Print Close

the INQUIRER

Oracle loses the social engineering competition at Defcon

Gives informatiom up too easily
By Lawrence Latif
Mon Aug 08 2011, 13:14

SECURITY RESEARCHERS at Defcon highlighted one of the reasons why there have been so many high-profile security breaches by showing how easily staff succumbed to social engineering techniques.

During the weekend, researchers at Defcon highlighted how easy it is for would-be 'hackers' to get employees of large companies to divulge information that could be used in attacks. The approach, known as social engineering, essentially results in sensitive information being acquired through subterfuge rather than stolen.

Reuters reports that in one case, a contestant taking part in a Defcon competition pretended to work for a company's IT department and got an employee to hand over information on what PC she was using. Chris Hadnagy, one of the Defcon organisers told Reuters, "A lot of this could facilitate serious attacks if used by the right people."

Hadnagy said that Oracle's employees handed over more data than those of any other company targeted in the competition. Other targets included Apple, AT&T, Symantec, United Airlines and Verizon.

Social engineering is a well known tactic of acquiring information from people. The application of social engineering in computer hacking became widely known following the 2002 publication of *The Art of Deception* by legendary hacker Kevin Mitnick following his release from prison.

What the security researchers have highlighted is that firms need to spend a great deal more time and money on training front line staff to be aware of such tactics. Although information given out through social engineering might on its own seem inconsequential, in some cases it can provide the 'in' that hackers are looking for. µ

Print Close