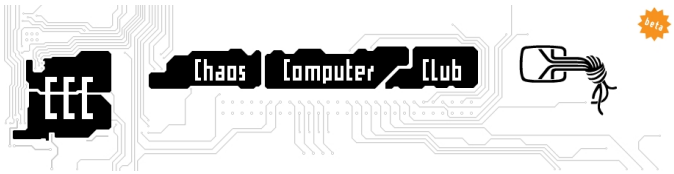
Geschrieben von: online@info8.ch
Mittwoch, den 29. Dezember 2010 um 15:18 Uhr



Seit dem 27. Dezember läuft im Berliner Congress Centrum der 27te Chaos Communication Congress. Ziel der Veranstaltung, welche jährlich vom Chaos Computer Club (CCC) organisiert wird, ist es potentielle Sicherheitslücken in den elektronischen Kommunikationssystemen aufzuzeigen. Seit einigen Jahren dient der Anlass auch dazu, Webseiten von politisch missliebigen Organisationen zu zerstören. **Grosse Lücken im Mobilfunkbereich** Nebst vielen praktischen Demonstrationen zu aktuellen Sicherheitslücken finden bis zum 30. Dezember diverse Vorträge rund um das Thema Sicherheit statt. Der diesjährige Schwerpunkt der Veranstaltung liegt hauptsächlich im Aufzeigen der Sicherheitslücken rund um die Mobilkommunikation. Der Höhepunkt bildet eine Demonstration zweier Informatikstudenten der Technischen Universität Berlin, welche mit präparierten Kurzmitteilungen Mobiltelefone verschiedenster Hersteller abstürzen liessen. Ausserdem haben Forscher gezeigt, dass es mit einfachen Hilfsmitteln und dem entsprechenden Fachwissen auch Zivilpersonen möglich ist, Telefongespräche über GSM Mobilfunknetze abzuhören. Diese Tatsache sorgte für grossen Wirbel in der Fachwelt, so war es doch bis anhin nur staatlichen Behörden möglich, mit teuren Profigeräten, Abhörungen in ähnlichem Ausmass durchzuführen.

Kontroverse um WikiLeaks

Wie bereits im Vorfeld vermutet, spielte auch die Plattform WikiLeaks eine entscheidende Rolle. Auf der einen Seite unterstützen die Forenteilnehmer die Bemühungen nach transparenten Abläufen bei Firmen und Organisationen. Der Eröffnungsredner Rob Gonggrijp befürchtet jedoch, dass die Regierungen aufgrund der veröffentlichten Dokumenten neue Gesetze im Bereich von Netzsperren und Internetzensur anstreben werden, was nicht im Sinn des CCC sei.

Komplexität bei Computerviren steigt

Mit Brunce Dang, einem berühmten Malewarespezialist von Microsoft, konnte der CCC auch eine internationale Berühmtheit für sich gewinnen. Dang erläuterte in seinem Vortrag, wie die äusserst komplexe und zeitaufwändige Suche nach den Sicherheitslücken ablief, welche der Computerwurm Stuxnet für sich ausgenutzt hat. Bei Stuxnet handelt es sich um den Wurm, der im Juni 2010 entdeckt wurde. Man vermutet nach wie vor, dass Stuxnet zum Ziel hatte, gezielt Urananreicherungsanlagen im Iran lahmzulegen. Auch andere Sicherheitsexperten von renommierten Antivirenherstellern räumten ein, dass es aufgrund der gesteigerten Komplexität von Computerviren immer schwieriger wird, zeitnahe Virendefinitionen und Updates zur Verfügung zu stellen.

Politische Abreibungen unter dem Deckmantel der Sicherheit

Seit einigen Jahren werden am Anlass Versuche unternommen, bei bestimmten Webseiten

Sicherheitslücken aufzudecken. Dazu wird jeweils zu Beginn des Kongresses eine Liste mit den potentiellen Zielen veröffentlicht. Wirft man einen Blick auf diese Liste, so beschleicht einem der verdacht, dass hier gezielt Ziele auserwählt werden, welchen der CCC eine persönliche Abreibung verpassen möchte. Auf dieser Liste potentieller Ziele befinden sich auch verschiedene Schweizer Webseiten, wie zum Beispiel die der SVP, SP oder PNOS. Auch kommerzielle Organisationen wie die Billag oder die Webseite des Fussballklubs Grasshoppers geraten ins Kreuzfeuer der Hacker. Bei Erfolg beschränkt sich der CCC oft nicht nur auf ein simples Anbringen einer Warnmeldung auf der infiltrierten Webseite. Im Falle eines Versandes wurden anschliessend Auszüge aus der Kundendatenbank inklusive Passwörter ins Internet gestellt. Spätestens mit diesem Vorgehen wurde der gewählte Slogan „We come in peace“ ad Absurdum geführt.