



Password Overload Makes Enterprise Systems Less Secure

The stricter security managers get with passwords, the more users work to undermine the effort, according to a study by RSA Security, which makes authentication technology that beefs up password-protection.

By Gregg Keizer
TechWeb News

A glut of passwords and mounting frustration over the clumsy way they're managed actually makes enterprise systems less secure, not more, a survey released by RSA Security claimed Tuesday.

According to the poll of some 1,700 enterprise end users, 28 percent of corporate workers juggle 13 or more passwords required to access Windows, specific applications, and Web portals. Another 30 percent have to deal with between 6 and 12 passwords.

And almost all are tired of it. Nearly nine out of ten said they were frustrated with managing so many passwords.

It shouldn't be a surprise, then, that strict password policies -- multiple passwords, long and complex passwords, and frequently-changed passwords -- spur users into risky behavior that undermines corporate security.

When memorizing passwords doesn't work, users instead turn to insecure techniques, said the survey, including recording passwords in a spreadsheet worksheet or on a PDA, or writing them down and keeping the paper or Post-It in the office.

More than 60 percent, in fact, admitted to recording passwords somewhere. Amazingly, 4 percent said they had a written record of passwords affixed to their work PC.

One solution, said Vic DeMarines, a senior product manager with Bedford, Mass.-based RSA, would be a master password that would lock up all other passwords, a "key to the kingdom" of sorts. But users are even leery of that fix.

"They like the idea of a master key, but they recognize that they would use it only if there was enough strength to that master password," DeMarines said. "That call for stronger security on the master could be a potential tie to a stronger authentication technology, like a token," he added.

The hit on enterprise bottom lines isn't measured only by the number of workers angry over password complexities, but also by the number of help desk calls for password resets, said DeMarines.

The vast majority (82 percent) of those polled said that the IT department's help desk had to be involved in any password change or reminder of an existing password. Lost productivity also comes into play, since 65 percent of the users surveyed said they waited for up to 15 minutes for IT to reset a lost or forgotten password.

Most depressing is that the situation is likely to get worse, not better. "There's a definite connection between the number of passwords and compliance initiatives like Sarbanes-Oxley and HIPPA," said DeMarines, "but people are also increasingly aware of passwords because of threats like spyware. Passwords will continue to grow, based on the heterogeneous composition of company's infrastructures and the [increasing] Web portals needed to do business."