Twitter Busted by Old Technique – Again

Jordan Robertson,AP Technology Writer

SAN FRANCISCO (AP) -- Breaking into someone's e-mail can be child's play for a determined hacker, as Twitter Inc. employees have learned the hard way — again.

For the third time this year, the San Francisco-based company was the victim of a security breach stemming from a simple end-run around its defenses. In the latest case, a hacker got the password for an employee's personal e-mail account — possibly by guessing, or by correctly answering a security question — and worked from there to steal confidential company documents.

The techniques used by the attackers highlight the dangers of a broader trend promoted by Google Inc. and others toward storing more data online, instead of on computers under your control.

The shift toward doing more over the Web — a practice known as "cloud computing" — means that mistakes employees make in their private lives can do serious damage to their employers, because a single e-mail account can tie the two worlds together.

Stealing the password for someone's Gmail account, for example, not only gives the hacker access to that person's personal e-mail, but also to any other Google applications they might use for work, like those used to create spreadsheets or presentations.

That's apparently what happened to Twitter, which shares confidential data within the company through the Google Apps package that incorporates e-mail, word processing, spreadsheet, calendar and other Google services for $50 per user per year.

Co-founder Biz Stone wrote in a blog posting Wednesday that the personal e-mail of an unnamed Twitter administrative employee was hacked about a month ago, and through that the attacker got access to the employee's Google Apps account.

Separately, the wife of co-founder Evan Williams also had her personal e-mail hacked around the same time, Stone wrote. Through that, the attacker got access to Williams' personal Amazon and PayPal accounts.

Stone said the attacks are "about Twitter being in enough of a spotlight that folks who work here can become targets."

Stone said the company is talking to lawyers about "what this theft means for Twitter, the hacker, and anyone who accepts and subsequently shares or publishes these stolen documents."

What the attacks on Twitter show is that Web sites don't need to get compromised in the traditional sense to put its users and employees at risk.

Hackers don't need to find a vulnerability in the site itself, or plant a virus on an employee's computer, to sneak inside. The easier approach is much more low-tech: All they need to find is an employee who uses weak passwords for his or her e-mail accounts, or has security questions that are easy to answer with a little information about the person.

Source URL (retrieved on *07/23/2014 - 1:19pm*):
http://www.wirelessdesignmag.com/product-releases/2009/07/twitter-busted-old-technique-%E2%80%93-again?qt-blogs=0&qt-digital_editions=0