» Print

Oracle, other companies "punkd" in hacking contest

Mon, Aug 8 2011

By Jim Finkle

LAS VEGAS (Reuters) - A weekend contest at the world's largest hacking convention in Las Vegas showed one reason why big corporations seem to be such easy prey for cyber criminals: their workers are poorly trained in security.

Amid a spate of high-profile cyber assaults on targets ranging from Sony Corp to the International Monetary Fund, one would think that many companies would be paying special attention to security these days.

But hackers taking part in the competition on Friday and Saturday found it ridiculously easy in some cases to trick employees at some of the largest U.S. companies to reveal information that can be used in planning cyber attacks against them.

The contestants also managed to get employees to use their corporate computers to browse websites the hackers suggested. Had these been criminal hackers, the websites could have loaded malicious software onto the PCs.

In one case, a contestant pretended to work for a company's IT department and persuaded an employee to give him information on the configuration of her PC, data that could help a hacker decide what type of malware would work best in an attack.

"For me it was a scary call because she was so willing to comply," said Chris Hadnagy, one of the organizers of the contest at the Defcon conference in Las Vegas.

"A lot of this could facilitate serious attacks if used by the right people," Hadnagy said.

Defcon is organized by benevolent hackers, partly to promote research on security vulnerabilities in order to pressure companies to fix them. The contest was sponsored by so-called white-hat hackers to show companies how weak their security is and encourage them to better educate their employees about the risks of hacking.

The company whose employees handed over the most data was Oracle Corp, according to Hadnagy. One of the world's largest software makers, Oracle got its start more than 30 years ago by selling secure databases to the Central Intelligence Agency.

Oracle spokeswoman Deborah Hellinger declined comment.

Other targets included Apple Inc, AT&T Inc, ConAgra Foods Inc, Delta Air Lines Inc, Symantec Corp, Sysco Corp, United Continental Holdings Inc's United Airlines and Verizon Communications Inc.

It was the second year that Defcon held a contest in "social engineering," or the practice where hackers con people into handing over information or taking actions such as downloading malicious software.

Social engineering is frequently used in attacks where the hackers send a "spear phishing" e-mail in which they impersonate a friend of the recipient and ask him or her to open a tainted file or visit a malicious website.

Security experts say spear phishing have led to many hacks over the past year, including ones on U.S. defense contractors, the IMF, EMC Corp's RSA Security division and government agencies around the world.

"It's better whenever you can get data non-confrontationally," said Johnny Long, a consultant who companies hire to hack into their data networks, using tools such as social engineering, to identify weaknesses.

The contestants were charged with obtaining specific information from their targets, including information about how the company backs up and secures its data, wireless network use, and the names of companies that provide on-site security, toner and copier paper.

(Reporting by Jim Finkle, editing by Tiffany Wu, Gary Crosse and Matt Driskill))