



Study says half of firewalls tested have serious flaws

13 February 2011
Luke Collins

Half of the firewalls tested by a security analysis company have serious flaws.

Rick Moy, president of NSS Labs, a security hardware test lab and analysis company, told delegates at last weeks NetEvents meeting: "We're doing a report on the security of the firewall itself, and we have found that half of the firewalls we tested from major manufacturers have serious flaws which allow an attacker to break through."

The problem, according to Moy, is that security threats are evolving so quickly that hardware is constantly being updated with new software.

"There are still software updates made quite regularly and every time you change the software you have the opportunity to break something," he said.

Moy said that poor software quality assessment strategies could lead to individual attacks or even whole classes of attack could be missed in the race to update the software.

"We need to be thinking about our security devices as software that needs constant testing," he added. "In antivirus we are rolling out multiple software updates to the desktop every day."

Moy said these constant updates break the acceptance criteria model that many companies use to control the introduction of new software.

"What I am advocating is that IT departments should have more of a mindset of continuous testing," he added.

Jason Brvenik, vice president for security strategy in the technology research group at IT security company Sourcefire, argued that the key to overcoming this issue was to use an open-source approach to code development.

"Openness is your only defence," he said. "You can review my stuff all the way down to the source code.

"A closed approach allows people to not be as diligent as they might."

<http://www.nsslabs.com/>

<http://www.sourcefire.com/>

<http://neteventstv.blogspot.com>

<http://eandt.theiet.org/news/2011/feb/half-fire.cfm>