommerziellen Betreibern der Web 2.0-Dienste auch neue Ansatzpunkte zur Erstellung von Profilen der Teilnehmer und die Diensteanbieter haben ein mächtiges Druckmittel gegen ihre Kunden in der Hand: „Peer pressure", denn was nicht zu anderen Anbietern mitnehmbar ist, sind die Kontakte. Man könnte sagen, die sozialen Netzwerke werden zu proprietären Sozialstrukturen. Viele Web 2.0-Freundschaften hinterlassen im Netz interessante Informationen über ihre Nutzer für die automatisierte Analyse sozialer Netzwerke und der Big Brother der staatlichen Geheimdienste hat längst Gesellschaft durch zahlreiche Little Brothers der Medienindustrie erhalten. Die versuchte Übernahme der Musiktauschbörse Napster durch den Medienmulti Bertelsmann vor sechs Jahren war hier nur ein Auftakt, jüngst gab es beispielsweise Widerstand der Nutzergemeinde gegen den Datenhunger der Betreiber des Web 2.0-Studentennetzwerks StudiVZ, der sich nicht einmal an das Kopplungsverbot des Datenschutzrechts halten wollte und seine User zum umfassender Preisgabe persönlicher Informati-

onen zur Verwertung in der Werbeindustrie zwingen wollte. Nach Protesten und einer Austrittswelle nahm StudiVZ diese Forderungen zurück.

Der entspanntere Teil des Computerkongresses vergnügte sich mit Computerkunst, Videogames, dem Quiz „Hacker Jeopardy", Visionen vom „Space Communism" und dem Knacken des Codes von Pfandflaschen-Rücknahmeautomaten. Das politisch belanglose Flaschenthema wurde in der Kongressberichterstattung seitens der Mainstreampresse (*Stern*, *Spiegel* etc.) genregerecht zum Highlight aufgebauscht. Eine potentiell gesundheitsschädliche Entwicklung sehen Hacker im Pharmasektor auf uns zu kommen: Immer mehr Krankenhäuser setzen auf automatische Medikamentendosiergeräte unter dem wenig vertrauenerweckenden System Microsoft Access. Sind diese Geräte sicher? Wenn sie über das Internet vernetzt werden, wohl kaum. Nach aktueller CCC-Statistik vergehen bis zum ersten Angriff eines online gegangenen Rechners nur noch 39 Sekunden. Täglich werden derzeit ca. 30.000 Websites gehackt und bekannt gewordene Sicherheitslücken kann die Computerindustrie erst nach durchschnittlich 348 Tagen beseitigen.