IBM i Security Best Practices

By Robert Andrews

Q: With all of the security breaches in the news, how do I ensure I'm following secure practices with my IBM i?

The IBM i, for the most part, is secure out of the box. However, we often see when administrators, or worse third-party products, make changes to the system that open it up to greater risk. First and foremost, the company must have a well-defined security policy. This does not mean that they have a Windows policy that is then twisted to the IBM i. Rather, the security policy should be written in platform agnostic terms and then include, either in line or in an appendix, platform specific implementation methods to meet those standards.

The heart of security on IBM i is our version of the "three-legged stool" or "fire triangle" – three parts where if any one fails, the entire model collapses. Those three items for us are the user profiles, object authorities, and system values. Let's start with user profiles. The most common issue with user profiles are that special authorities are granted too frequently. Special authorities are meant to be special, restricted to the true system administrators. We often see Job Control and Spool Control granted to almost all the users on a system. In addition, profiles must have strong passwords. This means checking for and denying default passwords (where the profile and password match) and standard well-known passwords, enforcing long, mixed case passwords, using a password change block rule, and ensuring all profiles follow these standards (Admins: no cheating with CHGUSRPRF, use *ALLCRTCHG – your profiles are often the most powerful and least protected!)

Next is object authorities, specifically libraries and profiles, that must be tightly controlled. User profiles should NEVER have *PUBLIC authority other than *EXCLUDE. If profiles have *PUBLIC authority, anyone on the system can use that profile's authority (including special authorities) without knowing the password. Libraries are the gateways to all other objects inside of them, so they too need to be locked down. Libraries should be *PUBLIC *EXCLUDE as well, but many people leave them as *PUBLIC *CHANGE. Remember, by default objects created in a library inherit the library's authority which further makes the library's authority very important.

Last, but not least, are system values. These control the overall security posture of your system. All system values should have an agreed upon, documented value and should be checked often to make sure they are not altered from their desired value. Don't forget about the ability to lock the security related system values inside of System Service tools (STRSST, Option 7). Review the Memo to Users (MTU) at all new releases for new system values and settings.

So how can you determine if your system is at risk? Most standards recommend an annual security assessment from an outside consultant. IBM System Lab Services offers just this type of assessment to get an unbiased picture of your risk from the professionals that wrote the operating system. You can find out more about getting your own system assessed and IBM's other offerings at our website located at http://ibm.biz/IBMiSecurity.