Staggering

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Most security administrators have figured out that having passwords expire on a specific day of the calendar is a prescription for a swamped help desk. The day after the expiration deadline, the poor help technicians are flooded with demands from irate users who have forgotten their new passwords (perhaps they forgot to write the new sequence on a sticky note attached to their screen or to "hide" the new password inside their unlocked desk drawer or under their keyboard)(sigh).

If you are still stuck using passwords, as most organizations are, a far better approach to password management is to force expiration of passwords on an individual basis, user by user. The load on the help desk thus gets distributed over all the working days instead of piling up on a few days a year.

I recently encountered another system management issue that could lead to a self-imposed denial of service. A correspondent informed me of a situation in which the technical services group needed a change of e-mail servers, forcing a change in the e-mail-client software of several thousand users. The staff allocated a week for the changeover, after which no one's unchanged e-mail configuration would work. The argument was that a fixed deadline would force users to act, whereas a longer period would simply lead to lower compliance as users forgot all about the change request.

Now, it's important to understand that the e-mail system actually allowed overlap of the old and new configuration for several weeks before the deadline. Given that overlap, I think that a better approach to handling this kind of network configuration change involving users would have been to partition the change among groups of users. For example, perhaps the Engineering Department could have been guided through the change over a couple of days, and then the Finance Department and later the Manufacturing Department, and so on. That way, difficulties arising from implementation glitches would not affect everyone in the company all at once and the help desk and other technical staff could avoid being overwhelmed.

In addition, a staggered implementation schedule would allow early adopters to help work the bugs out, if any. [Hah! Have you every encountered a project without bugs?] That's why I suggested beginning with a technically more sophisticated group (Engineering) who might better be able to cope with bugs and cooperate with the help desk members in sorting out unexpected problems. By the time the later, less sophisticated groups reached their turn, some of the early glitches could have been removed.

It's not exactly a staggering insight, but I hope it's a useful one.

* * *

< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.