NUCLEUS RESEARCH

September 2006 Document G68

RESEARCH NOTE
BENCHMARKING: PASSWORDS — THE SAD TRUTH ABOUT SECURITY

THE BOTTOM LINE

Unfortunately, more than one out of every three enterprise users keep a written record of their passwords. Contrary to popular belief, a survey of 325 users found that making users choose complex passwords or change them frequently doesn't make them more likely to write them down. Companies that want to ensure security should look beyond passwords to other authentication strategies.

Given the rise in security threats and the concern for greater security, many organizations have looked to multiple password schemes, biometrics, and other security measures to ensure only authenticated, authorized users can access corporate information. However, despite the greater investment in identity management technology, IT users may be their own worst security enemy.

In a recent survey of 325 respondents Nucleus Research fielded through KnowledgeStorm, Nucleus found that whether the companies require complex passwords or frequent password changes has little bearing on how individual end users manage their passwords.

Unfortunately, more than one in three enterprise users keep a written record of their passwords — despite the clear security risks of doing so.

Of the third of users that write down their passwords, one third of those do it on paper, such as a sticky note. Even more dangerous are the other two thirds: they keep their passwords as a text file on their laptop PC or mobile device, where it could be easily lost or stolen.

There was no clear correlation between password complexity and the propensity to write down passwords.

WHAT'S YOUR PASSWORD SECURITY PROFILE?

There are three key components that characterize a company's password policy and determine whether your policy is restrictive, average, or lenient:

- Complexity is how complicated users' passwords must be.
- Frequency is how often users are required to change their passwords.
- Quantity is how many passwords users have for enterprise applications.

Complexity

Fifty-four percent of companies require users to select passwords that include letters and numbers; 38 percent require letters, numbers, and a special character; 8 percent require only letters in passwords.

Corporate Headquarters
Nucleus Research Inc.
36 Washington Street
Wellesley MA 02481
Phone: +1 781.416.2900
Fax: +1 781.416.5252

Nucleus Research Inc.
www.NucleusResearch.com

RELATED RESEARCH

G41 Systems management ROI

F83 Desktop security best practices

D34 M-tech's ROI: solving the corporate IT identity crisis

Frequency

Twenty-two percent of enterprise IT users are required to change their passwords as frequently as once a month; 34.3 percent are required to change their passwords every one to three months; 23 percent are not required to change their passwords.

Requiring users to change their passwords often didn't drive a greater use of written password records either.

Quantity

Nineteen percent of enterprise IT users use only one password to access enterprise applications at work; 35 percent use two or three different passwords; 46 percent use four or more passwords.

Although single sign-on may be convenient, it didn't reduce the likelihood users would write down their passwords either: whether users had one, two to three, or four or more passwords to remember at work, roughly one third of all of them wrote down their passwords.

There was also no correlation between complexity, frequency, and quantity and how often users called the help desk with password-related issues. Seventy percent of enterprise users call the IT help desk once a year for help with a forgotten or missing password; 16 percent call two to three times a year; 9 percent call three to five times a year; and 5 percent call more than five times a year for password help.

CONCLUSION

Improving the security of the enterprise IT environment is always a challenge: companies must balance demands for security with the flexibility needed to get things done. In the case of passwords, it's important to recognize that no matter what process you put in place, the human factor is not going to change: one third of users will continue to keep written records of passwords.

Whether your current password policy makes you restrictive, average, or lenient has no impact on whether or not users write down their passwords — and any change in your password process will have little effect.

Educating users on password security may have some effect. However, this study shows that if you're looking for real access security, you'll need to look beyond passwords. Some companies look to biometrics to increase security; other vendors such as Unomi are promoting cognitive biometrics as a higher-level authentication technology. Companies concerned about password security should continue to watch innovation in the authentication market.