Leverage Security Features for IBM i

IBMer Robert Andrews explains the difference between security and securability.

By Scott McKinney - June 1, 2020

“You cannot prove security. You can only prove insecurity.” That’s one of IBMer Robert Andrews' favorite sayings. But security isn’t a theoretical game for Andrews. As a senior managing security consultant specializing in IBM i, he has a front-row view of the security threats facing IBM i clients—and the costs of not addressing them.

“The major risk that companies face surrounding IT security is related to brand reputation and corporate image,” Andrews says. “You can think of several breaches that have happened at various retail establishments—consumers double-think shopping at those stores simply due to their poor IT security habits.”

To fully leverage IBM i’s security features, it’s important to understand the concept of security versus securability. Security is the state of being protected from risk of potential harm or danger. The risk needs to be understood and dealt with appropriately. Securability goes to the degree at which something is able to be secured.

While the IBM i security statement makes it clear that no IBM i system can be considered completely secure, IBM i systems are considered highly secure out of the box, says Andrews. “We can take advantage of lots of security features on IBM i to remove that degree of risk from the system.”

Ransomware: An Indirect Threat to IBM i

One of the major concerns Andrews sees is ransomware. IBM i doesn’t run ransomware, but it can be a victim of ransomware that infects a PC. Once ransomware infects a PC, it starts encrypting all of the data locally, then looks for network connected resources, potentially including an IBM i server.

The major risk to the IBM i are shares at the root or lowest level of the IFS. Ransomware running on a PC can encrypt all of the files on the IBM i if these shares have insecure authorities.

Additionally, because the QSYS.LIB file system is part of the IFS, it can encrypt the OS itself, leaving it unusable. “This isn’t theoretical. We’ve investigated multiple IBM i systems where this has happened in the real world today,” Andrews says.

3 Ways to Protect the IBM i From Ransomware Attack

To protect the IBM i from exposure to ransomware, first ensure that File Shares are as far down the directory path as possible and marked as read-only. This alone will prevent any sort of ransomware from damaging files on the IBM i, as the PC wouldn’t be allowed to alter any of the files on the IBM i share.

Second, security settings should limit a user profile to the proper level of authority. If a user only needs read rights, they should only have read authority. “A user that only has read authority will never be able to modify or damage the file, even from a malware attack on a PC, " Andrews explains.

Finally, eliminate anonymous guest access via network share desk accounts. IBM i doesn't have guest support enabled out of the box, and the provided coupled shares are secured against user access. IBM i offers the anonymous feature, but Andrews recommends always using authenticated access.

Upgrading to IBM i 7.4 Augments Securability

IBM i 7.4, which was released in June 2019, offers two major improvements at the security level. The first is TLS v1.3, which provides the latest for data-in-motion security. It also incorporates newly created ciphers, such as elliptic-curve agreements and signatures.

The second is an enhancement to the authority collection feature introduced in IBM i 7.3. Authority collection allows an administrator or developer to trace security requirements at a very deep level as an app or program is running. The feature was limited to user level tracing in 7.3, but has been enhanced to allow for object level tracing. This allows a developer to put a trace on a particular library or set of objects, then watch how their application accesses and integrates into those particular objects.

"One of the major security risks we see is when users have too much authority to objects on the IBM i," says Andrews. "This allows for changes to occur when changes don't need to be made, and enables access from outside the application."

By using the authority collector, developers can assign the lowest required authority level without getting any authority errors or issues once the program is put into production. This allows for access for any interface beyond what the developer expected. It helps prevent cases where users access a database through outside programs—such as using FTP or ODBC—instead of the particular records they were accessing through their designated application.

The adopted authority model ensures that users only have access to the database via the designated application, thereby securing the database.

Annual Assessments Reveal Weaknesses

On top of understanding specific features in IBM i 7.4, it's important to have a better understanding of the security features in all current versions of IBM i. To start, an annual security assessment from an outside body or IBM can uncover where the weaknesses or risks lie.

"Part of my job is to help clients understand that risk, so they can choose to change that risk, try to reduce it or accept it," says Andrews. "Not all risk needs to be removed. Sometimes, knowledge of the risk can help guide a company to set a policy to handle that risk appropriately."

A thorough risk assessment explores the three major portions of the IBM i security model:

1. Analyzes user profiles to understand their privileges and authorities
2. Focuses on object authorities associated with libraries, underlying files and programs
3. Looks at overall system settings, including system values, networking access and other application-specific settings with relation to things like TCP

"Only by looking at all three pieces can you truly understand where the risk is on a particular system," Andrews says. "We then help clients understand each particular issue identified during an assessment."

Annual assessments allow clients to see where things have improved or sometimes worsened. Clients can also learn about security features such as password validation programs, network security and other settings that can be tweaked to improve security.

Security Is an HR Matter

Security threats are constantly evolving, and maintaining a staff of dedicated professionals is an ongoing challenge for most IBM i clients. “Too many companies assign security and IBM i responsibilities to employees who wear multiple hats: security, systems administration, even application development,” Andrews says.

Comprehensive IT security requires dedicated professionals to get it correct. Andrews emphasizes that you’re only as strong as the weakest link, and a single fault can expose everything. As fresh faces come on board, companies need to have a good succession plan in place to ensure continuous support of their IT environment—including IBM i.

Published at: https://ibmsystemsmag.com/Power-Systems/06/2020/leverage-security-features-ibm-i