news 31.12.2006 10:28

23C3: Netzbürger sollen "Problempolitiker" überwachen

Der Chaos Computer Club (**CCC[1]**) hat auf dem Jahreskongress der Hackerszene zu einer stärkeren Kontrolle von "Problempolitikern" durch die Netzbürger aufgerufen. Es gehe um einen "Ausbau der Überwachung auf allen Ebenen", wobei auch "Problemgruppen" wie Regierungsmitglieder stärker im Auge behalten werden müssten, betonte der Ex-CCC-Sprecher Ron am Abschlusstag des 23. Chaos Communication Congress (**23C3[2]**) in Berlin. Angesichts der vielen Berichte über schwarze Kassen handle es sich schließlich um potenzielle Straftäter, bei denen Maßnahmen zur Gefahrenabwehr zu treffen seien. "Politiker bestechen und drücken Gesetze durch, damit Firmen mehr Geld kriegen", ergänzte CCC-Veteran Frank Rieger. Im kommenden Jahr müsse daher eine "ordentliche Datensammlung über alle Politiker" aufgebaut werden, diese hätten schließlich prinzipiell "nichts zu verbergen".

Mit der Forderung schließt sich der CCC zivilgesellschaftlichen Bestrebungen zur Schaffung von mehr Transparenz in der Politik an, wie sie etwa mit der Plattform Abgeordnetenwatch **gestartet[3]** sind. Zugleich reagiert er auf die zahlreichen unlängst unter dem Aufhänger der Terrorismusbekämpfung **verabschiedeten[4]** oder **geplanten[5]** Gesetze, mit denen die Überwachung der Bürger deutlich verstärkt und die Grundrechte massiv eingeschränkt werden (sollen). Der Aufruf erfolgte allerdings in dem traditionell mit viel Hackerironie gewürzten Ausblick auf die kommenden "Sicherheits-Albträume" und die Entwicklungen "über die wir nächstes Jahr lachen werden".

Die Vorstellungen der Datenreisenden waren dennoch sehr konkret. "Einzelverbindungen, Transaktionsnachweise – wir wollen alles", machte Ron deutlich. Wenn sich etwa ein Politiker über "Killerspiele" aufrege, müsse der Öffentlichkeit bekannt sein, "was auf seiner Festplatte ist". Sonst könne man nicht erkennen, ob er wisse, von was er rede. "Fingerabdrücke wollen wir natürlich auch haben", sekundierte Rieger verknüpft mit dem Appell: "Sammelt Gläser!" Auf dem Hackertreffen war zuvor gezeigt worden, wie einfach man Fingerabdrücke zur Überlistung biometrischer Systeme auch bei Biergelagen erheben kann. Letztlich würde es sich bei der Öffnung der Politiker gegenüber den Bürgern laut Ron um vertrauensbildende Maßnahmen handeln.

"Wir sehen da auch Fortschritte beim E-Government", spann der Hamburger Hacker den Faden in die andere Richtung weiter. "Das BKA wird Trojaner einsetzen, das muss man konsequent weiterdenken." Es folge der "internetbasierte große Lauschangriff und die Self-Service-Hausdurchsuchung. Jeder muss eine Kamera haben, an den PC anschließen, damit die Staatsanwaltschaft die Schränke durchsehen kann." Um Geld zu sparen, würden die "**Online-Durchsuchungen[6]**" ausgelagert und mit einer "extended Workbench in Bangalore" verknüpft. Weiter prophezeiten die Hacker, dass 2007 Gerätetreiber "öfter mal fällig sind". In diesem Jahr seien bereits Probleme mit Grafikkarten, **dem WLAN-Chipsatz[7]** bei Intels Centrino-Plattform oder **Embedded Systems[8]** aufgetreten, führte Ron aus. Im kommenden Jahr würden Kopierer, Festplatten, "Media-Player-Extraboxen" oder "Null-Euro-Router" eine ganz neue Infrastruktur für großflächige, "homogene" Angriffe bieten. Besonders letztere hätten Attacken wenig entgegensetzen, da sie von den Providern häufig mit standardmäßig vorgegebenen Passwörtern ausgeliefert würden. Dies müsse man aber "wertneutral" sehen. Man könne ja nicht nur Spam- oder Trojanerbotnetze daraus basteln, sondern auch Knoten für das Anonymisierungsnetzwerk Tor. Es hätte "umwelttechnische Vorteile", wenn man diese "für wenig Watt am Tag" betreiben könne. Ron beklagte in diesem Zusammenhang auch, dass noch immer kein "computer-aided Industriespionagefall" veröffentlicht worden sei. Auf die Frage in die Runde, ob jemand in diesem Bereich Hinweise auf gezielte Trojanerangriffe habe, kamen keine Details zutage.

