Kriminelle Serviceprovider bieten ihre Dienste allen an

cirosec GmbH
Edisonstraße 21
74076 Heilbronn
Tel: 07131 / 59455-0
Fax: 07131 / 59455-99
info@cirosec.de
www.cirosec.de

IT-Sicherheit: Als 2008 der kalifornische Internetprovider McColo vom Netz genommen wurde, brachen auf einmal mehr als 30 % der weltweiten Spamlast weg. An bestimmten Orten trafen sogar 90 % weniger E-Mail-Müll ein. Doch McColo ist kein Einzelfall.

Der amerikanische Hoster McColo ist weit mehr gewesen als eine Spamschleuder, sondern ein sogenannter „Bulletproof Hoster“, ein nach außen gut getarnter Serviceprovider für das organisierte Verbrechen.

Einen Einblick in diese wenig bekannte Seite des Internets, wo organisiertes Verbrechen und staatlich kontrollierte Dienste zusammenarbeiten, gab Oberstleutnant Volker Kozok, Referent im Bundesministerium der Verteidigung, auf der diesjährigen Sicherheitstagung „IT-Defense“. Kozok sprach ausdrücklich als IT-Sicherheitsexperte und nicht als Behördenvertreter.

Offiziell fühlt sich Deutschland durch Bulletproof Hoster nicht bedroht. Bulletproof Hoster bieten Dienste rund um das Internet an, allerdings mit dem Unterschied, dass sie „ihre Angebote kugelsicher gegen Ausspähversuche durch Ermittlungsbehörden abschirmen, unter falschen Adressen residieren und ihren Datenverkehr mehrfach umleiten“, unterstrich Kozok. Man operiert international. McColo wurde von drei Russen gegründet, der Zahlungsverkehr wurde über Osteuropa abgewickelt und als Handelsware dienten unter anderem gefälschte Arzneimittel aus Indien. In den USA hatte die Firma ihren Sitz und dort standen ihre Server.

McColo, so weiß man heute, ging nicht aufgrund von Selbstreinigungskräften des Internets vom Netz. Vorausgegangen waren zweijährige Ermittlungen von neun US-amerikanischen Behörden, inklusive des FBI und der Nasa. In einem Hinterzimmer in Palo Alto in Kalifornien stießen Fahnder des FBI schließlich auf das Computerherz von McColo. Mehrere Regale voller Server. Fein säuberlich nach Verwendungszweck getrennt.

Mit einem Schlag verschwanden Hunderte von kriminellen Internetseiten aus dem Netz. Weltweit operierende Anbieter von gefälschten Medikamenten, von kinderpornografischen Darstellungen oder für Geldwäsche verloren ihre Handelsplattform.

In Deutschland beschränkte sich das Echo hauptsächlich auf das kurzfristig eingebrochene Spamaufkommen. Doch McColo erwies sich als eine weit größere Gefahr, das ergab ein internationaler Workshop, zu dem die Deutsche Bundeswehr eingeladen hatte. Auf der Messe IT-Defense erfuhren zivile Sicherheitsexperten dann erstmals etwas über die Ergebnisse dieser Tagung. McColo war, so weiß man heute, nur eines von mehreren kriminellen Hosting-Netzwerken, die dem organisierten Verbrechen, aber auch Staaten ihre Dienste offerieren.

Sie bieten qualitätsgeprüfte Schadsoftware wie Viren und Trojaner, in denen teilweise mehrere Mannjahre Entwicklungsarbeit stecken, sowie fertig programmierte Phishing-Seiten, um Kreditkarteninformationen abzugreifen. McColo-Kunden gelangten über solche Dienste in den Besitz von 500 000 Onlinezugangsdaten bzw. Kreditkartennummern.

Eine weitere wichtige Handelsware sind infizierte Roboternetze, sogenannte Botnets. Die Eigentümer dieser Rechner ahnen nicht einmal, dass ihr PC mit einem Trojaner infiziert wurde, und nun selbst als kriminelles Angriffswerkzeug dient. 15 000 Rechner eines Botnets kosten pro Stunde 1500 $ Miete. Die größten Spamschleudern der Welt verschicken über solche Botnets geschätzte 60 Mrd. Spammails pro Tag.

In den USA gibt es mittlerweile eine exakte Definition. Jeder Internet-Serviceprovider (ISP), der mindestens 90 % seiner Umsätze mit kriminellen Diensten erwirtschaftet, ist ein Bulletproof Hoster. Im Baltikum sollen nach Angaben von Experten 80 % aller ISP dieser Definition genügen. Da Milliardengewinne winken, vergrößert sich die Zahl ständig. Die größten Botnets umfassen nach US-Erkenntnissen über 100 000 Rechner. Eine Armee, die ausreicht, kritische Infrastruktur durch massenhaft versendete, sinnlose Botschaften lahmzulegen.

Während des Konfliktes mit Russland waren alle öffentlichen Einrichtungen von Georgien vom Netz abgeklemmt, Täter waren damals angeblich Studenten, Experten vermuten allerdings eher gekaufte Bulletproof Hoster. Deutschland beschwerte sich kurz darauf diskret bei China über – erfolglose – Attacken auf Bundeswehreinrichtungen und das Innenministerium, die über das Ghostnet liefen – ein weiteres Bulletproof-Netzwerk, das immer noch online ist. Wie andere auch.

vdi-nachrichten.com 30.07.10