

Motieven cybercrime veranderen

03-02-2010 - *Hacken als hobby en het waarschuwen van organisaties voor mogelijke veiligheidslekken behoren, volgens beveiligingsspecialist Sophos tot het verleden. Malwareverspreiders gaat het nu om commerciële, politieke, economische en militaire invloed te krijgen over tegenstanders.*

Branche: Automatisering

Volgens het onderzoek Security Threat Report: 2010 lieten de eerste tien jaar van de eenentwintigste eeuw een grote verandering zien op het gebied van computercriminaliteit. Waar vroeger hackers nog ging om aandacht en plezier, zitten achter de huidige malwareverspreiders professionele criminele organisaties verscholen. De onderzoekers constateren in plaats van onschuldig verspreide plaatjes, nu pogingen tot diefstal van intellectueel eigendom, het bouwen van complexe zombienetwerken en identiteitsdiefstal.

Internationale actie

Om de georganiseerde cybercriminelen een halt toe te kunnen roepen, vragen de malwarebestrijders om meer internationale actie. Landen moeten zowel lokaal als internationaal ervoor zorgen dat dit soort criminelen geen toevluchtsoord kunnen vinden en dat zogenoemde 'rogue nations' geen mogelijkheden krijgen om cybercrime in te zetten bij hun (politieke) doelen.

Gevaren

Tot de grootste gevaren voor het huidige internet, zien de onderzoekers van Sophos de opkomst van sociale netwerksites als Facebook, MySpace en Twitter. Sinds april 2009 zien steeds meer bedrijven en organisaties deze sociale netwerken als de grootste bron van malwareverspreiders. Ook zien zij het gedrag van hun medewerkers op deze websites als een toenemende risicofactor. Spam dat via deze netwerken wordt verspreid is inmiddels een algemeen gegeven. Ook worden sociale netwerksites in toenemende mate gebruikt voor sociale engineering en identiteitsdiefstal, aldus Sophos.

Bron: www.infosecurity.net, 03-02-2010