National Cybersecurity Awareness Month – Cybersecurity Checkup: Protect your IBM i

Robert Andrews

Well, we made it to October 2020. Where I live, the tree leaves are starting to turn colors, and my morning drink is now pumpkin spice flavored. And cyberattacks are at an all-time high. Due to world events, many people have been required to work from home without the protective IT bubble provided in our office spaces. And it just so happens that October is National Cybersecurity Awareness Month (NCSAM), so let's look more closely at how you can #BeCyberSmart with your IBM i systems.

Week 1: If You Connect It, Protect It

In the first week of NCSAM, the focus is on protecting the assets you connect to your network. For IBM i clients, many users still access the system through Telnet (green screen). And we've gotten good at restricting access using menus and in the applications we've written over the years. But when you have a user profile on IBM i, you're allowed access to all system interfaces. This includes bulk transfer interfaces like File Transfer Protocol (FTP), Open Database Connectivity (ODBC) and Microsoft Excel. And sadly, the databases beneath your applications are often not secured properly.

One of the best ways you can protect your IBM i is by limiting which interfaces users are allowed to access on your system. IBM i makes this very easy using exit points. Exit points are hooks built into the operating system that allow further security when connections are made. You attach programs to these exit points that can then review a connection before it is allowed to proceed. This stops unauthorized data access before your valuable data escapes the system. You can write your own exit point programs, purchase them from IBM Systems Lab Services or purchase them from an IBM i Security Business Partner.

Week 2: Securing Devices at Home and Work

When we work out of our homes and other new locations, we lose some of the protections provided on a corporate network. Some people are even placing their IBM i's directly on the public internet for remote access. Keep in mind, when you use protocols such as Telnet or FTP, the entire transaction happens in the clear. This means that anyone between you and your IBM i can see your user profile, your password and any data you send back and forth with the system.

However, there's a simple solution to secure your connections: Transport Layer Security (TLS). The same security technology you use to secure your web browsing and shopping can be used for almost every interface on your IBM i. Using the Digital Certificate Manager (DCM), you can create, sign and apply certificates to the services (interfaces) on your IBM i. And this gives you a chance to explore the all-new DCM web interface.

Week 3: Securing Internet-Connected Devices in Healthcare

Many hospitals and other medical providers use IBM i to power their business. According to the Administrative Safeguards provisions in the HIPPA Security Rule, covered entities are required to perform risk analysis as part of their security management processes. IBM Systems Lab Services provides

IBM i Security Assessments. These assessments show you where the risks are in your environment. Once the assessment is complete, we can help guide you in taking corrective actions to reduce the risk in your IBM i. CIS Benchmarks also now include IBM i in their very popular security hardening guidelines. You can find them at https://www.cisecurity.org/benchmark/IBM.

Week 4: The Future of Connected Devices

Looking into the future of security on IBM i, we see new ways of authenticating users. One advanced method of authentication is to use Kerberos-based Single Sign On (SSO). This ties your IBM i to your Active Directory, eliminating the need for passwords on your IBM i. Another new authentication technology for IBM i is Multi-Factor Authentication (MFA). Both solutions take skills to set up and get operational with as little manual effort as possible. Our team is available to discuss these options with you and find the best fit for your enterprise.

Conclusion

We've created a brief video to go along with each week's theme in Cybersecurity Awareness Month. You can view these and many other IBM i security and compliance-related videos on our YouTube playlist.

The IBM Systems Lab Services IBM i security team is here to help keep you and your IBM i safe in this new normal. Our team can help assess your systems, reduce risk, educate your IT staff and provide software to make your IBM i run smoothly and safely. To learn more about us, visit our website or contact us.

Published at https://www.ibm.com/blogs/systems/cybersecurity-checkup-protect-your-ibm-i/