Weitere Punkte für mögliche Sicherheitsdebakel waren die neuen Zigarettenautomaten mit Alterskontrolle

über Chipkarten, der zunehmende "ungeschützte USB-Verkehr" sowie Industrieroboter. Auch in der Fertigungsbranche gebe es langsam den Trend, auf Ethernet oder gar drahtlose Vernetzungstechniken umzusteigen und die Maschinenhelfer zusammenzuschalten, berichtete ein Kongressbesucher. Bald müsse man sich daher wohl nur noch auf "einen Parkplatz vor einem Opel-Werk stellen", um sich sein maßgeschneidertes Fahrzeug selbst zusammenbauen zu können.

Revue passieren ließen die Hacker zudem die Prophezeiungen aus dem vergangenen Jahr. "Die WM war ein großer Spielplatz, der Hacker brach sogar im Otto-Normal-Verbraucher durch", unkte Ron unter Anspielung auf die **Kernvoraussage[9]** von 2005. Selten seien Fragen nach den am wenigsten bewachten Eingangsschleusen in Stadien oder nach der Brisanz des Unterschieds zwischen einer physikalischen weiblichen Existenz und einem Männernamen auf einem Ticket öffentlich derart heiß diskutiert worden wie im Sommer. Das Vorhaben von CCC-Vertretern, die RFID-Chips auf den begehrten Einlasskarten zu klonen, scheiterte allerdings. Ein Test endete an einer rot aufleuchtenden Warnlampe. Wie auf dem Kongress zu hören war, sei man aber theoretisch dazu fähig gewesen, ein auf den Zustand "im Stadion" gepoltes Ticket auf "draußen" umzustellen und so Mehrfacheintritte zu ermöglichen.

Mit einiger Verspätung sahen sich die Sicherheitstester auch in noch früheren Blicken in die Glaskugel bestätigt. So hätten im Lauf des Jahres die längst angekündigten Trojaner-Kriege mit dem Fall "**SpamThru vs. Kaspersky Engine[10]**" begonnen, während es die Anti-Virenfirma Symantec Rieger zufolge mit dem "**Big Yellow[11]**"-Wurm "bis zur Botnetzplattform" gebracht habe. Noch immer nicht verwirklicht habe sich dagegen die Prognose eines "gesprengten Biometrie-Einkaufsystems in einem Supermarkt", was aber nur noch eine Frage der Zeit sei.

Der Prognose glatt entgangen sei die im Ausland **vermeldete[12]** "deutsche Spionage im britischen Müll" und dass die **dafür genutzten[13]** RFID-Chips in hiesige Mülltonnen schon seit längerem zum einfacheren Wiegen eingebaut würden. Es sei dann wohl bald mit einem "Mülltonnen-Blitzkrieg" zu rechnen, fiel Ron dazu nur noch ein. Abschließend forderte er die Hackergemeinde auf, sich angesichts der **Sicherheitslücken[14]** bei Wahlmaschinen in 2007 als Wahlbeobachter zu engagieren. (*Stefan Krempl*) /

(**vbr[15]**/c't) (vbr/c't)

URL dieses Artikels:
http://www.heise.de/newsticker/meldung/83063

Links in diesem Artikel:
[1] http://www.ccc.de/
[2] http://events.ccc.de/congress/2006/Home
[3] http://www.heise.de/newsticker/meldung/82978
[4] http://www.heise.de/newsticker/meldung/81859
[5] http://www.heise.de/newsticker/meldung/80785
[6] http://www.heise.de/newsticker/meldung/82962
[7] http://www.heise.de/security/news/meldung/76262
[8] http://www.heise.de/newsticker/meldung/33336
[9] http://www.heise.de/newsticker/meldung/83056
[10] http://www.heise.de/newsticker/meldung/79836
[11] http://www.heise.de/newsticker/meldung/82664
[12] http://www.schneier.com/blog/archives/2006/09/germans_spying.html
[13] http://www.heise.de/newsticker/meldung/77348
[14] http://www.heise.de/newsticker/meldung/83011
[15] mailto:vbr@ct.heise.de