BIZCOMMUNITY

three6five assesses local Internet threat levels

Local networking services company, three6five, recently conducted an experiment to assess the South African Internet threat levels and has concluded that there is no network that can afford to be caught naked on the Internet. Three6five co-owner, Jeff Fletcher said that it is critical to understand what a threat on the Internet looks like from a South African perspective and what steps to take to protect a network.

Fletcher said that three6five's local study addressed what local Internet threats look like, where they come from and how they are carried out. By installing a honeypot server on the three6five WiMAX link with a public IP address, Fletcher says the server acted as a decoy, luring in potential hackers to study their activities and monitor how they are able to break into a system.

"A honeypot exposes what appear to be standard network services to potential hackers and mimics systems that an intruder would likely attempt to break into without exposing any real services and risk the rest of the network," says Fletcher. If successful, the intruder will have no idea about being tricked and monitored. Most honeypots are placed outside the network on the Internet facing side of the firewall or DMZ.

The leading countries

The initial data was collected throughout September and revealed that the United States and China were the leading countries in terms of where attacks originated from, with 178 and 117 attacks per unique IP, per month respectively. Top exploits included ssh, Microsoft-DS, mail, Netbios and http.

The number of attacks by type was evenly split between Microsoft and Linux. While some services are Microsoft specific like Netbios, others are applicable to both (http) and some work on both (ssh) but are usually found on Linux. Fletcher says that when looking at the distribution from a unique IP source and not the total number, the picture changes slightly with Linux leading. Brute force attacks seem more concentrated on the Microsoft services.

User names that were used to attempt to break into the ssh service differed, but the word 'user' was by far the

most popular with over 4 000 attempts within a month. This was more than likely due to a brute force attack attempt. Fletcher says that 'oracle' was the next popular ssh user name used, with about 100 break in attempts followed by mundane words such as nagios (a popular nms system), admin and test."

Person or machine?

"One thing that was difficult to tell was whether these were attacks directed by a person behind a machine, or a compromised computer on the Internet running a set of scripts," says Fletcher. There was no evidence to correlate the time of day with the number of attacks from a particular area, which led Fletcher to conclude that this was mostly automated attacks.

Hacking is progressive, making a proactive approach to security and the implementation of firewalls critical. "The biggest issue when it comes to security and the maintenance thereof is people. Firewalls will provide you with the basic, minimum level of security needed to protect you from the outside world, but companies will need to ensure they manage the people that work on their systems as well," he says.

The company will continue to monitor and grow its honeypot server and network, working with other local security groups where possible and report on the results. Providing bespoke local information will assist local companies to better understand Internet threats and how to protect their networks.

"What we hope to achieve with the project is a better understanding of which networks in South Africa are more under threat and also to see if certain times of day or weeks of the year have a higher than average number of attacks and try understand why," concludes Fletcher.